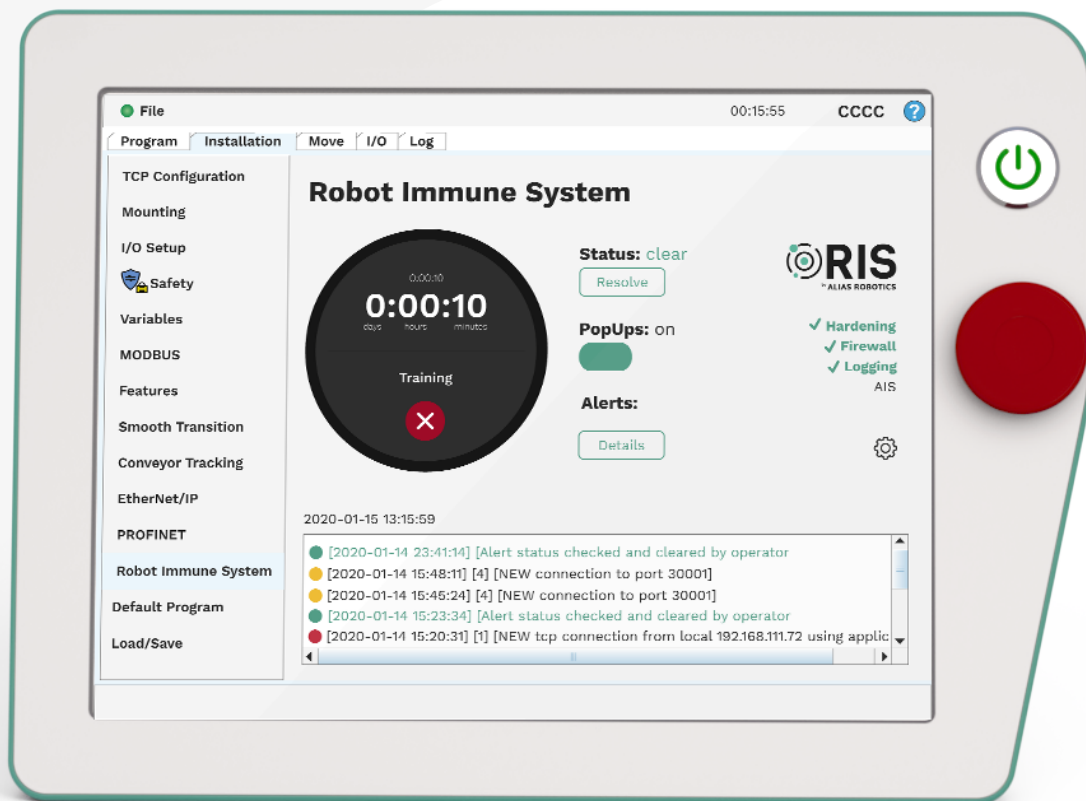


# Robot Immune System (RIS)



# Index


<b>1 What is RIS?</b>	03
<b>2 How does it work?</b>	03
<b>3 How is integrated with the system?</b>	04
3.1 Process	04
<b>4 Integration at infrastructure level</b>	06
<b>5 Compatible systems</b>	07
<b>6 Protection explanation</b>	08
6.1 How does it work?	08
6.2 Internet connection is required?	08
6.3 How does it work in connected systems?	08
6.4 How does it work when the robots are “Airgapped”?	09
<b>7 Threats examples</b>	09
7.1 Attack 1	09
7.2 Attack 2	11
7.3 Attack 3	12

# 1 What is RIS?

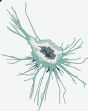
**The Robot Immune System (RIS)** is a software\* solution that protects robots and robot components against malware. Inspired by nature, it gets installed directly into your robotic system delivering an integrated suite of protection technologies. RIS is a Robot Endpoint Protection Platform (REPP), an integrated suite of endpoint protection technologies for robots —including a next-gen antivirus, hardening for known flaws, data encryption, intrusion prevention mechanisms, data loss prevention, etc.— that detects, prevents, stops and informs on a variety of threats that affect the robotic system.

# 2 How does it work?


**Gets installed and RIS provides 5 layers of protection.**

- 


**FIREWALL**  
**SKIN**

The adaptive firewall. Blocks unexpected communications. Simple adaptation on the go. Firewall listens to usual communications towards the robots and creates automatically firewall rules.
- 


**HARDENING**  
**INNATE IMMUNITY**

Patches vulnerabilities and weaknesses. Enforces security policies and primitives.
- 

**LOGGING**  
**MEMORY**

A forensics module. Registers and securely records all incoming communications and internal interactions within the robot.
- 

**AIS**  
**ADAPTATIVE IMMUNITY**

A bio-inspired artificial intelligence that adapts to novel security threats. Gets trained in the training phase, and examines interactions at the robot level in search for anomalous patterns of activity.
- 

**VISUALIZATION**  
**COMPLEX IMMUNITY**

Visualize and seamlessly interact with RIS while operating the robot. Re-train and control interactions with and within the robot. Get to know what's going on in each moment in your productive process.

\* The solution can be served as an external hardware device when required. Check availability with Alias Robotics team.

# 3 How is integrated with the system?

## 3.1 Process

How is the process with Alias when acquired RIS (timeline):



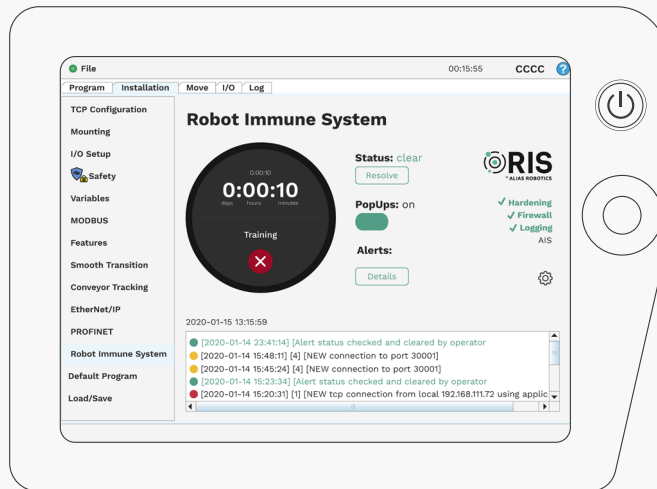
10



### Re- train it

Re configure easily RIS if your robot deployment or function changes.

#### INTERFACE

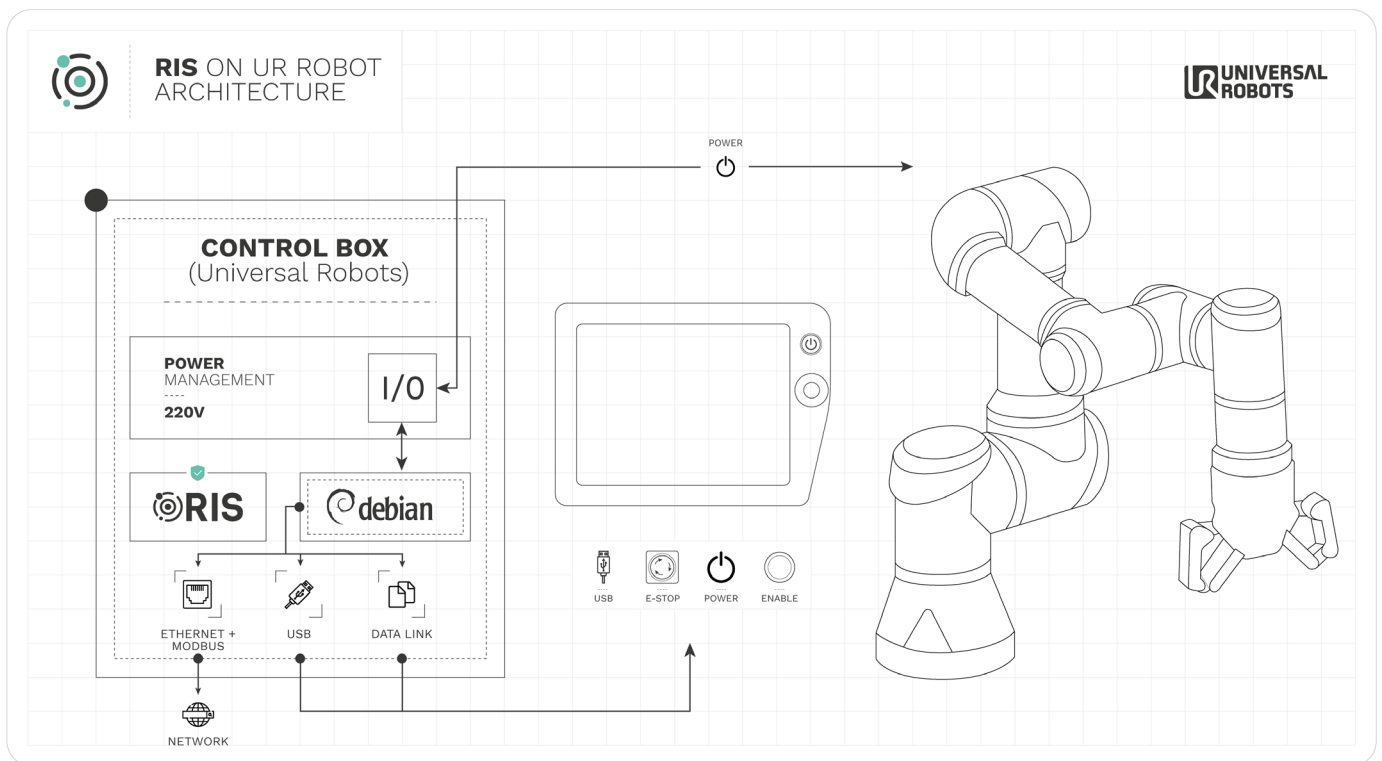


## 4 Integration at infrastructure level

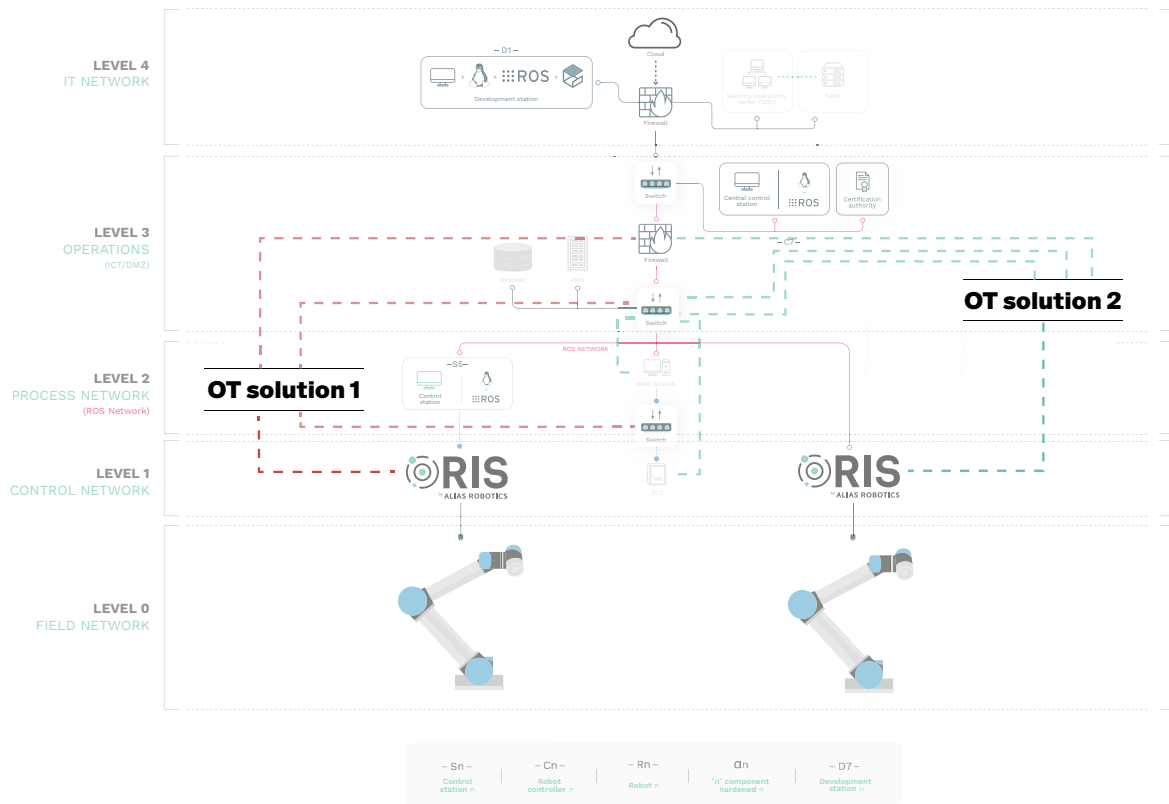
### What's RIS and where it's deployed.

Example: deployment in a robot from Universal Robot.

A technical scheme of where is RIS embedded, the software's architecture inside UR robots. Similar to this one.



**RIS and other security solutions at OT (Operational Technology) level.** A closer image of where is RIS installed and how it is compatible with other solutions. (RIS is compatible with other cybersecurity solutions for OT, RIS gets installed directly in the robot).



## 5 Compatible systems

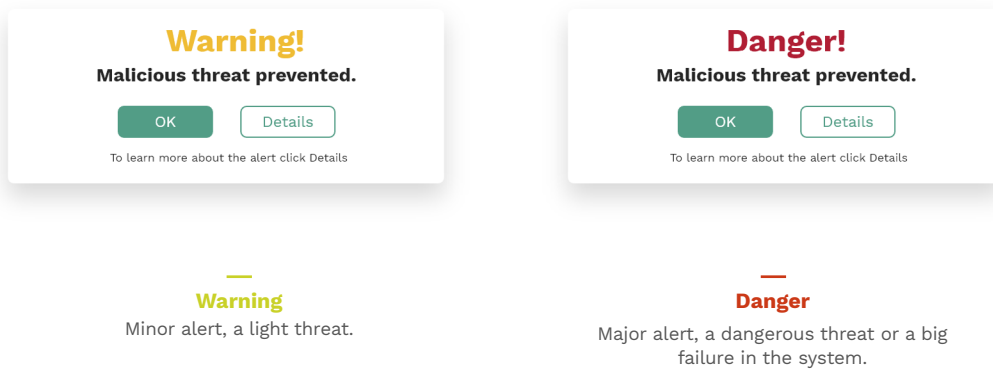


\* Check with Alias Robotics team for supported robot models.

## 6 Protection explanation

### 6.1 How does it work?

RIS is installed into the robot and monitors its operation at network and system level. If a threat is detected RIS takes appropriate actions to ensure business continuity and avoids robot downtime, as well as notifying the robot operator on incidents with pop-ups, if required.



### 6.2 Internet connection is required?

No. The current RIS version does not require connection to the internet.

### 6.3 How does it work in connected systems?

With the advent of industry 4.0 and the requirements in connectivity and control of industrial processes, most robots are connected to networks in industrial environments, even if this networks are segmented, micro segmented or only connected to some devices.

In some cases, connectivity requirements include robots connecting to vendors remotely, system integrators or other IoT applications. In these cases, it is critical to ensure your robots are protected. RIS protects connected robots against cyber breaches from the inside out.



## 6.4 How does it work when the robots are “Airgapped”?

The robotics air gap is a network security measure employed wherein the robot is assumed to be physically isolated from insecure networks.

Modern robots are highly complex interconnected (implying different networks) systems. Robots are networks of devices by definition. Networks of networks. Alias Robotics holds that the the air gap is a dead myth in robotics. Threats should be considered at the inter and intra networking levels, but also at the physical level, also at the device level.

In most cases, assuming a complete air gap between a robotic system and its enterprise/corporate/industrial network of operation is unrealistic. In some cases, Industry 4.0 visibility requirements will simply crash into theoretically air gapped robots.

While focusing security efforts on protecting a few obvious pathways (e.g. the network infrastructure authentication and authorization processes) is highly recommended, **not focusing in weak-endpoints provides a flawed defense**, since most attack pathways search for unprotected assets and entry points.



We advocate for a defense in depth for robotics systems, and that’s precisely the problem that RIS is solving.

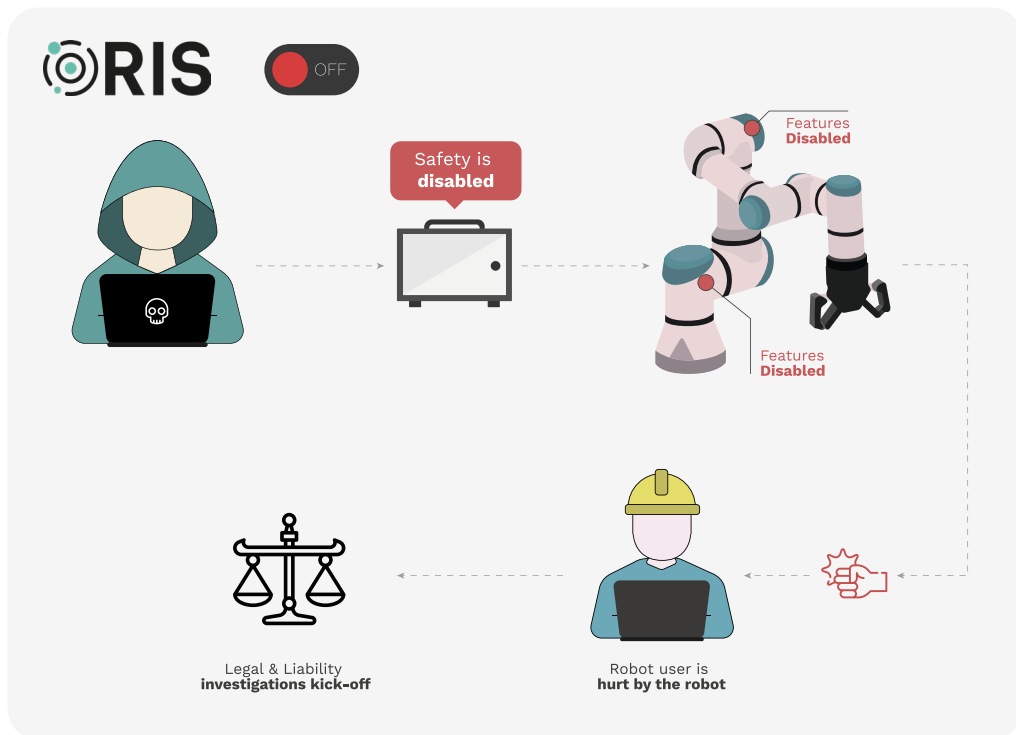
## 7 Threats examples

### ATTACK 1

**Network based attack:** Illegitimate attacker with right credentials access the robot and tries to control.

**DESCRIPTION** (Outcome of the attack without RIS).

- Malicious attacker targets safety systems in the UR robot.
- Safety is disabled inadvertently.
- Collaborative features are remotely disabled.
- Robot user is hurt without the collaborative features.
- Legal & Liability investigations kick-off.



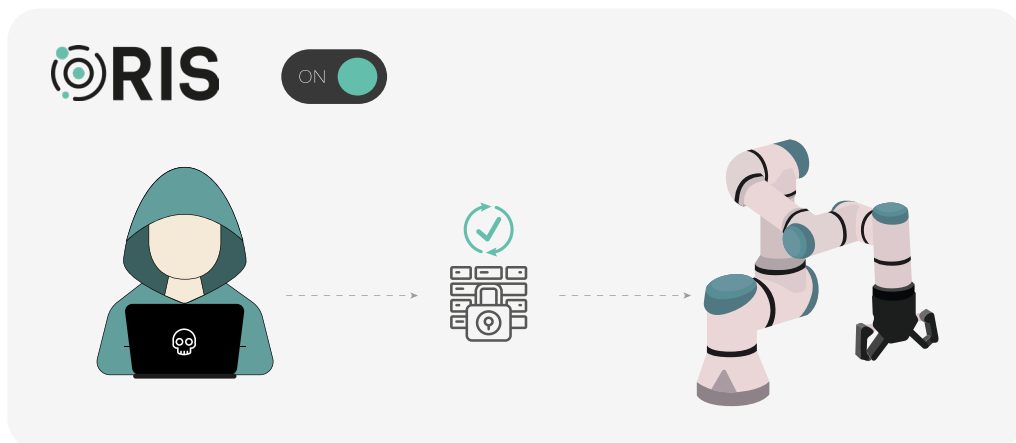
**DESCRIPTION** (Outcome of the attack with RIS).

**Attack stopped in 1st layer = Firewall**



- Intelligent firewall is configured so frequent origins of communications are learnt and no access to the robot is granted beyond common sources of traffic.
- Attacker is not able to exploit vulnerability leading to safety disabled.
- Displayed in RIS interface.

\* **Logging:** Holds a secure registry of all actions in the robot.

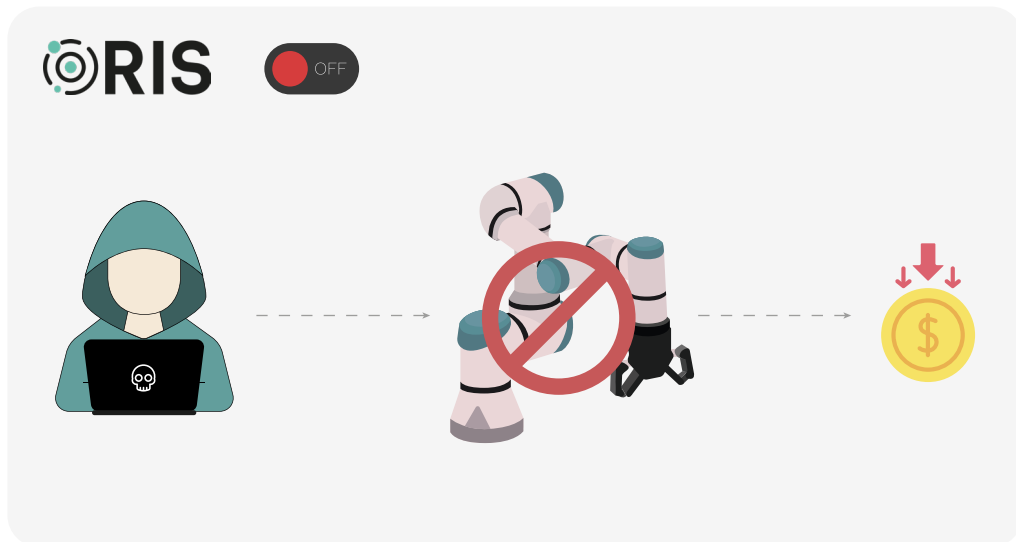


## ATTACK 2

**Physical attack:** USB attack - magic files

**DESCRIPTION** (Outcome of the attack without RIS - Akerbeltz).

- Encrypted robot.
- Encrypted IP.
- Robot is useless unless ransom is paid.
- Economic loss is caused by robot downtime.
- Need to search for internal/external contingency plans and disaster recovery.



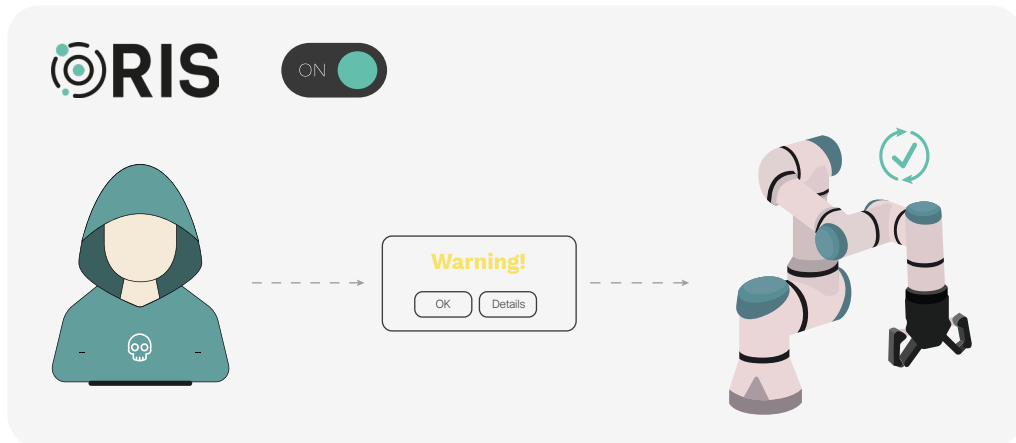
**DESCRIPTION** (Outcome of the attack with RIS).

**Attack stopped in 2nd layer = Hardening**



- UR continues normal operation.
- RIS user interface notifies the attack to robot operator.
- Displayed in RIS interface.

\* Logging: Holds a secure registry of all actions in the robot.

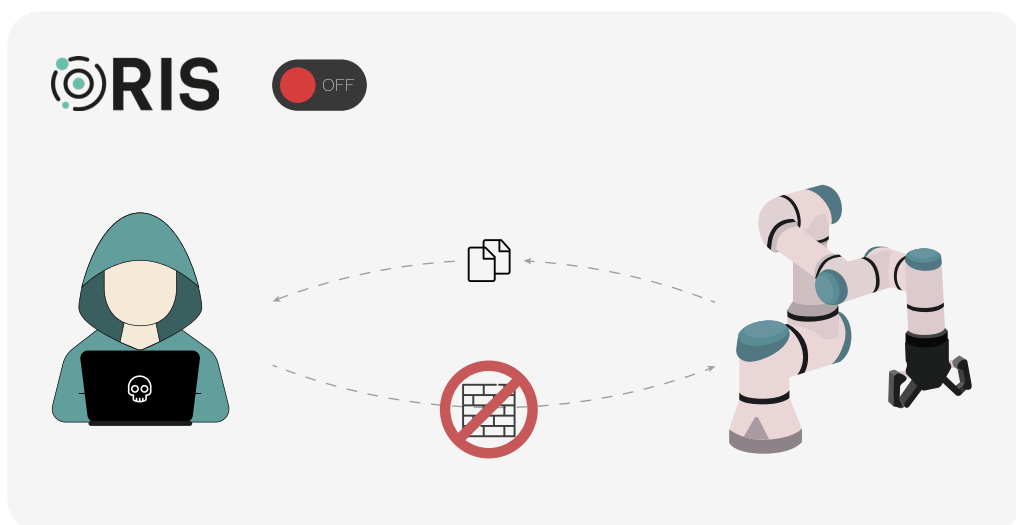


### ATTACK 3

**Remote network attack:** USB attack - magic files

**DESCRIPTION** (Outcome of the attack with RIS).

- Malicious attacker targets IP within the robot and succeeds to introduce micro-defects in robot operation.
- All intellectual property within the robot installation is stolen.
- Micro defects happen in a batch of the production.
- Sensitive information is leaked to attacker.
- Micro defect detection can lead to altered product batches.



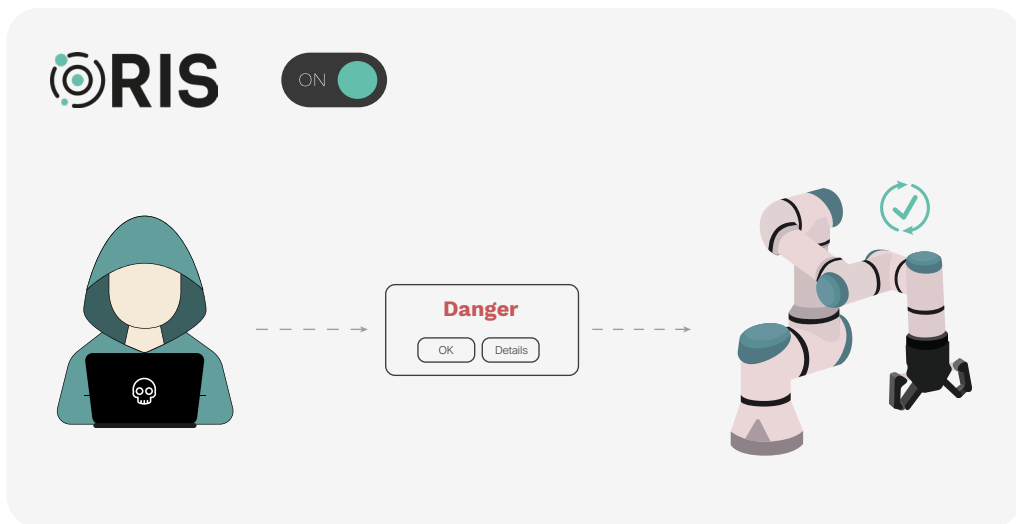
**DESCRIPTION** (Outcome of the attack with RIS).

**Attack stopped in 4nd layer = AI**



- UR continues normal operation.
- Alert is displayed on unusual behaviour and specially crafted unusual payloads to the robot.
- RIS user interface notifies the attack to robot operator.
- Displayed in RIS interface.

\* Logging: Holds a secure registry of all actions in the robot.





**ALIAS ROBOTICS**  
Robot Cybersecurity