SAFERTOS Supports ARM TrustZone: New Support Offered by WITTENSTEIN high integrity systems

Bristol, September – WITTENSTEIN high integrity systems' SAFERTOS now supports Arm TrustZone for safety critical applications. A free demo of SAFERTOS utilising Arm TrustZone is available at https://www.highintegritysystems.com/safertos/

WITTENSTEIN high integrity systems (WHIS) is continuing to expand the support provided by SAFERTOS® to ARM based environments, with integration available for ARM TrustZone. SAFERTOS is the safety critical real-time operating system available pre-certified to ISO 26262 ASIL D and IEC 61508 SIL 3. SAFERTOS integrated with Arm TrustZone is a natural choice for developers of safety critical systems, enhancing safety and security at the embedded level. The new, fully functional, demo is available for free download from https://www.highintegritysystems.com/safertos/

SAFERTOS from WHIS is a pre-emptive, safety critical RTOS that delivers unprecedented levels of determinism and robustness to embedded systems, whilst using minimal resources. It's used internationally across a range of safety critical applications and is renowned for its high quality. SAFERTOS is available pre-certified to ISO 26262 ASIL D and IEC 61508 SIL 3 by TÜV SÜD. A key advantage of SAFERTOS is the upgrade path from FreeRTOS to SAFERTOS; prototype using FreeRTOS and convert to SAFERTOS at the start of formal development.

Arm TrustZone technology provides hardware isolation for trusted software. It is both a security and safety feature that creates an isolated, secure world, which can be used to provide confidentiality and integrity to the system. It is used on billions of applications' processors to protect high-value code and data for diverse use cases including authentication, payment, content protection and enterprise. The family of TrustZone technologies supports the latest Cortex-M23 and Cortex-M33 based systems, and can be integrated into any Arm Cortex-A core.

WHIS have released an evaluation demo for the Arm Cortex-M33 with TrustZone, on an NXP LPC55S69 processor. In this evaluation demo WHIS engineers have made full use of both Arm TrustZone and SAFERTOS' integral Memory Protection Unit, partitioning the application into two sub-programs, secure, and non-secure. The secure application takes control of booting, and switches to the non-secure application after initialisation. SAFERTOS tasks can be created as secure or non-secure, where secure tasks will be using a stack allocated in the secure world. Secure tasks can make calls back into the secure world, while non-secure tasks cannot. Only secure callbacks that are marked as 'non-secure callable' can be called from the non-secure world.

"SAFERTOS and Arm TrustZone integration is a logical step that will great help safety critical software developers" Says Steve Ridley, Head of Engineering at WHIS. "SAFERTOS is able to make the best possible use of Arm architectures while easing the developers' path to certification"

The new SAFERTOS demo is available for download from the WHIS website at https://www.highintegritysystems.com/safertos/