MicroSys
Creating Embedded Systems

Platforms for Functional Safety

Realizing functional safety with modular hardware architectures

Introduction

Functional safety minimizes the risk of injuries and damages in human-machine interactions, redundancy and multi-channel data processing ensure high availability and prevent catastrophic malfunctions. While obtaining certification for safety-relevant control systems remains the responsibility of systems manufacturers, they can obtain certification-friendly System-on-Modules and an application-ready hardware platform from MicroSys to help them develop application specific safe solutions for highly automated machinery and plant faster.

Highly automated, in some cases autonomous devices, vehicles, machines and plant exchange data and interact with each other. The Internet of Things (IoT) further boosts this trend. Nevertheless, they still require direct or indirect interactions between humans and machines.

Preventing Malfunctions

Safe operation is a key prerequisite for using automated systems. Therefore, functional safety (FuSa) plays a major role key in all technology-heavy industries, from power generation to transportation to industrial production and medical technology to, food, chemical and pharmacy, including home appliances and entertainment systems.

The aim of functional safety is to minimize the risk of injuries and damages by preventing malfunctions resulting from design, production or documentation flaws,exceptional operational situations and operating errors and hardware failure and putting the system into a safe state.

To minimize the risk of injuries and damages, FuSa is expected to prevent malfunctions resulting from design, production or documentation flaws, exceptional operational situations and operating errors and put the system into a safe state. To reduce the risk of injuries, machine and plant manufacturers prevent human access to the moving parts of complex equipment. Opening doors or hatches is a protection violation like pressing an emergency button and results in an emergency stop.

Safety increases Productivity

For several decades, Safety circuitry involved hard-wired solenoid switches and was fully independent of the equipment's control system. This hampered flexible reactions beyond a sudden system shutoff. The circuitry's lack of flexibility also made it difficult to modify or expand the protected equipment. Increasingly complex, often modular machines with the ability to rearrange during operations to adapt to changeable requirements require differentiated reactions to various protection violations. Moreover, fencing in production lines or cells is not always easy. For mobile machines or transport systems in particular, this is no feasible option at all, while their rising degree of automation causes the safety requirements imposed on their control systems to skyrocket.

Consequently, programmable safety controllers have become the standard. Connected to advanced safe sensors, these allow designing both user-friendly and effective safety systems. Time-of-Flight (ToF) cameras and 360° Laser scanners, for instance, facilitate safe person and object recognition as the foundation for safe autonomous guided vehicle (AGV) or autonomous mobile robot (AMR) operation.

In state-of-the-art FuSa concepts, the safe PLC exchanges data with I/O modules, sensors and actors via field busses. Albeit in Ethernet-based networks, data usually travel via the "Black Channel". Safety data protocols eliminate potential sources of error along the transmission path, for instance by keeping data in the telegrams redundant and protecting them by checksums or encryption. This allows acknowledging messages and periodically validating the correct function of the transmission path.

Safety enhances freedom

This also makes it possible to place safety PLCs and I/O modules connecting the sensors anywhere in the system. Furthermore, current electric drives come with safe functionality according to EN 61800-5-2 such as Safe Torque Off (STO), Safe Direction, Safely Limited Speed (SLS) or Safely Limited Acceleration (SLA), offering a variety of alternatives to a shutdown.

Using these softer mechanisms to protect people helps prevent damages caused by abrupt safety shutdowns. A safe operating state without a full standstill also makes setup operations easier and facilitated developing collaborative industrial robots commonly known as Cobots. These are sufficiently safe to work hand in hand with human colleagues even without separating fences. Using a common bus, the non-safe PLC can enquire the

While in industrial applications functional safety (FuSa) was in the past mainly ensured by protective fencing, open production automation solutions such ascollaborative robots (Cobots), autonomous guided vehicles (AGV) and autonomous mobile robots (AMR) call for more differentiated solutions. Future-orientedtopics like autonomous road vehicles or construction machinery are unthinkable without FuSa.

state of the safety sensors, which reduces the time required for commissioning and error diagnostics. It also allows preventing detrimental upstream or downstream operating conditions in case of emergency standstills by adjusting processes. Parametric FuSa programming can be modified later, allowing demand-driven alterations of the configuration of modular plant or machinery to provide it with the aptness for the challenges of Industry 4.0.

Availability is Safety

While it is good practice to get industrial machinery into a defined state with a reduced hazard potential, in many other applications there is no such state. Consider an engine or tailplane failure in a flying airplane, failing brakes in a train or a malfunctioning steering in an automobile.

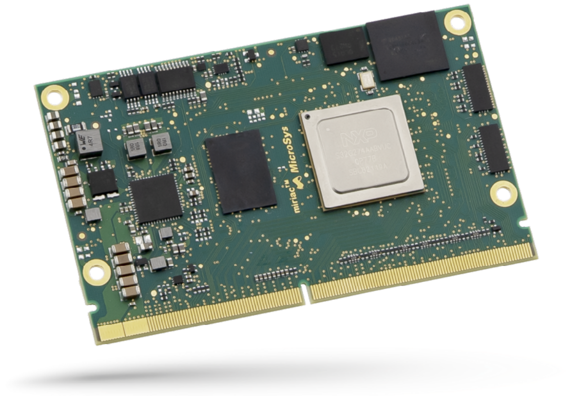
Cases like these require a different form of safety, that is to say, high availability as protection against system failure. So-called failsafe systems are usually designed using redundant computer systems. Their architectures reach from a simple duplication of processing channels with information redundancy (both processors have access to input and output data) to multiple redundant dissimilar systems with 5-15 computers, various fallback levels, and emergency operation modes in aviation.

Dissimilarity of processing channels is particularly well sought after in applications with a very high risk potential such as aviation, but also for applications in industrial and rail applications requiring high safety levels (SIL3, SIL4). In order to counteract single event upsets, memory failure, common-cause failures or cascading errors that are difficult to resolve, different processor types are typically used for the redundant processing channels. This also protects against faulty batches. In view of target failure rates below 10-9 or 10-10 per operating hour, this should also be considered.

Modular Safety

Off-the-shelf safety systems from many automation system manufacturers are certified according to IEC 61508 and a good choice for the safe design of industrial plant or machines. For many other tasks and for the design and production of such Safety CPUs, it is necessary to start from a different hardware level.

Using System-on-Modules (SoM) is a more economical, low-risk alternative to board-level hardware design. Using SoMs, system manufacturers do not need to tackle the highly complex microprocessor-related issues when designing electronic assemblies. Due to the processors' high clock speeds, these reach deep into physical fundamentals. System designers can thus focus on developing software and taking care of manageable interfaces on the edges of the modules.



Due to the architecture of the NXP multicore processors used and their certification-friendly design, the easy to integrate System-on-Modules (SoM) from MicroSys are particularly well-suited for use in safe control systems.

miriac® MPX-S32G274A

The Bavarian manufacturer MicroSys Electronics GmbH is an NXP Gold Partner. MicroSys Electronics designs and produces SoMs using that European processor manufacturer's processor technology. "Current NXP multicore processors such as the S32G not only deliver high performance. Due to their specific architecture, they are also better suited than most for safe control system design", says Jörg Stollfuß, Field Application Engineer with MicroSys Electronics. "Using this processor, we created easy to integrate modules with a certification-friendly design as an alternative to board-level FuSa development."

MicroSys miriac® SoMs have all prerequisites preventing hitting hardware-related obstacles during the certification process, appropriate external circuitry and software provided. This includes features like separate power supply monitoring that also facilitates implementing an independent watchdog timer. For the miriac®-SoMs, MicroSys exclusively uses components qualified to the strict AEC-Q100 automotive standard to cover elevated requirements in terms of the manufacturing quality of the semiconductors. As the application software has a main influence on the certifiability of computer systems, however, other than safety sensors, SoMs are not available as pre-certified safety elements.

Application Ready Platform

The multi-kernel architecture of current processors cannot be used to run safe and non-safe applications (mixed criticality) in parallel on a single processor. Due to its multitude of common cause failure potentials and the general basic failure rates of the complex semiconductors, it is even less suited for the design of single-processor redundant systems or multi-channel systems for failsafe applications.

The task specific but not custom Autonomous Control Unit can accommodate a miriac® MPX-LX2160A SoM and up to three SSD memory modules or one or twoHailo-8™ AI processor modules in three M.2 Slots. It is also prepared for an optional extension using a miriac® MPX-S32G274A or miriac® MPX-S32G399A SoM.This makes it a ready-to-install, modular hardware platform for use in safe automation systems.

MicroSys developed hardware for a task specific but not custom control system platform. This ready-to-install comprehensive system was mainly created for use in mobile machinery. At the core of the product is a carrier board accommodating the central miriac® MPX-LX2160A SoM and providing three M.2 Slots. These can be used to add up to three SSD memory modules or one or two Hailo-8™ AI processor modules. It is also prepared for an optional extension using a miriac® MPX-S32G274A or miriac® MPX-S32G399A SoM. This facilitates very high processing power for complex applications or alternatively an independent dissimilar processing channel to achieve safety levels up to SIL 3.

What makes the electronics a ready-to-install comprehensive system is the specifically designed enclosure. Rated IP68 for dust and water resistance, it serves not only to protect the electronics but also for heat dissipation. In spite of the extremely high performance and the multitude of interfaces, MicroSys managed to keep the power consumption of the fully equipped unit below 60 W, so the passive device comes without fans or other active cooling.

"With this Autonomous Control Unit based on the miriac® MPX-LX2160A SoM, MicroSys offers a ready-to-install, modular and scalable hardware platform for the automation not only of mobile machinery", MicroSys Managing Director Ina S. Schindler confirms. "System design engineers can fully concentrate their focus on software design."

“Current NXP multicore processors such as the S32G not only deliver high performance. Due to their specific architecture, they are also better suited than most for safe control system design. Using this processor, we created easy to integrate modules with a certification-friendly design as an alternative to board-level FuSa development.”

Jörg Stollfuß, Field Application Engineer,
MicroSys Electronics GmbH

“With this Autonomous Control Unit based on the miriac® MPX-LX2160A SoM, MicroSys as a ready-to-install, modular and scalable hardware platform for the automation mobile machinery, System design engineers can fully concentrate their focus on software design.”

Ina S. Schindler, Managing Director,
MicroSys Electronics GmbH

About MicroSys Electronics

MicroSys Electronics has been designing and developing embedded system solutions since 1975, is an NXP Gold Partner and widely integrates NXP's S32 Automotive, Layerscape and QorIQ processor technology. Designs based on System-on-Modules (SoMs) are the strengths of this German company, with the portfolio ranging from application-ready SoMs and customer-specific carrier board designs to fully integrated systems. Application areas for these extremely rugged designs with long-term availability are primarily found in markets where safety standards analog to IEC 61508 are required, such as railway technology (EN 50155), aviation (DO-160), and mobile machinery (ISO 13849), as well as manufacturing robots (ISO 10218), control systems (IEC 61131-6), and drive systems (IEC 61800-5-2). Further application areas can be found in medical technology (60601), and in critical infrastructures, for instance in the nuclear sector (IEC 61513) or the process industry (IEC 61511). MicroSys works closely with its customers in all these industries to ensure that the specific applicable standards are fully met.

For more information, visit www.microsys.de

NXP
Gold
Partner

MicroSys Electronics GmbH

Mühlweg 1
82054 Sauerlach, Germany
Tel: +49 (8104) 801-0
Fax: +49 (8104) 801-110
Web: www.microsys.de
Email: info@microsys.de