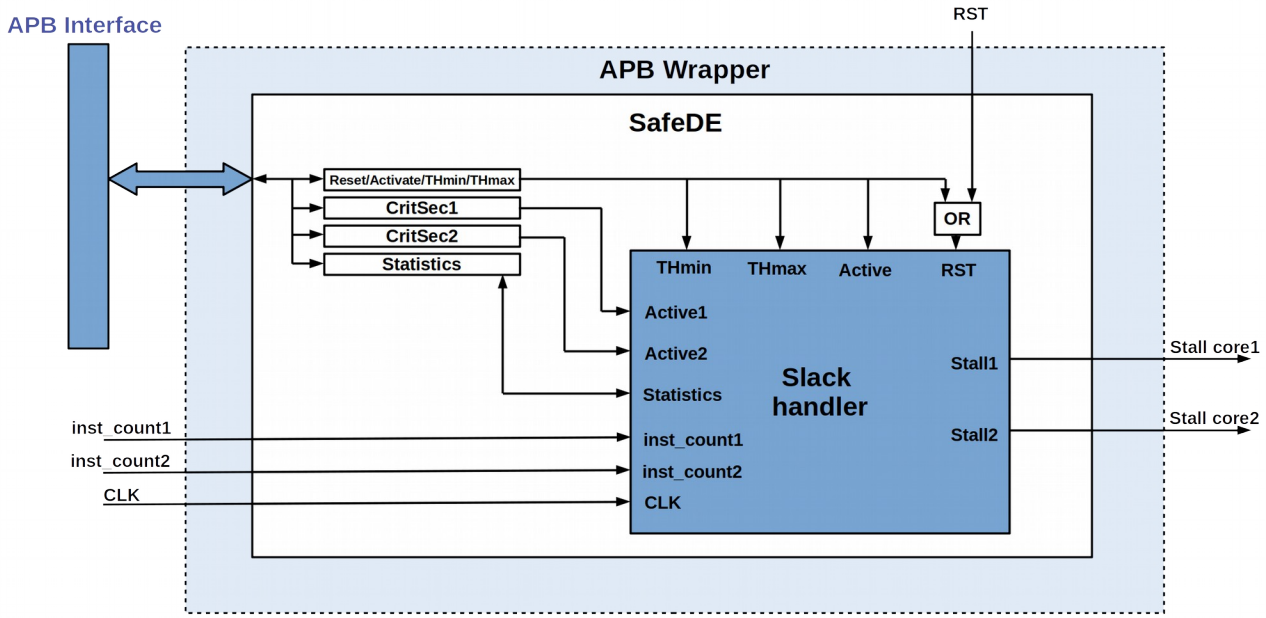
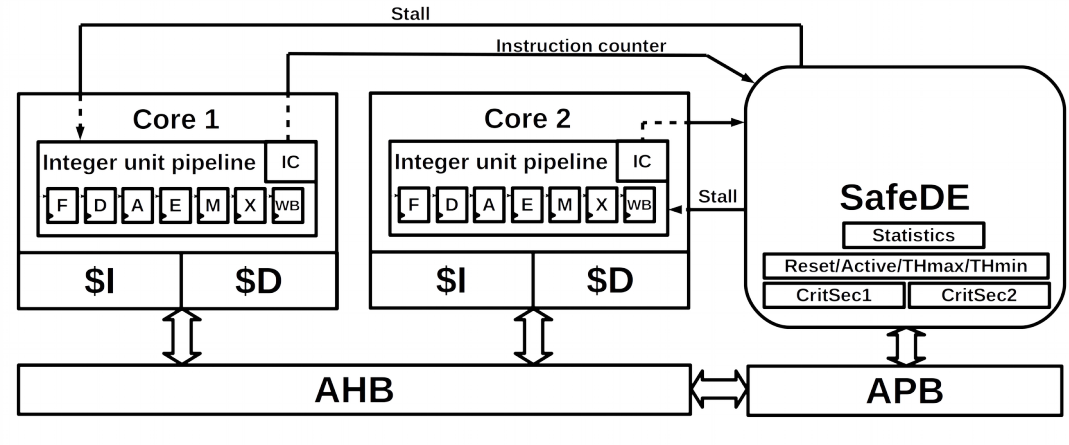
SafeDE

Brief functional description of SafeDE:

SafeDE is an RTL digital IP (Intelectual Property) of a hardware monitor that allows coupling two independent cores to operate in lockstep mode. Lockstepped execution is needed to avoid Common Cause Failures due to Common Cause faults. Current lockstep schemes have a significant penalty in terms of performance (the user sees two coupled cores just like one). SafeDE overcomes this limitation by offering the flexibility to change between lockstepped and normal execution depending on the criticality of the tasks. SafeDE is attached to the AMBA APB interface, so every system including an APB interface can easily integrate SafeDE. SafeDE is controlled by means of three internal registers that are modified through standard load and store operations.

Technical description (please provide a block diagram or software architecture diagram, if possible):





Detailed specs can be found here: “https://gitlab.bsc.es/fbasjalo/specs-safede” a BSC gitlab user account is required.

5.3 Anticipated date of publication

Date: 30/06/2021

Conference name: The 27th IEEE International Symposium on On-Line Testing and Robust System Design

Presentation title: SafeDE: a flexible Diversity Enforcement hardware module for light-lockstepping

Francisco Bas' signature: