



Arm Solutions at Lightspeed

Protected Video Playback on NXP i.MX8MQ

Rouven Czerwinski

About me



Rouven Czerwinski

✉ rouven.czerwinski@linaro.org

 Emantor

- Embedded Linux Engineer for 10 years
- Worked on OP-TEE, Linux, Openembedded, Barebox, TF-A, gstreamer, ...
- Recently working on the intersection of security & multimedia

Linaro

- ARM focused services company
 - Training
 - Consulting
 - LTS Support
 - BSP
 - Upstreaming
 - Test Automation
- Forge
 - HPC Debugging & Profiling

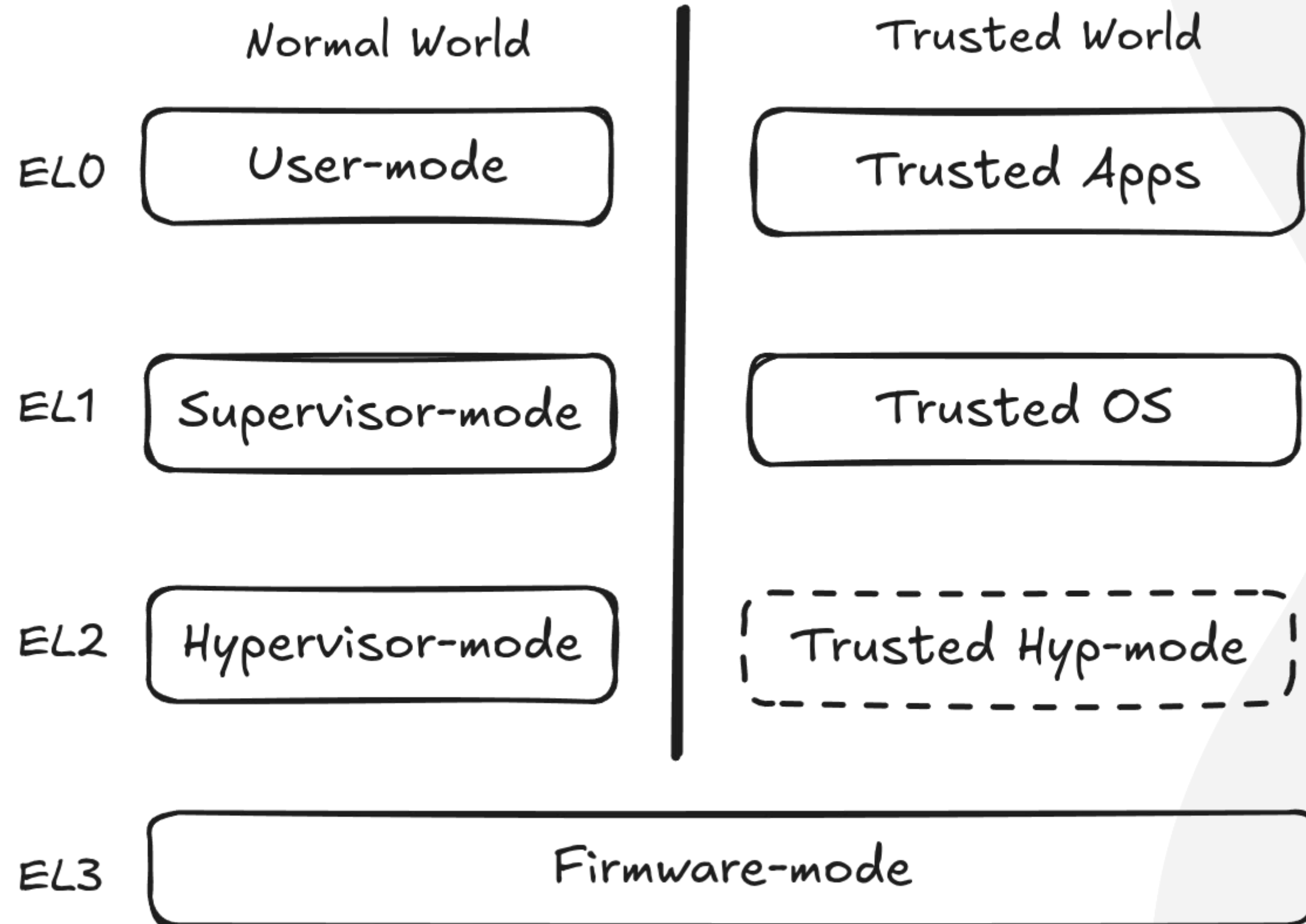
Contents

- TrustZone & i.MX8MQ crash course
- Current Stack
- Upstreamable Stack

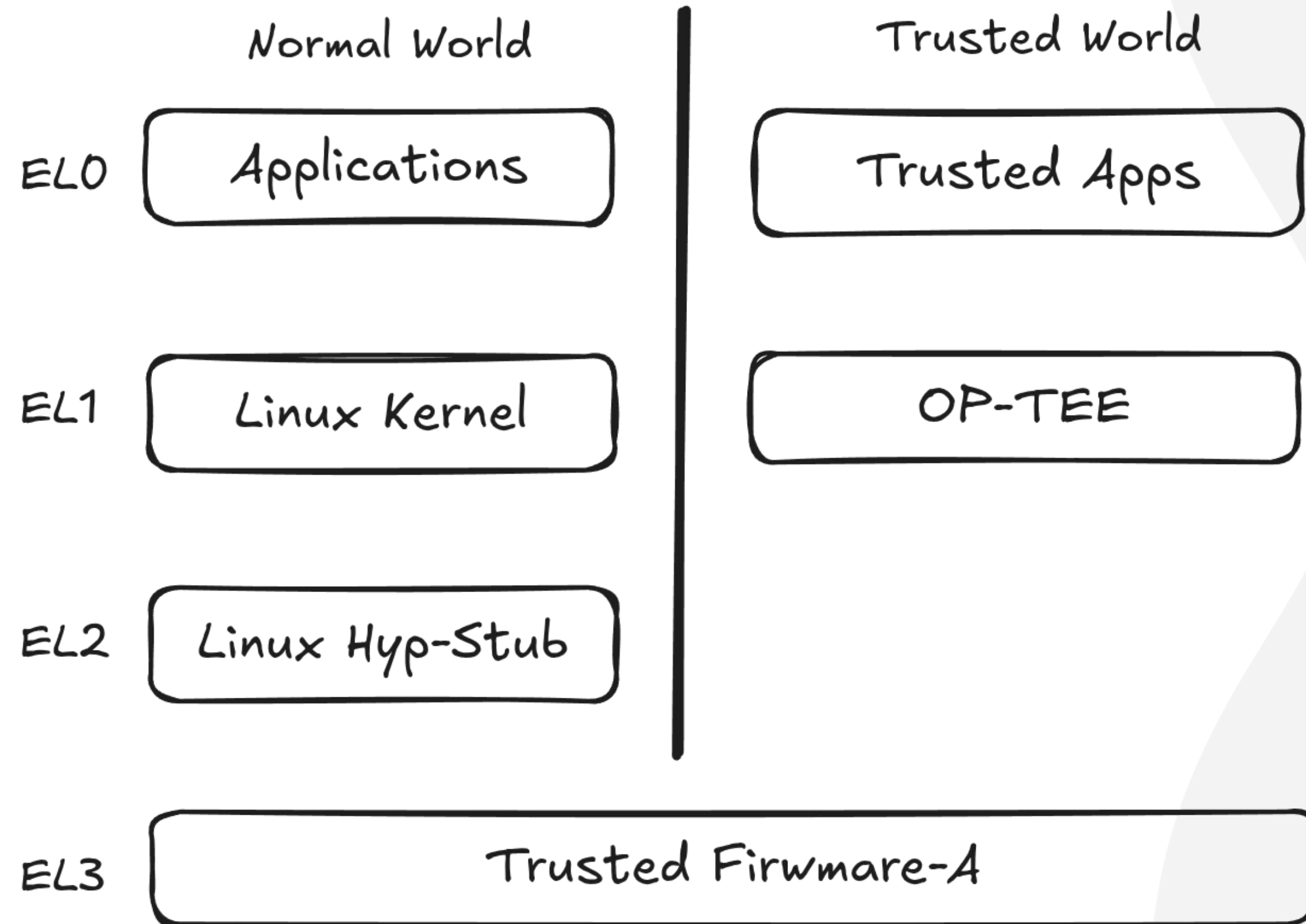
TrustZone & NXP i.MX8MQ



TrustZone

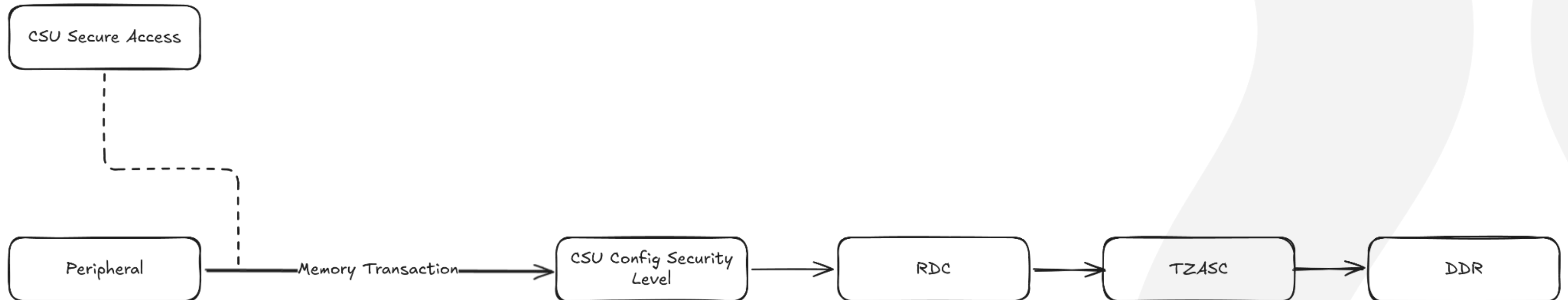


TrustZone with components



NXP i.MX8MQ components

- RDC: Resource Domain Controller, controls memory and MMIO access
- TZASC: TrustZone Address Space Controller, allows only secure access to certain memory areas
- DDR: Double Data Rate memory, main memory
- CSU: Central Security Unit, manages security for non-trustzone aware masters



NXP Policy definitions

- Policy 1: Only protected content is decrypted to the secured memory location
 - GPU access to unprotected content is possible (composition)
 - Protected content needs to be directly accessed by IP display core (DCSS)
- Policy 2: All content is decrypted to secured memory
 - No GPU composition
 - All video content needs to go through display IP (DCSS)

Current stack

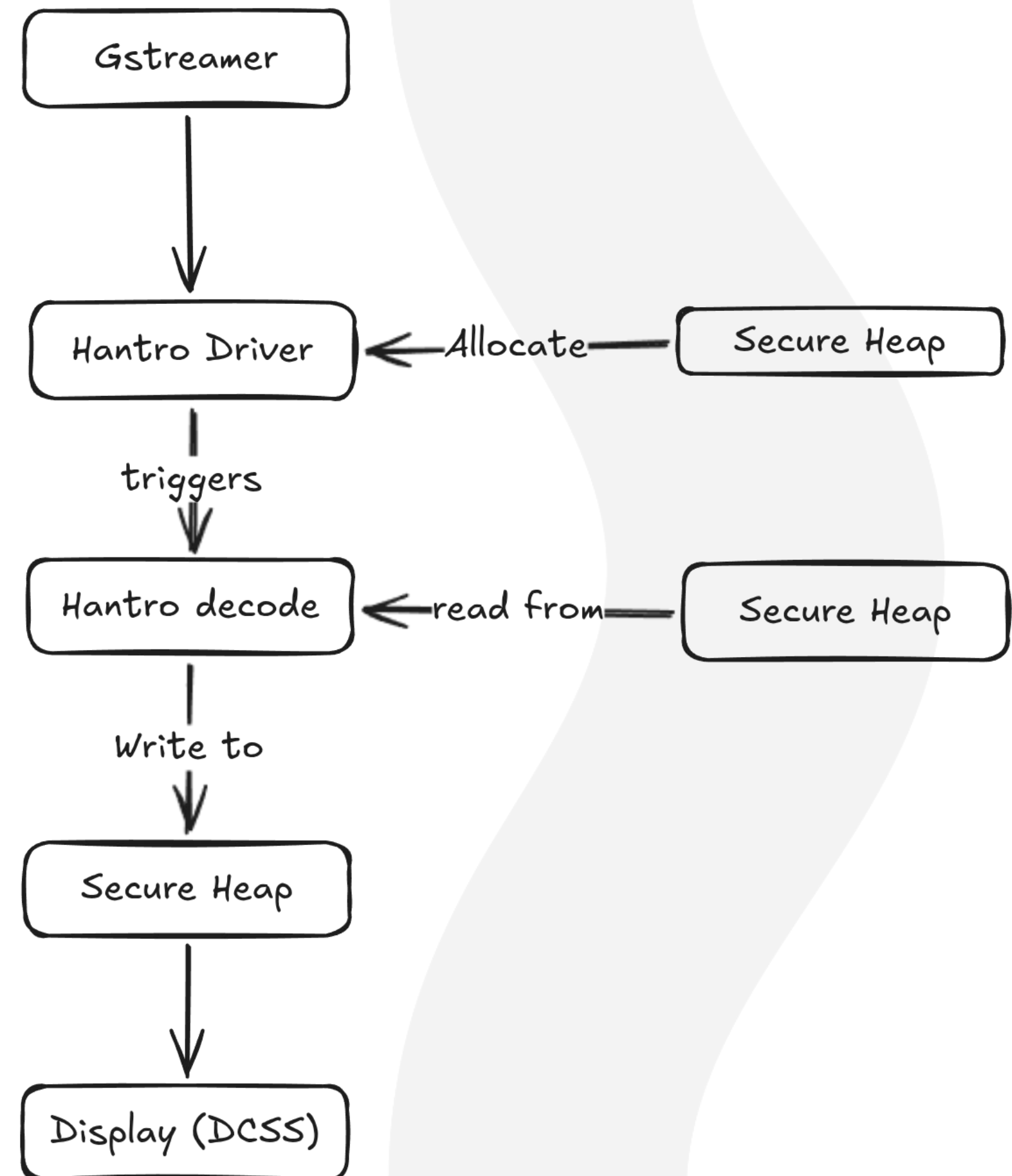


Current stack

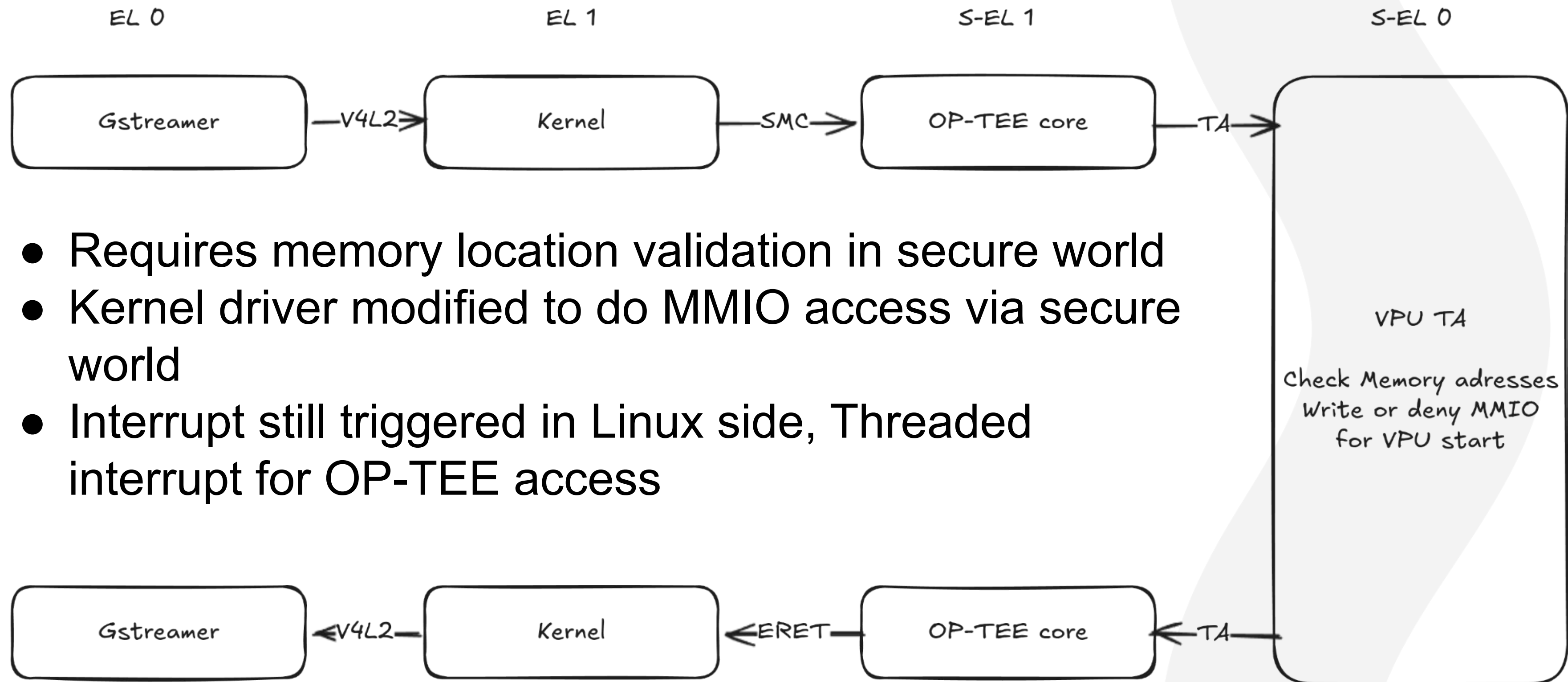
- Downstream heap implementation in the kernel (2 heaps)
- Heaps are Linux Kernel managed
- V4L2 patches for kernel DMA buf heap allocation applied
- V4L2 patches for secure video queues applied (policy 1)
- HACK patches to allocate secure DMA heap buffers via MMIO
- Patches to allocate required buffers for stateless codec
- Both Policy 1 & 2 patches available
- Proprietary gstreamer element to interface with Widevine CE CDM
- gstreamer element hooks up before v4l2h265decoder
- Decoding happens directly after HTTP download

Policy 2 Flow

- Hantro R/W location enforced by SoC RDC
- No secure world interaction needed on V4L2
- Heaps managed by Linux, No OP-TEE involvement
- Secure Heap location fixed in memory (platform constrain)



Policy 1 flow



- Requires memory location validation in secure world
- Kernel driver modified to do MMIO access via secure world
- Interrupt still triggered in Linux side, Threaded interrupt for OP-TEE access

Upstreamable stack



Upstreamable Stack

- Upstream OP-TEE protected video heap ✓
- Rework gstreamer module based on [gstreamer!5640](#) or come up with better design
- Patches for kernel internal DMA heap allocations
 - Fix lifetime considerations from [Boris Brezillon](#)
 - required for stateless Hantro intermediate buffers
- Patches for Secure Memory queues
- Patches for Hantro to allocate from DMA heap

Open questions

- Where does heap allocation happen?
 - Kernel? Needs internal allocation patches.
 - Userspace via DMA Heap? May need Device information?
- Decoder needs CMA, does OP-TEE protected heap provide CMA?
 - Upstream does not want flags
 - Additional heap with CMA constrain? (protected_video_cma?)
- Second heap requirement for bitstream?
 - More of a security question for implementor requirements
- Protected Heap memory status validation?
 - Not relevant for this SoC, but for other platforms that can change privileges dynamically
- Interrupt handling for Hantro: Keep in Linux? Move to OP-TEE?
- Probe from OP-TEE instead of device tree?



linaro.org

Thank you

rouven.czerwinski@linaro.org



Arm Solutions at Lightspeed

Title Slide DARK

Content slide 1 column DARK

Content slide 2 column LIGHT

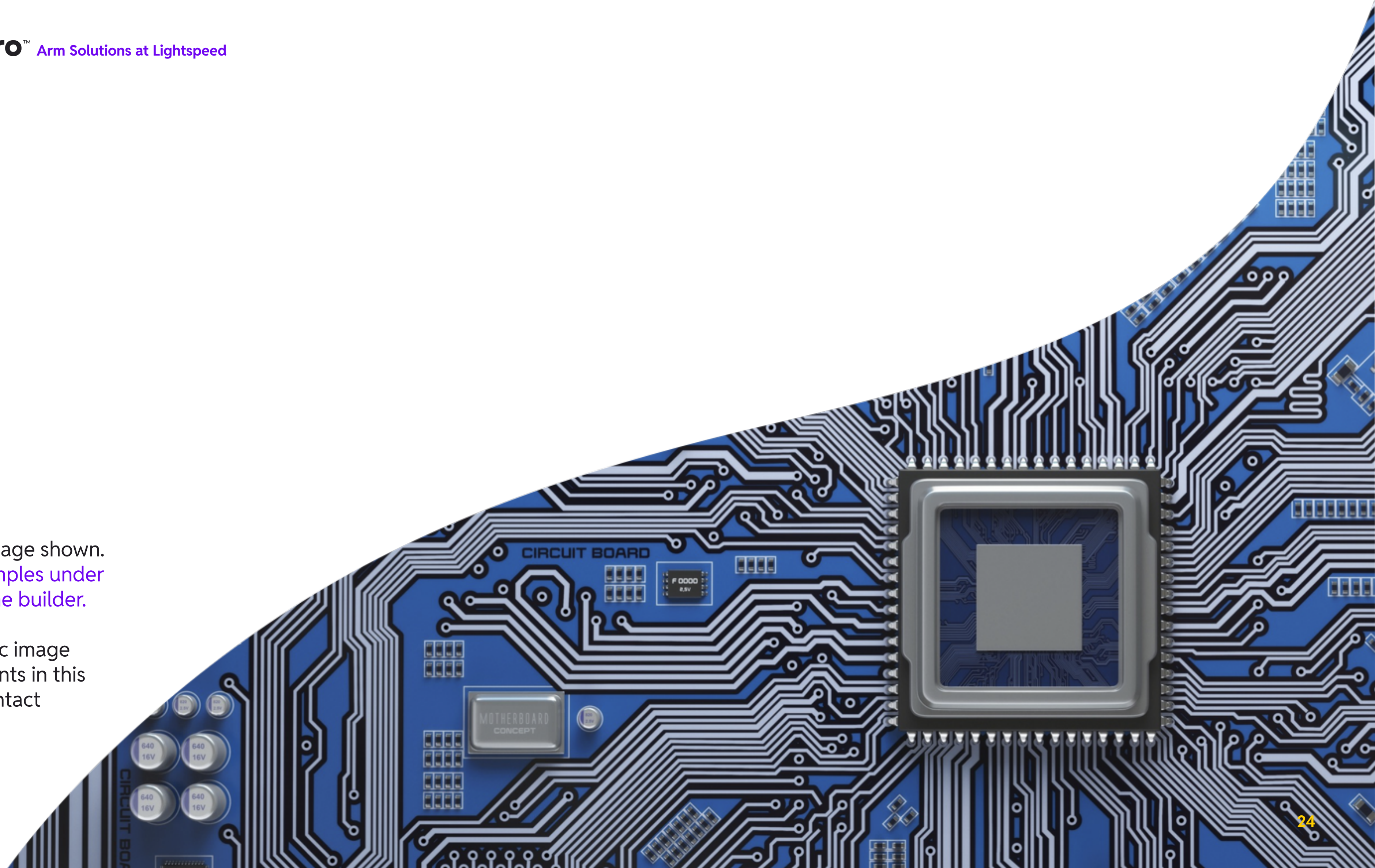
Content slide 2 column DARK

Content slide 3 column LIGHT

Content slide 3 column DARK

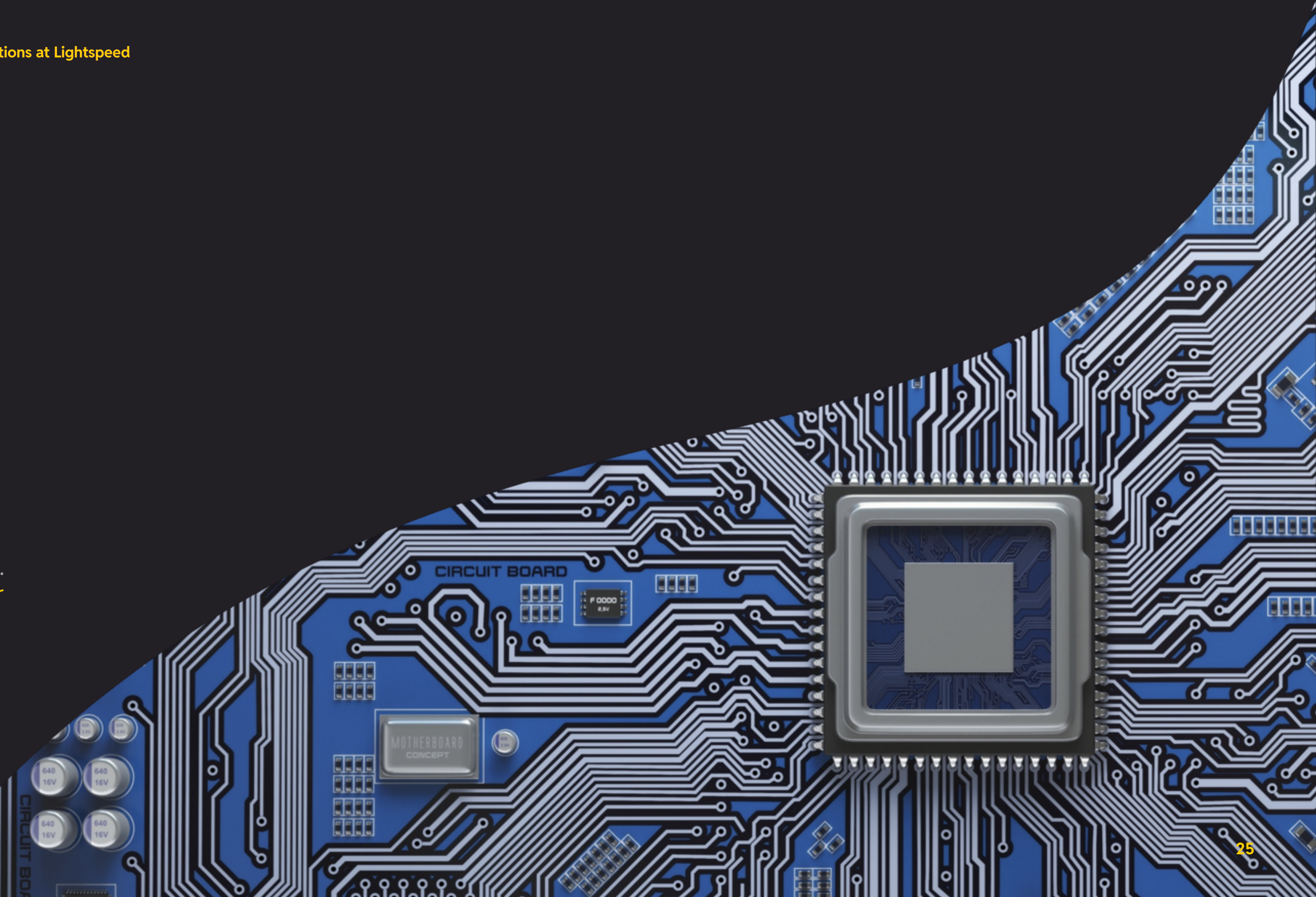
Sample Image shown.
[More examples under
view/theme builder.](#)

For specific image
requirements in this
format contact
Marketing



Sample Image shown.
More examples under
view/theme builder.

For specific image
requirements in this
format contact
Marketing



Primary colours

R - 103
G - 21
B - 232

#6715E8

R - 255
G - 205
B - 0

#FFCF00

Secondary colours

R - 255
G - 0
B - 153

#FF0099

R - 0
G - 178
B - 255

#00B2FF

R - 255
G - 153
B - 0

#FF9900

R - 106
G - 255
B - 0

#6AFF00

R - 200
G - 0
B - 255

#C800FF

- **PLEASE** always ‘make a copy’ first
- Always check that the entire presentation is in Reddit Sans font
- Consistency is fundamental to spread the Linaro visibility and brand image. We value customizations, so if you need one ask Marketing and we’ll be more than happy to support
- v2 update - increase body text default to 40pt
- ‘subtitles’ are optional, delete fields if not required