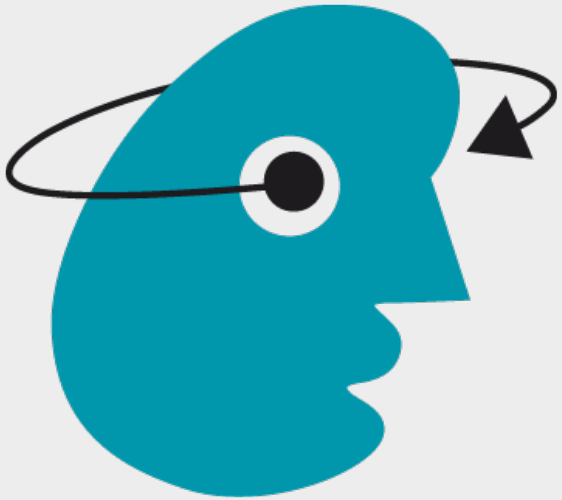


DAVe
Embedded Systems

Real-Timeness and System Integrity on a Asymmetric Multi Processing configuration

D&E Event – **November 2nd**
Relator: Manuele Papais
Sales & Marketing Manager

DAVE Embedded Systems

DAVE Embedded Systems' HEADQUARTER
Via Talponedo, 29/A
33080 Porcia, Italy

DAVE Embedded Systems' BRANCH OFFICE
Maximilianstrasse, 13
80539 München, Germany

DAVE
Embedded Systems

DAVE Embedded Systems

DAVE Embedded Systems' HEADQUARTER
Via Talponedo, 29/A
33080 Porcia, Italy

DAVE Embedded Systems' BRANCH OFFICE
Maximilianstrasse, 13
80539 München, Germany

Sales Offices:

- USA – California
- UK – Swindon
- France – Paris
- Israel – Tel Aviv
- Belgium / The Netherlands
  - **Telerex B.V.**
- Now opening: Japan

DAVE Embedded Systems

DAVE Embedded Systems

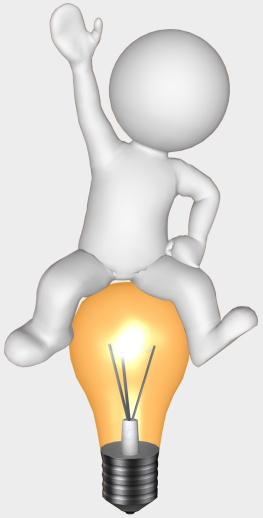
Concept and Design
of Embedded Systems

DAVE
Embedded Systems

DAVE Embedded Systems

Concept and Design
of Embedded Systems

Solutions Provider



Supporting and Promoting
Customer Ideas and
Concepts
from Scratch to Business

DAVE
Embedded Systems

Products Portfolio

DAVE Embedded Systems

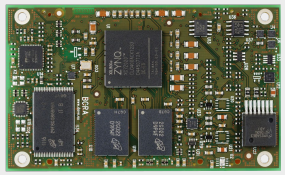
Products Portfolio

System On Modules

Texas Instruments
SITARA, DA VINCI

NXP i.MX6...

XILINX Zynq



DAVE Embedded Systems

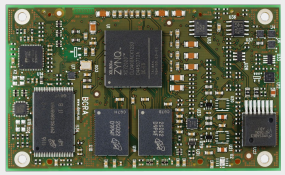
Products Portfolio

System On Modules

Texas Instruments
SITARA, DA VINCI

NXP i.MX6...

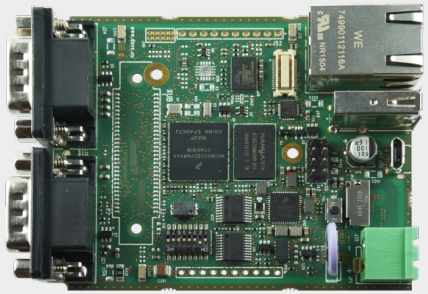
XILINX Zynq



Single Board Computers

Wall mount

DIN Bar mount



DAVE Embedded Systems

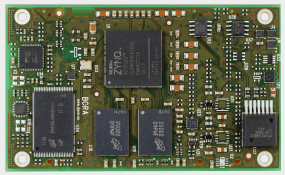
Products Portfolio

System On Modules

Texas Instruments
SITARA, DA VINCI

NXP i.MX6...

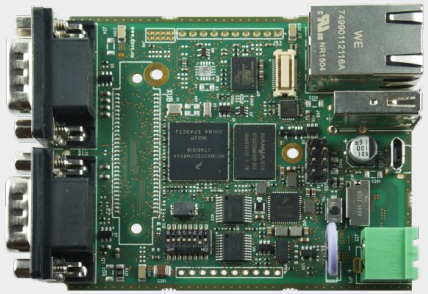
XILINX Zynq



Single Board Computers

Wall mount

DIN Bar mount



Customized Solutions

Based on customer requirements

Based on existing proven solutions

DAVE Embedded Systems

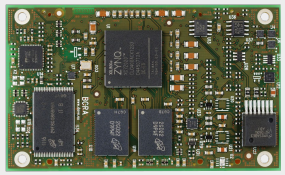
Products Portfolio

System On Modules

Texas Instruments
SITARA, DA VINCI

NXP i.MX6...

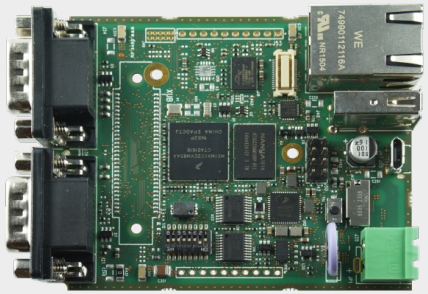
XILINX Zynq



Single Board Computers

Wall mount

DIN Bar mount



Customized Solutions

Based on customer requirements

Based on existing proven solutions

Available with advanced SW elements

DAVe Embedded Systems

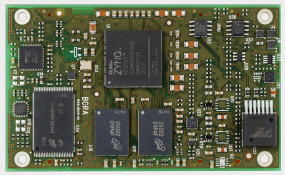
Products Portfolio

System On Modules

Texas Instruments
SITARA, DA VINCI

NXP i.MX6...

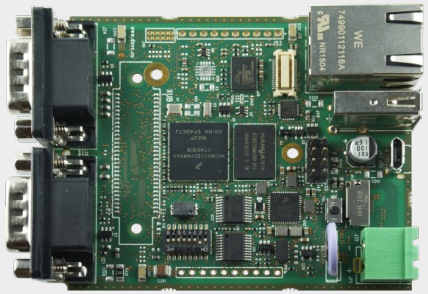
XILINX Zynq



Single Board Computers

Wall mount

DIN Bar mount



Customized Solutions

Based on customer requirements

Based on existing proven solutions

Available with advanced SW elements

Linux Kernel & Drivers

DAVE Embedded Systems

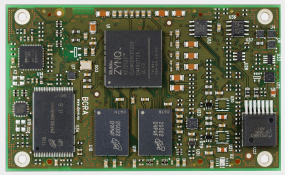
Products Portfolio

System On Modules

Texas Instruments
SITARA, DA VINCI

NXP i.MX6...

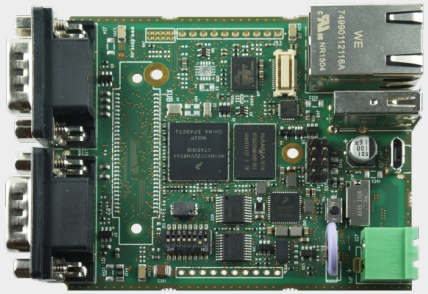
XILINX Zynq



Single Board Computers

Wall mount

DIN Bar mount



Customized Solutions

Based on customer requirements

Based on existing proven solutions

Available with advanced SW elements

Linux Kernel & Drivers

Android BSP

DAVE Embedded Systems

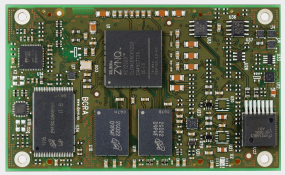
Products Portfolio

System On Modules

Texas Instruments
SITARA, DA VINCI

NXP i.MX6...

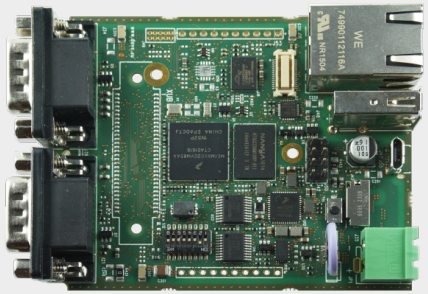
XILINX Zynq



Single Board Computers

Wall mount

DIN Bar mount



Customized Solutions

Based on customer requirements

Based on existing proven solutions

Available with advanced SW elements

Linux Kernel & Drivers

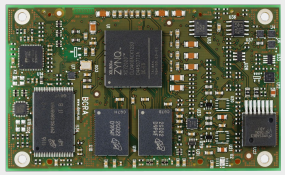
Android BSP

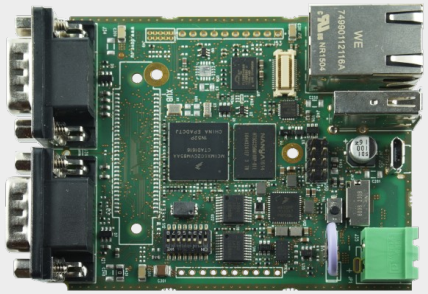
FPGA Vivado Project
and
SDSoC/HLS examples

DAVe Embedded Systems

Products Portfolio

System On Modules	Single Board Computers	Customized Solutions
Texas Instruments SITARA, DA VINCI	Wall mount	Based on customer requirements
NXP i.MX6...	DIN Bar mount	Based on existing proven solutions
XILINX Zynq		





Available with advanced SW elements

Linux Kernel & Drivers

Android BSP

FPGA Vivado Project and SDSoC/HLS examples

RTOS Integration/examples

DAVe Embedded Systems

AMP Asymmetric Multi Processing

BIG - LITTLE

- NXP Vybrid
- TI AM335
- ...

DAVE Embedded Systems

AMP Asymmetric Multi Processing

BIG - LITTLE

- NXP Vybrid
- TI AM335
- ...

SIMMETRIC

- NXP i.MX6 DUAL Lite
- NXP i.MX6 DUAL
- NXP i.MX6 QUAD
- ...

DAVE Embedded Systems

AMP Asymmetric Multi Processing

BIG - LITTLE

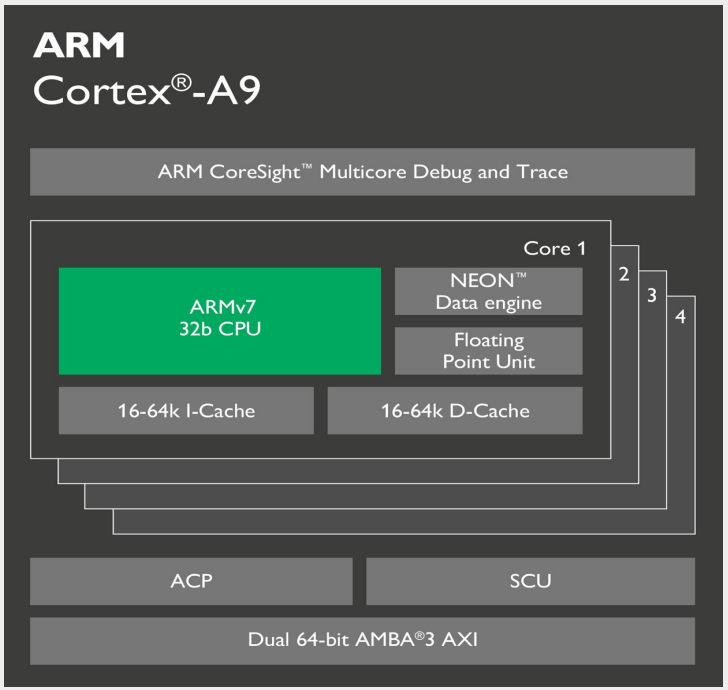
- NXP Vybrid
- TI AM335
- ...

SIMMETRIC

- NXP i.MX6 DUAL Lite
- NXP i.MX6 DUAL
- NXP i.MX6 QUAD
- ...

DAVE Embedded Systems

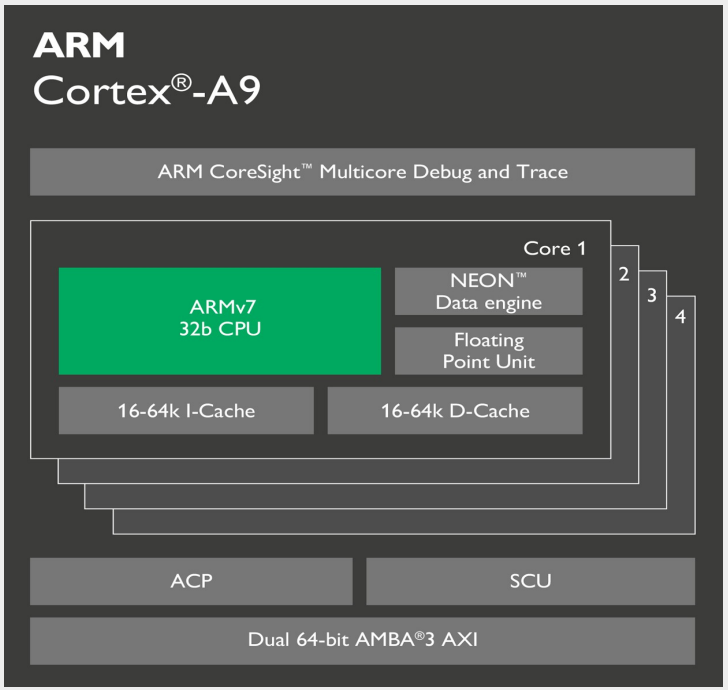
Cortex-A9 architecture



- Multicore platform approach
- Low power architecture
- Industrial grade proof

DAVE
Embedded Systems

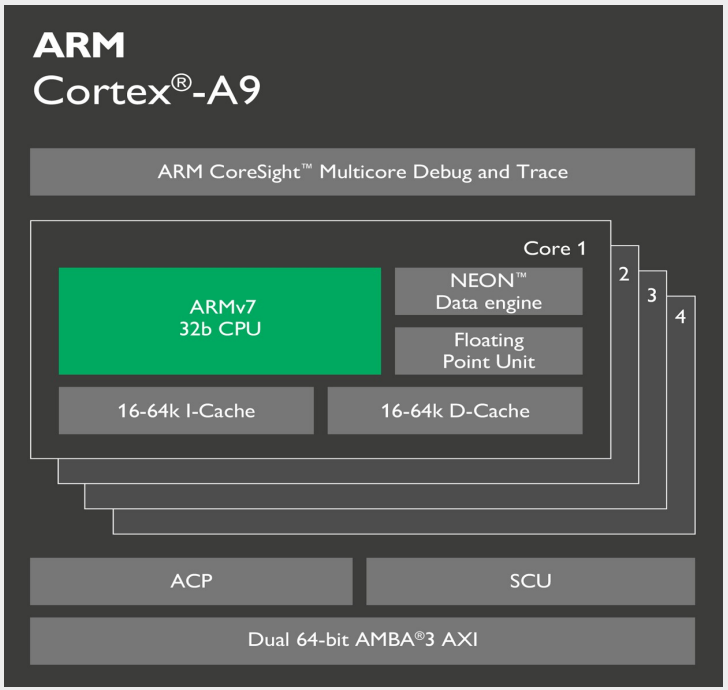
Cortex-A9 architecture



- Multicore platform approach
- Low power architecture
- Industrial grade proof
- **TrustZone IP integrated**

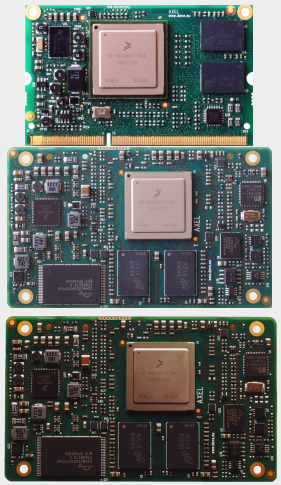
DAVE
Embedded Systems

Cortex-A9 architecture



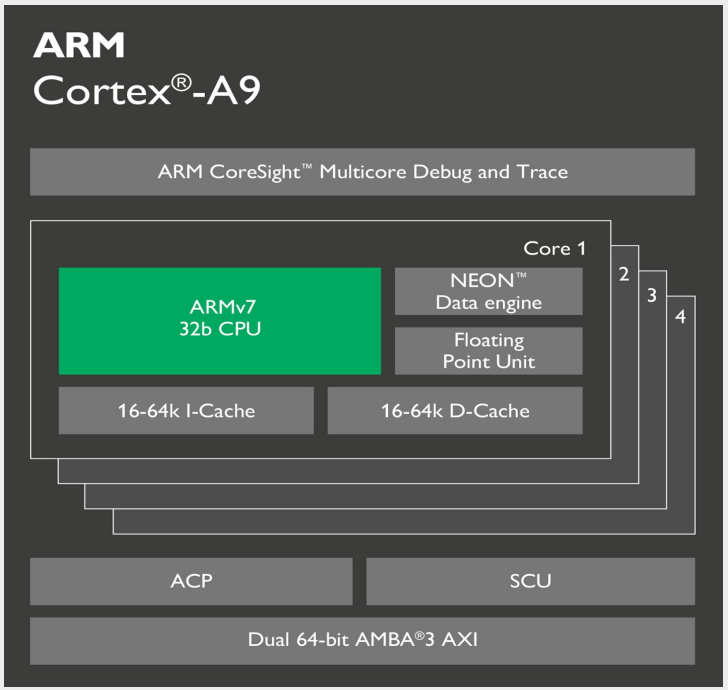
- Multicore platform approach
- Low power architecture
- Industrial grade proof
- **TrustZone IP integrated**

NXP i.MX6



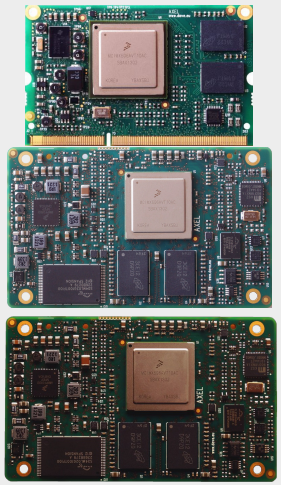
DAVE Embedded Systems

Cortex-A9 architecture

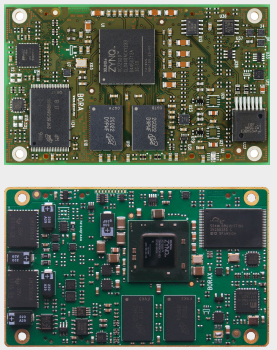


- Multicore platform approach
- Low power architecture
- Industrial grade proof
- **TrustZone IP integrated**

NXP i.MX6

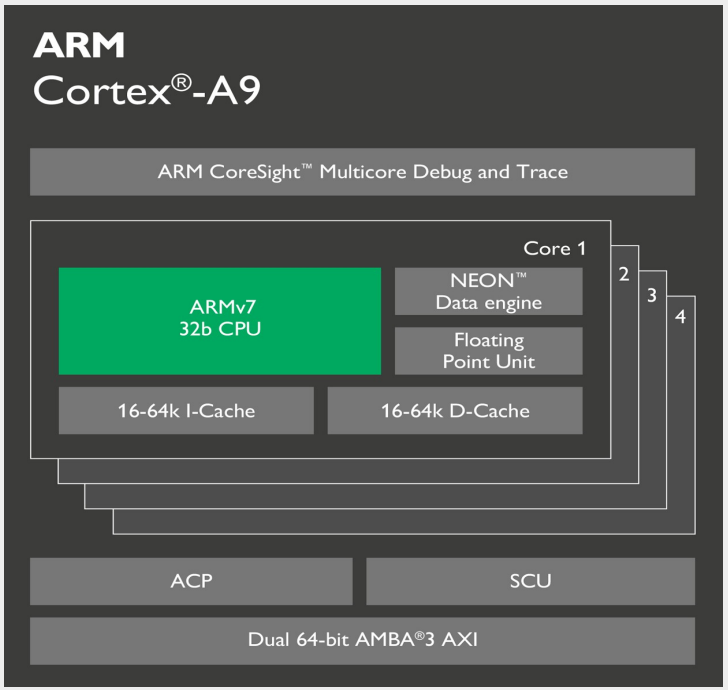


Xilinx Zynq



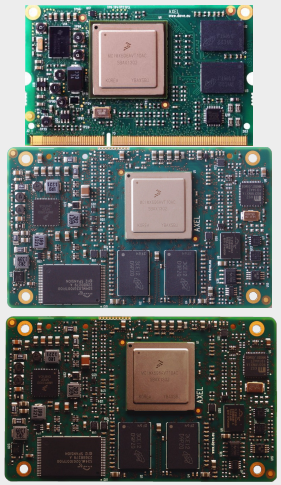
DAVE Embedded Systems

Cortex-A9 architecture

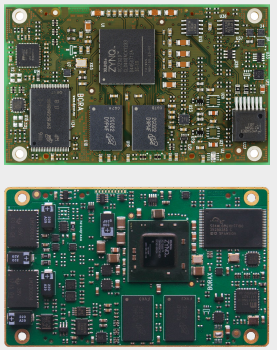


- Multicore platform approach
- Low power architecture
- Industrial grade proof
- **TrustZone IP integrated**

NXP i.MX6

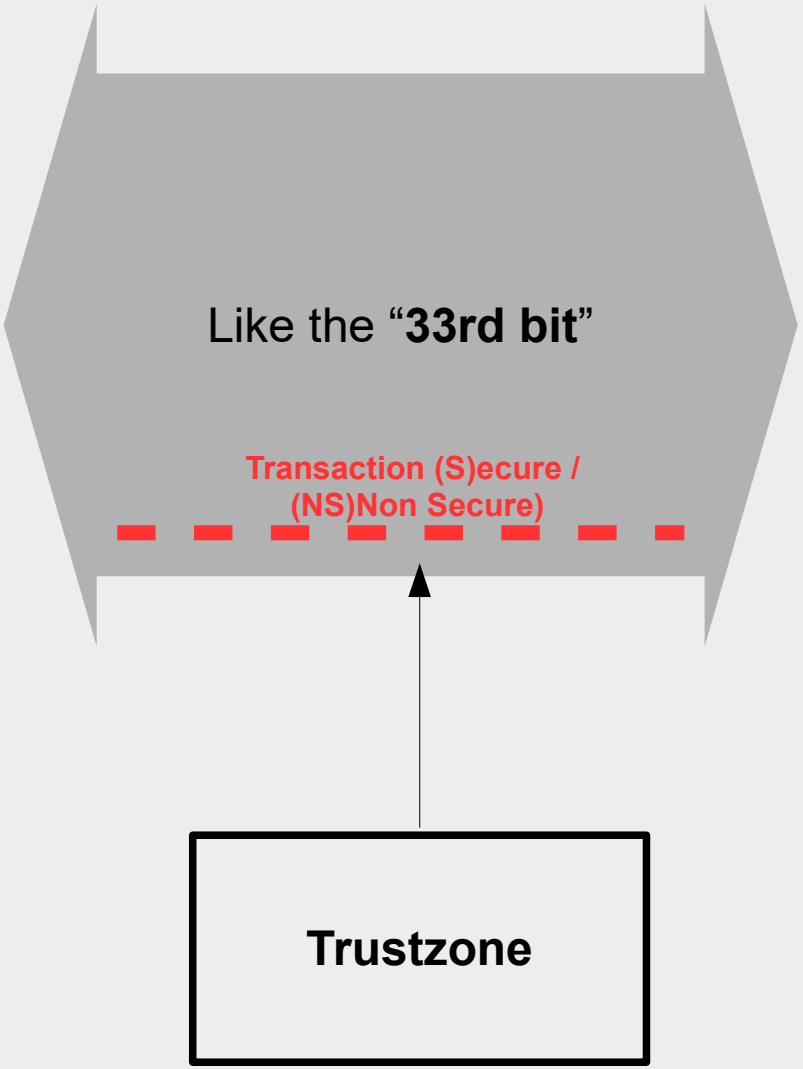


Xilinx Zynq



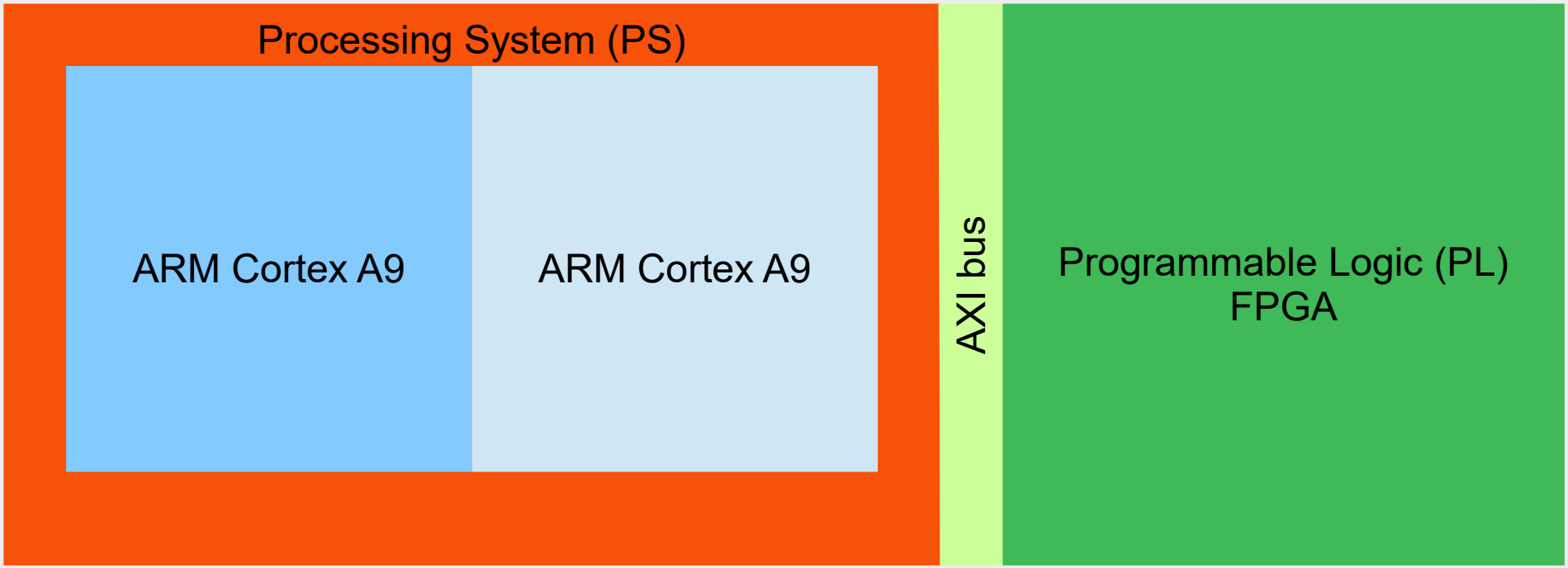
DAVE Embedded Systems

The TrustZone IP



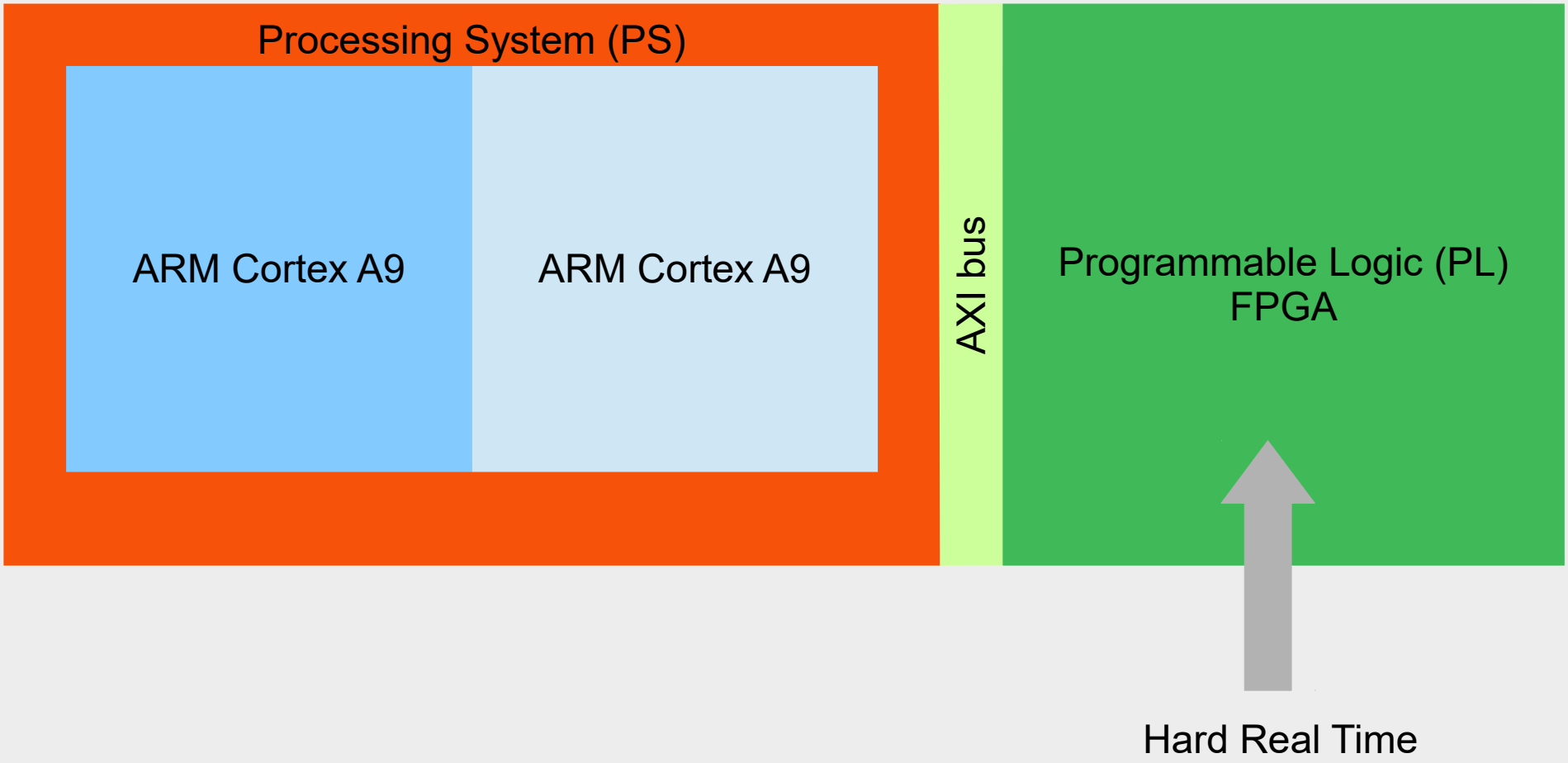
DAVE
Embedded Systems

The Asymmetric Multi Processing on Zynq Architecture



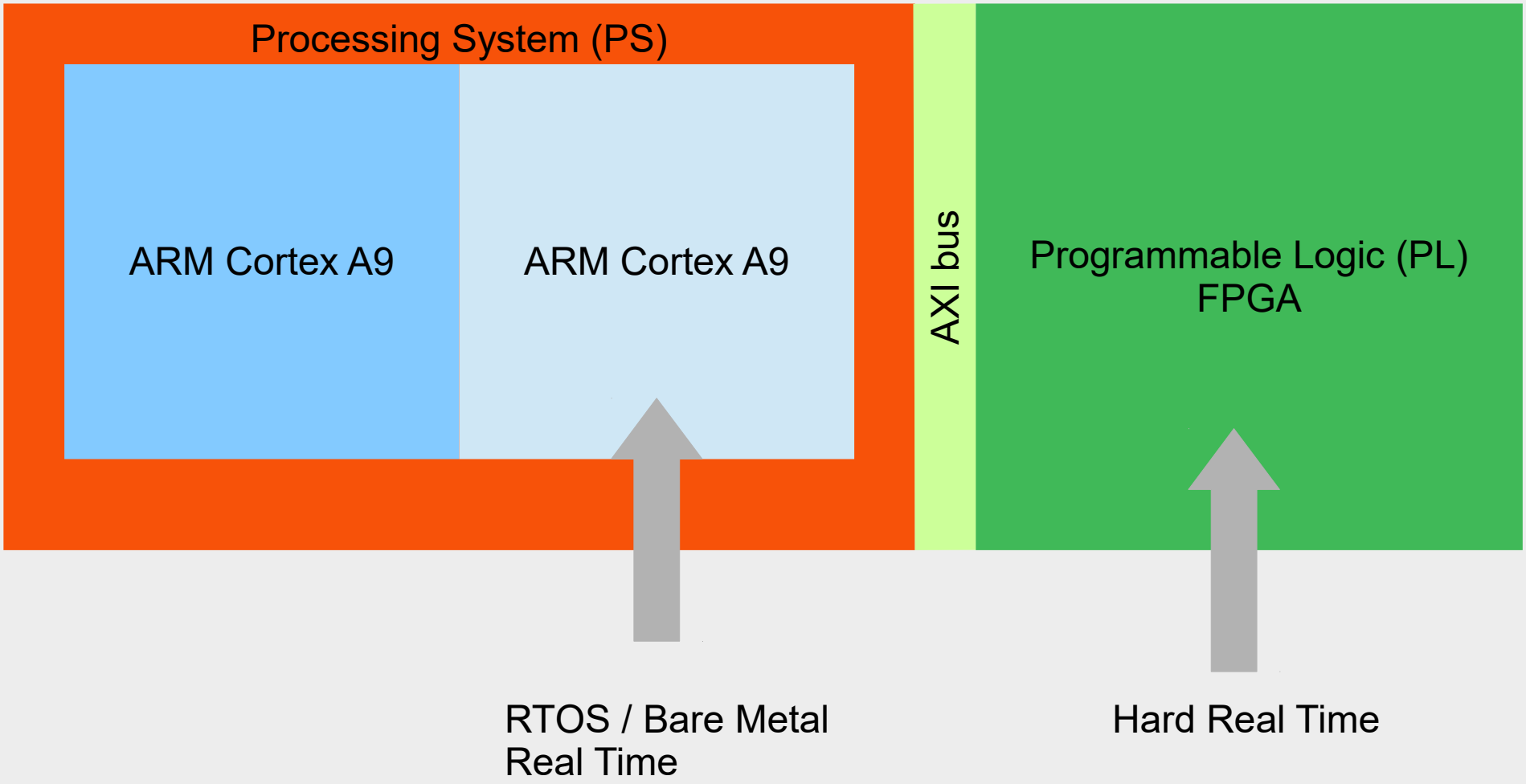
DAVE Embedded Systems

The Asymmetric Multi Processing on Zynq Architecture



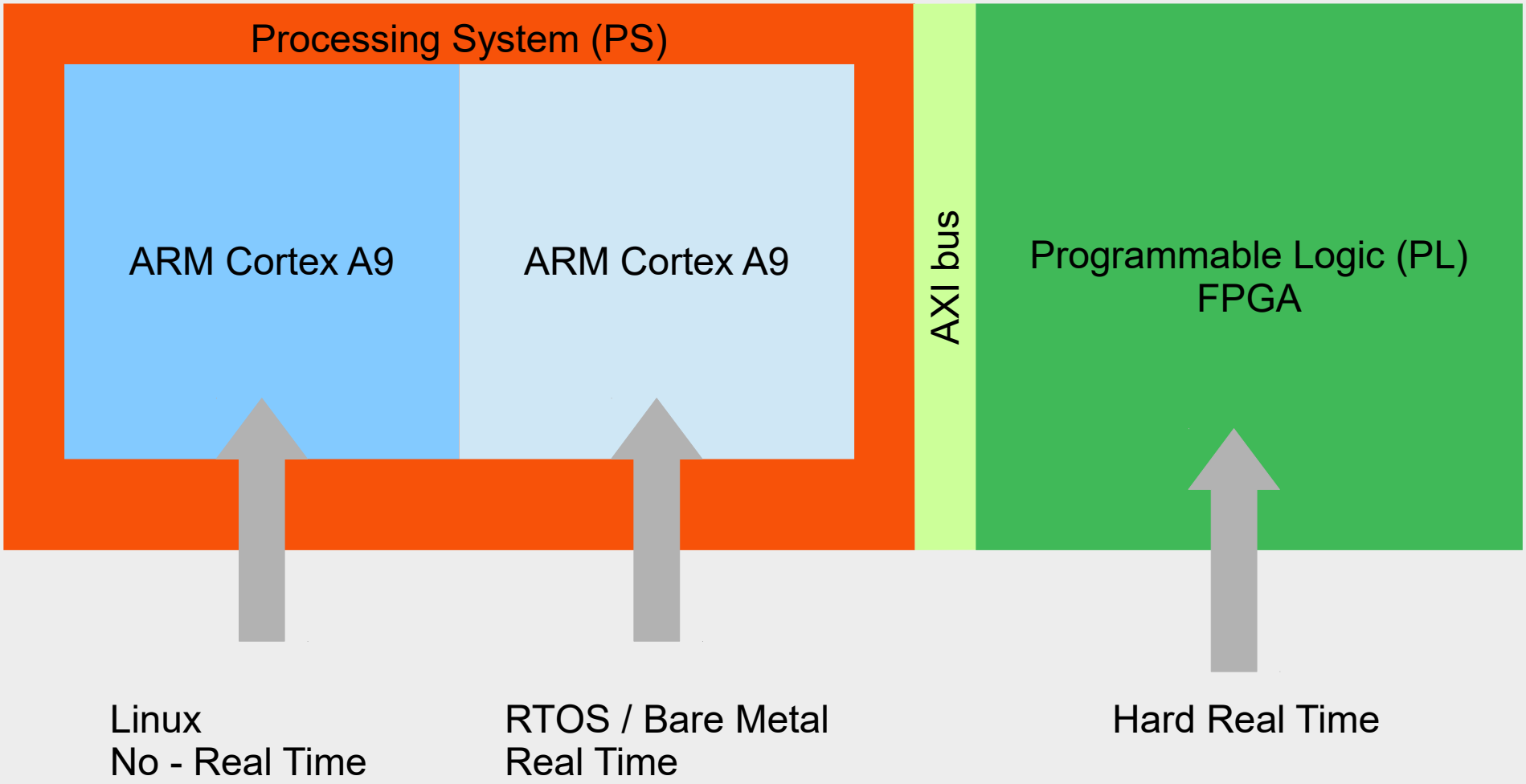
DAVE Embedded Systems

The Asymmetric Multi Processing on Zynq Architecture



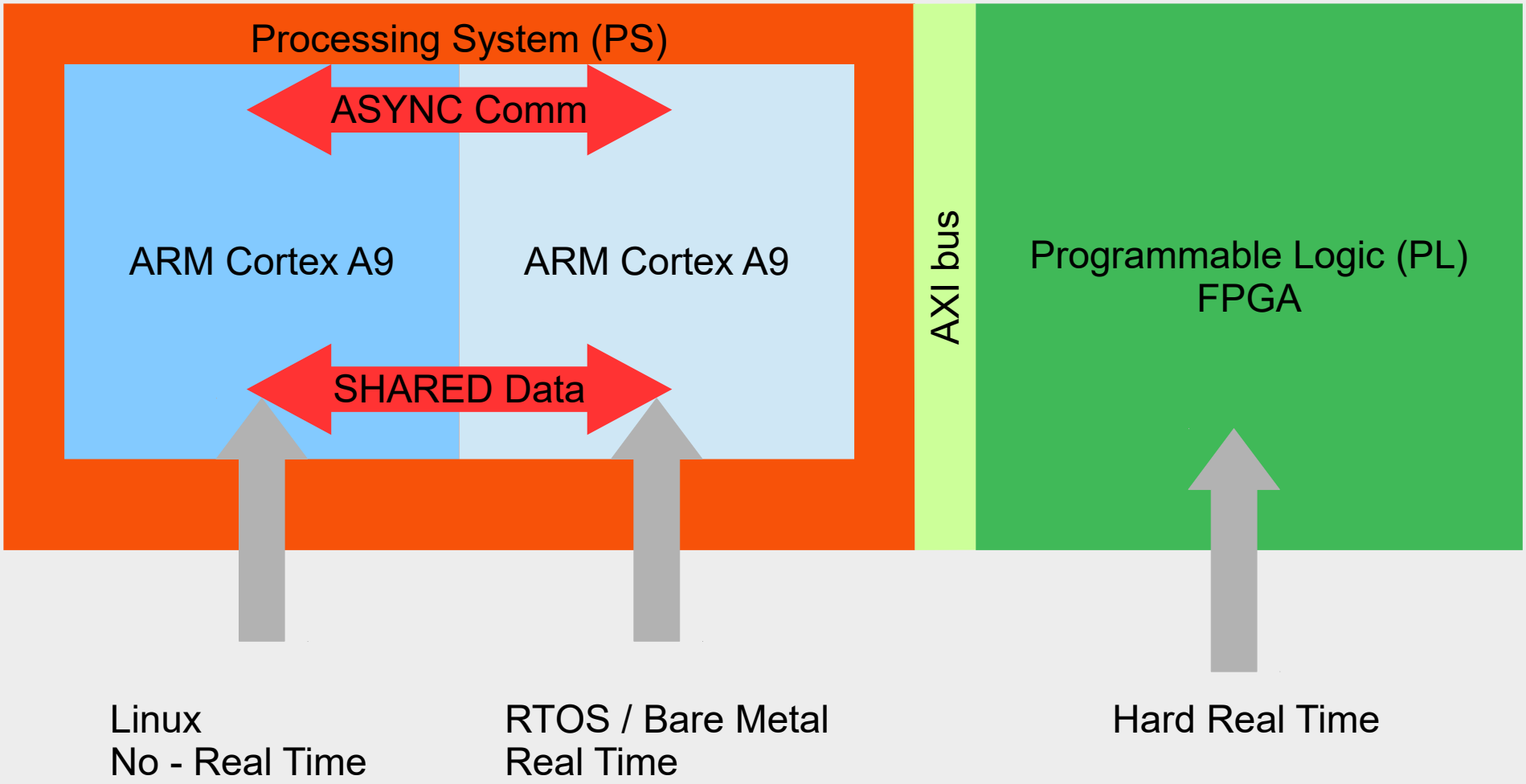
DAVE Embedded Systems

The Asymmetric Multi Processing on Zynq Architecture



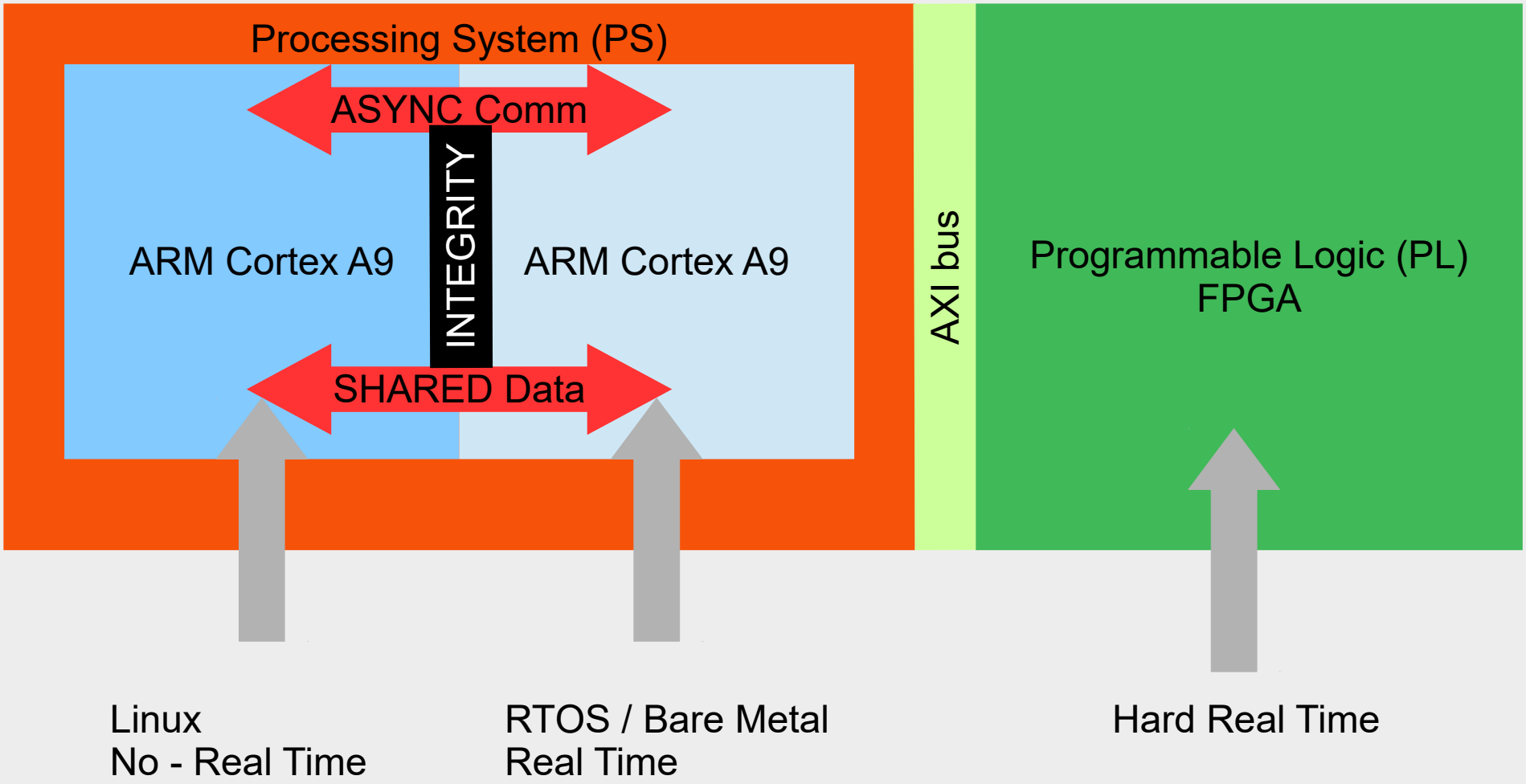
DAVE Embedded Systems

The Asymmetric Multi Processing on Zynq Architecture



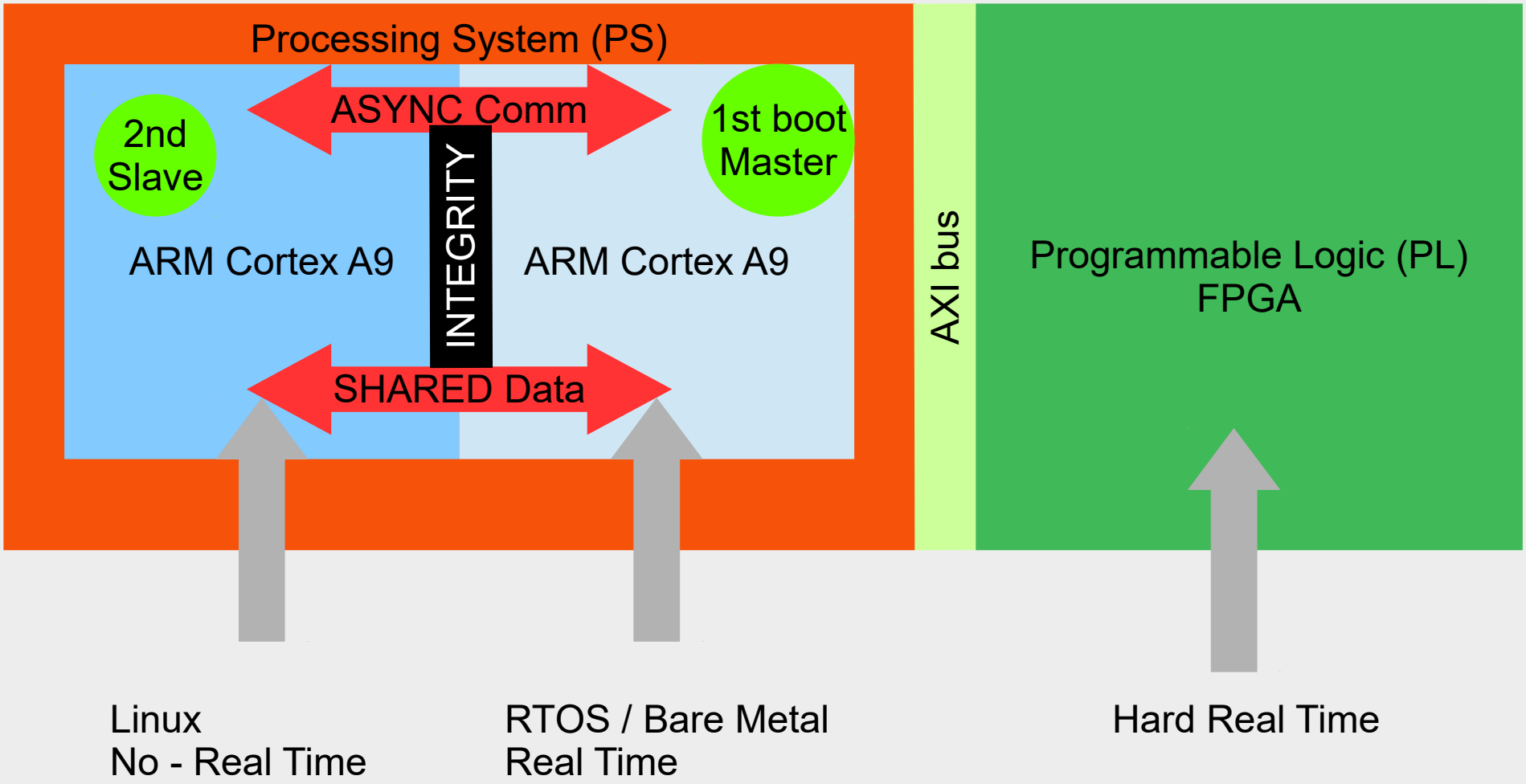
DAVE Embedded Systems

The Asymmetric Multi Processing on Zynq Architecture



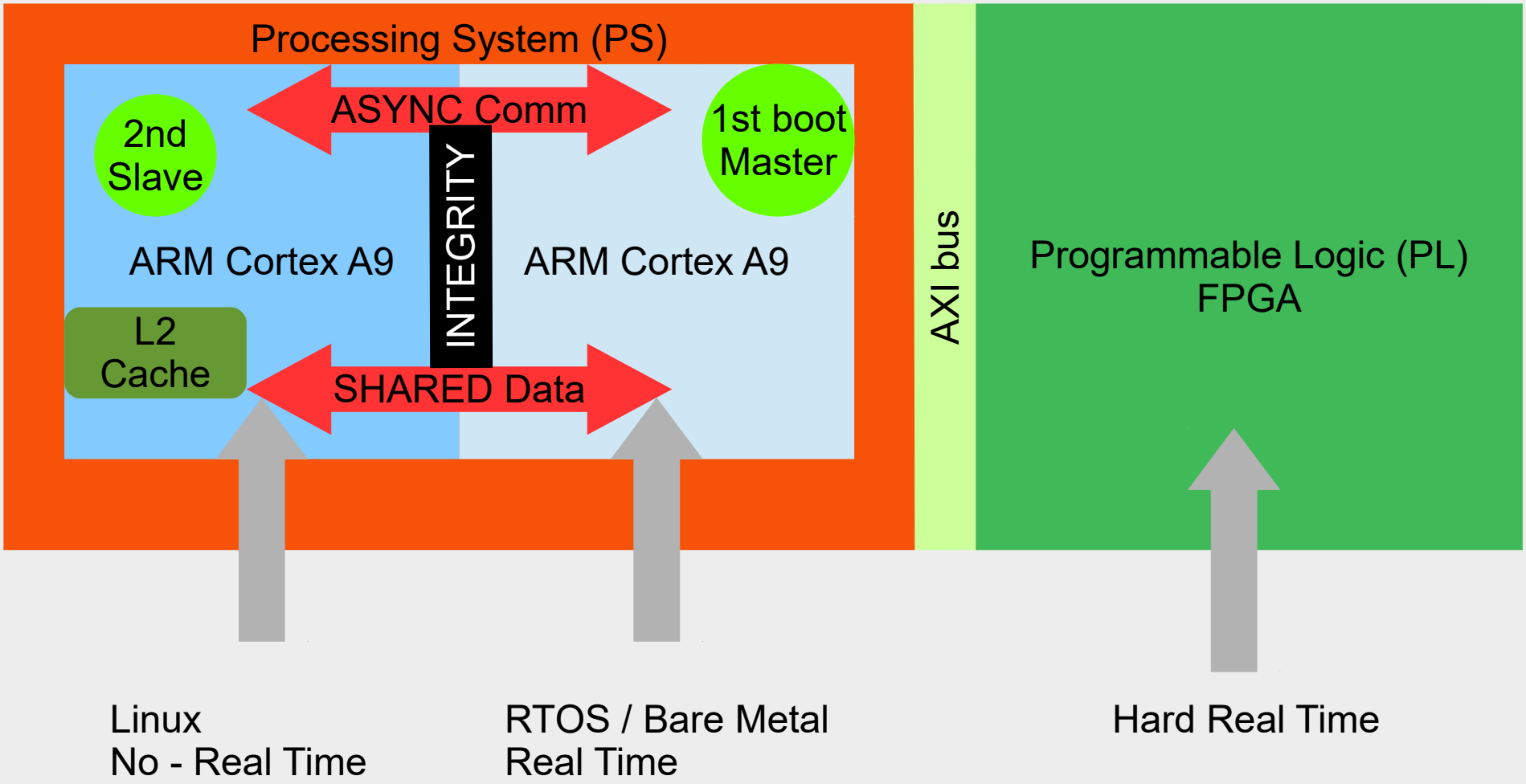
DAVe Embedded Systems

The Asymmetric Multi Processing on Zynq Architecture



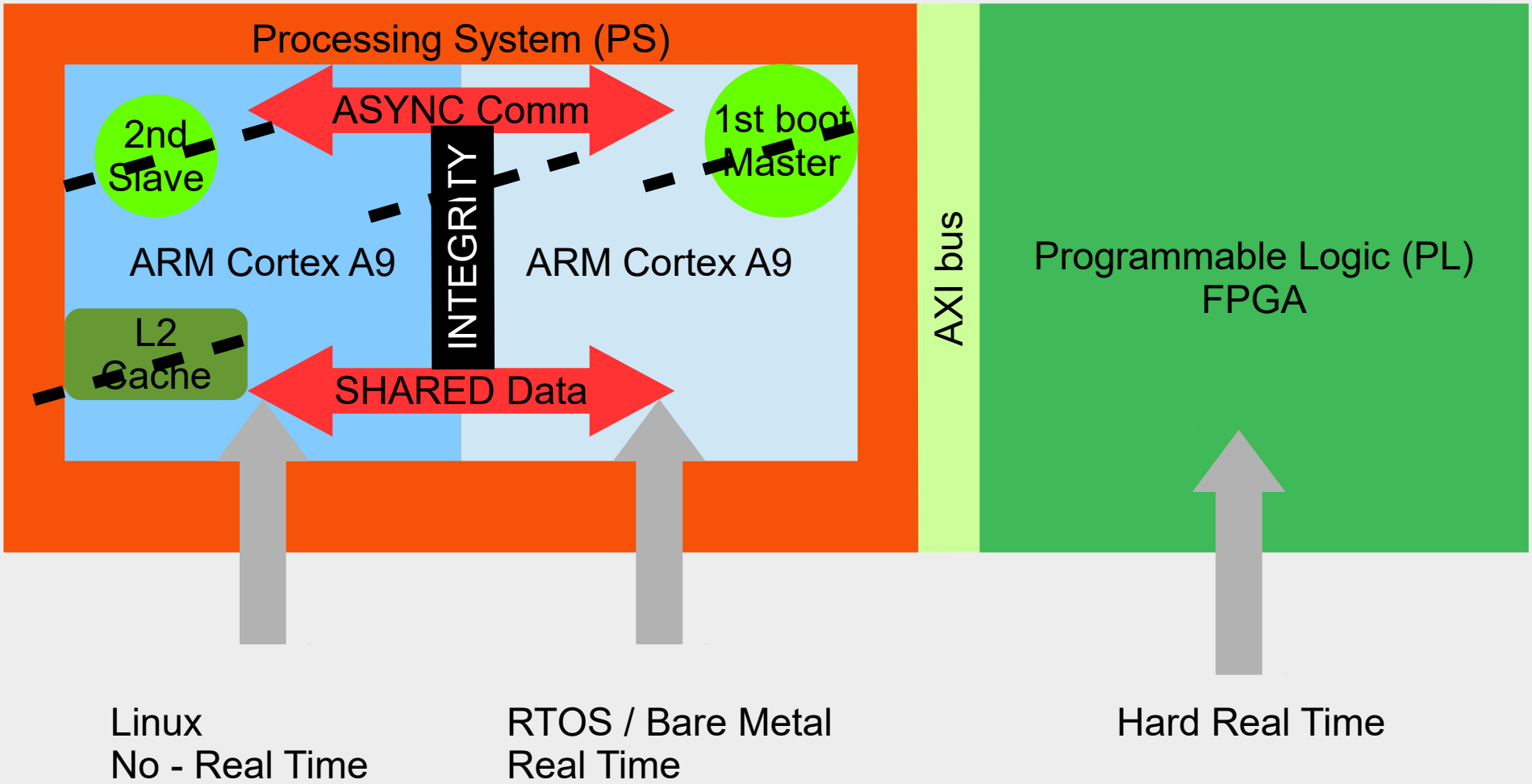
DAVE Embedded Systems

The Asymmetric Multi Processing on Zynq Architecture



DAVE Embedded Systems

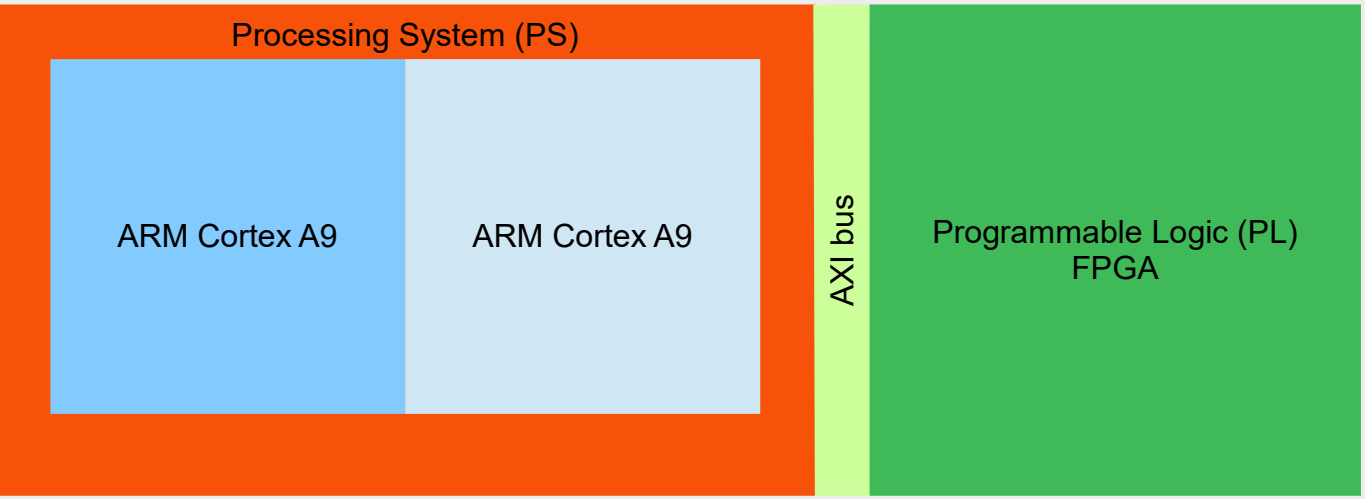
The Asymmetric Multi Processing on Zynq Architecture



DAVE Embedded Systems

Traditional AMP has not ALL these feature so, integrate all new feature listed?

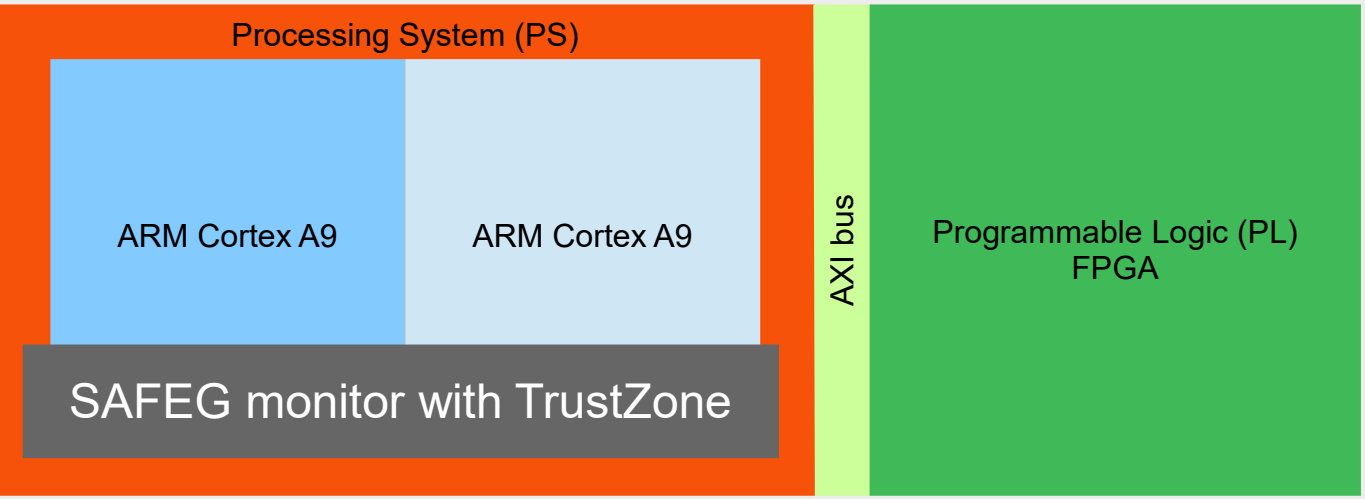
The TrustZone-based Approach



- It is required a Software Monitor

DAVE
Embedded Systems

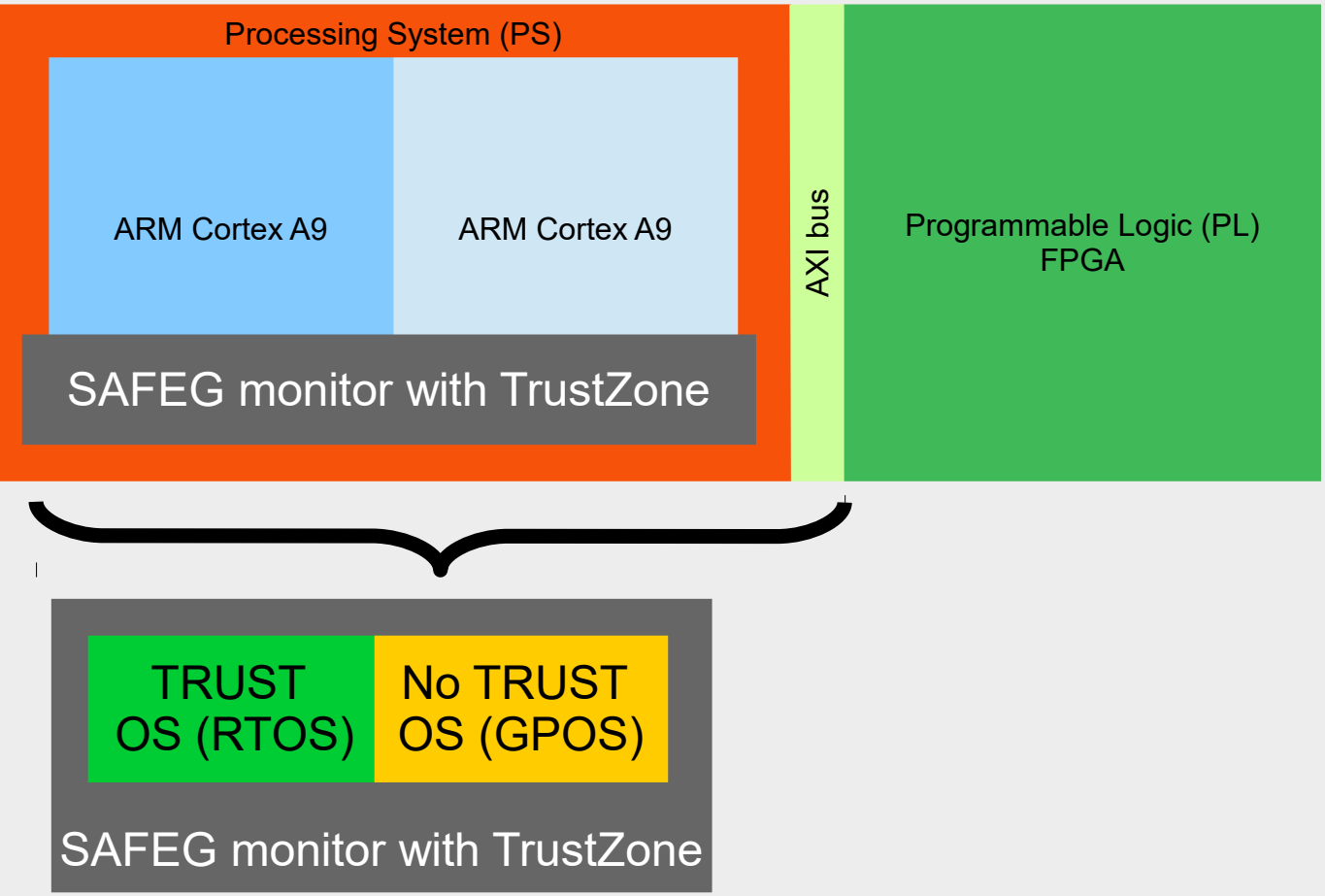
The TrustZone-based Approach



- It is required a Software Monitor
- Customized version of SAFEG

DAVE Embedded Systems

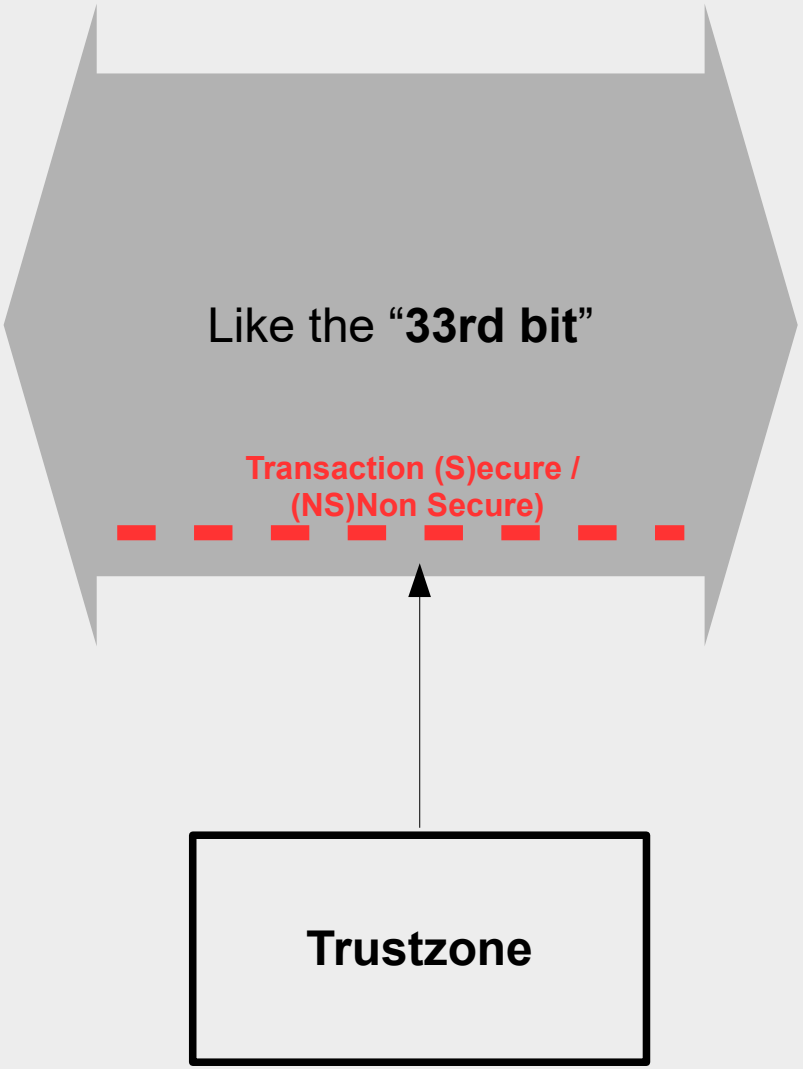
The TrustZone-based Approach



- It is required a Software Monitor
- Customized version of SAFEG
- The monitor is responsible for:
  - Enable TrustZone IP
  - Initialize Trusted /Non Trusted areas

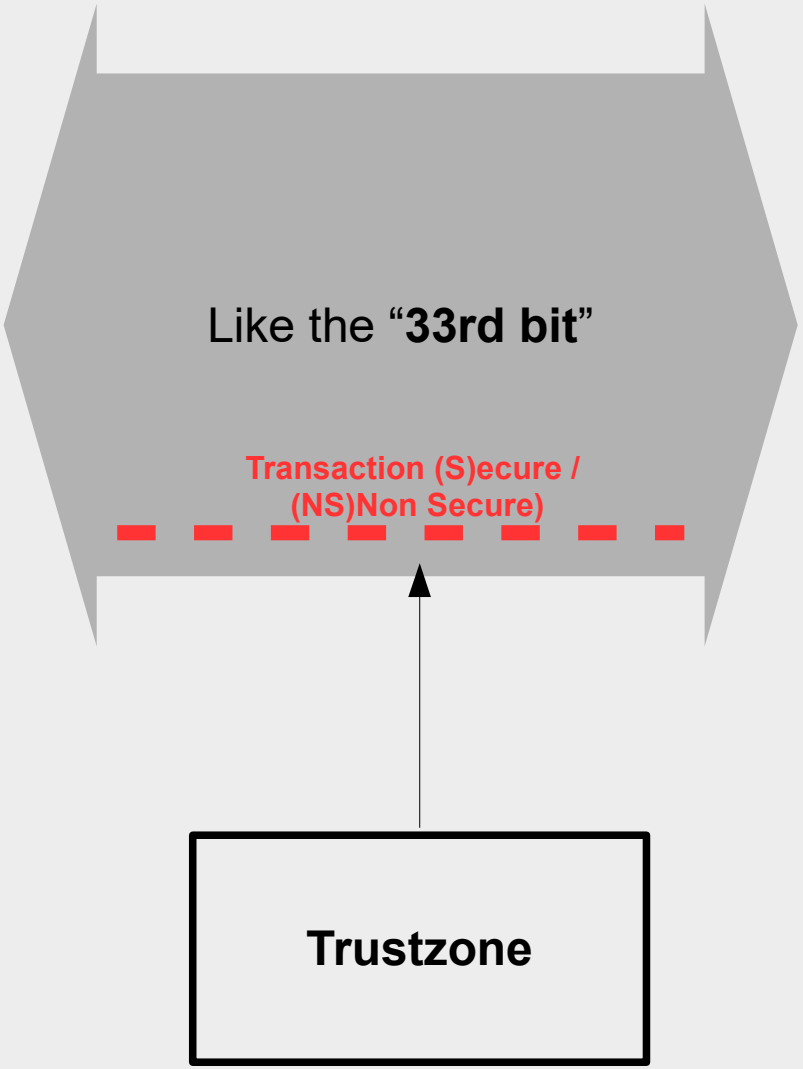
DAVE Embedded Systems

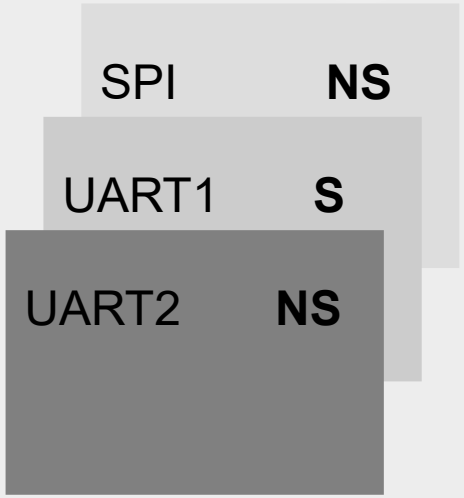
The TrustZone - based Approach



DAVE
Embedded Systems

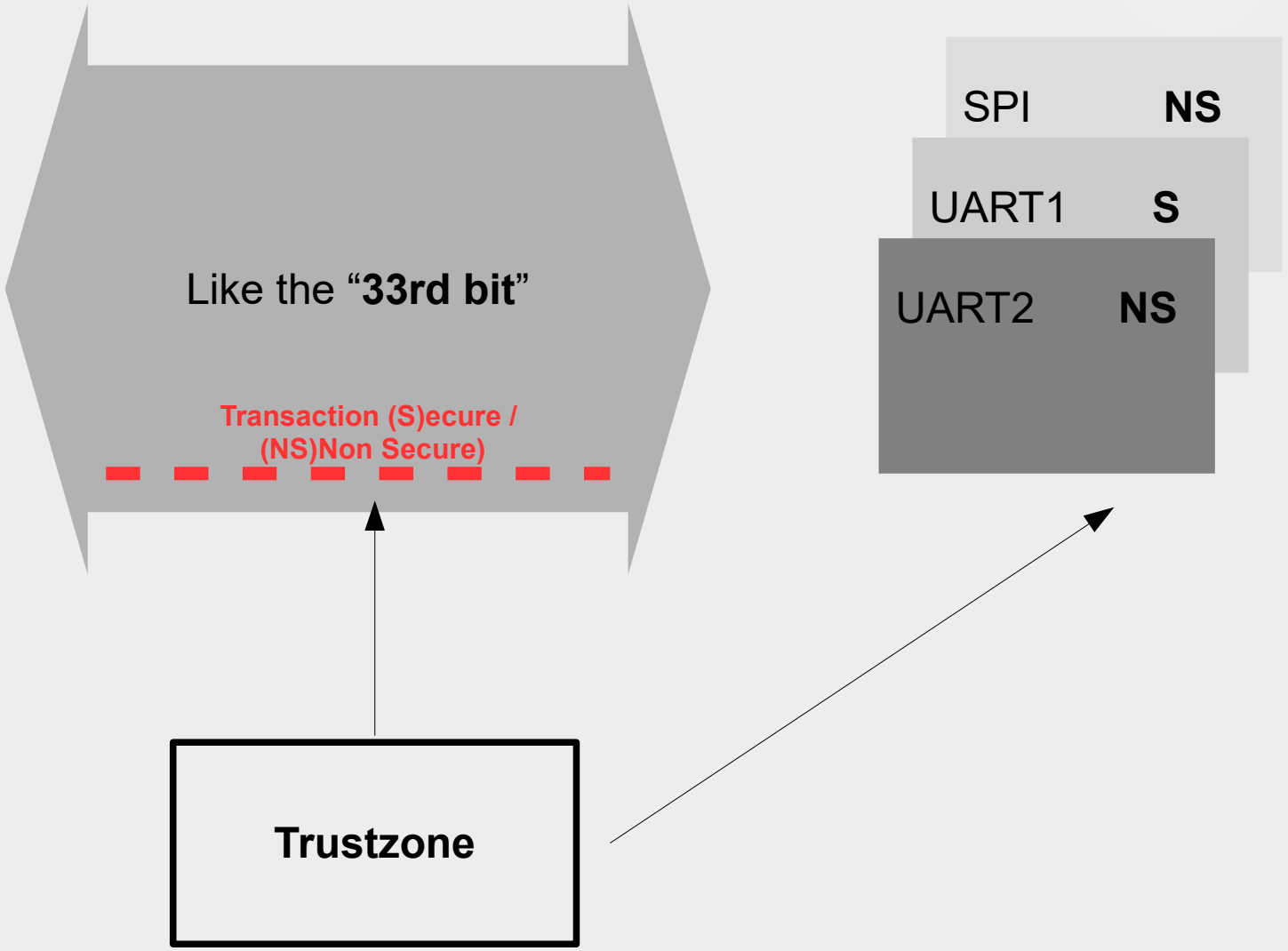
The TrustZone - based Approach





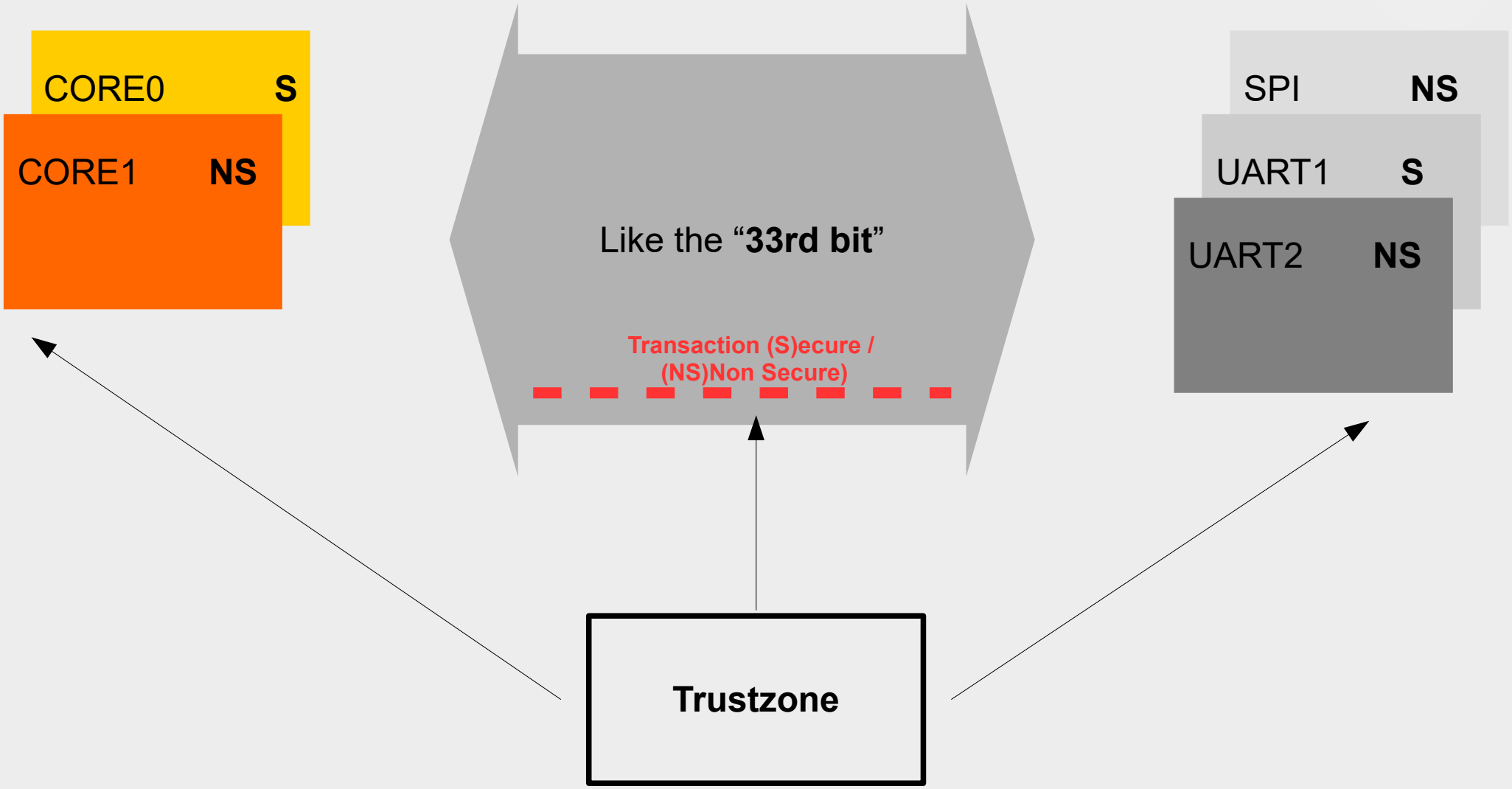
DAVE Embedded Systems

The TrustZone - based Approach



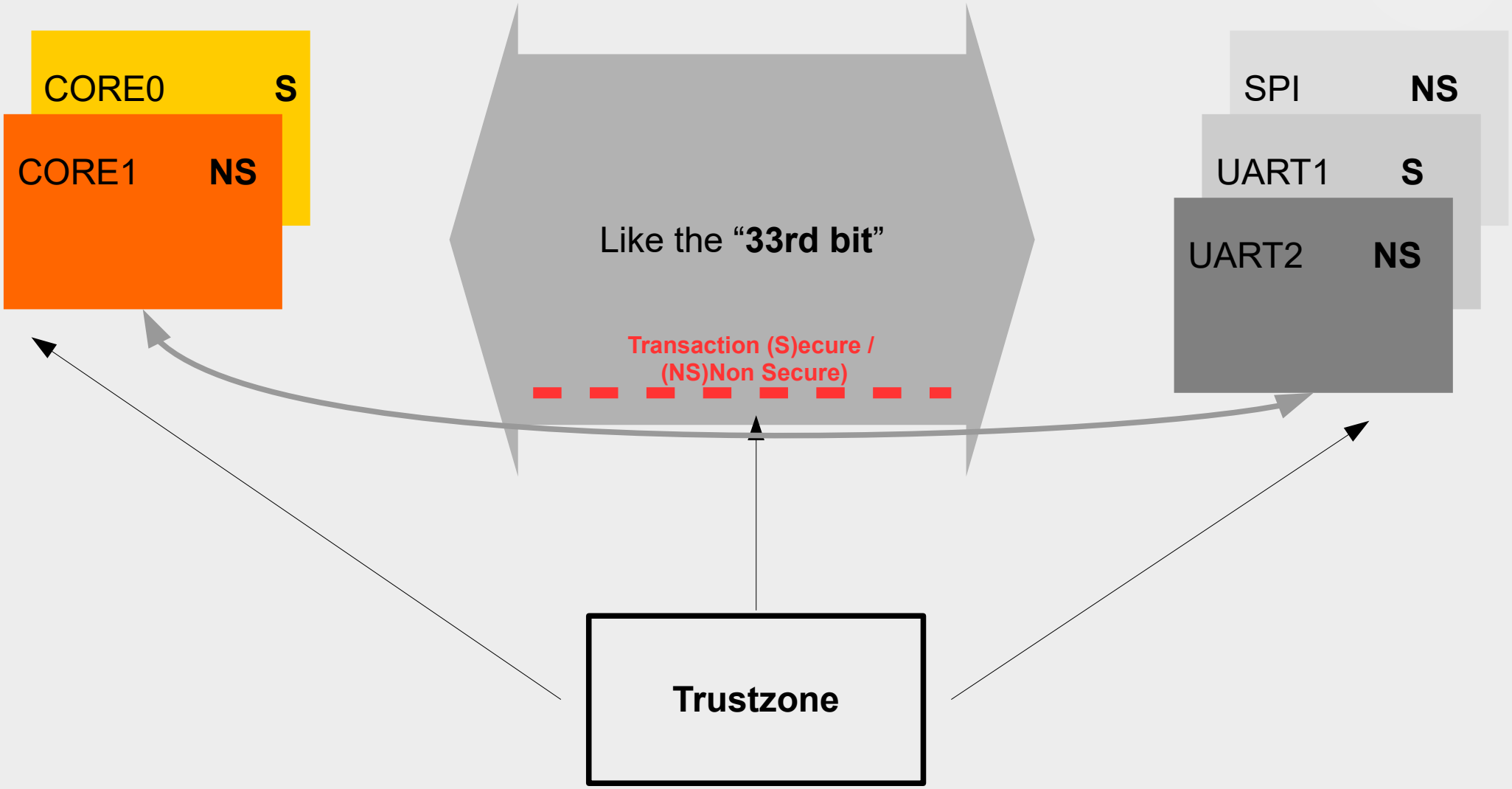
DAVE Embedded Systems

The TrustZone - based Approach



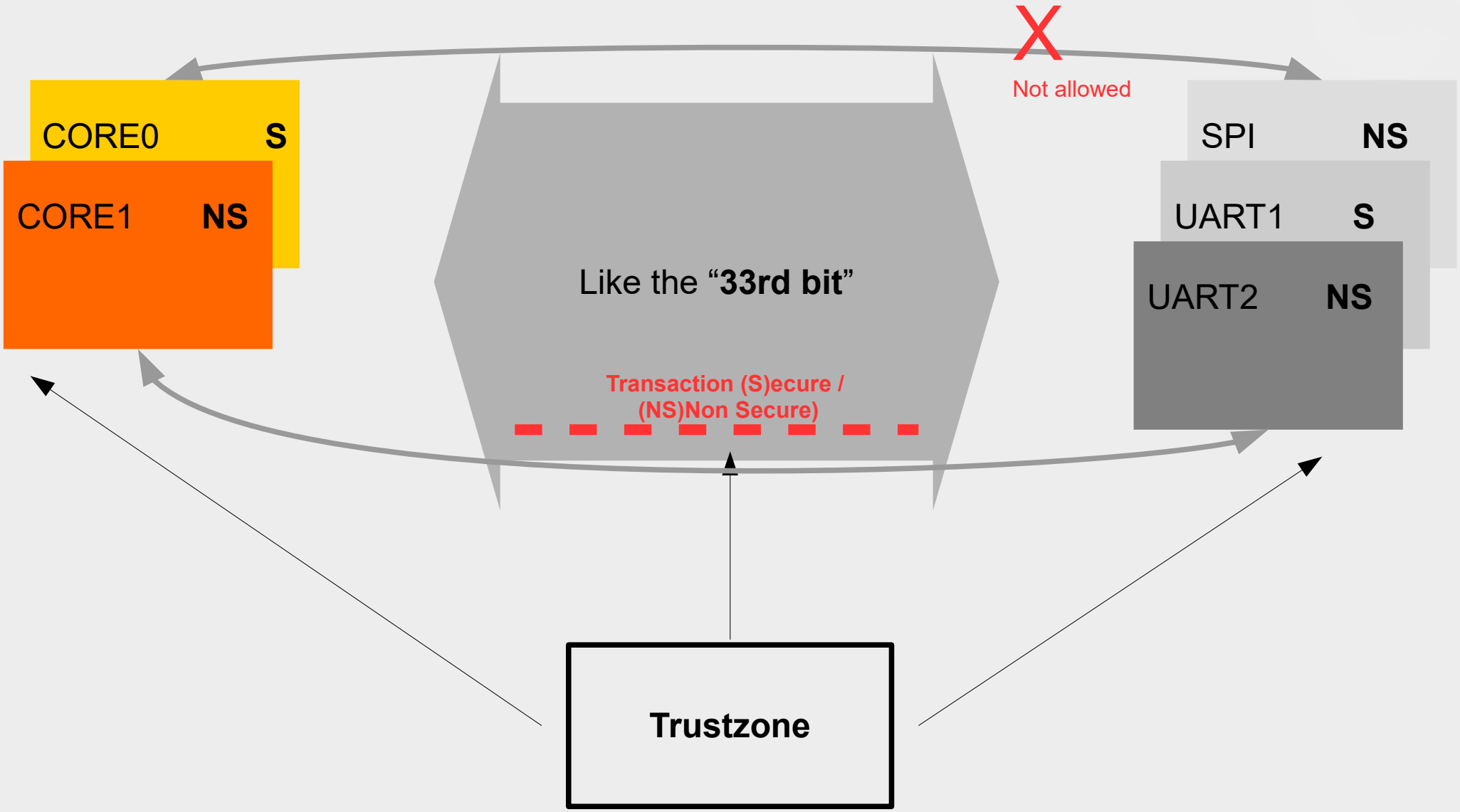
DAVE Embedded Systems

The TrustZone - based Approach



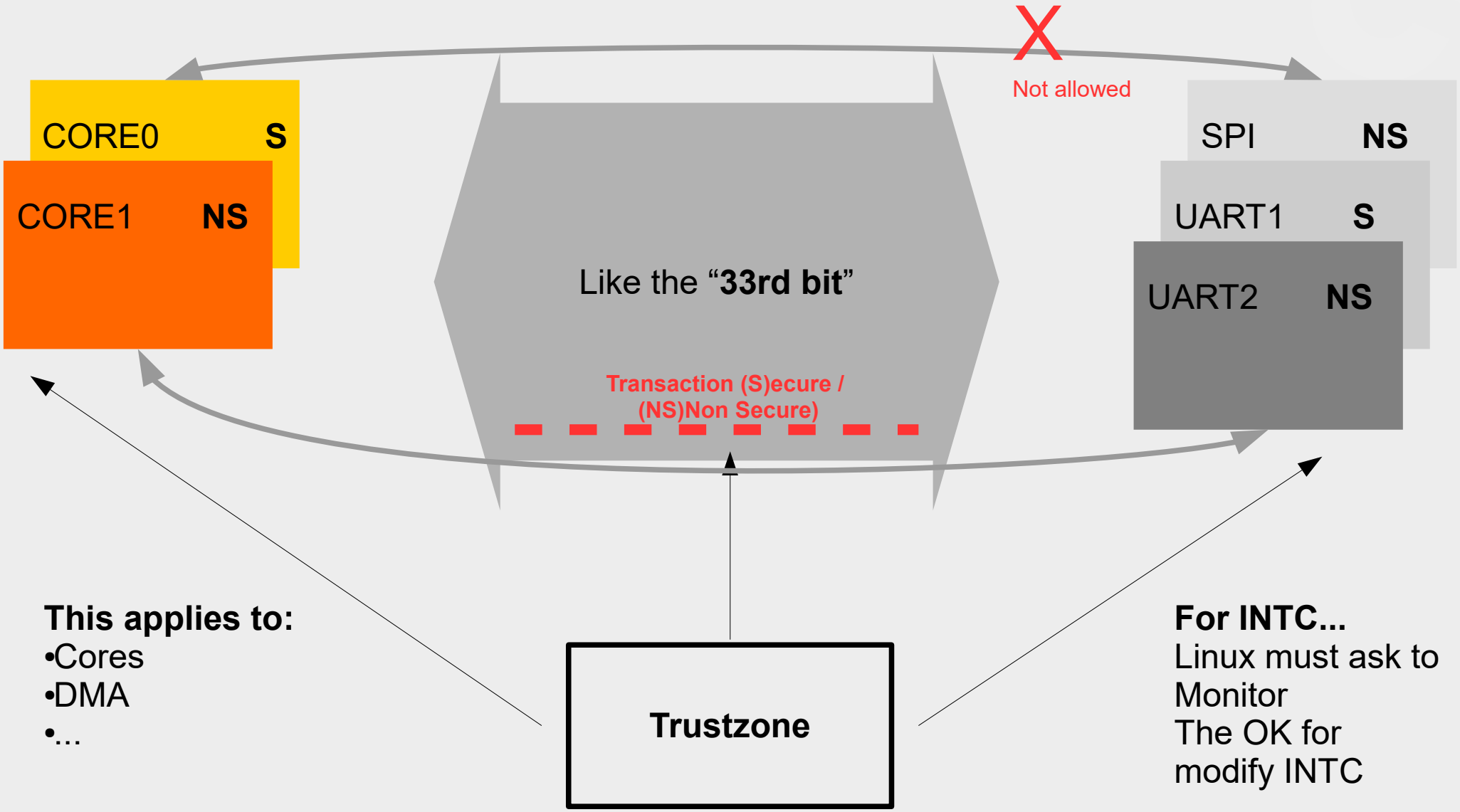
DAVE Embedded Systems

The TrustZone - based Approach



DAVE Embedded Systems

The TrustZone - based Approach

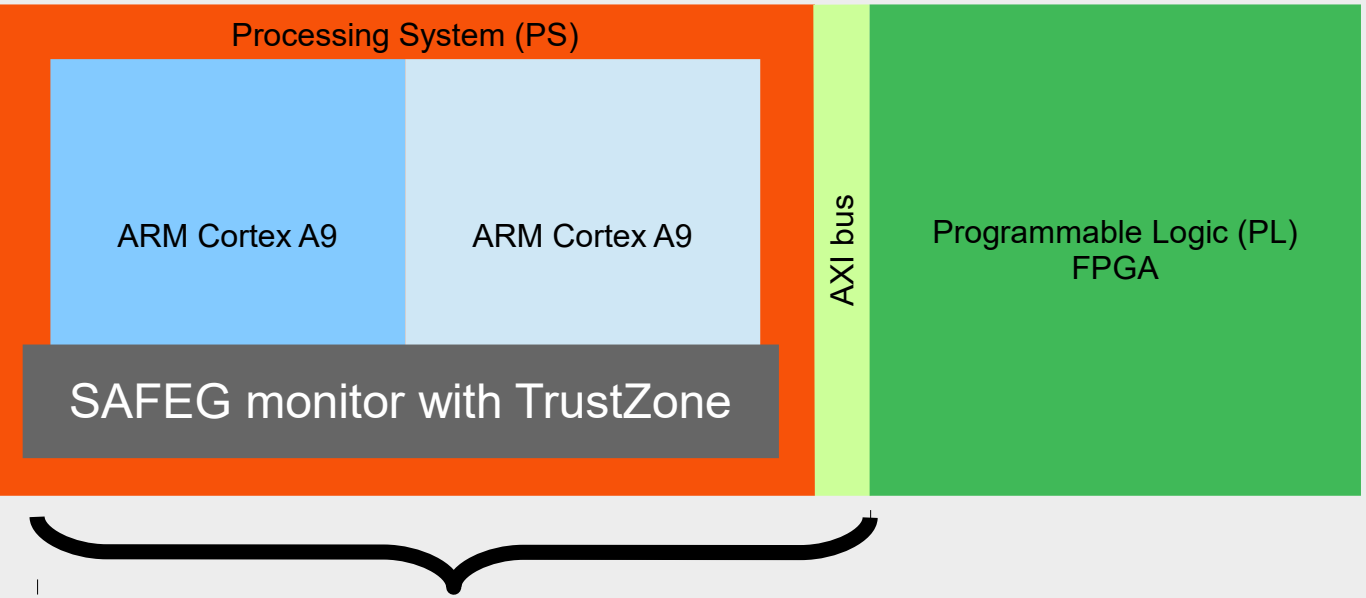


This applies to:
- Cores
- DMA
- ...

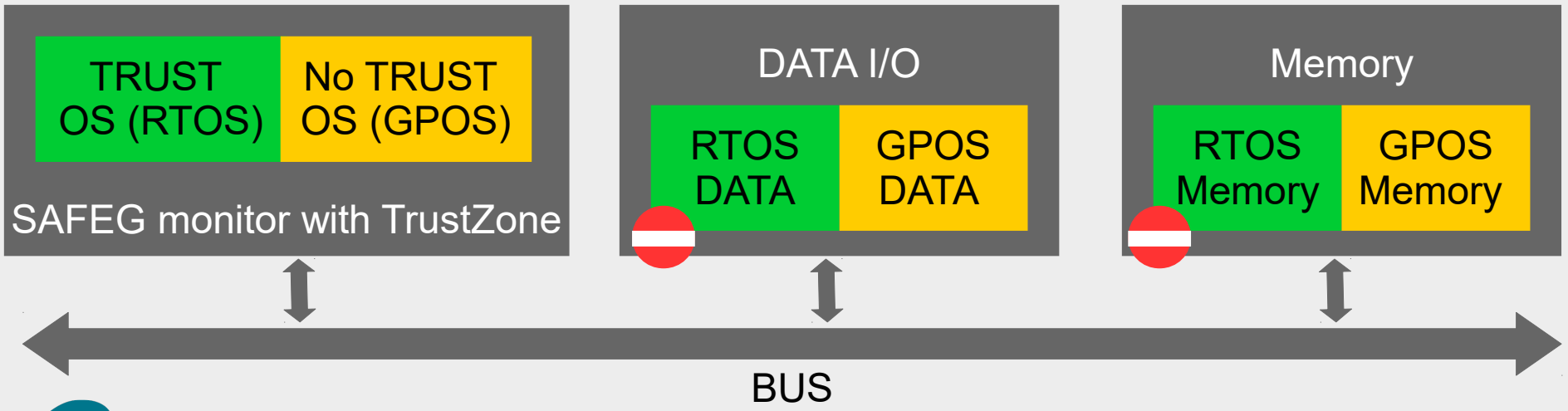
For INTC...
Linux must ask to Monitor
The OK for modify INTC

DAVE Embedded Systems

The TrustZone-based Approach

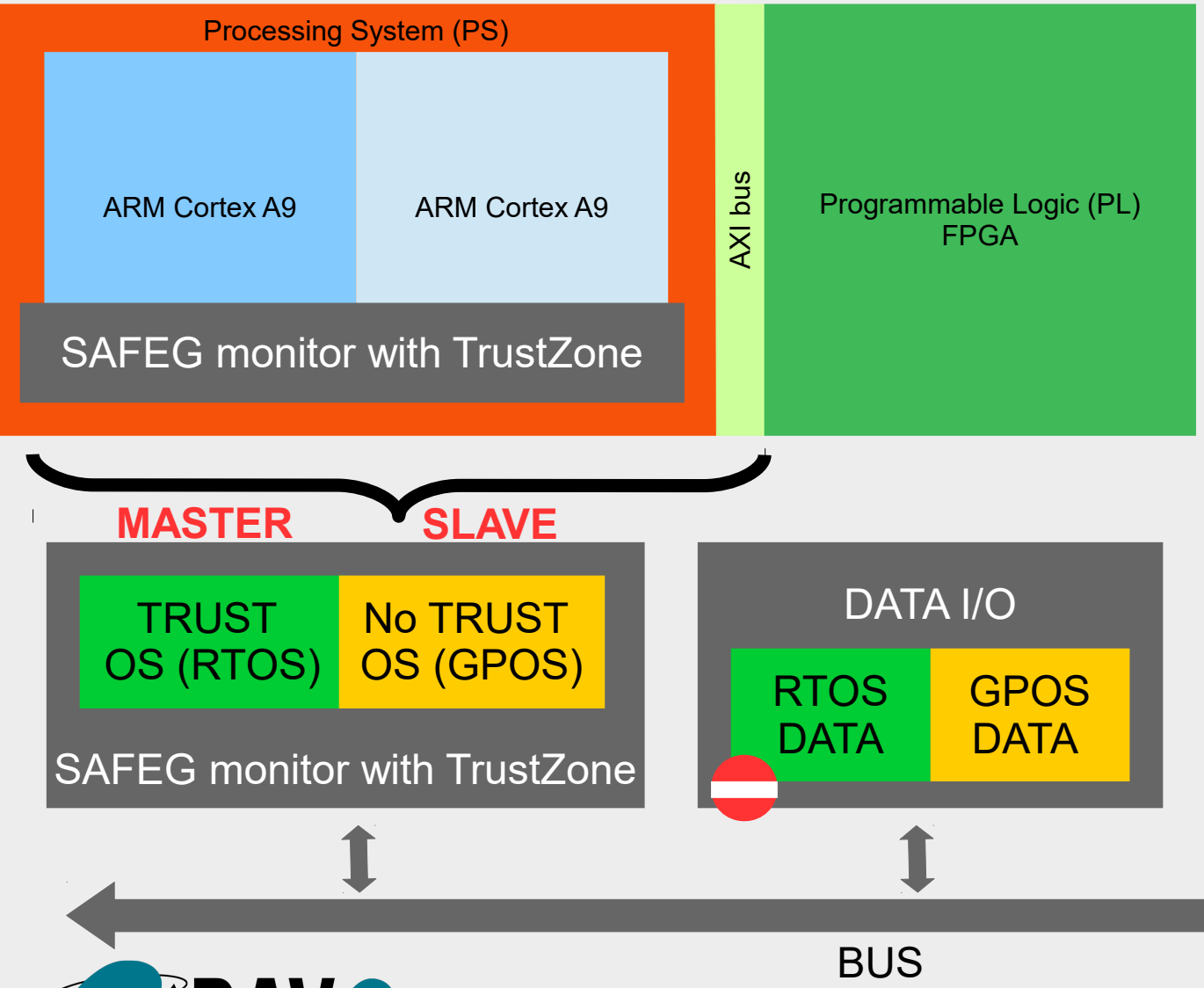


- It is required a Software Monitor
- Customized version of SAFEG
- The monitor is responsible for:
  - Enable TrustZone IP
  - Initialize Trusted /Non Trusted areas
  - Setup data struct and except handlers



DAVe Embedded Systems

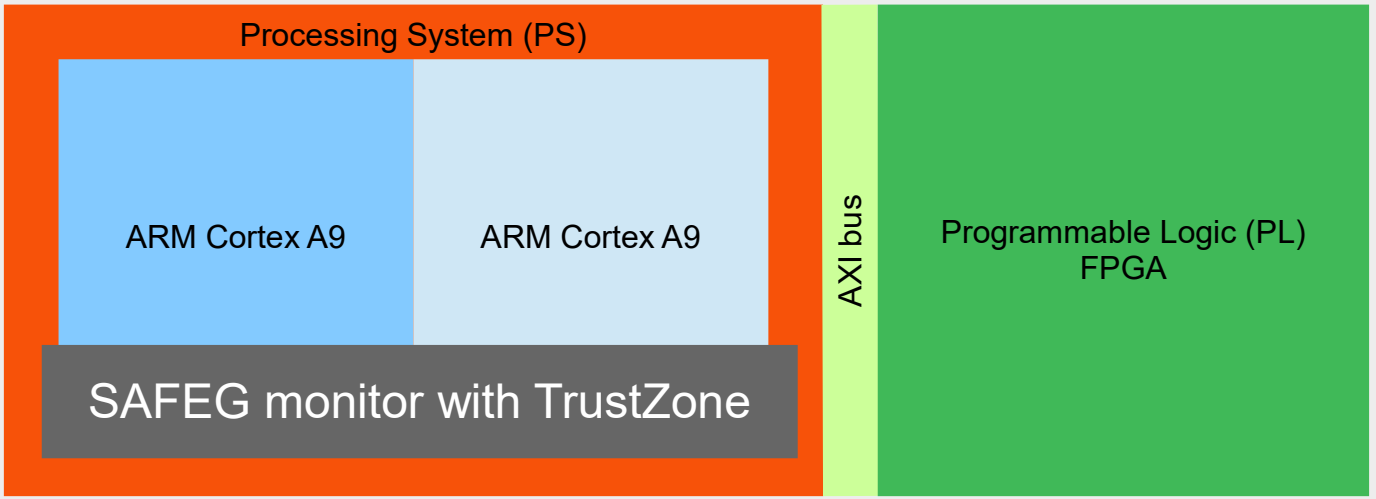
The TrustZone-based Approach



- It is required a Software Monitor
- Customized version of SAFEG
- The monitor is responsible for:
  - Enable TrustZone IP
  - Initialize Trusted /Non Trusted areas
  - Setup data struct and except handlers
  - Start Trusted OS

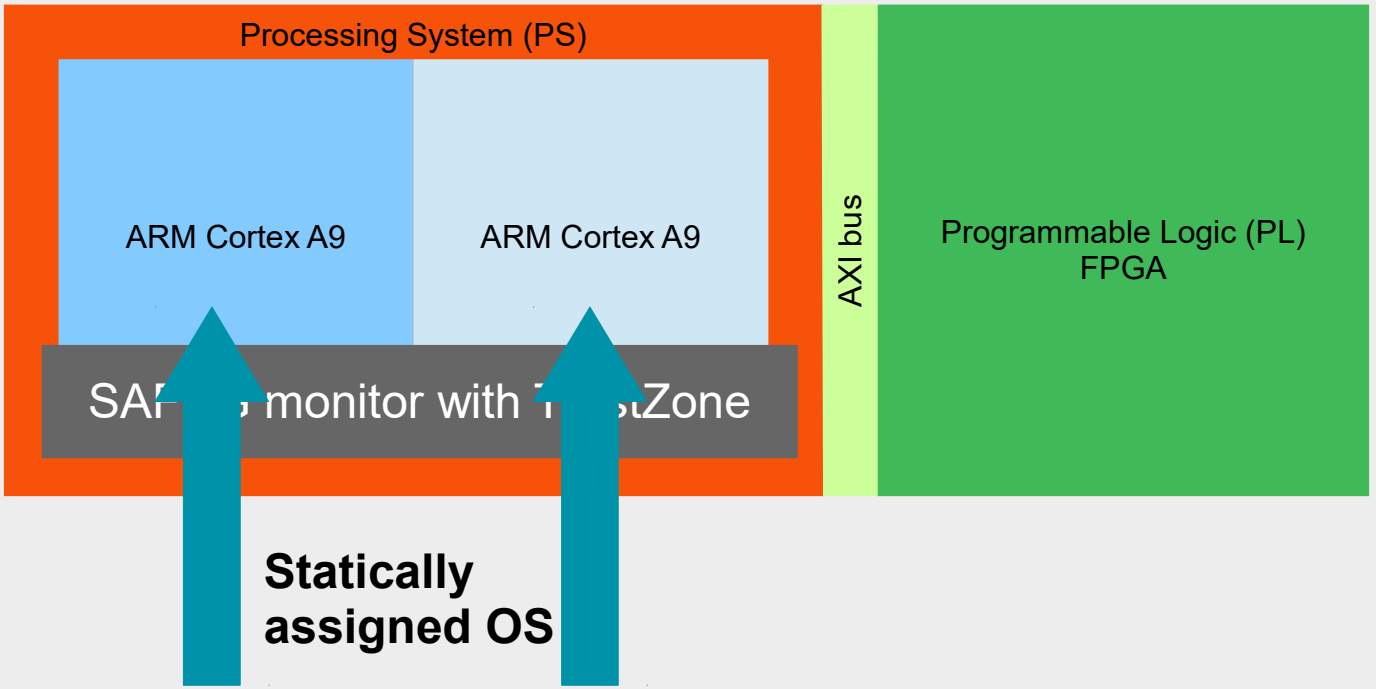
DAVE Embedded Systems

DAVE Embedded Systems' example



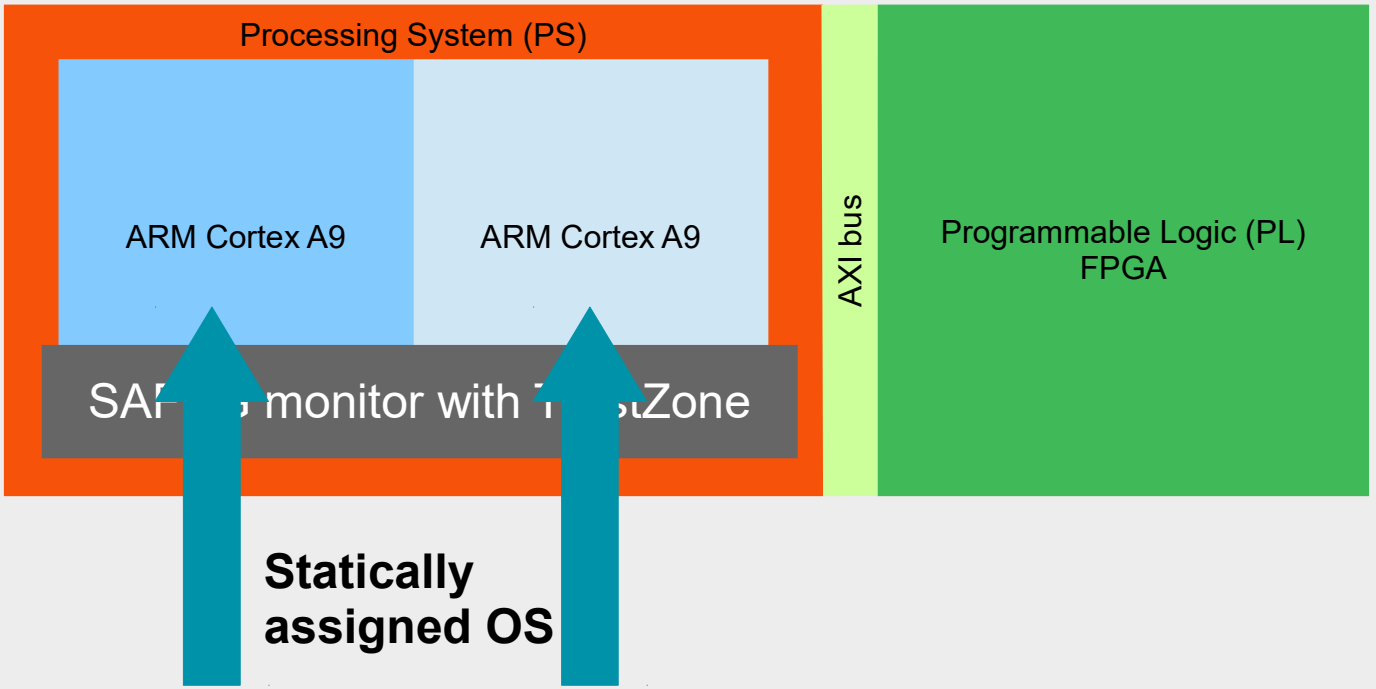
DAVE Embedded Systems

DAVE Embedded Systems' example



DAVE Embedded Systems

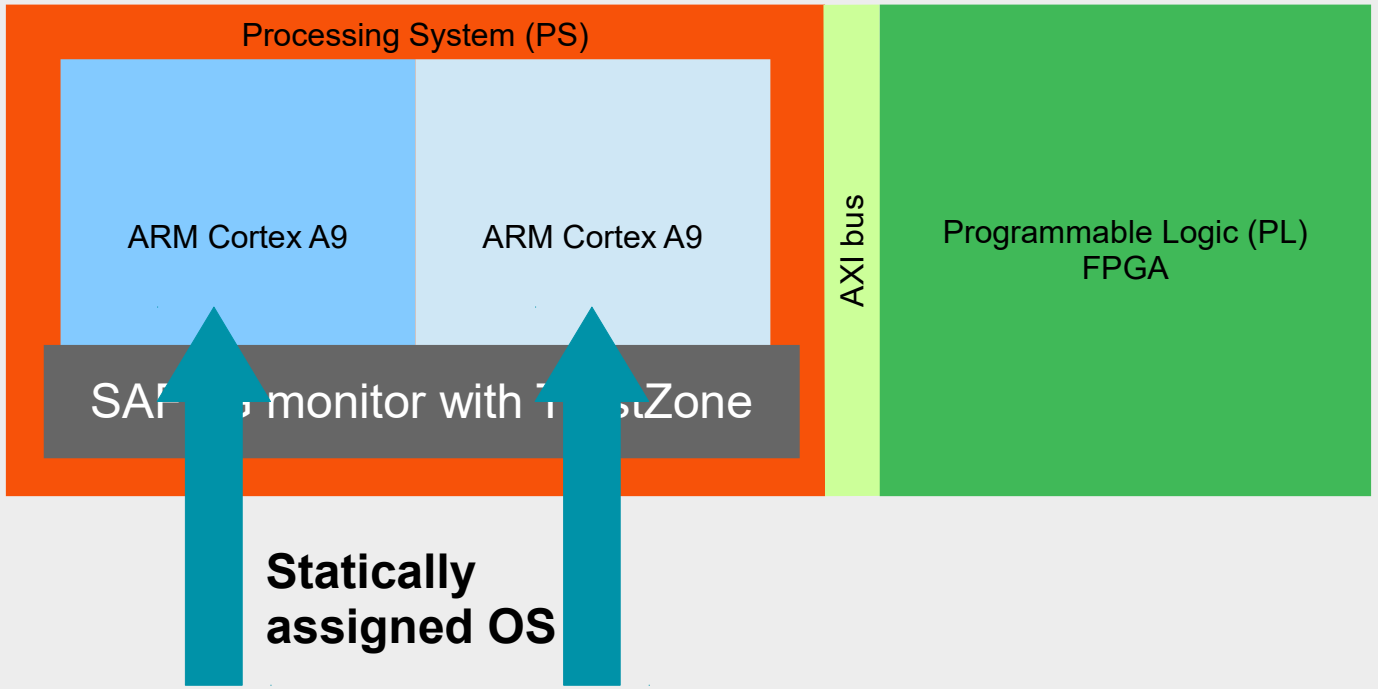
DAVE Embedded Systems' example



100% No Trusted
Linux

DAVE
Embedded Systems

DAVE Embedded Systems' example



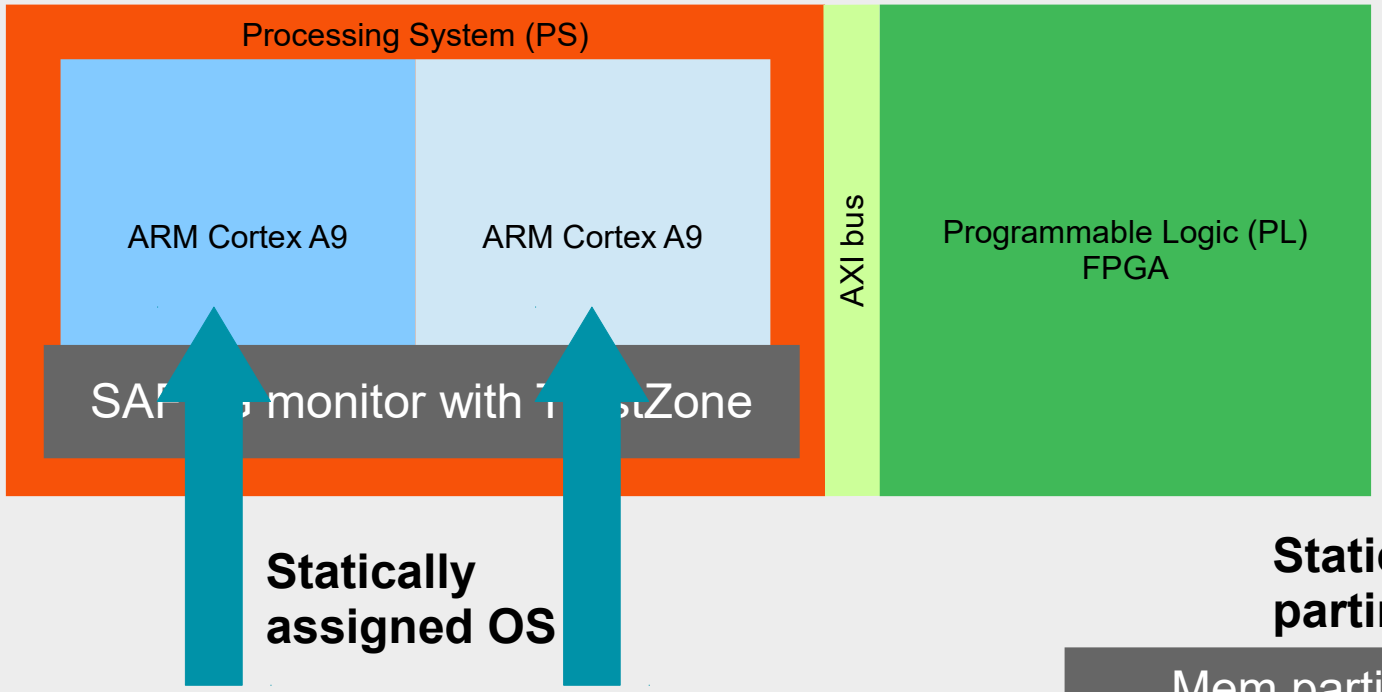
100% No Trusted
Linux

100% Trusted
FreeRTOS

No context switch
Reduced latency

DAVE
Embedded Systems

DAVE Embedded Systems' example

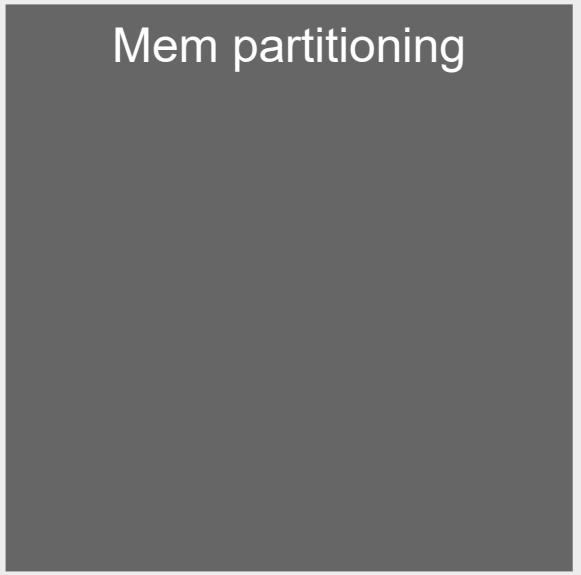


100% No Trusted
Linux

100% Trusted
FreeRTOS

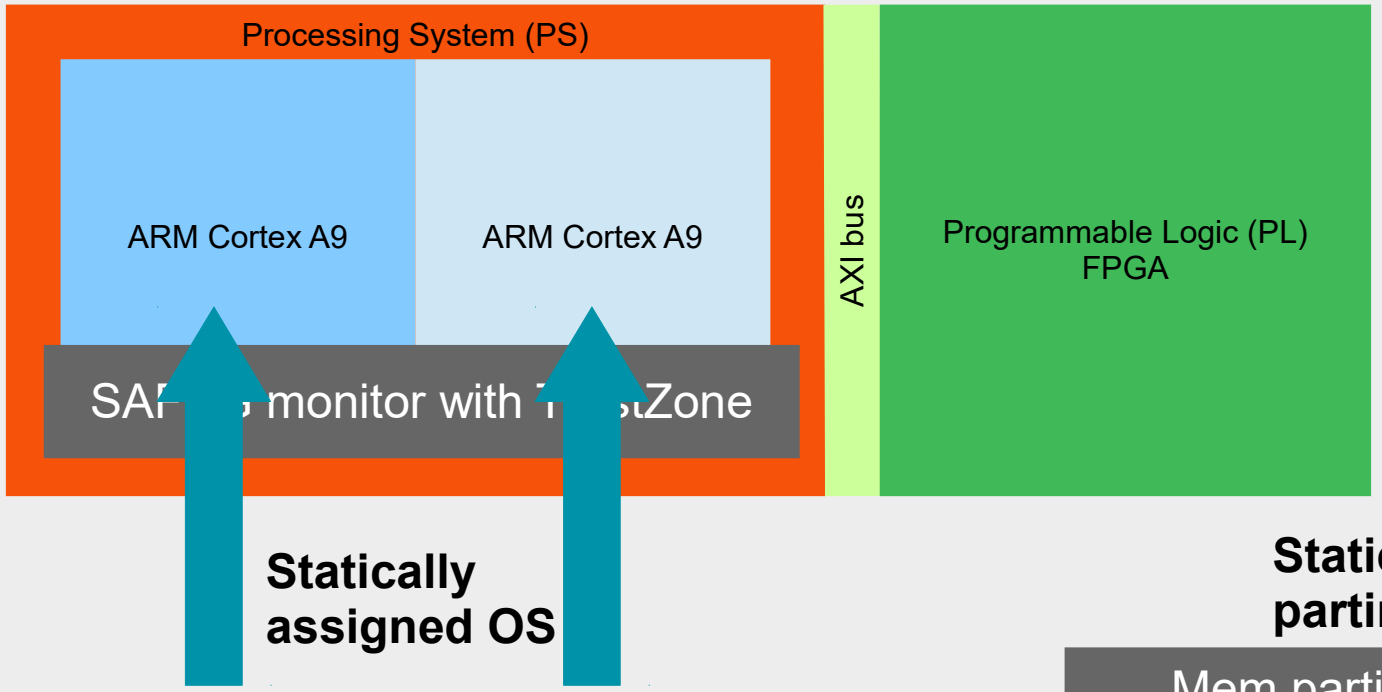
No context switch
Reduced latency

**Statically
partinioned**



DAVE
Embedded Systems

DAVE Embedded Systems' example



100% No Trusted
Linux

100% Trusted
FreeRTOS

No context switch
Reduced latency

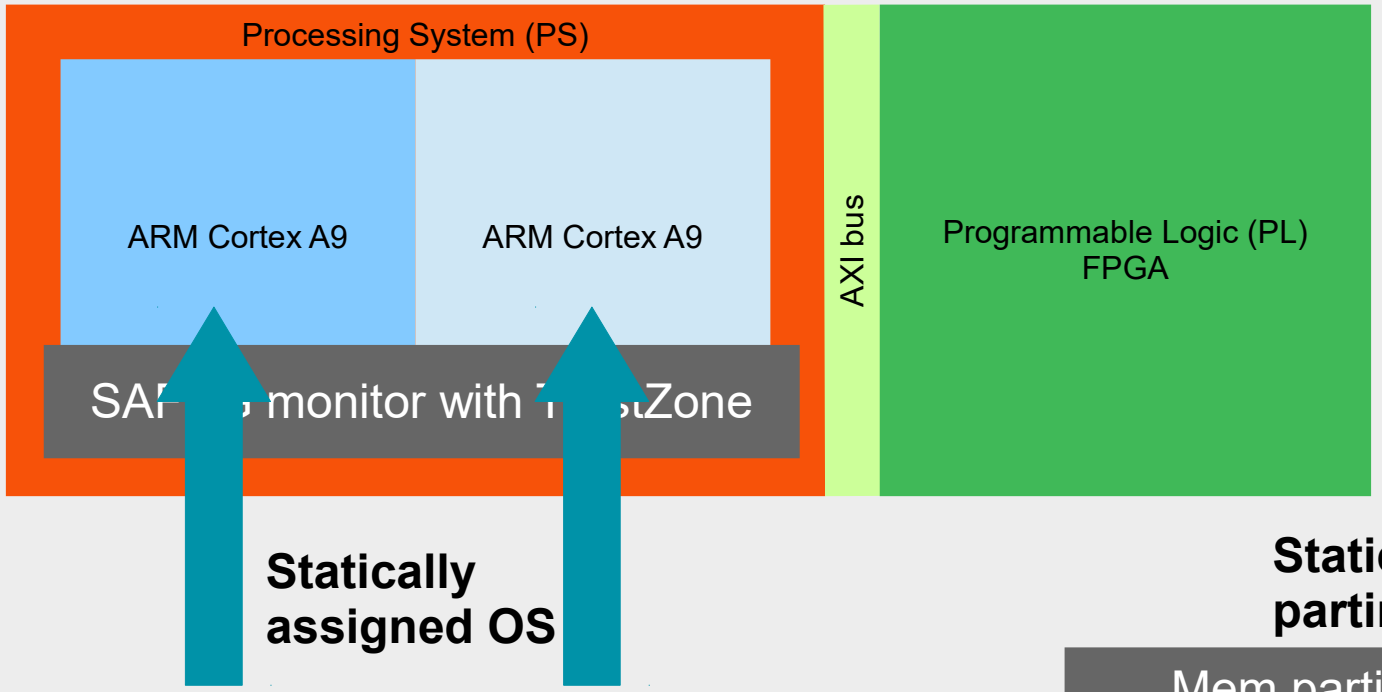
Statically partinioned

Mem partitioning

No trusted private
Area (MMU level)

DAVE
Embedded Systems

DAVE Embedded Systems' example

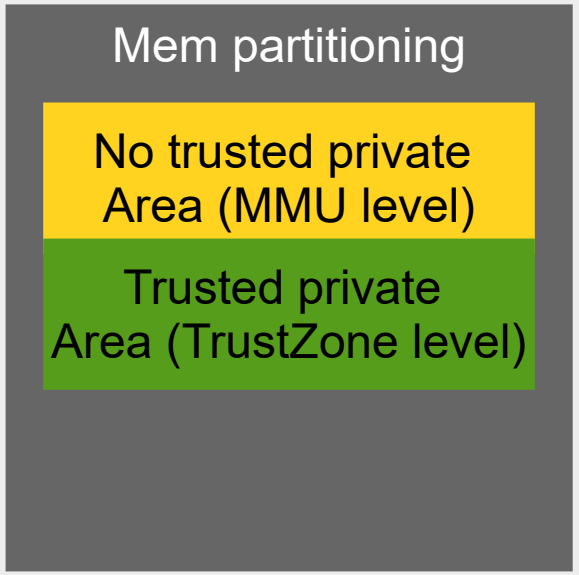


100% No Trusted
Linux

100% Trusted
FreeRTOS

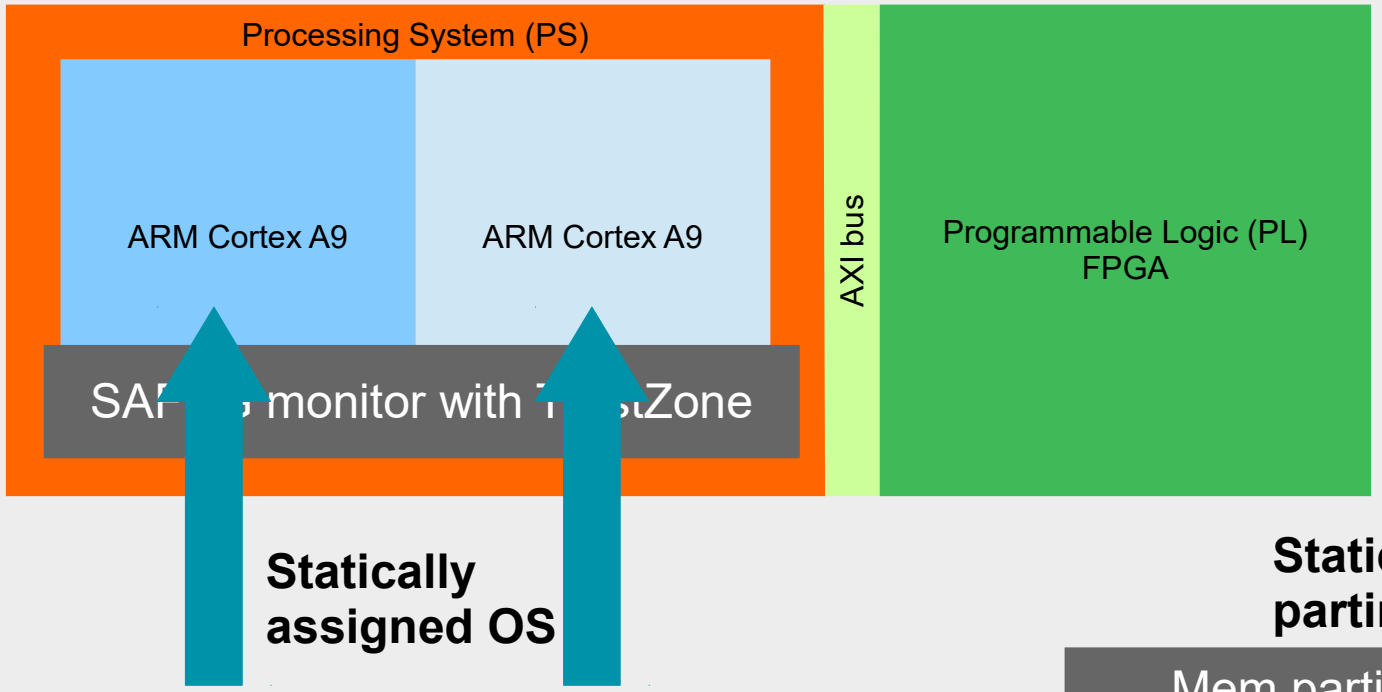
No context switch
Reduced latency

**Statically
partinioned**



DAVE
Embedded Systems

DAVE Embedded Systems' example

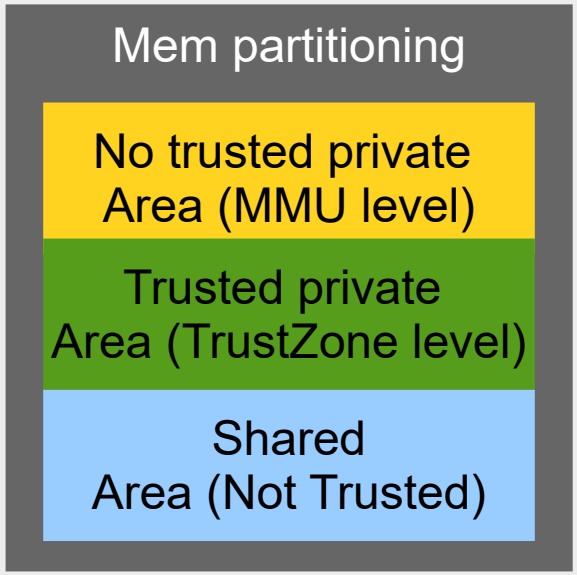


100% No Trusted
Linux

100% Trusted
FreeRTOS

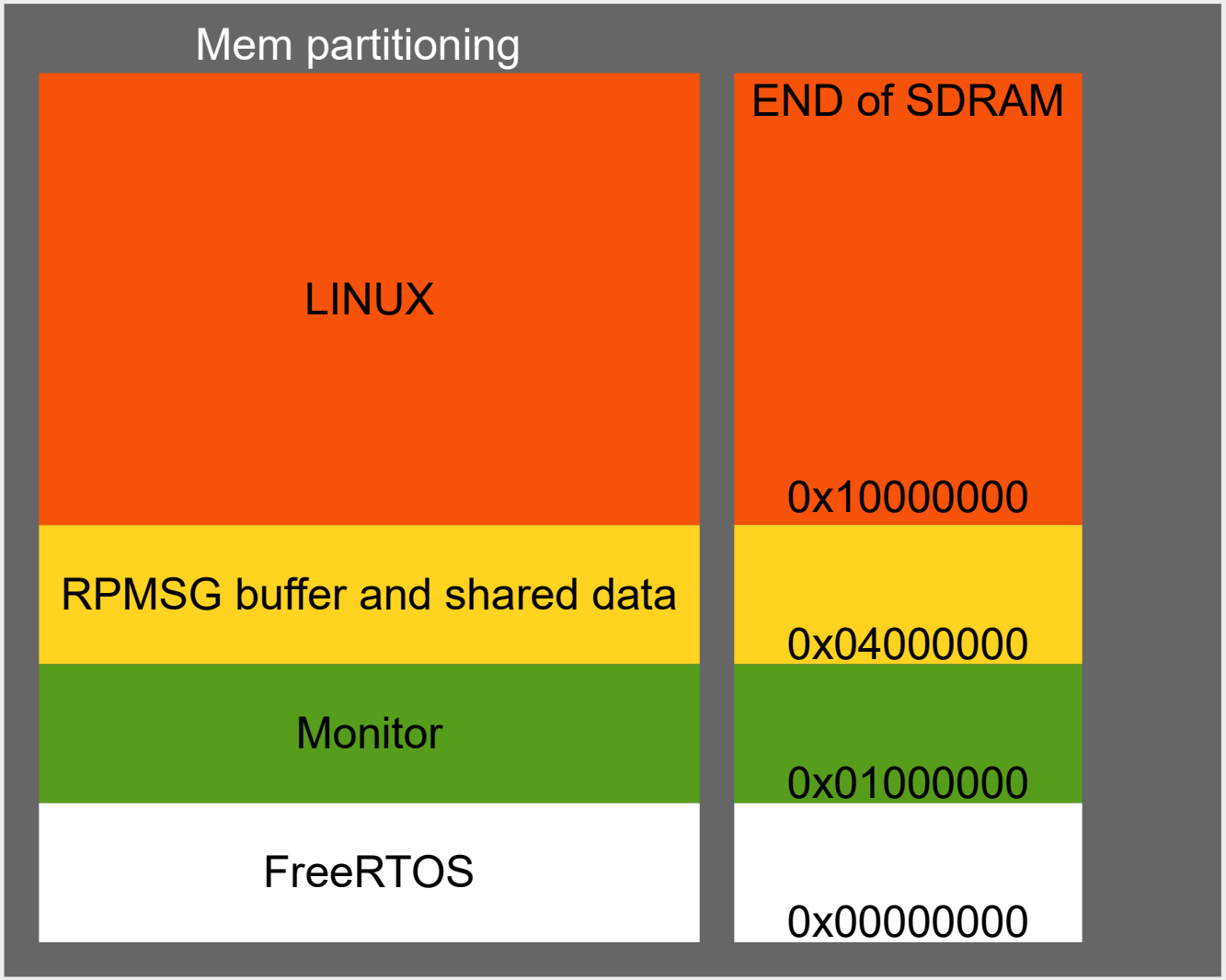
No context switch
Reduced latency

Statically partinioned



DAVE
Embedded Systems

Details: The MEM partinioning



DAVE Embedded Systems

Details: The BOOT process

0 – **RESET**

DAVE Embedded Systems

Details: The BOOT process

0 – **RESET**

1 – **BootROM**: FSBL taken from NV-memory and loaded on On Chip Memory

DAVE Embedded Systems

Details: The BOOT process

0 – **RESET**

1 – **BootROM**: FSBL taken from NV-memory and loaded on On Chip Memory

2 – **FSBL**: SDRAM init and Uboot image load in memory

DAVE Embedded Systems

Details: The BOOT process

0 – **RESET**

1 – **BootROM**: FSBL taken from NV-memory and loaded on On Chip Memory

2 – **FSBL**: SDRAM init and Uboot image load in memory

3 – **Uboot:** loads in SDRAM:

- Monitor
- Trusted code FREERTOS
- No Trusted code LINUX

DAVE Embedded Systems

Details: The BOOT process

0 – **RESET**

1 – **BootROM**: FSBL taken from NV-memory and loaded on On Chip Memory

2 – **FSBL**: SDRAM init and Uboot image load in memory

3 – **Uboot:** loads in SDRAM:

- Monitor
- Trusted code FREERTOS
- No Trusted code LINUX

4 – **Uboot**: gives control to Monitor

DAVE Embedded Systems

Details: The BOOT process

0 – **RESET**

1 – **BootROM**: FSBL taken from NV-memory and loaded on On Chip Memory

2 – **FSBL**: SDRAM init and Uboot image load in memory

3 – **Uboot:** loads in SDRAM:
- Monitor
- Trusted code FREERTOS
- No Trusted code LINUX

4 – **Uboot**: gives control to Monitor

5 – **Monitor**:
- Init TrustZone
- Enable data structures and Handlers for both cores
- Gives to Trust code the control of machine FREERTOS **MASTER**

DAVE Embedded Systems

Details: The BOOT process

0 – **RESET**

1 – **BootROM**: FSBL taken from NV-memory and loaded on On Chip Memory

2 – **FSBL**: SDRAM init and Uboot image load in memory

3 – **Uboot:** loads in SDRAM:
- Monitor
- Trusted code FREERTOS
- No Trusted code LINUX

4 – **Uboot**: gives control to Monitor

5 – **Monitor**:
- Init TrustZone
- Enable data structures and Handlers for both cores
- Gives to Trust code the control of machine FREERTOS **MASTER**

6 – **RTOS** FreeRTOS:
- Under his control decides to start No Trusted OS (LINUX) **SLAVE**

DAVE Embedded Systems

Details: Inter-World comm

Several methods available

OP - TEE

dualoscom

Based on TOPPERS
Very specific
Too SW layers

RPMsg

Based on TI DSP accepted on mainline
Used by Xilinx in AN
Very well structured on buffers and cache handlings

OpenAMP

Similar to RPMsg
Used on MPSoCs

DAVE Embedded Systems

Details: Inter-World comm

Several methods available

OP - TEE

dualoscom

RPMsg

OpenAMP

Selection Criterias

DAVE Embedded Systems

Details: The BOOT process

Several methods available

OP - TEE

dualoscom

RPMsg

OpenAMP

Selection Criterias

Acceptance into
Mainline Linux Kernel

DAVE Embedded Systems

Details: The BOOT process

Several methods available

OP - TEE

dualoscom

RPMsg

OpenAMP

Selection Criterias

Acceptance into
Mainline Linux Kernel

Control over the
isolation level between
the two worlds

DAVE Embedded Systems

Details: The BOOT process

Several methods available

OP - TEE

dualoscom

RPMsg

OpenAMP

Selection Criterias

Acceptance into Mainline Linux Kernel

Maintenance – future developments

Control over the isolation level between the two worlds

DAVE Embedded Systems

Details: The BOOT process

Several methods available

OP - TEE

dualoscom

RPMsg

OpenAMP

Selection Criterias

Acceptance into Mainline Linux Kernel

↓

Maintenance – future developments

Control over the isolation level between the two worlds

↓

The level of isolation is application dependent

DAVE Embedded Systems

Details: The BOOT process

Several methods available

OP - TEE

dualoscom

RPMsg

OpenAMP

Selection Criterias

Acceptance into Mainline Linux Kernel

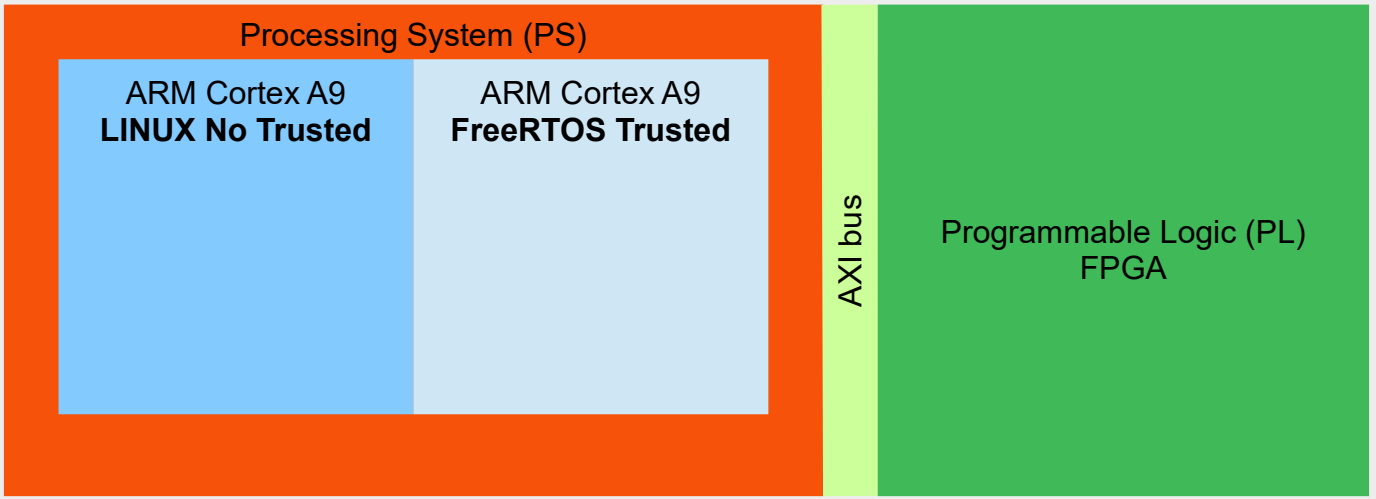
Maintenance – future developments

Control over the isolation level between the two worlds

The level of isolation is application dependent

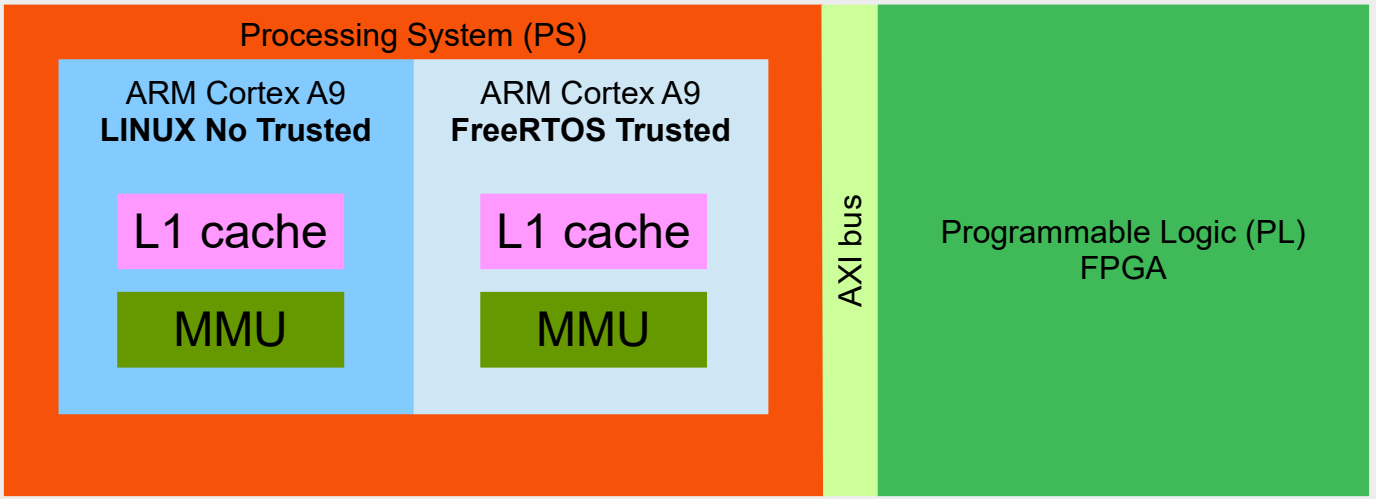
DAVE Embedded Systems

Details: L2 cache management

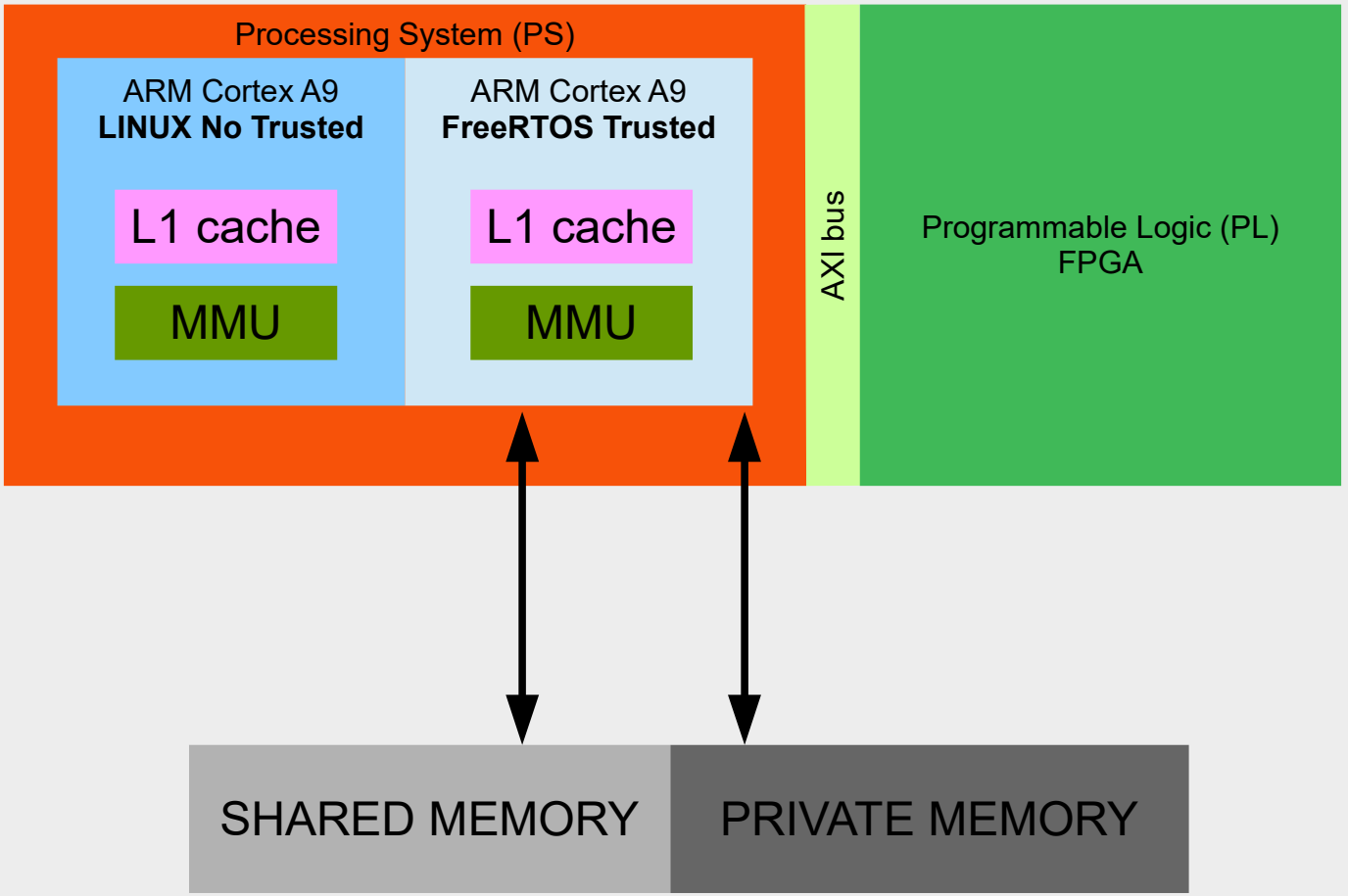


DAVE Embedded Systems

Details: L2 cache management

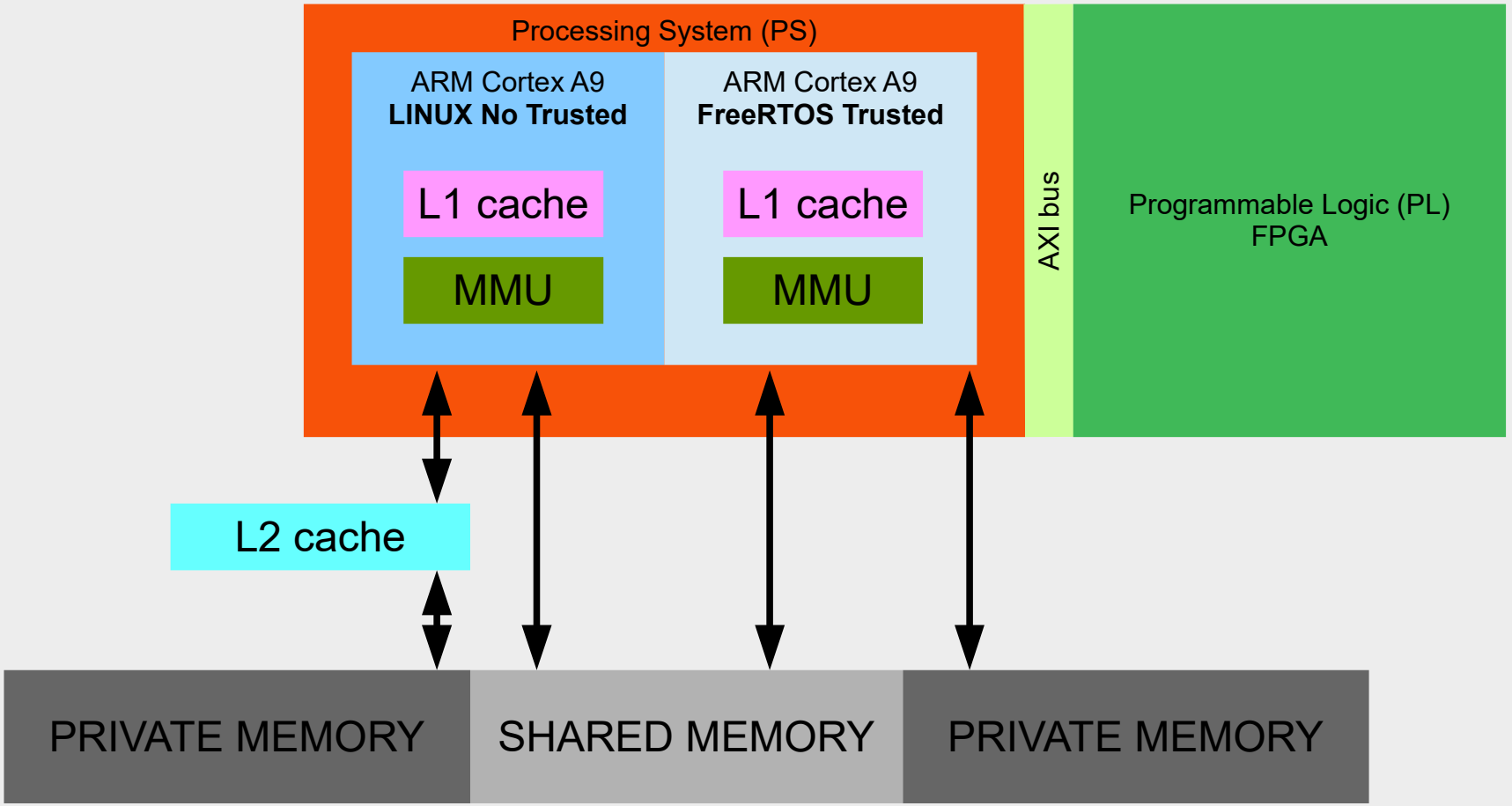


Details: L2 cache management



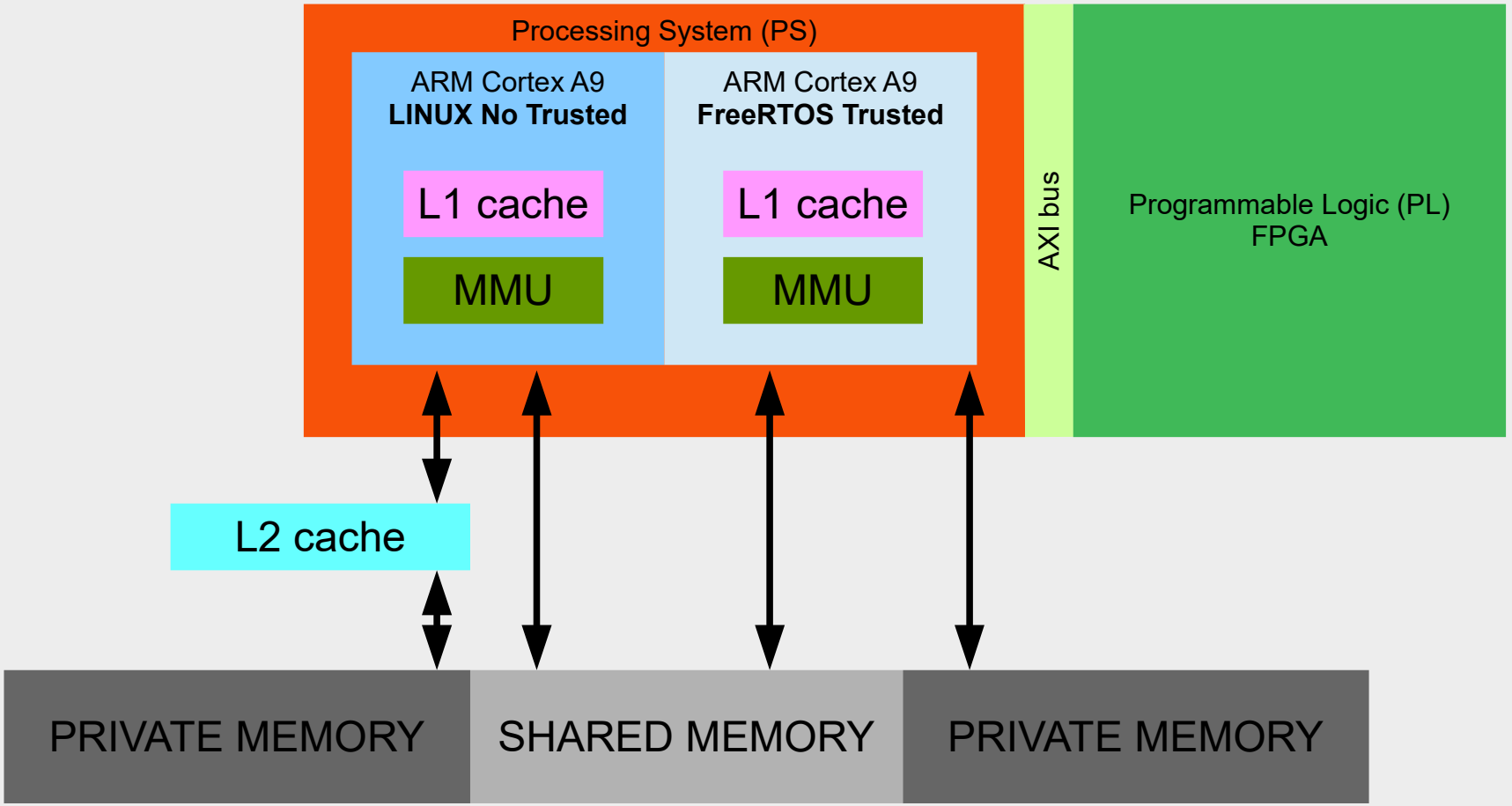
DAVE Embedded Systems

Details: L2 cache management



DAVE Embedded Systems

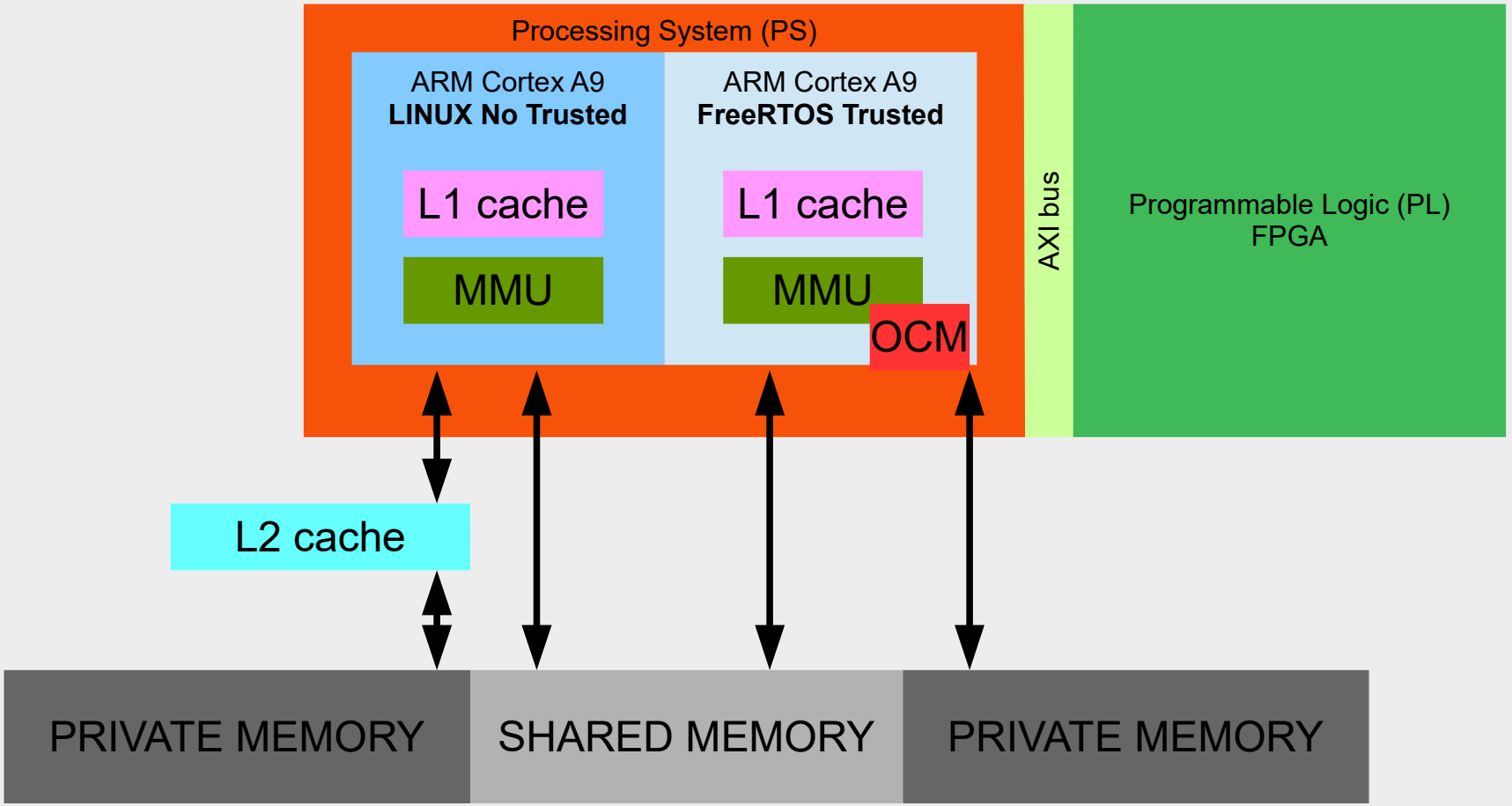
Details: L2 cache management



- Linux performances are not affected by dual OS solutions
- FreeRTOS determinism is granted
- Shared mem is not cached

DAVE Embedded Systems

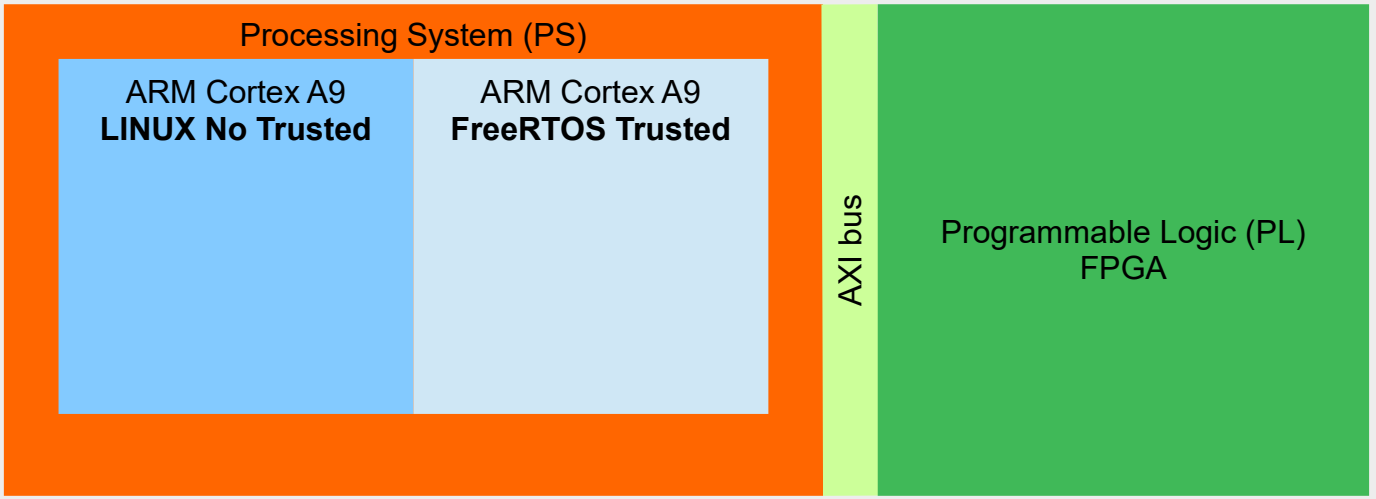
Details: L2 cache management



- Linux performances are not affected by dual OS solutions
- FreeRTOS determinism is granted
- Shared mem is not cached
- Internal OCM can be granted only to Trust OS

DAVe Embedded Systems

Details: Performances achieved

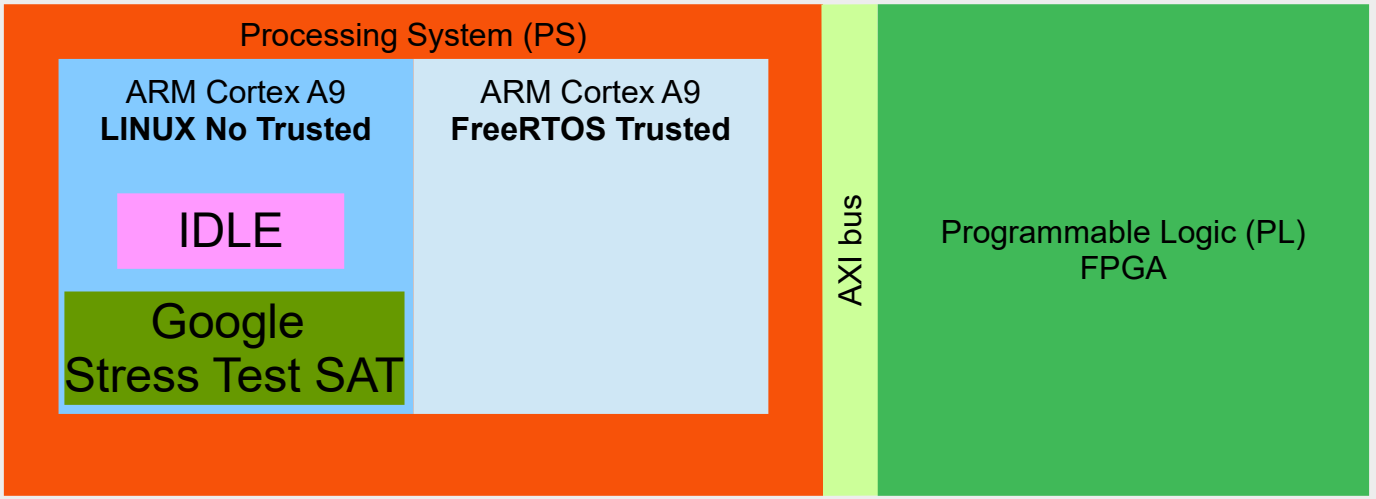


TEST BENCH: used the internal timer to measure the latency between:

- INT handling
- INT service

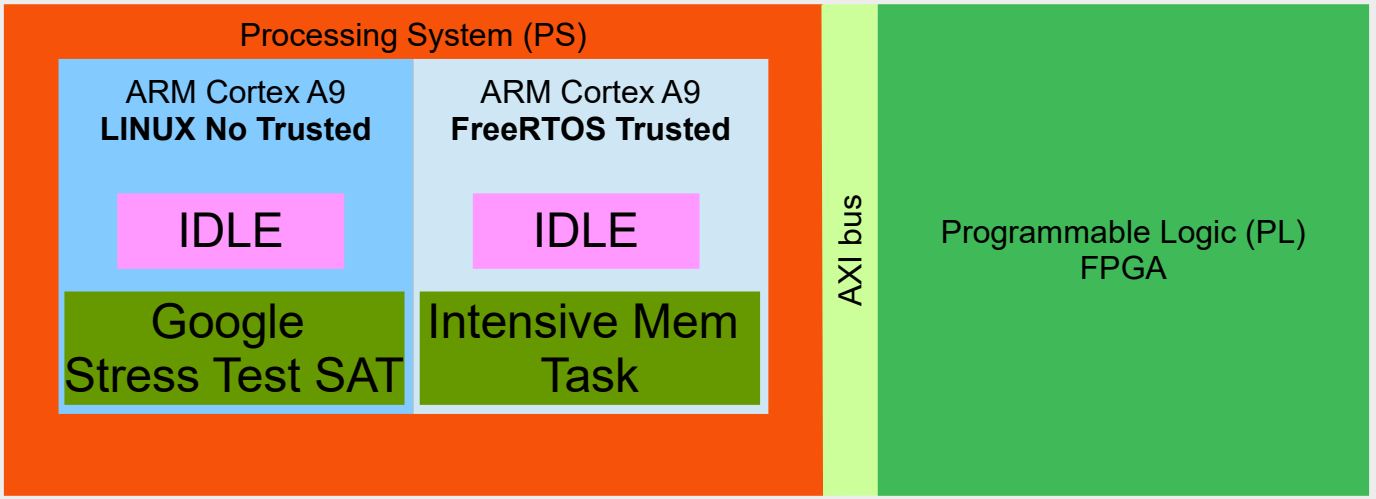
DAVE Embedded Systems

Details: Performances achieved



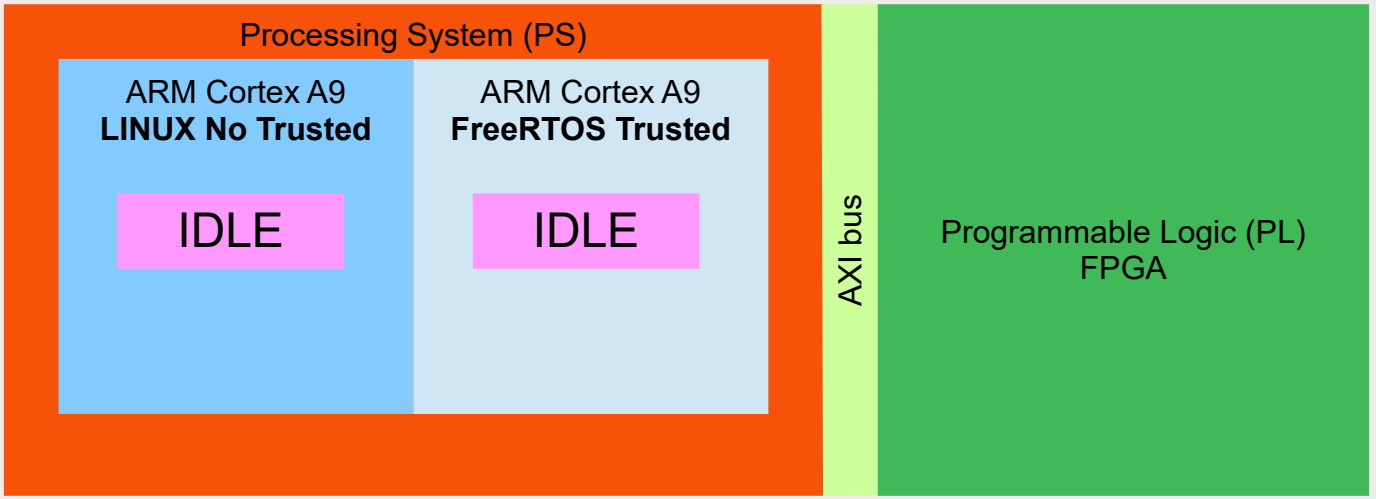
DAVE
Embedded Systems

Details: Performances achieved



DAVE Embedded Systems

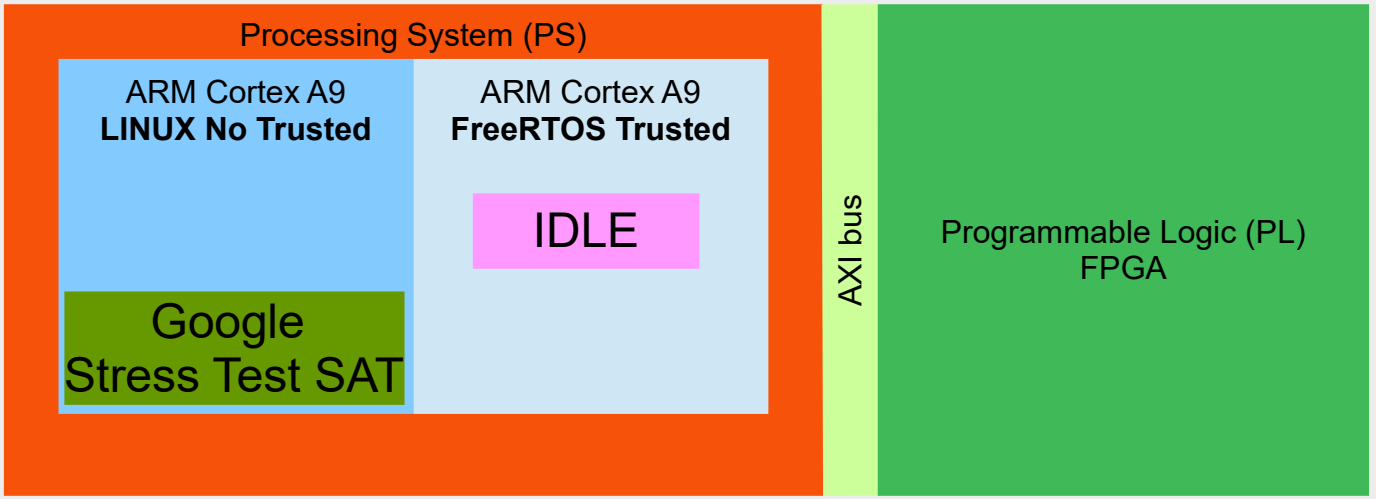
Details: Performances achieved



Latency	Linux IDLE RTOS IDLE	
min	287ns	
avg	287ns	
max	548ns	

DAVE Embedded Systems

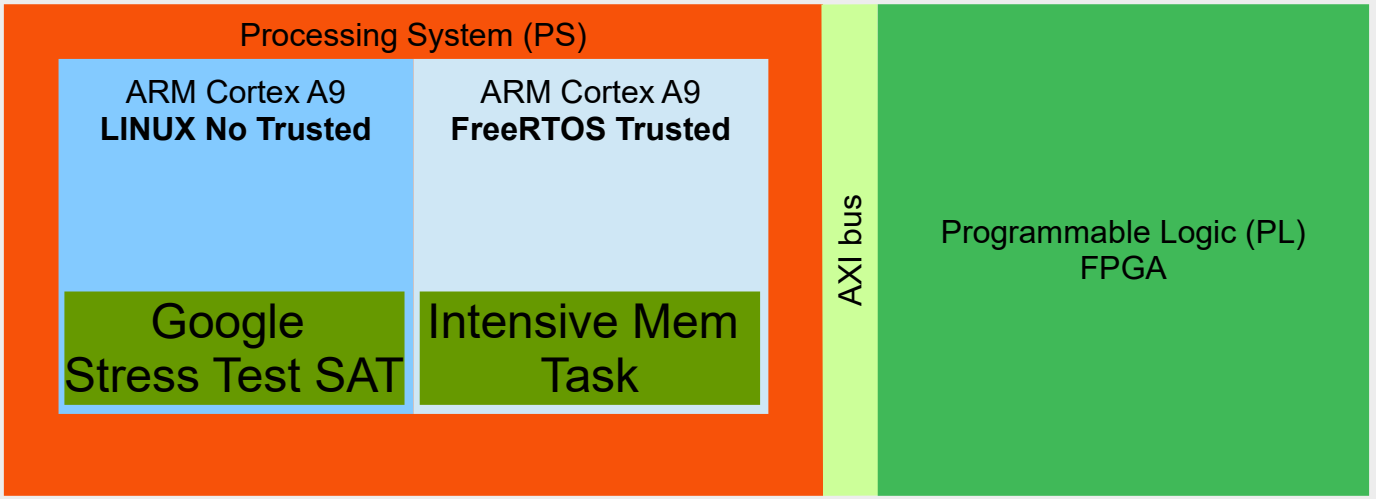
Details: Performances achieved



Latency	Linux IDLE RTOS IDLE	LINUX SAT RTOS IDLE
min	287ns	287ns
avg	287ns	296ns
max	548ns	539ns

DAVE Embedded Systems

Details: Performances achieved

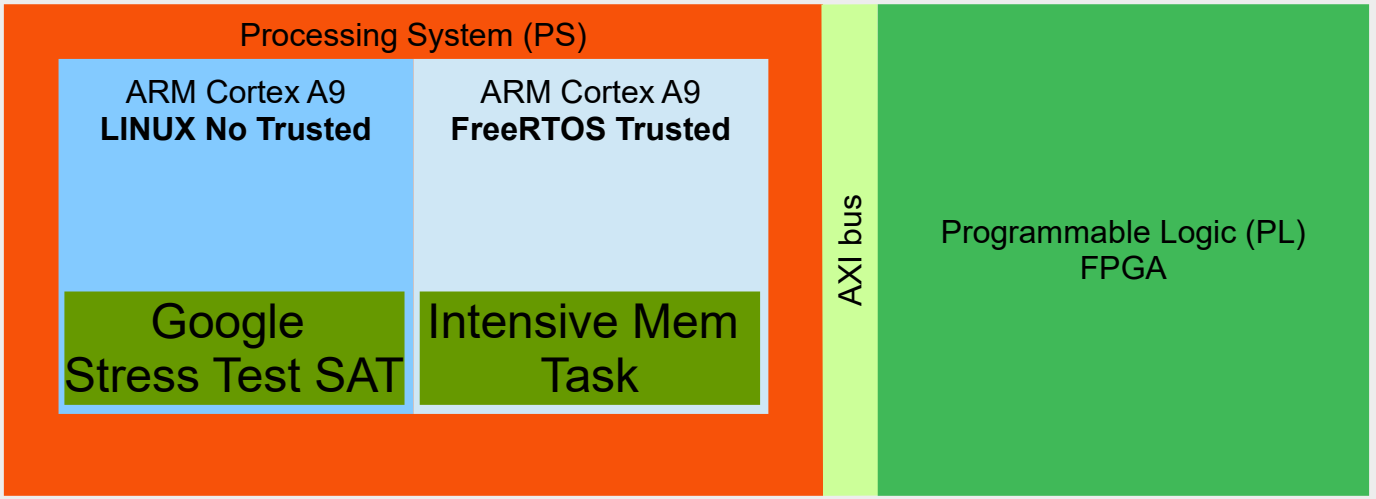


Latency	Linux IDLE RTOS IDLE	LINUX SAT RTOS IDLE	LINUX SAT RTOS 16k task load
min	287ns	287ns	287ns
avg	287ns	296ns	205ns
max	548ns	539ns	575ns

- Linux performances not affect RTOS in any condition
- FreeRTOS latency is granted with not heavy load tasks

DAVE Embedded Systems

Details: Performances achieved

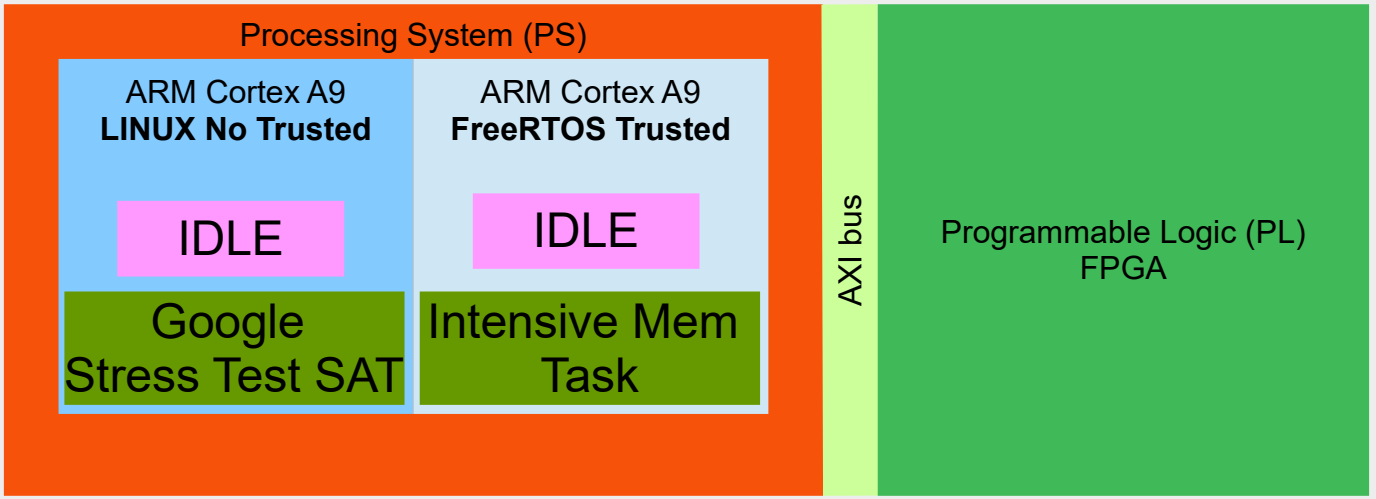


Latency	Linux IDLE RTOS IDLE	LINUX SAT RTOS IDLE	LINUX SAT RTOS 16k task load	LINUX SAT RTOS 128k task load
min	287ns	287ns	287ns	1268ns
avg	287ns	296ns	205ns	2024ns
max	548ns	539ns	575ns	3050ns

- Linux performances not affect RTOS in any condition
- FreeRTOS latency is granted with not heavy load tasks
- FreeRTos is affected by high mem loads due to it is not cached

DAVE Embedded Systems

Details: Performances achieved



Latency	Linux IDLE RTOS IDLE	LINUX SAT RTOS IDLE	LINUX SAT RTOS 16k task load	LINUX SAT RTOS 128k task load
min	287ns	287ns	287ns	1268ns
avg	287ns	296ns	205ns	2024ns
max	548ns	539ns	575ns	3050ns

- Linux performances not affect RTOS in any condition
- FreeRTOS latency is granted with not heavy load tasks
- FreeRTos is affected by high mem loads due to it is not cached

  The L2 cache can be also used only on Trust OS – there are pro and cons (typically a determinism reduction is noted)

DAVe Embedded Systems

Future works and references

DAVE
Embedded Systems

Future works and references

- Complete Reboot of Slave core from Master Core

DAVE Embedded Systems

Future works and references

- Complete Reboot of Slave core from Master Core
- Deep understanding and optimization of INTerrupt handling and communication data interchange between two worlds related to determinism and latency aspects

DAVe
Embedded Systems

Future works and references

- Complete Reboot of Slave core from Master Core
- Deep understanding and optimization of INTerrupt handling and communication data interchange between two worlds related to determinism and latency aspects

- Refers to:

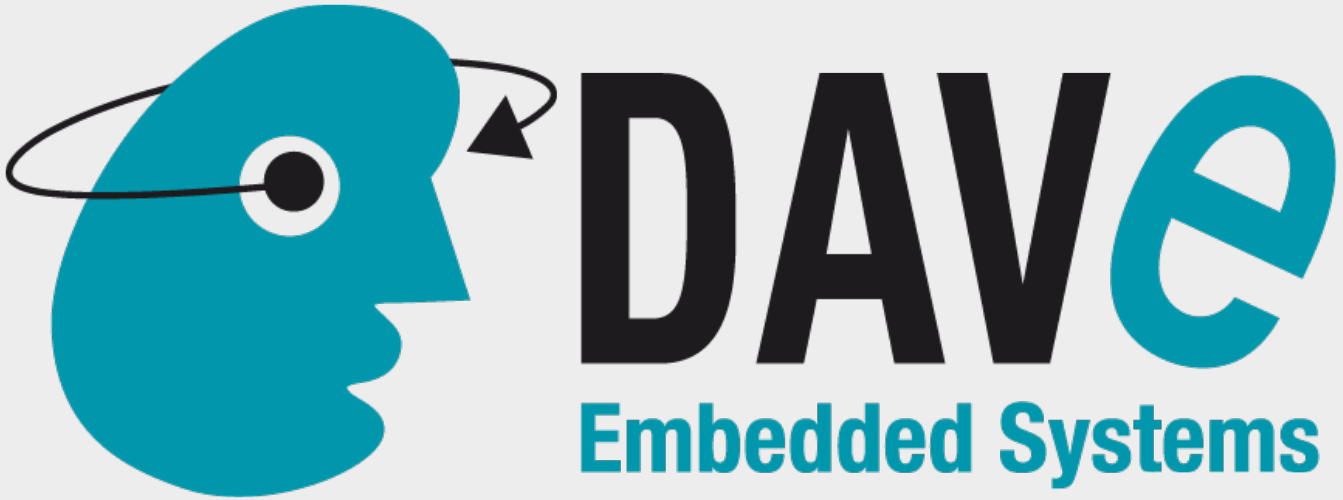
http://www.dave.eu/sites/default/files/BRX-WP001.pdf
Yashu Gosain and Prushothaman Palanichamy, Xilinx WP429 - TrustZone Technology Support in Zynq-7000 All Programmable SoCs (v1.0), May 20, 2014
DAVE Embedded Systems, AN-BELK-001: Asymmetric Multiprocessing (AMP) on Bora – Linux FreeRTOS, -
TOPPERS SafeG home page (English), -,
https://www.toppers.jp/en/safeg.html

and many others

DAVE Embedded Systems

Question and answers

DAVE Embedded Systems



DAVE S.r.l.

Via Talponedo, 29/A
I-33080, Porcia (PN) Italy

Tel +39 0434 921215
Fax +39 0434 1994030

www.dave.eu
info@dave.eu
wiki.dave.eu