Virtual memory for real-time systems using hPMP

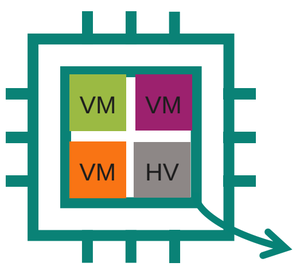
Authors:
Konrad Walluszik, Daniel Auge, Gerhard Wirrer, Holm Rauchfuss, Thomas Röcker

Introduction and Motivation

To satisfy automotive safety and security requirements, memory protection mechanisms are an essential component of automotive microcontrollers

- Fully physical address-based protection → MPU
- Virtual to physical address translation + protection → MMU

MMU Challenges: Latency introduction due to lookup mechanisms



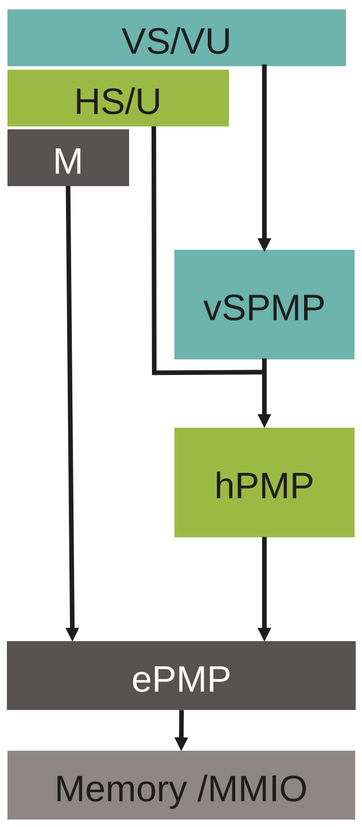
Virtual memory advantages:

Considering growing SW footprints and agile development approaches, agnosticism to physical addressing allows easier SW integration during the lifecycle

Instead of rebuilding/linking because of a VM update (effort in ECU revalidation) we propose a hpmp mechanism

Virtual MCUs running in VMs, managed by a HV

Objective



RISC-V specifies virtualization support by introducing H extension

- Virtual user (VU)
- Virtual supervisor (VS)
- Hypervisor-extended supervisor (HS)

To address the real-time needs a two level configuration of SPMP is considered

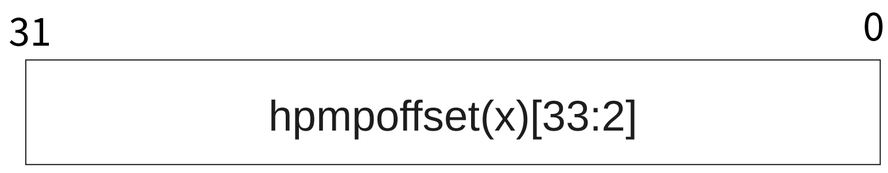
Introduce address translation in hPMP stage with OFF-TOR matching mode configuration

RISC-V CPU Extension

Already defined hPMP CSR:

- *hpmpcfg* defining matching mode and permissions
- *hpmpaddr(x) and hpmpaddr(x+1)* defining start and end address of a protection region

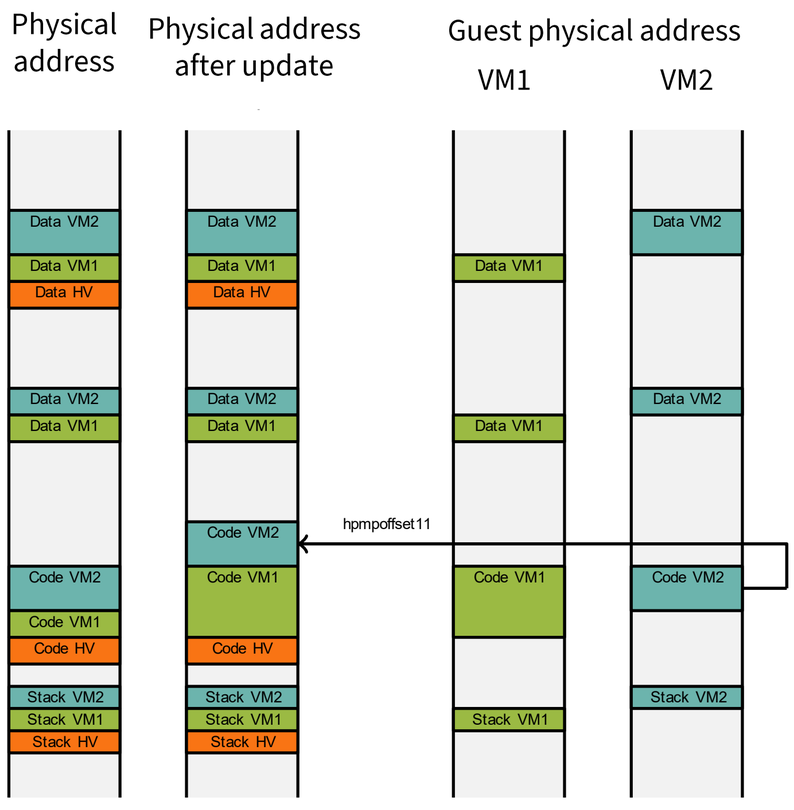
Adding new hpmpoffset(x) register for RV32:



Use model:

- pmpcfg OFF-TOR to define start/end address
- Use hpmpoffset(x) to move VMs
- For a guest physical address which has a hit within a defined hPMP region, offset will be added

Case Study and future work



Scenario description:

- Application running in VM1 increases it's code footprint due to an update (e.g. due to feature extension)
- In the original integration scenario this would result into overlapping address regions
- Configure hpmpoffset register by the HV to move all addresses of Code VM2 region

→ No need to update/modify VM2 image

Future investigations

- Investigate corner cases (e.g. overlapping regions)
- Impact on timing, area and power
- Hypervisor impact

www.infineon.com

For more information read our full paper:

Placeholder QR Code