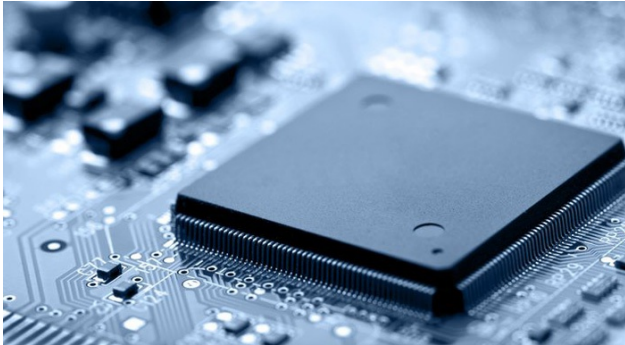


SIL-2 PLC software on Aurix micro-controllers

At the SPS tradeshow 3S Smart Software Solutions has introduced its Codesys functional safety software running on Aurix MCUs by Infineon.



(Source: 3S)

About 1000 different device platforms can be programmed with Codesys, a PLC (programmable logic controller) software implementing IEC 61131. This makes the program a market-leading integrated development environment (IDE), for example for ECUs (electronic control units), embedded controllers, gateways, or PLCs - especially for the automation of mobile machines.

For several years now, the Codesys Group has been offering an additional product pre-certified according to IEC 61508 (SIL-2), the general standard for functional safety. Device manufacturers benefit from this pre-certification. Numerous validated software extensions in the IDE or the runtime system further speed up the development and certification of safety controllers and safety ECUs.

The Platform Support Package (PSP) for the Service Pack 16 of Codesys V3.5, which will be released in spring 2020, makes according to the supplier the implementation faster and more effective: For the Aurix TC29x micro-controller from Infineon, the safety extensions have been upgraded. The entire runtime environment for the Aurix platform has already been adapted and pre-certified in advance - including the interfaces for specific extensions or drivers from device manufacturers. This eliminates a major part of the effort required to implement and certify the runtime environment. This shortens the time-to-market. Due to the multi-core architecture normal control and functional safety applications can be processed in parallel on one CPU ("Compound PLC").

The software includes optionally CANopen Safety and CANopen protocol stacks. Therefore, safe and non-safe devices can be configured and used simultaneously within one and the same network.

The Aurix TC29x series of MHz MCUs features six on-chip CAN FD controllers. Its multi-core architecture, based on up to three independent 32-bit TriCore CPUs, has been designed to meet safety standards, while simultaneously increasing performance significantly. Equipped with a Triple TriCore with up to 300 MHz, 8 MiB of flash-memory and a timer module (GTM), the MCU series aim for a reduced complexity. The integrated Safety Management Unit (SMU) is a central hardware module that collects the alarms from every hardware safety mechanisms, as well as the error signals related to the architecture. The severity of each alarm can be configured accordingly with the needs of the application. Whenever an input alarm event is detected and the SMU state machine is in Run or Fault state, the module checks what are the configured actions to be done.

The SMU recovery timers (RTs) are available to enable monitoring of the duration of internal error handlers. The RT duration can be configured. If an RT is enabled and any of the configured alarm events occurs, this RT is automatically started. Once an RT event occurs, the RT starts and counts until software stops it. If the timer expires, an internal SMU alarm (Recovery Timer Timeout) is issued.

The SMU is connected to all safety mechanisms that are within the micro-controller It is also connected to the System Control Unit, the Interrupt Router and the Ports in order to trigger the configured reaction when an alarm is set. The Codesys runtime software uses these hardware safety features, which simplifies the safety programming.

[hz](#)