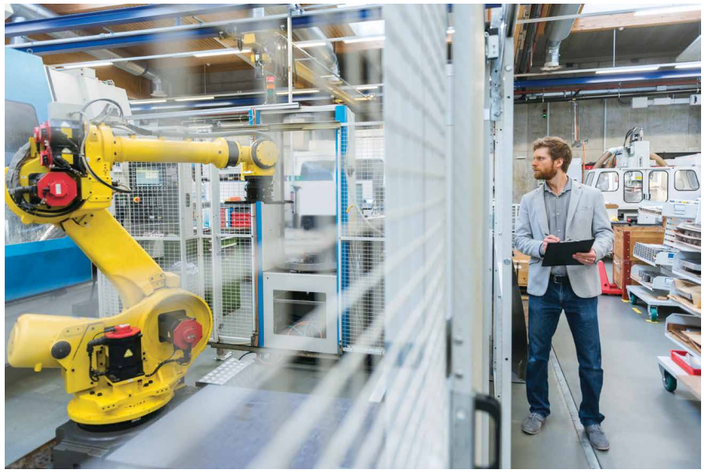
DESIGN-BASED SAFETY AND SECURITY OF ROBOTIC SYSTEMS



Why functional safety and data security are important features, and not just decorative accessories? Contribution by **Andreas Genser**, Senior Manager at Infineon Technologies

AT the beginning of the 20th century, Henry Ford revolutionised automobile manufacturing. He was inspired by the use of conveyor belts in grain elevators. Combined with other productivity gains that resulted from assembly line manufacturing, this allowed Ford to reduce the time it took to produce a vehicle from more than twelve hours to nearly 90 minutes.

Today, most products are created through collaboration between people and machines, with people protected from potential harm by doors, light barriers and interlocking mechanisms.

However, to benefit from further potential productivity gains, we need to make the leap from simple collaboration to true collaborative working. Initiatives around Industry 4.0 are making robots smarter and – through their sensors – better equipped to interact with their environment.

But one big question remains: Can this revolution happen safely?

Focus On Safety

The assembly line concept allows us to benefit from the speed and efficiency of machines. At the same time, it also limits how products can be manufactured. As long as the products manufactured are all the same – no problem. But today's customers expect choice, customisation, and uniqueness. That won't mix well with a linear manufacturing process.

Instead of being limited to this linear, step-by-step process, there are now other options. Innovations offered by the Industry 4.0 concept allow other ways of realising manufacturing processes. One method here is to move to a series of manufacturing islands, with each island executing one element of the manufacturing process. The product to be manufactured is then conveyed from one station to another, with each station performing the assigned task.

This also offers the possibility of supplying the same product in different variations. The basic model of a product only has to go through the most important manufacturing stations, while a higher-quality model goes through further stations where additional manufacturing steps take place.

These manufacturing steps may require human intervention in some cases. However, a safety concept is required to enable interaction between humans and machines, which must be defined at the beginning of the development of the production system. This is also common practice in the development of systems in many industries, for example in automotive engineering.

In automotive applications, occupants rely on electronics to control many critical systems. Malfunctions or complete failures can affect both vehicle occupants and other road users. This is true, for example, of ABS braking systems, electronic parking brakes and power steering systems. When defining such products and selecting the associated control systems, the implementation of functional safety must be considered at every stage.

The architecture of devices such as the 32-bit microcontrollers of the AURIX family is specifically designed for use cases that place high demands on safety integrity. They meet the most stringent automotive ISO 26262 requirements and can therefore be used in systems together with safety manuals and dedicated safety software routines to meet IEC 61508 specifications. IEC 61513 is an adaptation of IEC 61508 for machinery, while IEC 61511 is aimed at the process industry.

To ensure that a failure of the processing element within a system can be detected, many fail-safe systems use two different microcontrollers. One of these microcontrollers executes the application program while the second monitors the first (Figure 1). This concept ensures redundancy within the control system since a software error or failure of one device will not also occur in the other device.

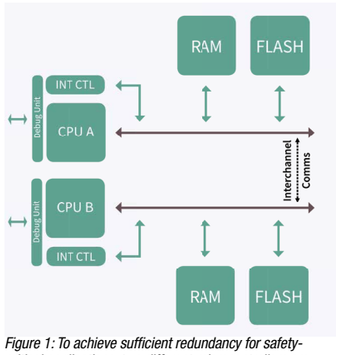


Figure 1: To achieve sufficient redundancy for safety-critical applications, two different microcontrollers are often used in a loosely synchronized dual-processor architecture.

Safety Today And In The Future

Until now, industrial robot arms have been developed independently of the tools with which they are equipped. Typically, the power supply and control system of a welding tool is attached to the side of the robot arm via a heavy cable bundle. In part, this separation is done for safety reasons, as it allows the robotic arm supplier to maintain complete control over their safety-certified device. And it does so regardless of the manufacturer of the tooling used. If they were to share their communication buses and power systems with third-party tools, it would be difficult to enable the safety of the system.

With Industry 4.0, however, the need arises to connect all systems and sensors so that machines are able to communicate and cooperate with each other and with their human operators. This can lead to a potential security risk: a vulnerability that could be abused as a point of attack.

Even more critically, extensions and tools could be added in the future whose security implementation have not been adequately tested. Such elements could become a backdoor for network attacks, or they could even be misused to reconfigure industrial equipment and the robots themselves. Given that humans and machines are so close, there is a significant risk to life and limb if robots are reprogrammed or rely on manipulated sensor data.

Reliable tools and sensors, as well as accessories and spare parts, will be essential to maintain not only functional safety but also network security in the factory of the future. However, in the fast-paced manufacturing world, it is equally important that the implementation of reliable systems does not hinder maintenance or spare parts replacement. Because that would inevitably lead to longer downtimes.

Functional safety measures, like security measures, cannot simply be added later. Safety and security must therefore be integrated into the development process from the start so that it provides the necessary protection and can be used intuitively at the same time. In addition, safety and security can no longer be considered independently of each other.

In collaborative automation systems, functional safety can only be realised if suitable security measures have been taken: With redundant configurations, as already mentioned in connection with safe microcontrollers, there is a risk of unsafe behavior if, for example, a critical calibration can be tampered with without authorisation. With AURIX microcontrollers, an embedded security module takes care of this problem.

In most cases, there is no universal solution that is suitable for all applications. For consumables, a simple, low-cost solution may be sufficient to determine whether the material used is actually approved by the supplier. On the other hand, a fully networked control subsystem requires self-authentication with a security anchor (Trust Anchor) before it is allowed to participate in a critical production system.

Robots with control systems must not only authenticate each other – it is also essential that these systems be protected against data theft and tampering. Securing the integrity of robots can best be realised through IP protection of calibration files, authentication of components, and protected logging to support detection of attacks.

To protect the security of data, interfaces and communication channels in intelligent robots and industrial networks, Infineon offers embedded OPTIGA security solutions that can be easily integrated.

As humans and machines come into closer, more intimate contact, the success of their collaboration depends to a large extent on trust. But this trust can only be built if we feel safe in the company of machines. Functional safety must be integrated at the beginning of the initial design and constantly reviewed until the design of the robot, cobot or AGV is completed. But safe software can only be relied upon if it is unchanged and communicates with a reliable network of systems, modules, and sensors.

Therefore, security is elementary from the very beginning. It allows the authentication of highly complex robotic systems and their human operators to establish and maintain the all-important trust during operation by confirming the flawless integrity of industrial devices.

	OPTIGA™ Authenticate IDoT	OPTIGA™ Trust M	OPTIGA™ TPM
Security Level	Enhanced	CC EAL 6+ *	CC EAL 4+
Functionality	Authentication	Connected device security - Toolbox based	TCG standard
NVM (Data)	1k,2k, 4kByte	10 kByte	6 kByte
Cryptography Private key stored in secure HW	ECC163	ECC384 RSA2K	ECC256 RSA2K
Type of Host System	MCU without OS / proprietary OS / RTOS	Embedded Linux	Windows / Linux
Interface	SWI, I2C	I2C	I2C, SPI, LPC
System integration	✓	✓	Platform vendor

✓ Done by IFX
* Based on certified HW
** Code & Data

Security and Complexity

Table 1: Infineon offers hardware security controllers for various purposes with the comprehensive OPTIGA family.