FRANÇAIS ENGLISH

cea leti

eArgos

PATENT 1 PATENT

Detection of abnormal behavior in critical embedded systems

What it is

CEA-Leti's eArgos safeguards critical embedded systems against cyberattacks by analyzing system behavior. This software solution collects internal signals from the IoT device's processor, memory, or other hardware components, or from the operating system, applications, or process data. Artificial intelligence then uses the signal data to detect any deviations from the system's expected behavior.

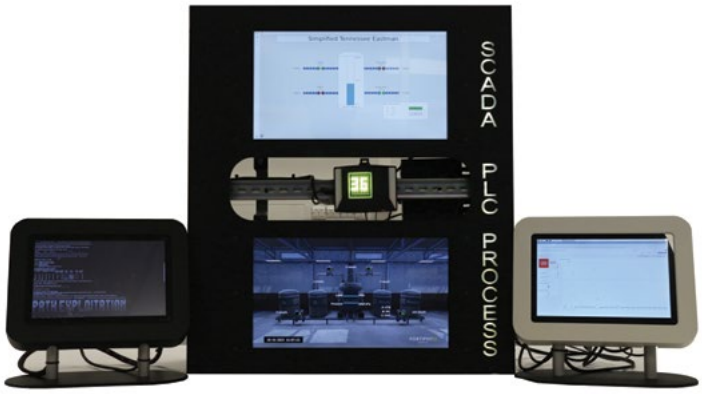
eArgos can identify abnormal behavior in real time, alerting the control server of the threat and its severity level. The solution is designed to enable Security Operations Centers (SOC) to take any necessary action to secure the system.

What it can do

The number of cyberattacks targeting embedded systems in critical infrastructures is growing. Critical systems are more vulnerable to attacks than conventional IT systems and, when compromised, these systems also pose a much higher risk of financial losses, personal injury, and property damage.

Certain industries are particularly exposed:

- Transportation
- Connected medical devices
- Industry 4.0
- Defense
- Space
- Smart cities and grids



▲ *Center: industrial controller managing a physical process visible on the bottom screen and supervised by a SCADA system (top screen). Left console: launches attacks that impact the controller and the physical process. Right console: displays the threat level to the controller calculated in real time by AI.*

What makes it unique

eArgos protects IoT devices from cyberattacks, even zero-day attacks that exploit previously unidentified or unpatched vulnerabilities, through several CEA-Leti innovations:

- Extraction of internal system signals for behavior monitoring
- Real-time detection of known and unknown threats using artificial intelligence algorithms deployed either locally or on a secure server

Together, these innovations enable a particularly lightweight, embeddable solution that responds to the constrained environments of IoT systems.

Working with CEA-Leti

In its current form, the eArgos demonstrator can detect attacks leveraging MITRE ATT&CK for ICS tactics and techniques on a emulated industrial control system. An eArgos agent integrated into the Programmable Logic Controller (PLC) detects any malicious acts and alerts the server. CEA-Leti can use the same approach to develop eArgos implementations suitable for any embedded system on the market, for any industry.

Critical device manufacturers and cybersecurity solution providers of all sizes can work with CEA-Leti to customize eArgos and enhance the security of their products and solutions for critical systems.

On GitHub

Discover HENDRICS, a HIL (Hardware-in-the-Loop) testbed designed to test, evaluate, and improve intrusion detection, response, and recovery.
github.com/CEA-Leti/HENDRICS/

Scientific publications

- Breux, V., Thevenon, P.-H. (2025). "Hardware Performance Counters for Anomaly Detection in Embedded Devices." HS3 workshop co-located at the ESORICS 2025 conference
- Arnoud, L. et al. (2025). "HENDRICS: A Hardware-in-the-Loop Testbed for Enhanced Intrusion Detection, Response and Recovery of Industrial Control Systems." ANUBIS workshop co-located at the ESORICS 2025 conference

Interested in this technology?

Contact:
Marion Andrillat
marion.andrillat@cea.fr
+33 438 784 651

CEA-Leti, technology research institute
17 avenue des Martyrs, 38054 Grenoble Cedex 9, France
cea-leti.com

@CEA-Leti

Research for industrial innovation