HIMA | SMART SAFETY.

Cost-effective development of safety electronics

Faster development of safety applications for factory automation

The factory automation market increasingly demands safety solutions that meet the requirements of IEC 61508 as well as the requirements of ISO 13849-1. If Performance Levels (PL) d or e are to be achieved, it should be noted that the requirements for the safety architecture for Category 3 or 4 are sometimes higher. Precertified safety System-on-Chip (SoC) solutions help avoid unnecessary risks and extra costs in the development process and significantly shorten time to market.

IEC 61508 is not the same as ISO 13849-1

Among hardware and software developers in the factory automation sector, there is a clear trend toward designing more and more controller solutions that comply with the requirements of IEC 61508 – the standard for functional safety of electronic systems – as well as ISO 13849-1 for the safety of machine controllers. Many automation specialists who do not deal with safety aspects every day are not aware that the safety requirements of ISO 13849-1 in PL d or PL e of Category 3 or 4 can be higher in terms of architecture than those of IEC 61508. For example, the former specifies two-channel architecture as mandatory for all safety-relevant structures at Category 3 or above, which is not absolutely necessary for SIL applications. This can lead to unpleasant surprises with TÜV certification if it turns out that the design cannot comply with ISO 13849-1 or can only do so at considerable extra efforts.

Up to now, manufacturers of automation technology have mainly opted for one of the following options to resolve this issue in practice:
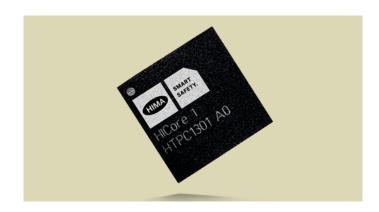
A) They select a SoC platform that meets the requirements of ISO 13849-1 but is not correspondingly certified. In this case, the developed solution fulfills the technical requirements in principle, the manufacturer is directly responsible for carrying out the costly certification process though. This drives up development costs and significantly extends time to market.

B) They implement a solution based on standard components with two separate processors and discrete safety logic. With this frequently chosen option, development costs are even higher than with option A because the application software and the logic have to be developed twice in nearly the same way. Furthermore, there are inestimable risks extending as far as complete failure of the project if it is discovered during the course of development that the intended solution cannot

fulfill the ISO 13849-1 criteria up to PL e and category 4, or can only do so at considerable extra expense. Furthermore, obsolescence can become an issue because the life cycles of factory automation products are significantly longer than the life cycles of standard electronic components.

C) They steer development toward fulfilling lower safety requirements, such such as SIL 2 / PL c, if possible. In this case, they fail to meet the originally set development goal and do not achieve the safety standard demanded in the project.

On the safe side with the certified HICore 1 SoC

Automation technology manufacturers that wish to avoid taking any risks opt for a precertified SoC platform such as HICore 1. Its safe functionality, such as high-precision four-quadrant counter inputs, safe I/Os or safe PWM outputs, fulfill all requirements of IEC 61508 (up to SIL 3) and ISO 13849-1 up to PL e and category 4. Thanks to the certification, developers can rely on achieving ISO 13849-1 certification with their selected platform. This saves the customer the costly effort of testing the processor architecture. That drastically shortens the development process, and with it the time to market. HICore 1 also makes it possible to realize designs with an extremely small footprint. The architecture of the SoC, with two synchronously clocked processors, simplifies software design because exactly the same code is executed on both processor cores of the safe system. HICore can be used in a wide variety of safety applications in factory automation, including sensors, actuators, drive systems, robotics and automated guided vehicles.

Along with the actual product – consisting of the HICore 1 SoC, the certified operating system and extensive documentation (including a safety manual) – experience and know-how are a decisive success factor in the development of embedded electronics, which, along with the target product, must also be certified according to the ISO 13849-1 standard. Drawing on their experience, the certified safety engineers at HIMA Embedded Solutions help customers upon request to avoid typical pitfalls in the development process.

The key benefits of HICore 1 at a glance

- **Shorter time to market:** The ISO 13849 certificate guarantees platform compliance with the standard, so clients do not have to invest time on suitability testing. It also eliminates the need for the time-consuming verification process (test, documentation, calculation of performance data).
- **Cost savings:** HICore and the certified operating system form a safe platform that drastically reduces development effort by limiting development to the actual application.
- **Space savings:** Minimal footprint on the PCB – solutions up to SIL 3 or PL e can be implemented with the compact SoC solution in the smallest of spaces.
- **Future-proof:** With HICore, products meeting the strictest safety requirements according to current standards (SIL 3 / PL e) can be developed. If the safety standards are updated, there is a greater likelihood that these products can also be certified according to the updated standards and can continue to be marketed.
- **State of the art:** The client uses a state of the art platform, which can be relevant in the event of an insurance claim.

Full flexibility for developers

Hardware and software developers can purchase the HICore 1 Safety SoC together with a tested development environment, including a secure, certified operating system and detailed documentation – in case you perform the development and certification process yourself – or you entrust HIMA's competent experts with the complete solution. Co-development – joint development with the client – is also possible.

SAFE System		**COM** System
P1	**P2**	**P3**
32 Inputs / 30 Outputs / 2 PWM / 4 Counter / UART / SPI / CRC, 80390, FLASH, SRAM	80390, FLASH, SRAM / 32 Inputs / 30 Outputs / 2 PWM / 4 Counter / UART / SPI / CRC	80390, FLASH, SRAM / Ethernet / 2 CAN / 2 UART / SPI / 8 I/O