Building a functional Safety-compliant Industry Solution for IEC 61508

Matteo Salardi, Intel
Franz Walkembach, SYSGO

ABSTRACT

Today, Electrical / Electronic / Electronic-programmable systems (E/E/PE systems) enable a wide range of applications. They not only power the everyday computing devices such as laptops and servers, but also serve in Safety-relevant areas such as the Electronic Control Unit (ECU) of a car, the control system of a robot, or the manufacturing setup in discrete Automation.

Strict Safety standards for embedded systems maximize the protection of the operators and to minimize the risks in any possible and reasonable way. Nowadays, specific Safety standards have been defined for almost every branch of industry, including requirements for electronically programmable systems. The number of branch-specific standards is constantly growing, while the standards themselves are becoming more extensive.

This paper starts with an introduction on the foundational standard IEC 61508, offers an overview of industrial areas of application, and then focuses on an exemplary robotic arm controller, explaining the functional Safety hurdles and solutions for both hardware and software. In particular, it describes a Safety ecosystem, including a System-on-Chip (SoC) based on Intel's Atom® x6000FE processor series and SYSGO's real-time operating system and hypervisor PikeOS.

1. Introduction

Today, Electrical / Electronic / Electronic-programmable systems (E/E/PE systems) enable a wide range of applications. They not only power the everyday computing devices such as laptops and servers, but also serve in Safety-relevant areas such as the Electronic Control Unit (ECU) of a car, the control system of a robot, or the manufacturing setup in discrete Automation.

Strict Safety standards for embedded systems maximize the protection of the operators and to minimize the risks in any possible and reasonable way. Nowadays, specific Safety standards have been defined for almost every branch of industry, including requirements for electronically programmable systems. The number of branch-specific standards is constantly growing, while the standards themselves are becoming more extensive.

This paper starts with an introduction on the foundational standard IEC 61508, offers an overview of industrial areas of application, and then focuses on an exemplary robotic arm controller, explaining the functional Safety hurdles and solutions for both hardware and software. In particular, it describes a Safety ecosystem, including a System-on-Chip (SoC) based on Intel's Atom® x6000FE processor series and SYSGO's real-time operating system and hypervisor PikeOS (refer to Figure 1).

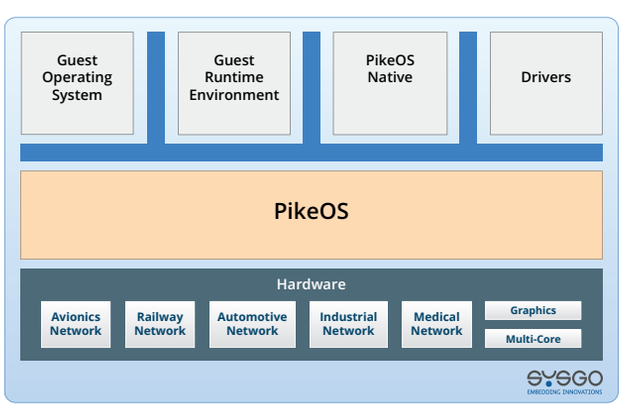

Figure 1: Eexample of a software and hardware stack

2. Functional Safety Overview

The original standard, from which many contemporary industry-specific Safety standards have been derived, is **IEC 61508**. It is a generic standard applicable to all branches of industry that dictates the Safety concepts of embedded systems, dividing application areas into Safety levels. IEC 61508 specifies that a system must be planned and monitored throughout its entire life cycle. The standard's strict requirements cover all the Safety-relevant areas to ensure a comprehensive approach to Safety.

IEC 61508 encompasses seven sub-documents totalling several hundred pages, including:

- IEC 61508-1, describing general requirements for the system;
- IEC 61508-2, providing requirements for hardware;
- while the IEC 61508-3 specifies requirements for software.

These three sub-documents define the mandatory requirements. The remaining ones provide supplementing application examples, guidelines for classifying the criticality level, lists of terms and abbreviations, and other practical guidelines. IEC 61508, for example, prescribes the requirements for a risk analysis: The dangerous effects of the system under analysis should be recognized and safeguarded accordingly. This includes, as stated in IEC 61508-1 under 7.4.2.3, that all foreseeable harmful events should be dealt with, including hardware faults, human error and Security problems.

Along with Safety, Cybersecurity plays a crucial role in modern devices. Both areas, while different, closely influence each other: Ensuring functional Safety requires a certain level of Cybersecurity, which we will discuss later.

Because IEC 61508 covers the entire life cycle of a system, Safety requirements must be specified at the inception of a project for both the design and development phases. IEC 61508-2 and IEC 61508-3 prescribe suitable measures to prevent systematic hardware and software errors during all phases of the project. Distinct specifications apply to each phase of the life cycle.

To summarize, the Safety standards require system architects and developers to establish a robust Safety architecture based on a comprehensive understanding of the system; to properly design, validate, and verify both hardware and software; and to complement them with the appropriate set of collaterals. The overriding goal is to guarantee Safety through a profound understanding of the system and its associated Safety mechanisms.

The classification by **Safety Integrity Levels (SIL)** lays the foundation for ensuring system Safety. The SILs range from 1 (lowest criticality) to 4 (highly critical). The SIL classification distinguishes between operation in high-demand and low-demand modes:

- in systems that fall under high-demand mode, the specified Safety function is triggered at a regular frequency
- low-demand mode systems generally only trigger the Safety function less than one per year, if at all

IEC 61508 provides precise probability specifications for the two modes. For example, a high-demand mode system would intercept certain regularly occurring hazardous situations in a chemical plant, such as avoiding pressure

peaks by opening a pressure relief valve. A low-demand mode would be an emergency stop system that stops operation in the event of a hazardous situation.

Several additional functional Safety standards build on IEC 61508, specializing and extending its concepts to meet the needs of specific segments and sectors. For instance, ISO 13849, widely used in various industrial applications, focuses on safe machinery.

3. The Situation in the Industry

Electrically programmable systems have been making their way into the industry for many decades, known as the third industrial revolution. While the second industrial revolution optimized mass production, the third revolution enabled electronically programmable systems such as articulated robots, which are used in the Automotive industry for the assembly of car parts or welding work, for example. With such systems, it quickly became clear not only what potential they held, but also that these systems require functional Safety in order to protect human lives.

The first sector standards emerged in highly critical areas such as the nuclear industry, which used semiconductor technology to control and monitor nuclear power plants. Other sectors followed suit, resulting in the original Safety standard for E/E/PE systems, IEC 61508, which is still valid across all industries today and from which many sector standards such as **EN 50657** for the railroad industry or **ISO 26262** for the Automotive industry have emerged.

The fourth industrial revolution is in full swing. Existing digitalized processes are becoming more efficient, more connected, more distributed and more autonomous. So, while the aforementioned robotic articulated arms were still fitting car doors to car bodies at high speed a few years ago, today they are increasingly networked, can be serviced remotely and provide information about their health status as well as coordinate with each other (partly autonomously).

Data is also collected for analysis and process optimization. This data serves as learning material for autonomous systems. Predictive maintenance, remote maintenance, autonomous operating and increased efficiency, combined with high availability, self healing, highly managed, auto provisioned software-defined systems, are therefore the concrete fields of action of this industrial revolution.

The convergence of **Information Technology (IT)** and **Operational Technology (OT)** is enabling an increase in Overall Equipment Effectiveness (OEE). This is happening gradually by replacing traditional serial-based with real-time Ethernet systems, so that there is a continuous high-bandwidth network between the control room/level down to the specific application on site to the field devices. These new real-time requirements, which these systems must fulfill, not only locally as individual modules, but also network-controlled in a network, enable a completely new orchestration basis for industrial plants. Time-Sensitive Networking (TSN) has therefore made headlines in recent years and is currently in the implementation phase for many players. To enable machines to communicate with each other, the **OPC Unified Architecture (OPC UA)** has existed for several years alongside well-known protocols such as, e.g. **MQTT (Message Queuing Telemetry Transport)**. Compared to MQTT, the further development of OPC UA over TSN has the advantage of being fully real-time capable. Efforts are also being made to make this open source, such as the open-source stack **open62541**, which is to be further developed so that TSN can be used.

4. Safety and Security

Making systems compliant against standards such as IEC 61508 however is not a trivial undertaking. In addition to the Safety objectives that must be defined, Security must also be considered because networked systems enable attack scenarios that can have serious consequences. As already mentioned, IEC 61508 also touches on the topic of Security, but without making more concrete specifications.

However, with **NIS2 (Network and Information Security Directive)** and the **Cyber Resilience Act (CRA)** and given the specific threat situation, a security architecture is no longer just an accessory, but a legal requirement and urgently needed. The following use-case illustrates what an industrial implementation could look like: It meets Safety requirements, is networked, has a Cybersecurity architecture and is real-time capable.

4.1 Use Case: Cyber-physical System Network of 6-Axis Robot Arms in Automotive Production

Hereafter, an exemplary 6-axis robot arm is used to explain the development of a cyber-physical system that meet real-time requirements and comply with the Safety requirements of IEC 61508. This could for example be the automation of a production line in the Automotive industry responsible for the assembly of vehicle chassis. In a modern Automotive production line, several of these robotic arms could perform various assembly tasks such as welding, sealing, painting and final assembly. The robot arms are connected via a highly integrated network, which enables efficient coordination and communication.

The technical specifications and requirements for such a system are extensive. The robot arms must be able to react to sensor information in milliseconds, in order to carry out precise movements and operations. This ability to react quickly is necessary to ensure high-precision during assembly and to avoid collisions between the individual robot arms. Synchronized coordination maximizes the efficiency of the assembly line.

Regarding the Safety requirements according to IEC 61508, the robots must be developed and certified according to the Safety integrity levels. As described above, this includes a comprehensive analysis to identify and mitigate all potential Safety risks. A conceivable risk scenario within the meaning of IEC 61508 could be, for example, that in the event of a collision between the robot arms, fragments could fly through the assembly hall like projectiles and injure people. This requires Safety mechanisms such as emergency stop functions. Limit sensors would also have to prevent the arms from being overloaded and a vision application could be used to enable safe coordination.

Cyber-physical integration requires the use of advanced control systems and algorithms for real-time data processing and analysis. A connection to the **Internet of Things (IoT)** enables continuous monitoring and optimization of production processes as well as remote maintenance and control room orchestration. **OPC UA over TSN** could now be used to communicate and network the systems, as could **EtherCAT (Ethernet for Control Automation Technology)** implementations. These protocols not only ensure real-time communication, but also create the foundations for the implementation of Cybersecurity resilient systems.

Functional Safety-compliant hardware and software systems are also required to meet real-time requirements and can leverage virtualization technology to implement workload consolidation. The basis would therefore be an SoC with sufficient performance to execute several Safety-critical processes in parallel and a suitable execution environment that orchestrates this on the software side. Traditionally, a hypervisor and a real-time operating system are therefore required. Hardware and software demonstrably fulfill Safety functions. The execution environment and hardware must be able to guarantee real-time communication - as mentioned using OPC UA over TSN for example.

The implementation of such a system requires the development and implementation of a user-friendly interface for monitoring and controlling the robot arms. Through this interface, operators can effectively manage the production process. This must be ensured by a suitable Integrated Development Environment (IDE) in which the corresponding applications can be developed, running on hypervisor and real-time operating system.

5. Functional Safety of the Integrated Circuits

The processor is a crucial part of a system, especially for the controller part, and its complexity can be hard if not impossible to deal with if a proper understanding of how it works internally is lacking. Such understanding includes not only failure rates and their distribution, but also how hardware, firmware, and software are able to avoid or control the occurrence of dangerous faults. Shared parts within the silicon require further attention, in order to address common cause failures and their effects, and how freedom from interference can be achieved requires dedicated analysis.

Intel designed the **x6000FE series processors** specifically for functional Safety applications. Several new features in the silicon make sure hardware failures are timely detected and reported, so that the system can take proper actions to switch into state. Such features, known as Intel® Silicon Integrity Technologies, include ECC, parities, CRC, error reporting and on-demand proof test flows, etc., that check the health of SoC blocks used by a Safety-critical applications.

Dedicated mechanisms take care of faults on shared parts that may generate common cause failures, that is affect multiple blocks in parallel or in cascade. Furthermore, a dedicated Intel® Safety Island is integrated in the SoC: It is in charge of orchestrating the internal diagnostics, monitoring, collecting, and reporting any faulty condition outside of the silicon boundary. It also provides additional features such as error logging.

Additional diagnostic software help reach the proper diagnostic coverage and Safety targets as required by IEC 61508 and also ISO 13849. Pre-OS Checker (POSC) software is also available to check that bootloader has performed the silicon initialization correctly, before the operating system or hypervisor take control of the hardware resources.

The **x6000FE series** Safety package fully documents all of these features. It includes the Safety manual with detailed description of the Safety features, the rigorous Safety process adopted for development and validation, possible Safety concepts targeting different standard and Safety targets and how to implement them, and most importantly all conditions of use that the system integrators have to fulfil in order to use the silicon properly. Information on the Safety analysis, including F**ailure Modes, Effects and Diagnostic Analysis (FMEDA)**, **Dependent Failure Analysis (DFA)**, and **Freedom From Interference Analysis (FFI)** is also provided.

The **x6000FE series** has been assessed and certified by third-party agency for single chip solutions up to SIL 2 according to IEC 61508 and Category 3 performance level according to ISO 13849. This will give system integrators full confidence when building their own solutions on top of this silicon (high-level diagram with main functional blocks is shown in Figure 2 below).

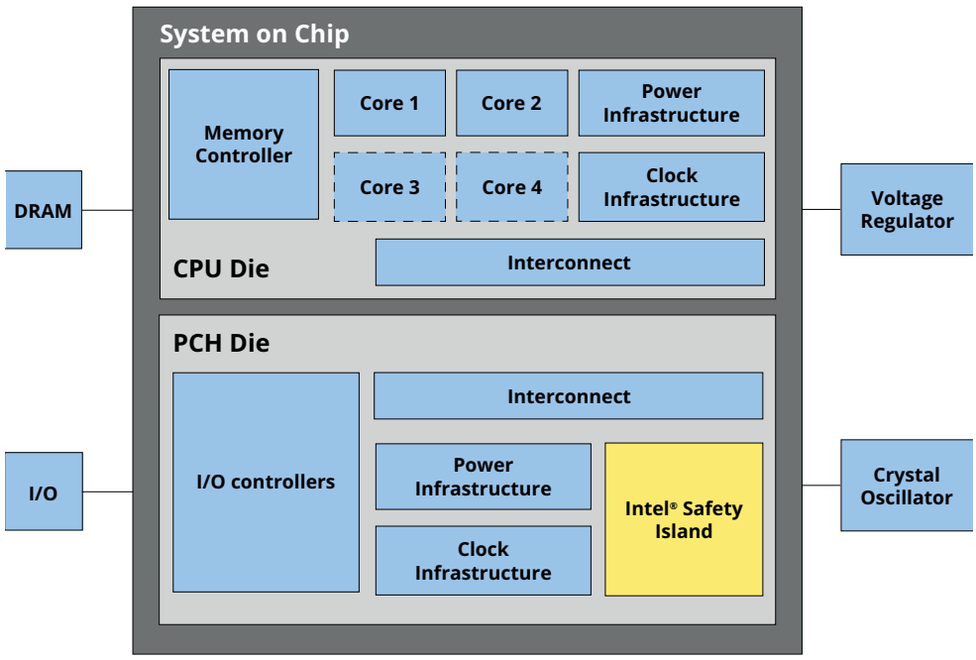

Figure 2: x6000FE series high-level block diagram

6. Functional Safety of the Software

There is a broad market of providers who supply execution environments. Most of these are individual solutions. The real-time operating system and hypervisor are often separate systems.

PikeOS, however, combines both of these features. This allows several real-time capable applications to run in parallel without causing interference. This is made possible by separating resources in space and time, so that, among other things, certain memory blocks are reserved for previously defined application blocks, also known as partitions or personalities.

The **PikeOS Safety concept** provides for this information on the partitions to be defined in advance in a master partition so that no changes can be made at runtime. This is an essential prerequisite for deterministic application behavior. For example, one partition could contain the motor control of a 6-axis robot arm, while communication via OPC UA over TSN takes place in a parallel partition on the same hardware. This also enables out-of-band communication for any remote maintenance or cold starts of the systems.

In this example, a health monitoring partition would monitor the status of the system. Another partition could contain the application of the vision solution, which has a connection to the vision sensor or the optics. Of course, it would also be conceivable to use a LiDAR sensor or MQTT as a communication protocol for machine-to-machine communication (M2M). The decisive factor here is that PikeOS fulfills the requirements of IEC 61508, as described in the third part (61508-3) in Annex F, among others. This requires temporal and local independence for software that runs on the same hardware and should not generate any interference. This evidence is available for PikeOS; PikeOS is certified at the highest level for software, SIL 3, against IEC 61508.

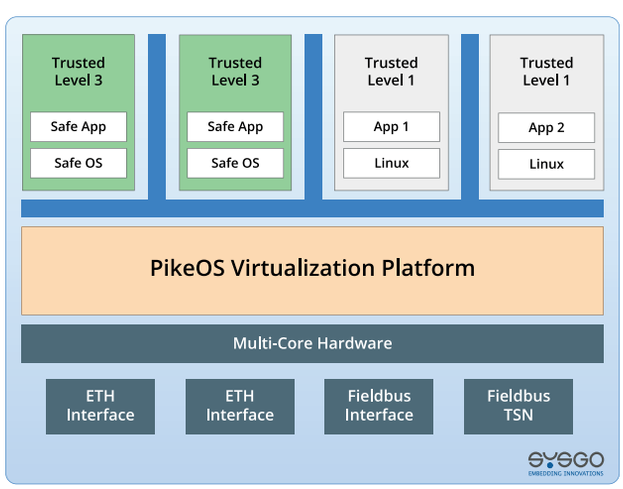

Figure 3: Example of a multi-core architecture performing applications or operating systems of different criticality

However, PikeOS is so flexible that - if necessary - communication can also take place between the partitions. The extent to which this is necessary is a question of the specific design of the application. In addition, the PikeOS Separation Kernel version 5.1.3 meets the requirements of the **Common Criteria Security standard** at the very high **EAL 5+** level for various architectures. Common Criteria is a

robust framework for evaluating and certifying the Security features of a product.

PikeOS covers more than 70% of the upper EAL 6 and 7 levels. Among other things, this includes the AVA_VAN class defined there at the highest level EAL 7 (Evaluation Assurance Level), which represents a vulnerability analysis. In addition, it demonstrates the comprehensive Security architecture of PikeOS, so that it is possible to prevent attacks resulting from networking as well as physical access, for example, using the on-board tools and configuration. This is done via an elaborate privilege system that is so comprehensive that even side-channel attacks, which are not checked in simple pen tests, are covered. Secure communication in real-time is thus functionally and cyber-securely possible.

7. Conclusion

This paper provided an overview of existing Safety requirements and ongoing market trends that will shape the industry in the years to come. Fulfilling Safety standards is a fundamental and demanding undertaking for any Safety-critical project.

Safety does not persist in isolation, much rather interacts with other system requirements such as Cybersecurity and real-time. Selecting the right components can substantially reduce the time to market and minimize the investment risk.

Intel Atom® x6000FE processor series, combined with SYSGO's real-time operating system and hypervisor PikeOS, provide the ideal building blocks to tackle the challenges of complex Safety projects.

Acknowledgment

This whitepaper benefited from the valuable contributions of Gabriele Boschi, Darshan Raj, Maurizio Iacaruso, Alex Klimovitski and Demetrius Whye (all from Intel) and Joe Richmond-Knight (from SYSGO).

SYSGO Headquarters
+49 6136 9948 500

SYSGO France
+33 1 30 09 12 70

SYSGO Czech Republic
+420 222 138 111

sales@sysgo.com

www.sysgo.com