Certifiable System-on-Chip for Safety Critical Industrial Applications

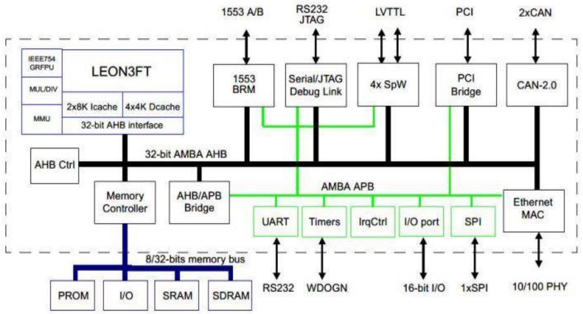
CAES PIONEERING ADVANCED ELECTRONICS

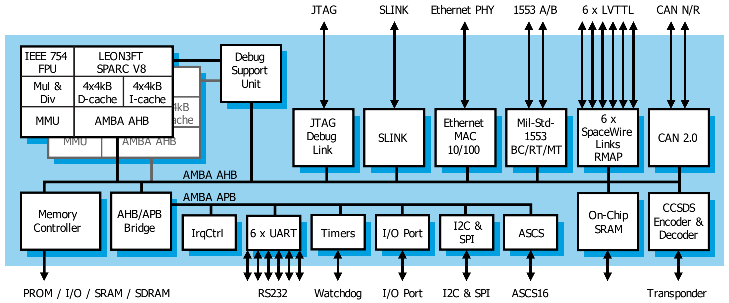
AVANCEZ 1829

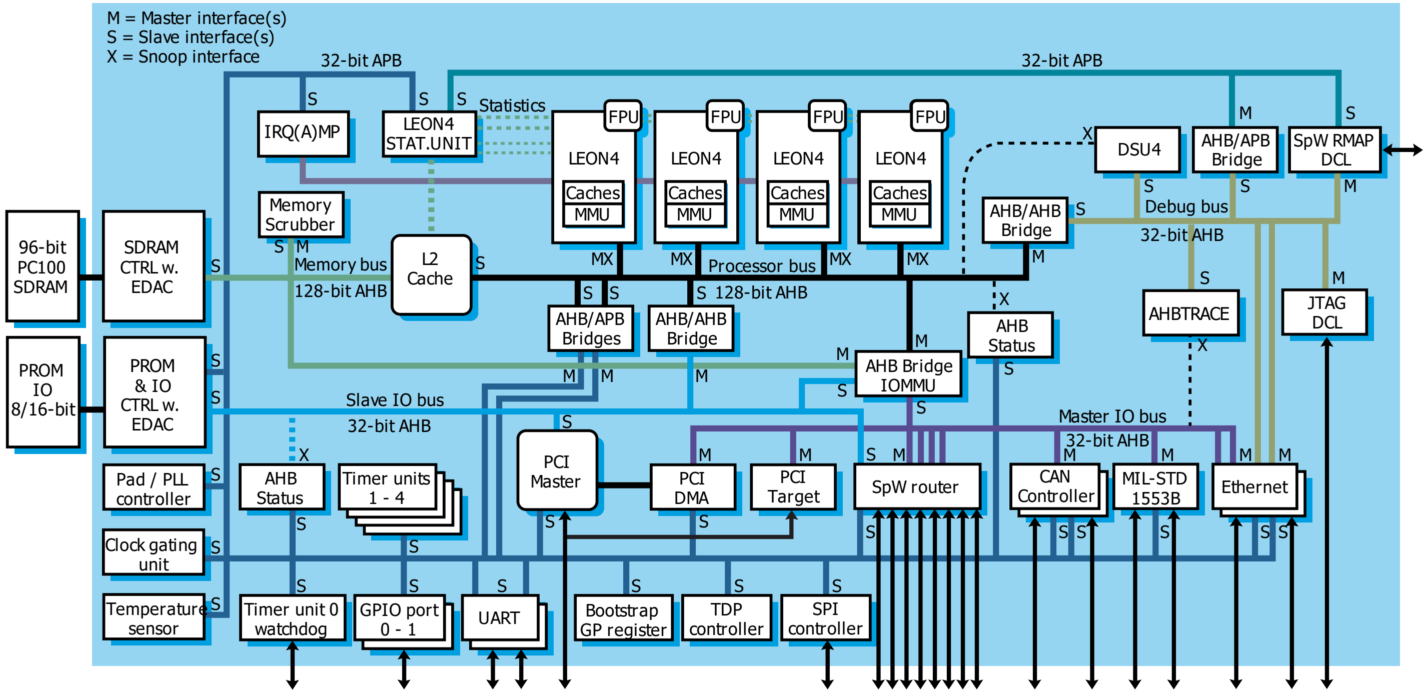
@sec the information security provider

Background

- Security gap in Systems between software & Hardware
- Users rely on software for security, but often hardware platforms offer no guarantees.
- Todays trend in SoCs: increasing degree of integration and compute power on-chip
    - More cores, more parallel software threads,
    - More sharing of chip resources
        - E.g., Caches, interconnects
    - Lower system cost (area, power)
    - New safety and security issues, e.g. side-channels

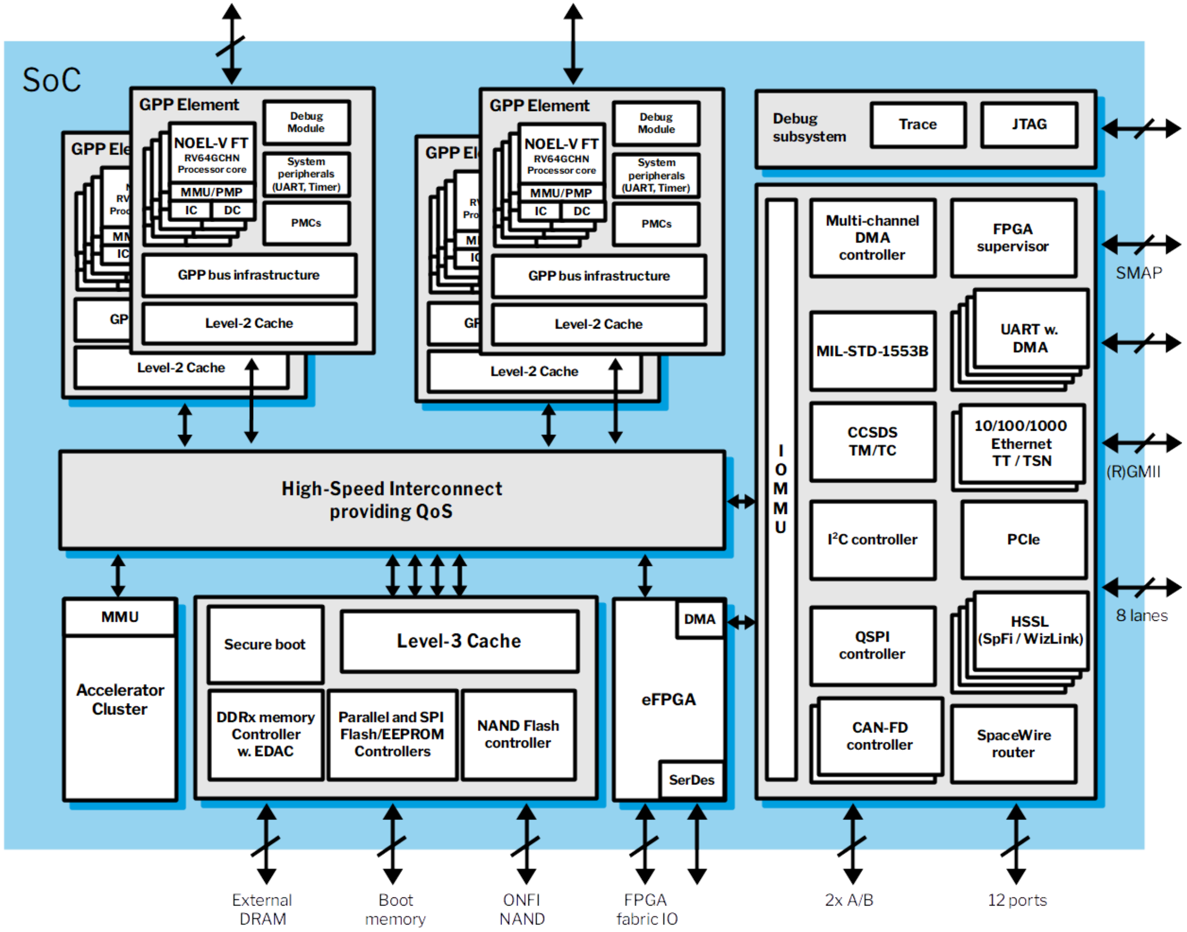






Purpose and goals of the project

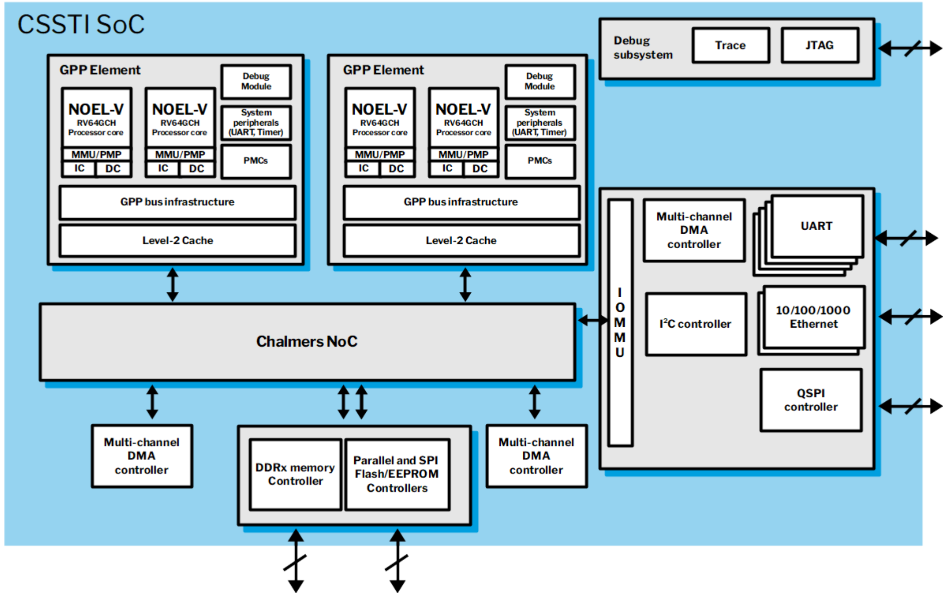
- The project extends an existing hardware design to provide
  - timing isolation between Software modules.
  - hardware evaluation to ensure it provides security guarantees
- Goal:
  - increase awareness of cybersecurity in the hardware design
  - Bridge the gap between certified software and hardware platforms.
- The project will perform a Common Criteria security evaluation of a hardware platform. This, combined with a CC evaluated SW environment, will enable the creation of a CC certified HW+SW platform.
- **Expected project outcomes:**
  - Increased awareness of problem area
  - Demo of a CC security evaluated HW (ATSEC)
  - Extensions of HW building blocks (CG/CTH)
  - Results applied to GR7xV product



Results so far

- Established first iteration of security targets
- Established SoC requirement specification
- Developed FPGA prototype design to be extended within the project
- Outreach: Project presentations to potential end users, invited to present during HiPEAC 2022 workshop.

- Some scope creep – intent was to focus on timing isolation features, security targets now also depend on functional separation features.
- Strategy to increase impact: Release platform as FPGA bitstream complemented by user's manual and debug tools.
- Long term strategy to increase project impact: Release of open source hardware variant.



Desired collaboration

- End users interested in evaluating the prototype platform
- End users with requirements on security evaluation
- Software vendors with CC evaluated SW products
- Designers interested in the hardware building blocks

Contact persons:

Jan Andersson, Gaisler, jan@gaisler.com

Ioannis Sourdis, Chalmers Tekniska Högskola, sourdis@chalmers.se

Rasma Araby, atsec information security, rasma@atsec.com