

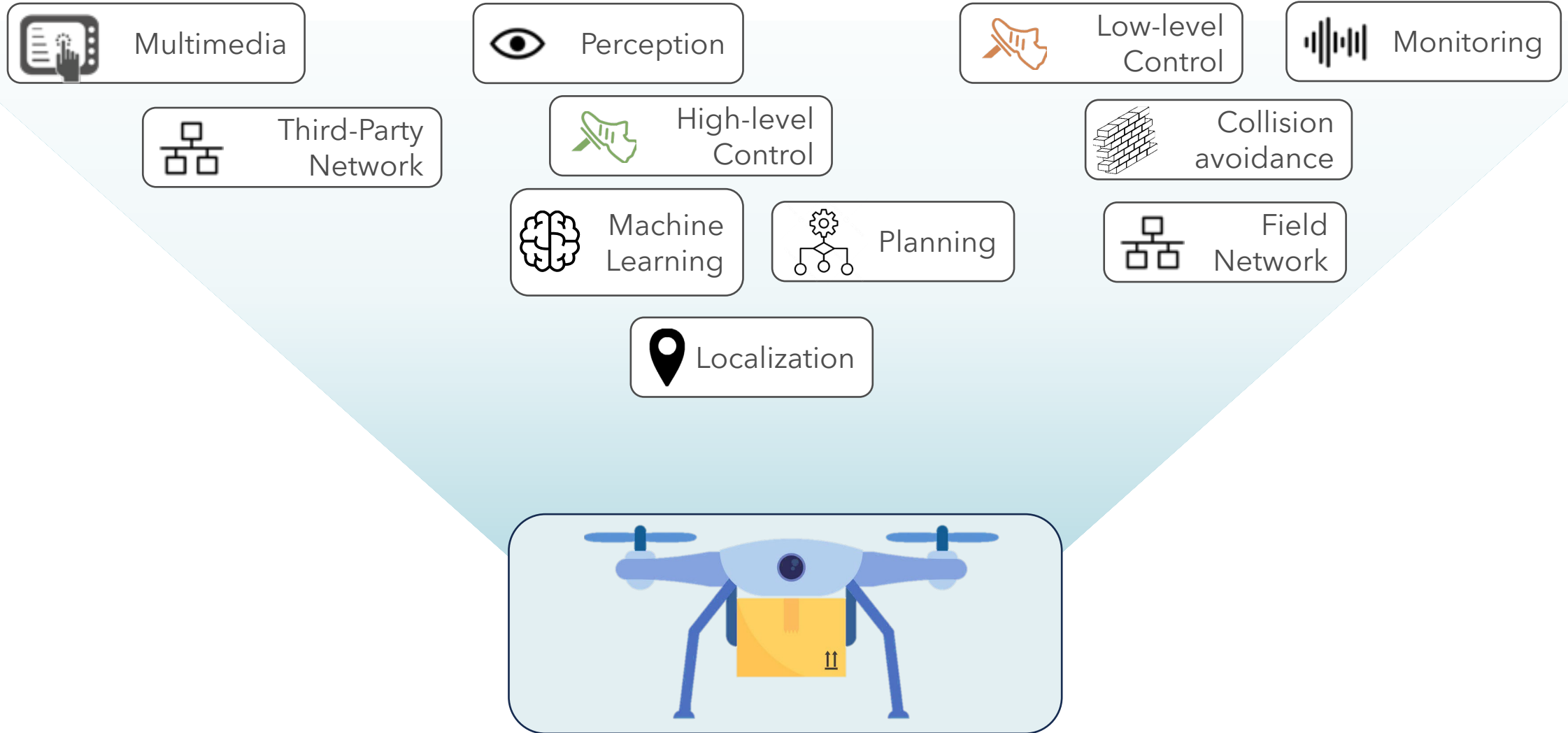


Simplifying complexity

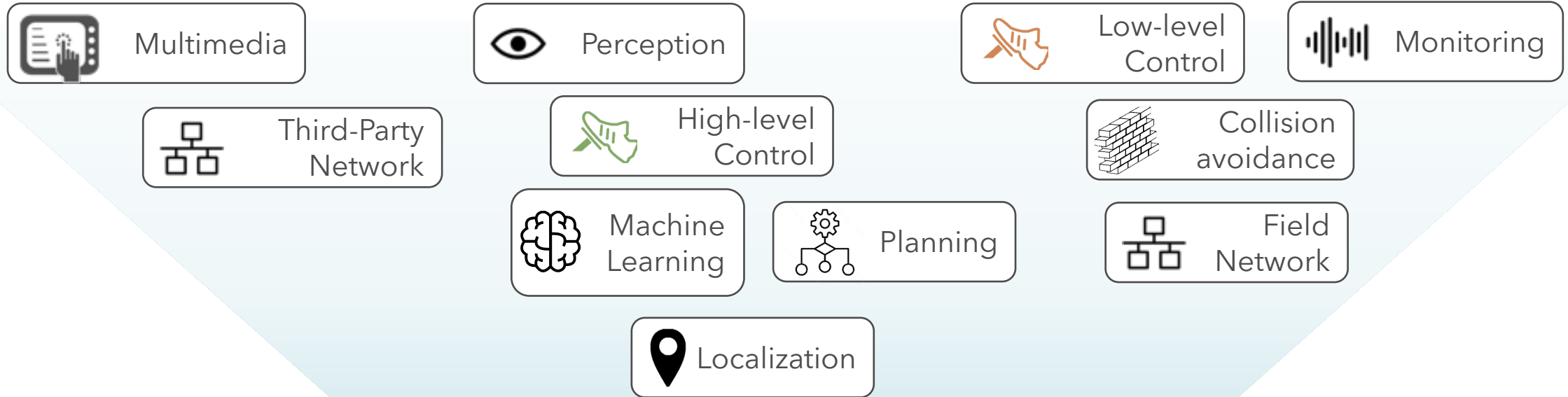
A Safe and Secure ROS 2 Multi-Domain Architecture for AMD Embedded Heterogeneous Platforms

Alessandro Biondi, *Accelerat SRL & Scuola Superiore Sant'Anna*
Tomas Thoresen, *AMD*

Mixed-Criticality Software for Robotics

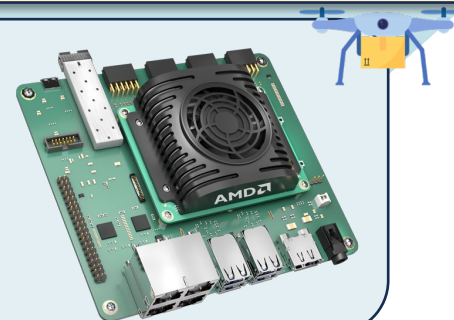


Mixed-Criticality Software for Robotics



All in one platform to contain *space, weight, wiring, power,* and **cost** (SWaP-C)!

AMD Kria™
KR260
Robotics

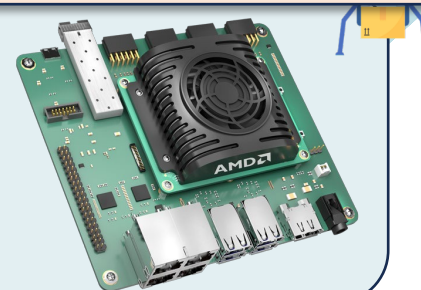


Cyber-Security Threats

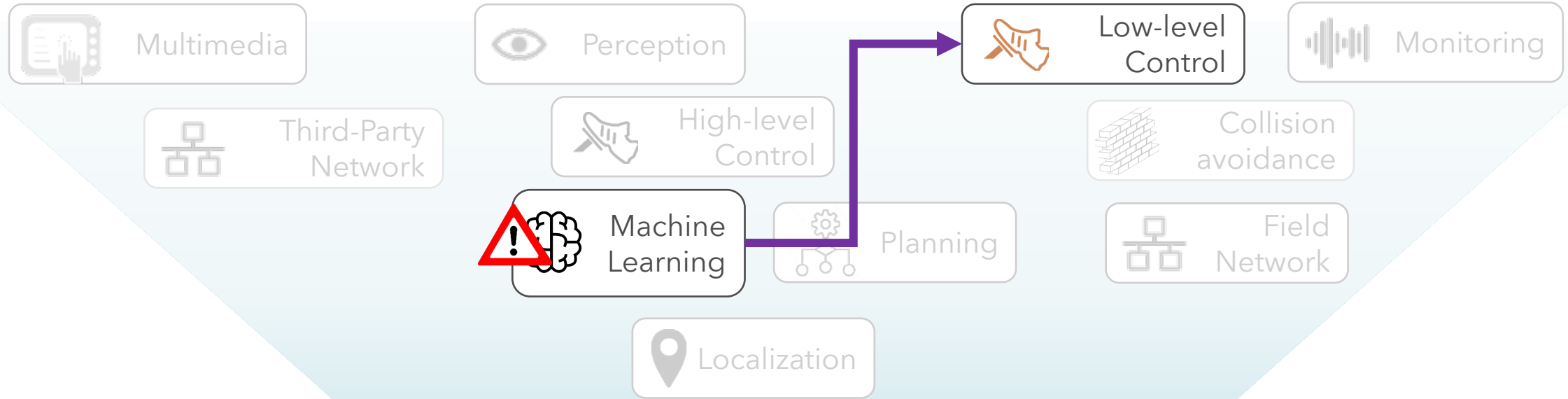


Cyber-attacks starting from *low-criticality* software can **compromise** the mission of the system

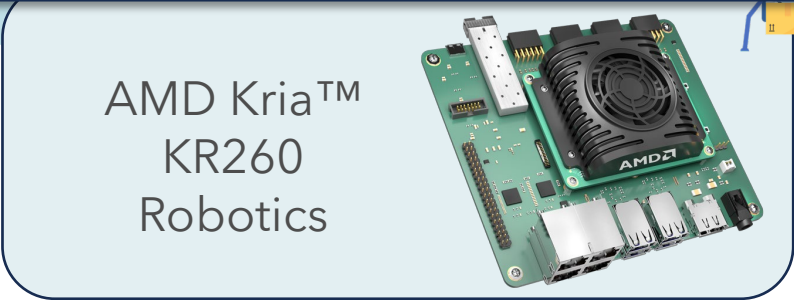
AMD Kria™
KR260
Robotics



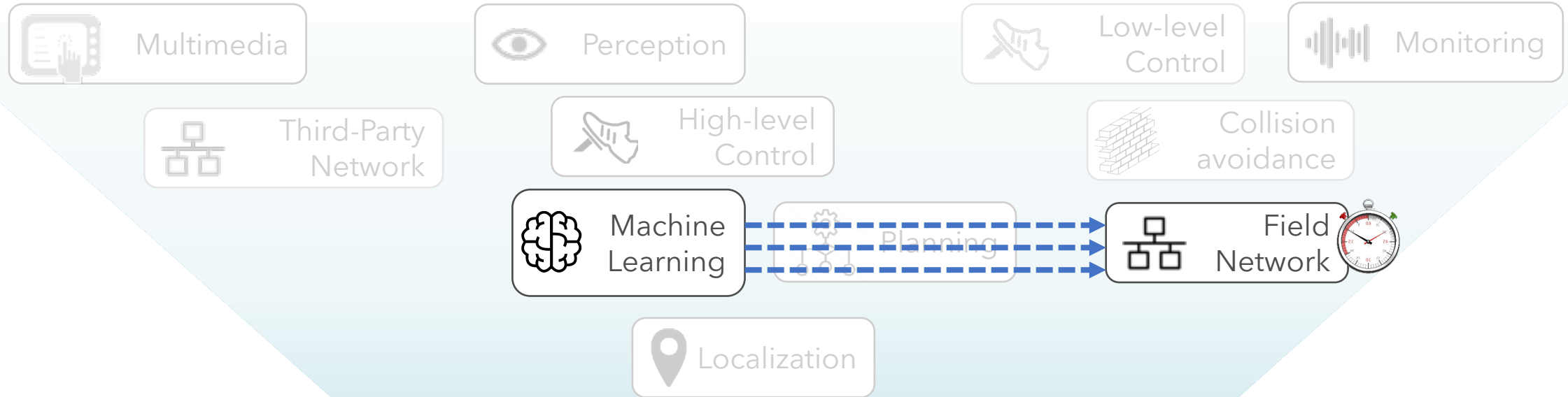
Safety Issues



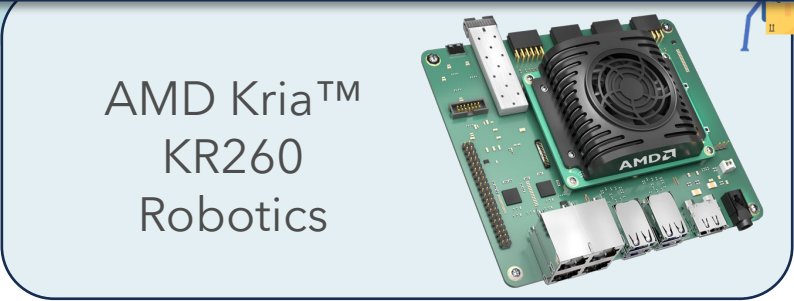
Safety issues that interest complex, *mid-criticality* software can **propagate** to *safety-critical* software



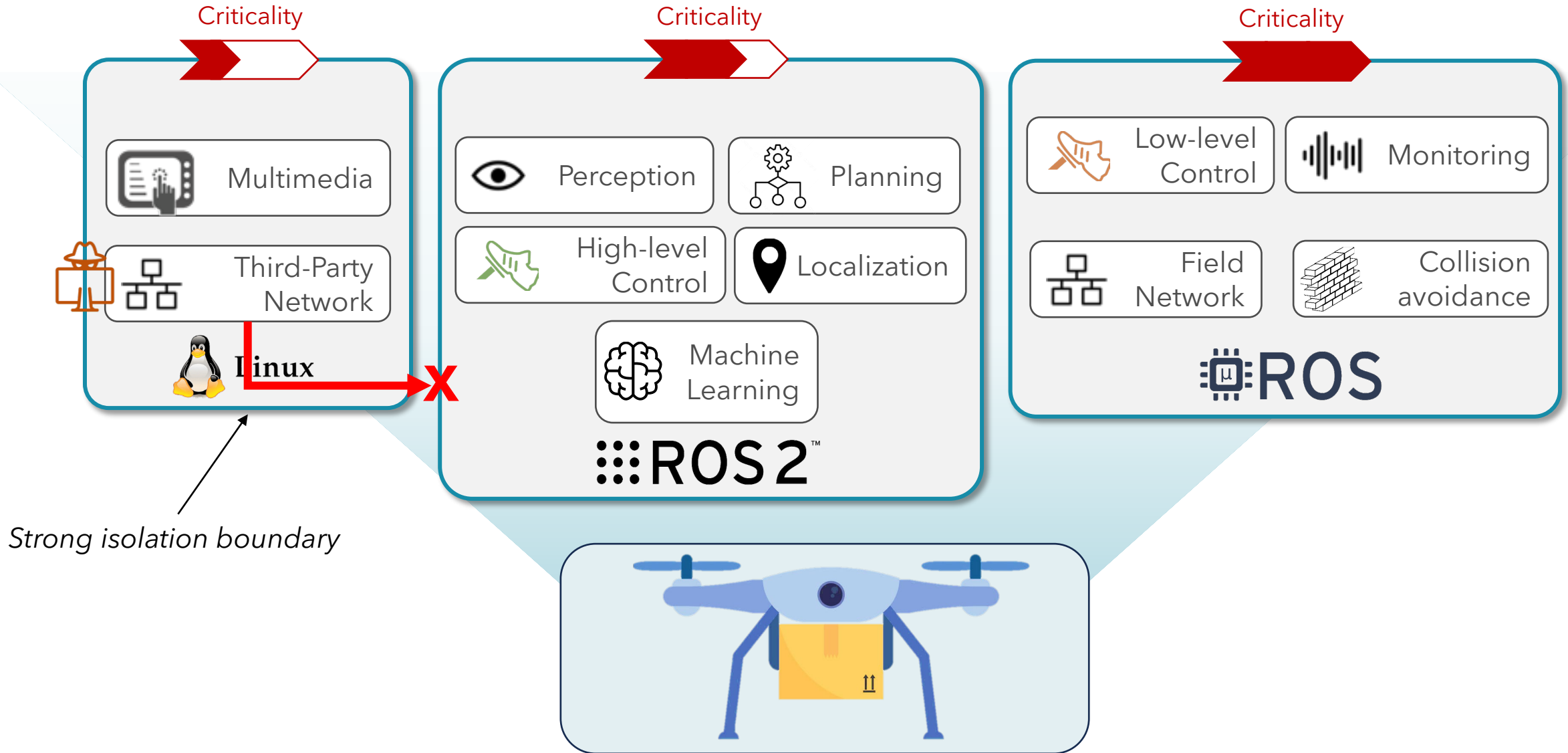
Time-Predictability/Determinism Issues



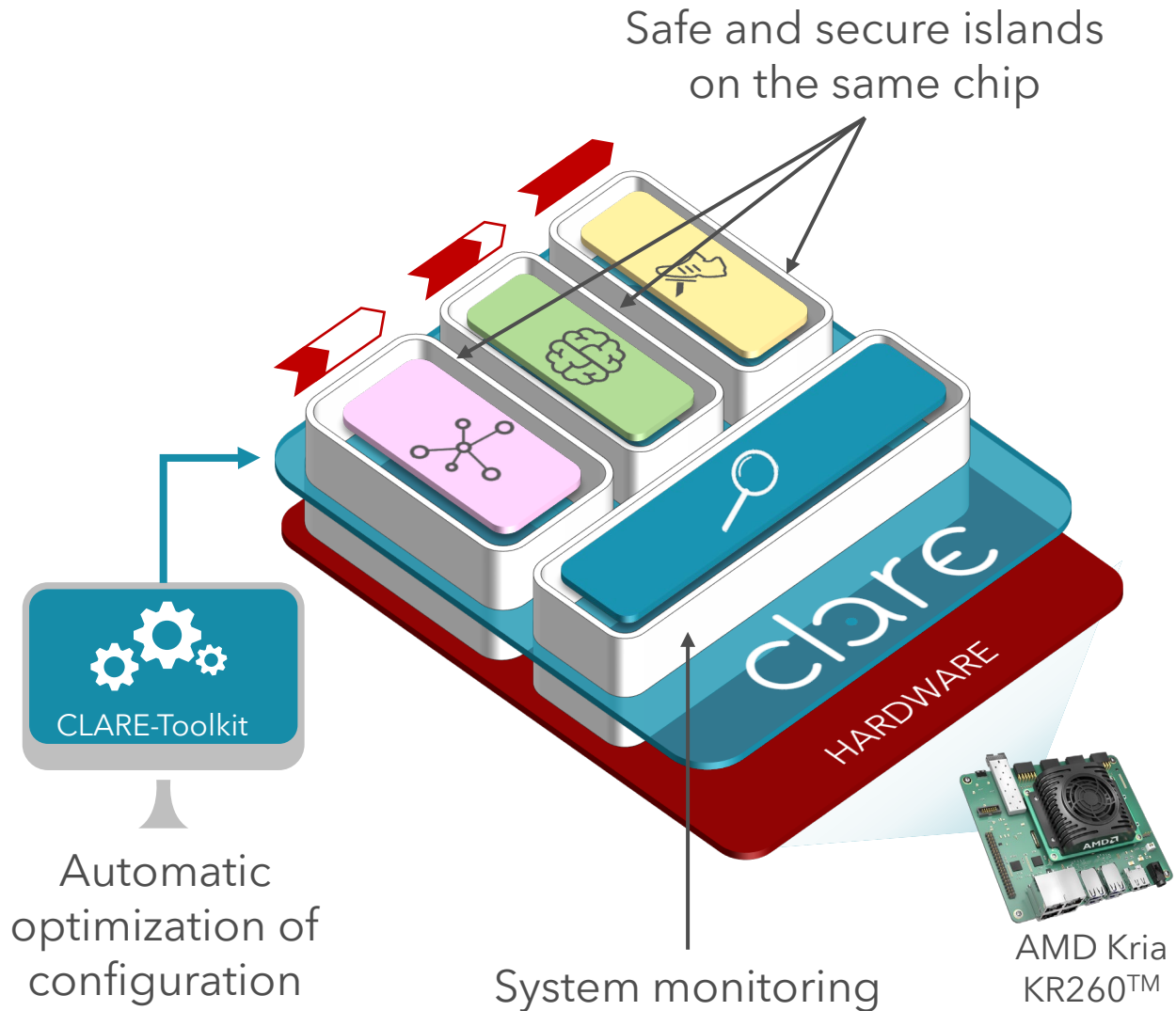
The temporal properties of *safety-critical* software can be **disrupted** by complex, *mid-criticality* software due to *on-chip interference*



Multi-Domain Architecture



The CLARE Software Stack



Strong isolation between islands
(next-gen Hypervisor technology pioneered with research activities)



Automatic optimizations



Intelligent machine verification
(Design Rule Checking for avoiding mistakes in the configuration)

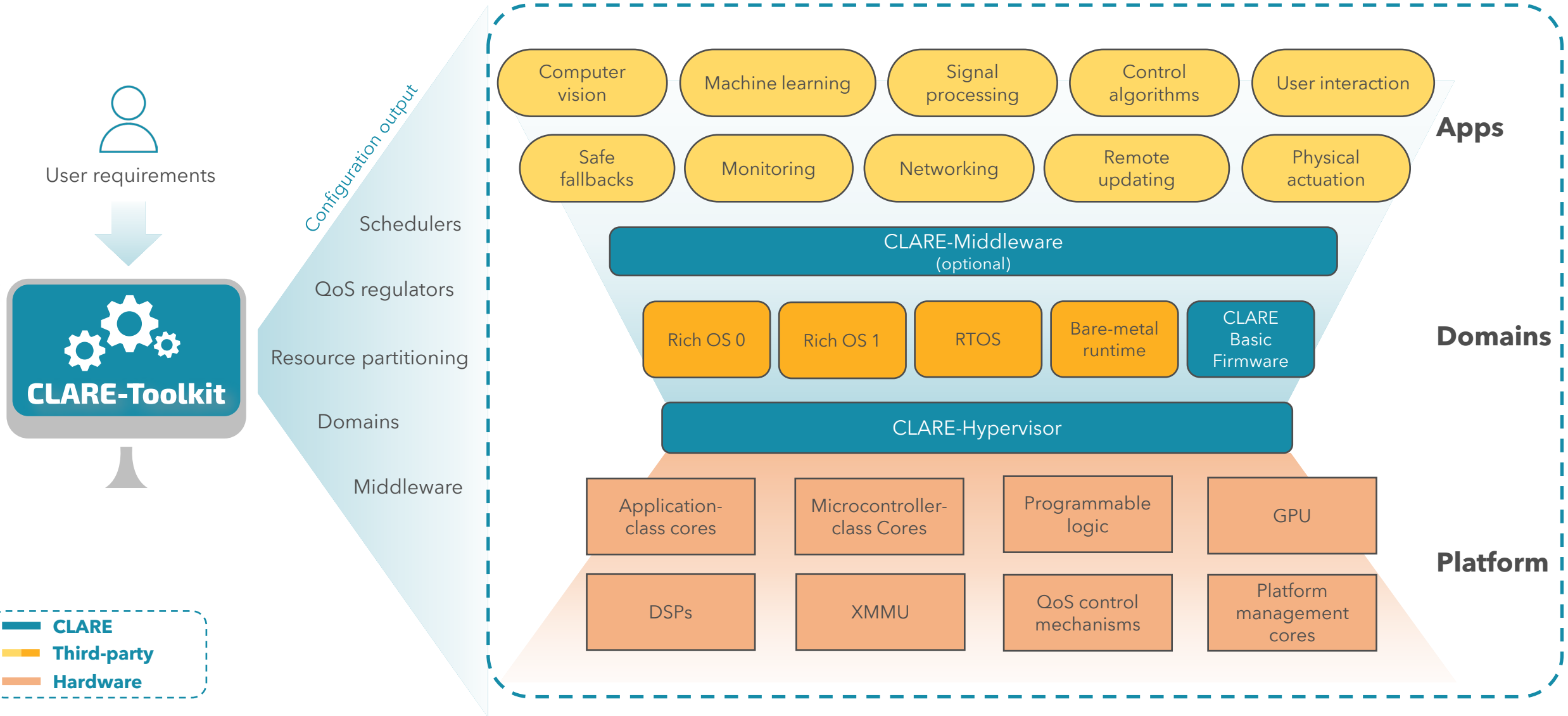


The expert is CLARE-Toolkit
(no need for experts in system-level software and hardware)

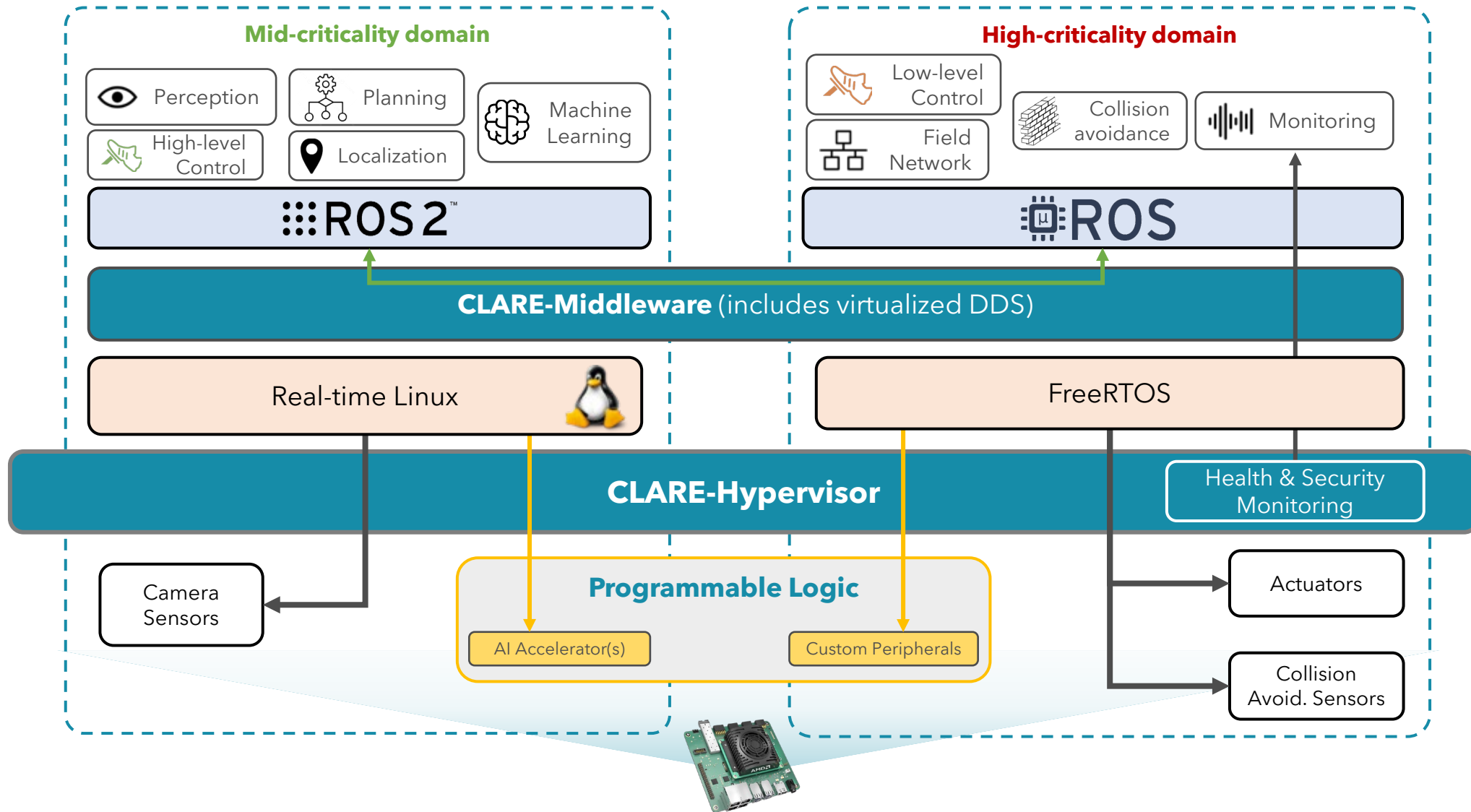


< 1 hour for the whole configuration

The CLARE Architecture



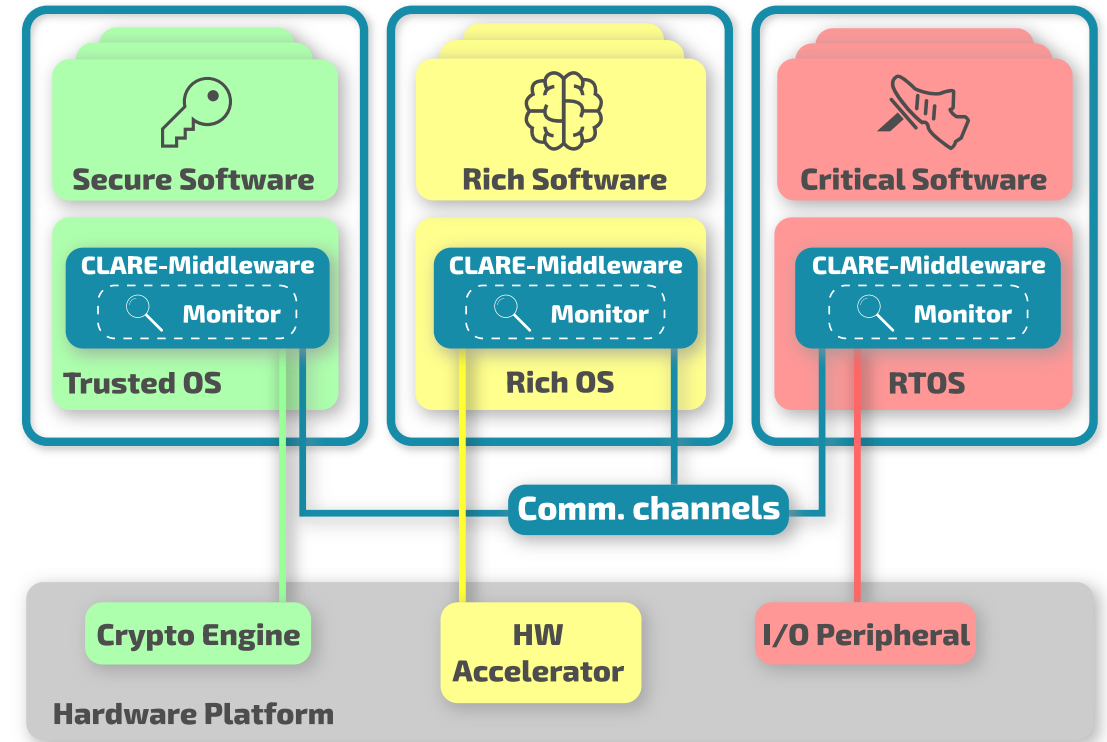
CLARE for Multi-Domain ROS



Unified and **simplified API** to access CLARE and platform services

Main features relevant to Multi-Domain ROS2:

- Transparent, virtualized **publisher/subscriber** data distribution service
 - Uses CLARE's built-in time-predictable, safe and robust **inter-domain communication**
- Signaling for **health and security monitoring**





- Fixed-priority and EDF scheduling
- Bounded latency for event dispatching
- Super low-latency FastBoot
- Secure cache partitioning
- Bank-aware memory allocation
- Memory bandwidth reservation



- Address-Space Layout Randomization
- Control-Flow Integrity
- Secure boot for VMs
- TrustZone support
- Strong VM space separation
- Robust to denial-of-service and side-channel attacks



- Totally static
- MISRA compliancy
- Off-line auto-generated configuration
- Ongoing SIL4/ASIL-D certification
- ~ 8K LoC
- VM-level health-monitoring

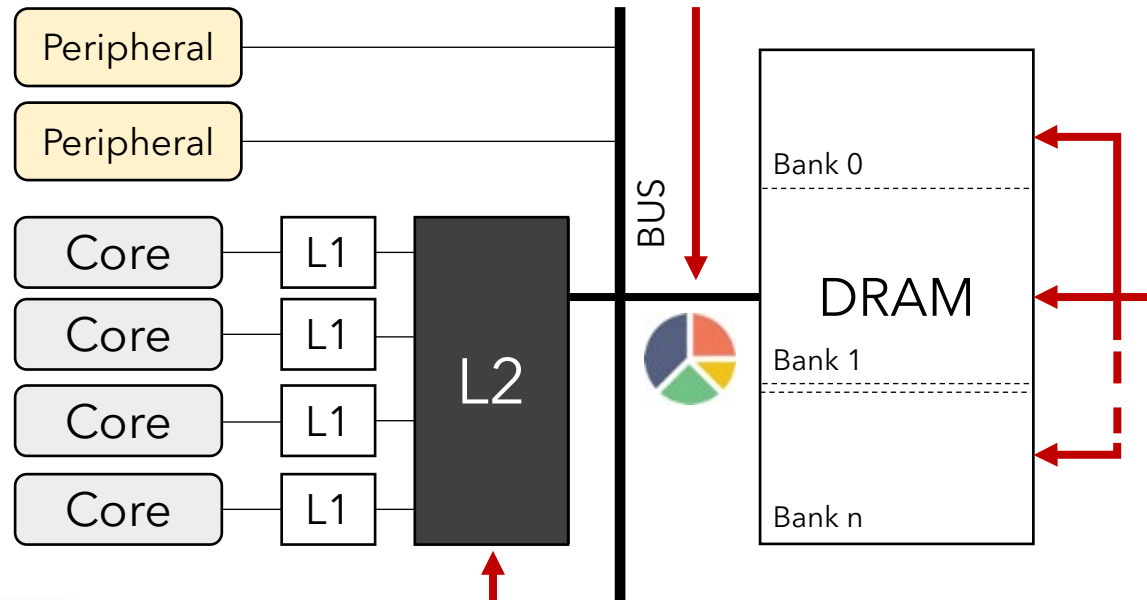
Strong Isolation

CLARE-Hypervisor implements advanced mechanisms for **strong isolation**, which can be optimally and automatically configured from CLARE-Toolkit

Memory bandwidth reservation

Budgeting the number of transactions that can be issued by each core and each I/O peripheral over time

Countermeasure for memory-related *inter-domain* **DoS attacks**



Bank-aware partitioning

Allocating domains to different DRAM banks to control memory contention

Countermeasure for DRAM-related *inter-domain* **side-channel attacks** (e.g., Row Hammer)

Countermeasure for cache-related *inter-domain* **side-channel attacks**

Secure cache partitioning

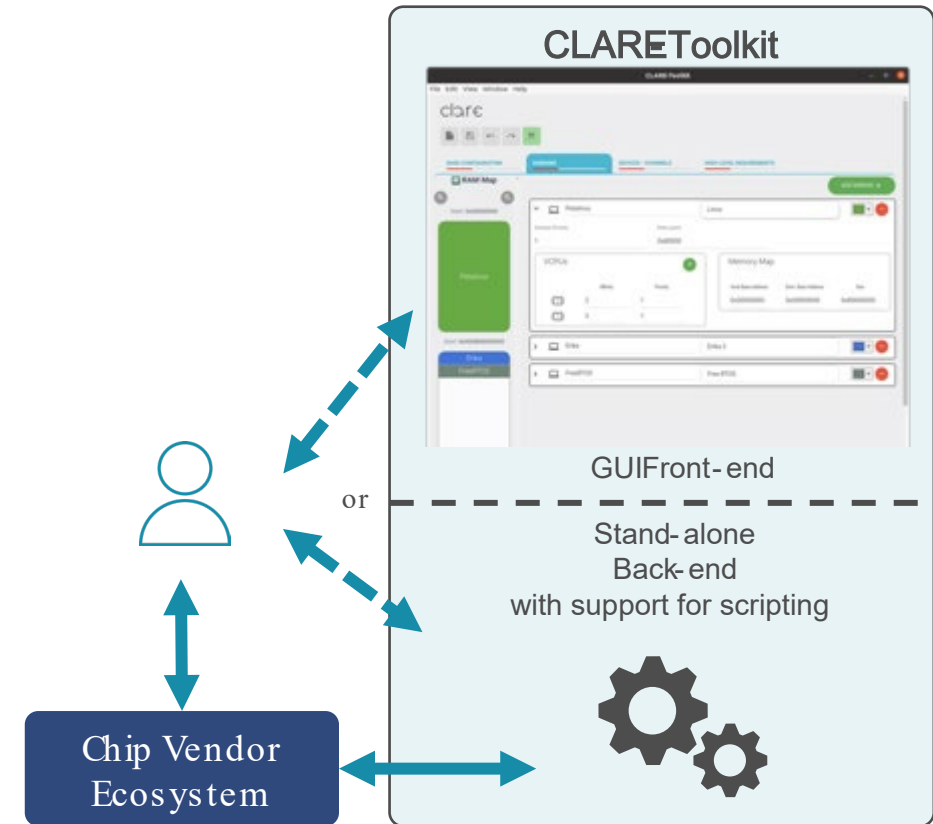
Partitioning the shared levels of cache to control inter-core interference

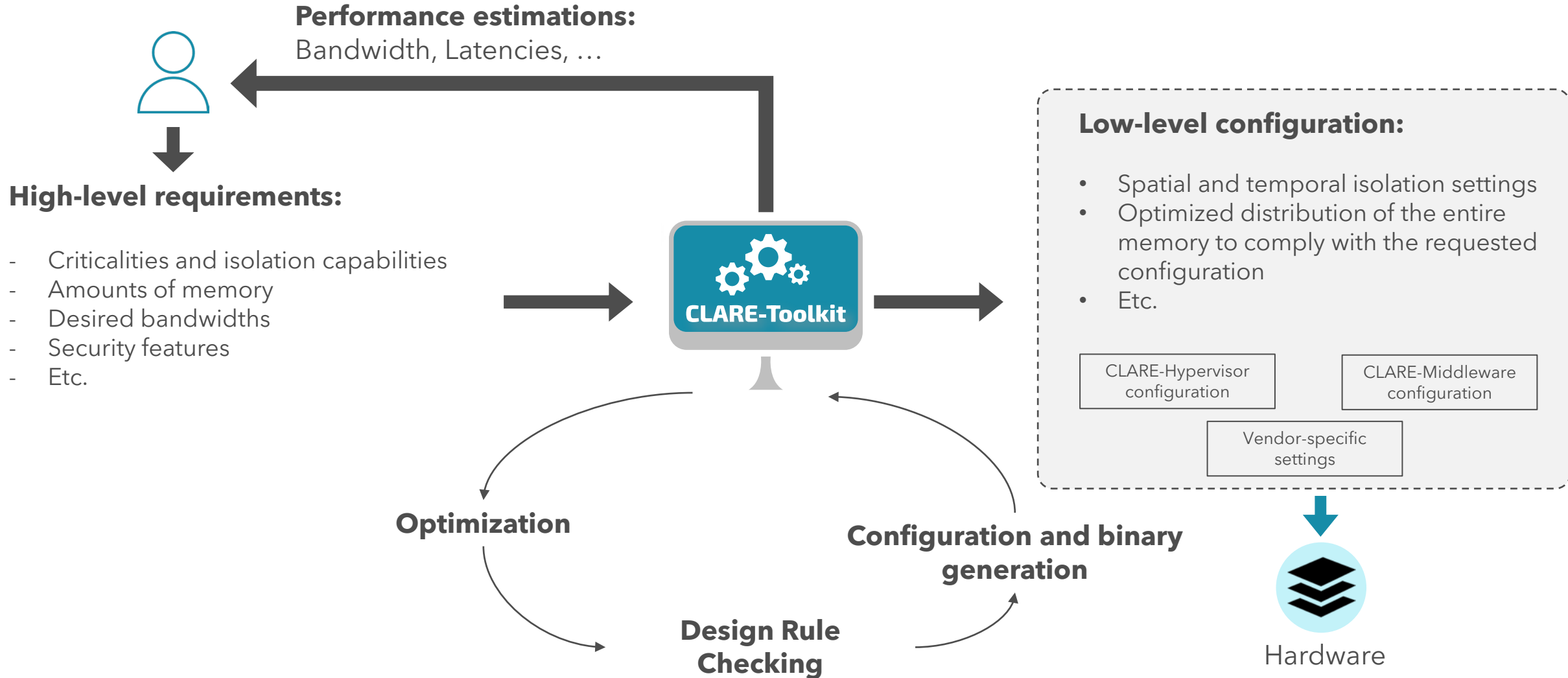
Configuration of the entire CLARE Software Stack with availability of a rich **template library**

Automatic optimization of the deployment and configuration of complex **mixed-criticality applications**

Platform-awareness for low-level isolation mechanisms

Designed to be **integrated with Chip Vendor Ecosystems**





Scalable AMD Kria™ Portfolio

Choose the **Starter Kit**



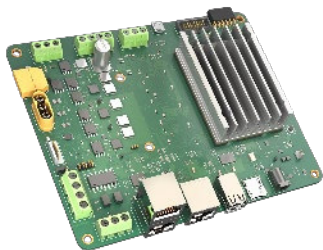
Select the right **Production SOM**



Develop your **Custom Carrier Card**

KD240 DRIVES

For Drives and Motor Control Systems



KV260 VISION AI

For Vision AI Cameras and Systems



KR260 ROBOTICS

For Robotics and Machine Vision Systems



KRIA™ K24 SOM

Half the size of a credit card
Power efficient
ECC support



KRIA K26 SOM

VCU and larger DPU
55% more I/Os
Transceivers



Safety Certifications for AMD

CERTIFICATE / CERTIFICADO / CERTIFICAT / CERTIFICADO / CERTIFICATE

CERTIFICATE
No. Z10 084605 0005 Rev. 01

Holder of Certificate: Xilinx Inc.
2100 Logic Drive
San Jose, CA 95124
USA

Certification Mark:

Product: Software
Model(s): Tool Chain
Vivado

Parameters: A list of parameters classified for use in any SIL 1, 2 or 3.

Tested according to: IEC 61508, ISO 26262

Test report no.: X90019

Valid until: 2024-08

Date: 2021-12-17

CERTIFICATE NO FS/71/220/21/0732 **PAGE 1/1**

LICENCE HOLDER: Xilinx Inc.
2100 Logic Dr.
San Jose, CA 95124
USA

MANUFACTURING PLANT: Xilinx Inc.
2100 Logic Dr.
San Jose, CA 95124
USA

PROJECT NO/ID: K3ZF-AU07

LICENSED TEST MARK: K3ZF0010

CERT. REPORT NO.: K3ZF0010

Certificate / Certificat / Zertifikat / 合格証

XILINX 1502011 C001

exida hereby confirms that the:

Xilinx® Zynq® UltraScale+™ devices
Xilinx, Inc.
San Jose, CA, USA

Has been assessed per the relevant requirements of:

ISO 26262:2018 Parts 2, 4, 5, 6, 7, 8 and 9
IEC 61508:2010 Parts 1, 2 and 3

and meets requirements providing a level of safety integrity to:

Systematic Capability LPD: ASIL C / SC 3 (SIL 3 Capable)
Systematic Capability FPD: ASIL B / SC 2 (SIL 2 Capable)
Systematic Capability PL: ASIL B / SC 2 (SIL 2 Capable)

Safety Function:
The Full-Power Domain (FPD), Low-Power Domain (LPD), and Programmable Logic (PL) of the Xilinx Zynq UltraScale+ device, support the execution of safety related software. A failure in the FPD or LPD caused by a hardware fault shall not cause the system to go into an unsafe state for a time greater than the specified fault tolerance time interval.

Application restrictions:
The device shall be used per the requirements described in the Zynq UltraScale+ documents listed on the reverse side.

Evaluating Assessor: *David Smith*

Evaluating Assessor: *A. P. P. P.*

Certifying Assessor: *Michael W. P. P.*

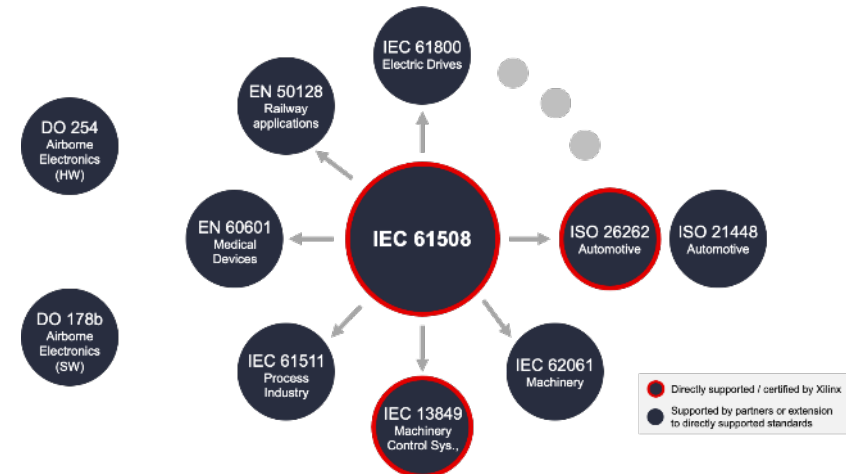
CERTIFICATE

> Functional Safety Certifications

- >> ISO 26262
- >> IEC 61508
- >> ISO 13849

> Certified

- >> Vitis/Vivado Developer Tools
- >> MicroBlaze compiler
- >> Zynq Ultrascale+ MPSoC



Target Applications for Embedded Developers



Robotics

- Joint Control
- Actuation
- Motion



Power Generation

- Pitch/Yaw Control
- Multi-level Inverter
- Communications



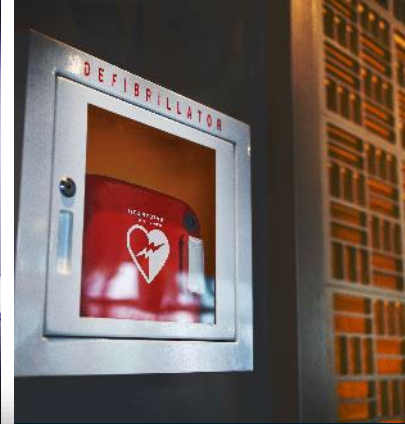
EV Charging

- Inverter Control
- V2G Communication



Medical Control

- Gantry and Bed
- Surgical Actuation
- Surgical Generator



Patient Care

- Sensor Fusion
- 3D Graphic Display
- Precision Calculations



Public Transportation

- Train Control / Mgmt.
- Comfort / Information
- Comms / Recorder

AMD
together we advance_



Simplifying complexity

THANK YOU

See more at accelerat.eu and amd.com



Simplifying complexity

All content and information on this presentation is for informational and educational purposes only. Although we strive to provide accurate general information, the information presented here is not a substitute for any kind of professional advice, and you should not rely solely on this information. Always consult a professional in the area for your particular needs a circumstances prior to making a professional, legal, instructional and financial decisions.