Co-Guard: Guarding Safety-Critical Embedded Devices in Emergencies

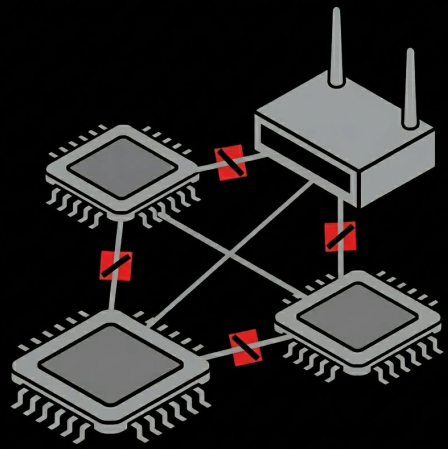
Christian Niesler, Christian Scholz, Nils Hannappel, Lucas Davi
University of Duisburg-Essen
paluno - The Ruhr Institute for Software Technology

Proc. of 2nd Constructive Approaches for SeCurity Analysis and Design of Embedded systems Conference (CASCADE'26). Springer, Regensburg, Germany, 2026.

Post-Compromise Security

Recon and Weaponize	Deliver and Exploit	Tamper	Act
Gather intelligence on targets	**Deliver Payload and Exploit weakness**	**Change the rules**	**Real-World Impact**
software versions, network diagrams, PLC configurations	inject code, privilege escalation, gain system control	modify logic, spoof sensor data, create unsafe conditions	equipment damage, process failures, hazardous material release

Core Problem



Co-Processor based security & safety architecture

on-chip solution
no network
dependency

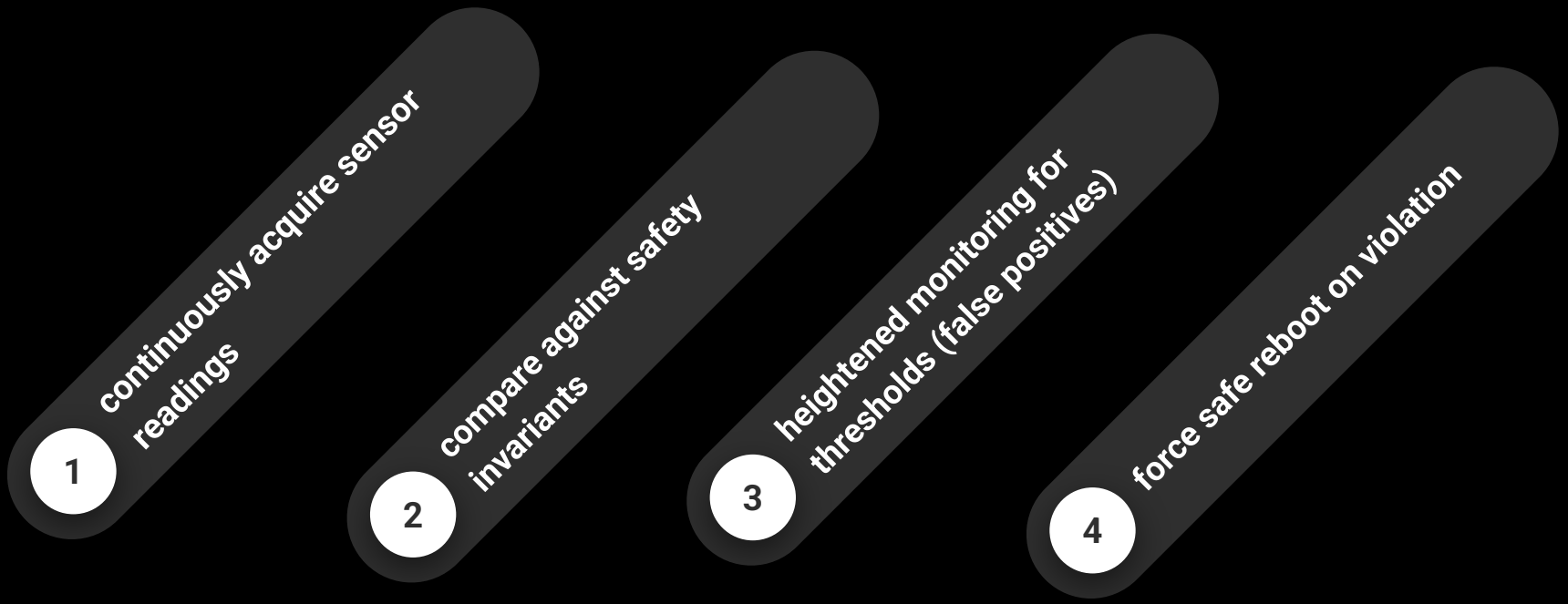
monitor physical
sensor data

detect safety violations
(indicates compromise)

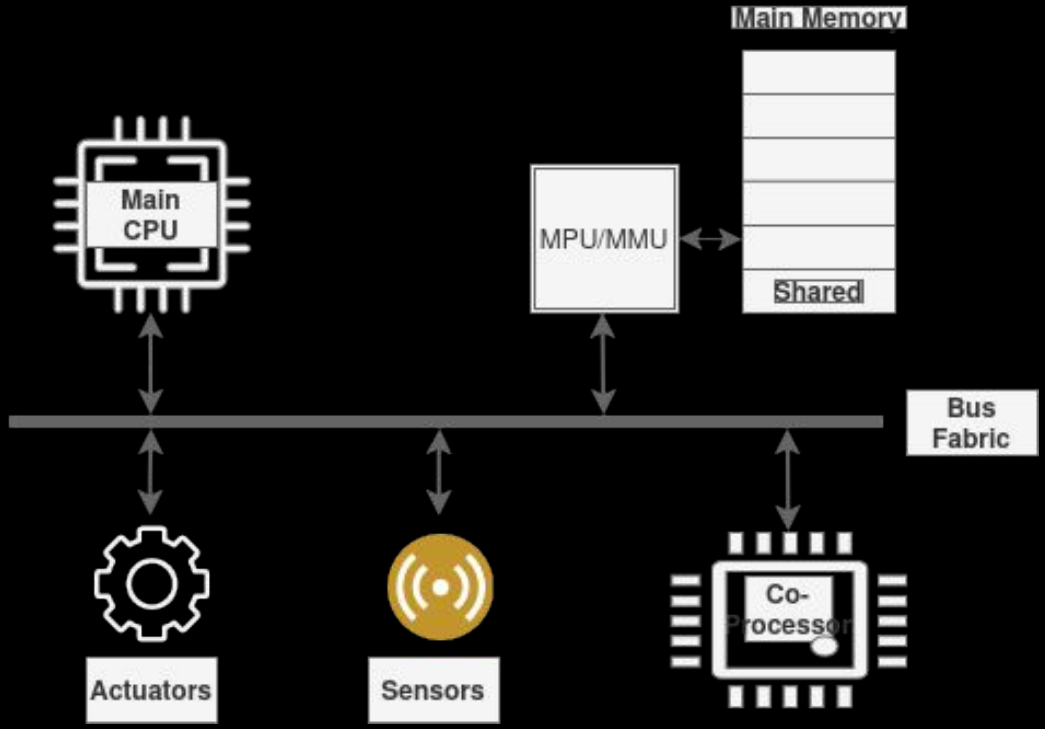
trigger remediation

preserve real-time
constraints

Co-Processor based security & safety architecture

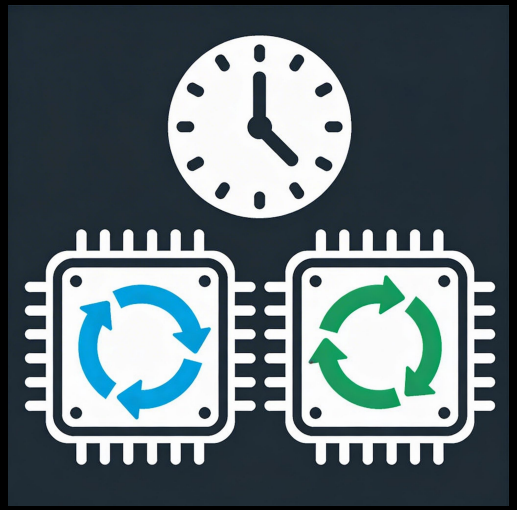


Co-Processor based security & safety architecture

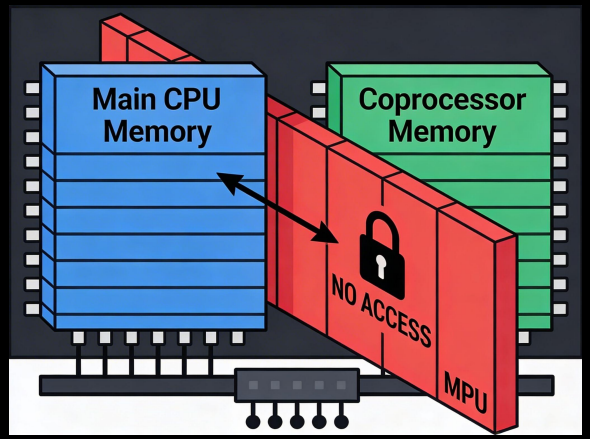


Co-Processor Design Benefits

Parallel Execution
of main cpu and co-processor



co-processor is an independent
on-board unit and can be isolated

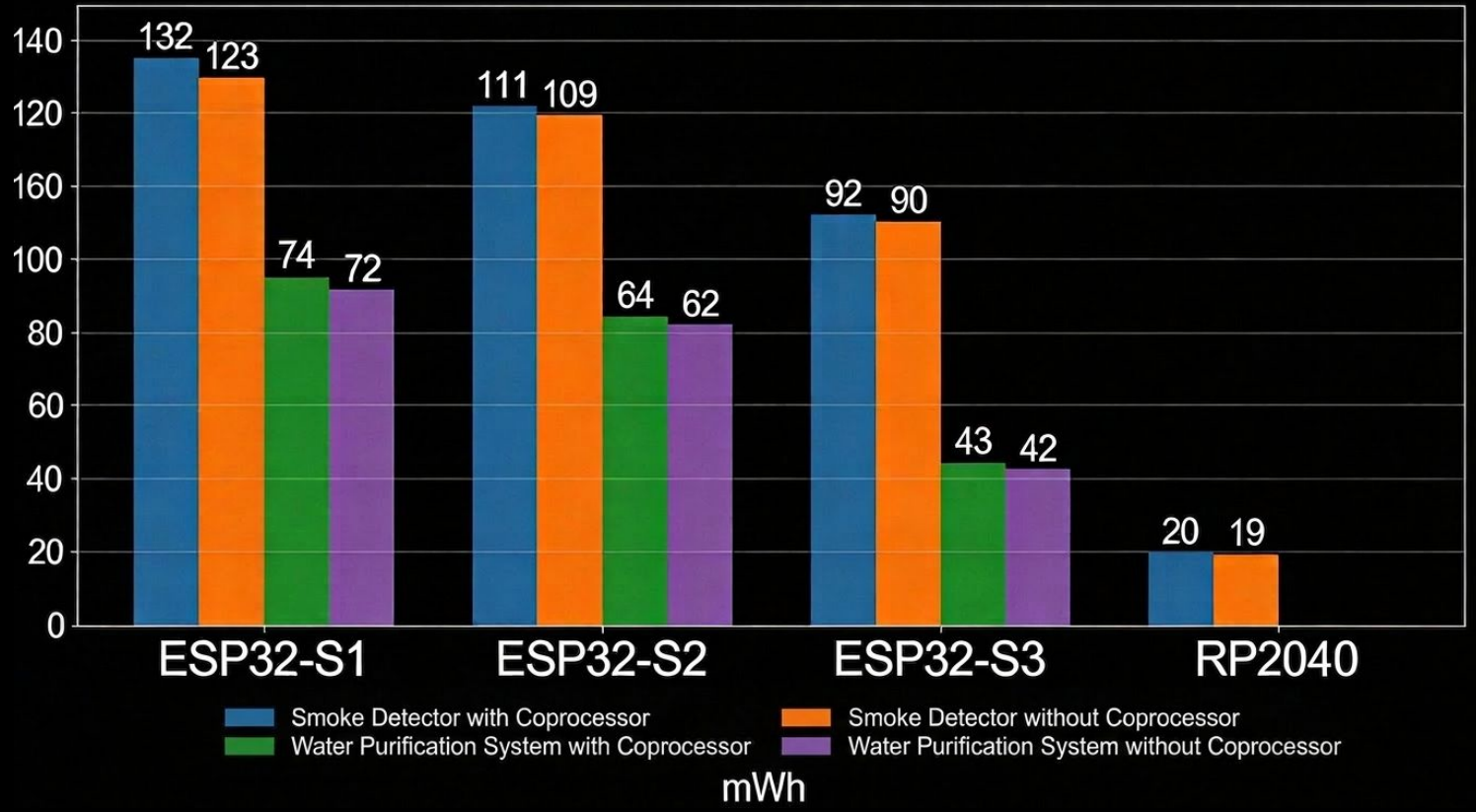


Case-Study

Water Treatment

Smoke Detection

Power Consumption

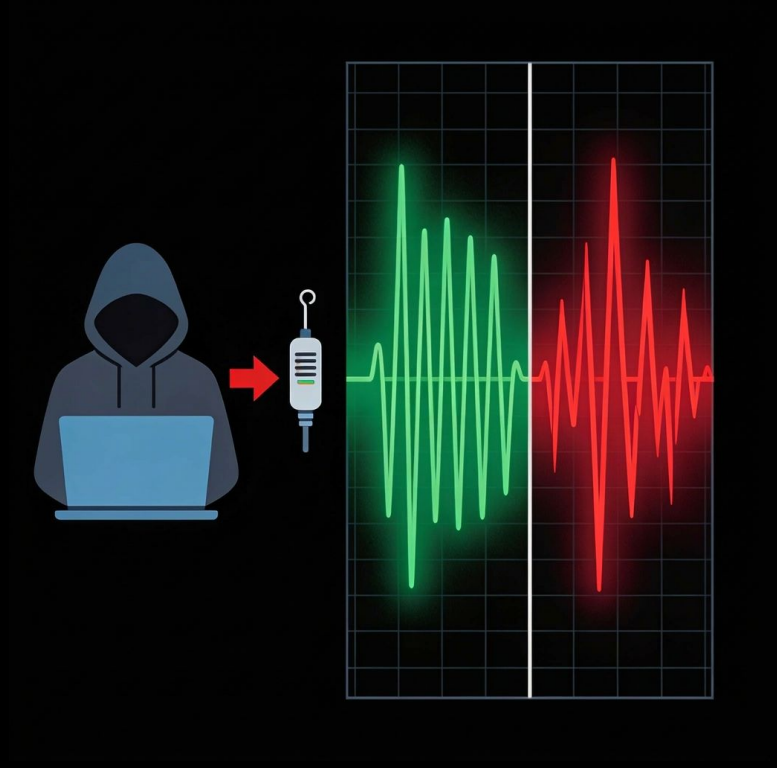


Key Results

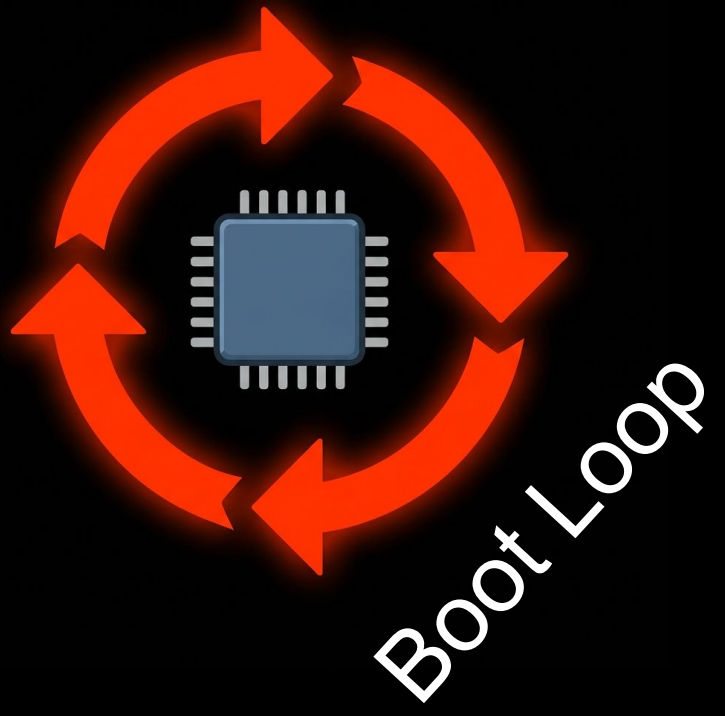
- ✅ Successfully detects and mitigates attacks on water systems and smoke detectors
- ✅ Power consumption minimal
- ✅ Implementable on commodity hardware (no custom chips)
- ✅ Compatible with FreeRTOS and real-time constraints
- ✅ Works on range of platforms: already on ESP32-S1/S2/S3 and RP2040

Security Considerations, Pre- and Post-Compromise

Security Considerations, Sensor Data Spoofing



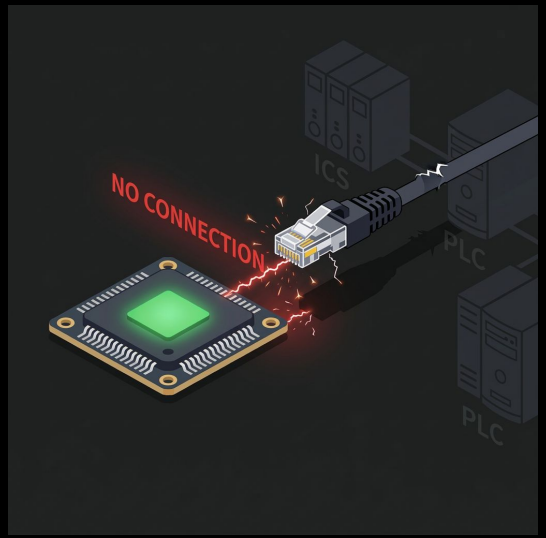
Security Considerations, Denial of Service



Security Considerations, Defense in Depth

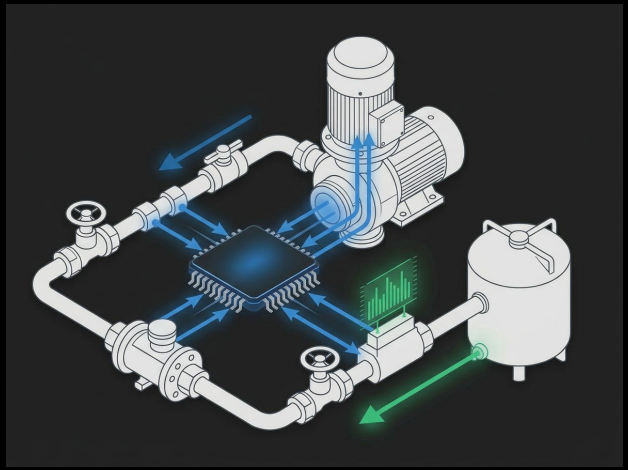
Why Co-Guard matters?

ICS networks can fail in reality



key positioning in ICS kill chain i.e. Last-Stop before Doom

real-time capable protects industrial control processes



Time for **Q**uestions and **A**nswers