Functional Safety and Industry 4.0

Tom Meany
Analog Devices, Inc.

Abstract

Industry 4.0 offers a new vision for the factories of the future. In these factories of the future, safety will be critical. Functional safety addresses confidence that a piece of equipment will carry out its safety functionality when required to do so. It is an active form of safety in contrast to other forms of safety. Integrated circuits are fundamental in the implementation of functional safety and, therefore, to Industry 4.0. This article explores the implications of functional safety for Industry 4.0. The implications include requirements for networks, security, robots/cobots, software, and the semiconductors used to implement these features.

Introduction

Functional safety is the part of safety that deals with confidence that a system will carry out its safety related task when required to do so. For instance, that a motor will shut down quickly enough to prevent harm to an operator who opens a guard door or a robot that should operate at a reduced speed and force when a human is nearby.

Industry 4.0 is the next evolution of manufacturing plants promising increased flexibility and reduces costs.

This article will explore some of the implications of functional safety for Industry 4.0.

Functional Safety

A. Standards

The basic functional safety standard is IEC 61508.[1] The first revision of this standard was published in 1998, with revision two published in 2010 and work beginning now to update to revision 3 for 2020. Since the first edition of IEC 61508 was published in 1998, the basic IEC 61508 standard has been adapted to suit fields such as automotive with ISO 26262,[2] process control with IEC61511,[3] programmable logic controls with IEC61131-6,[4] machinery with IEC 62061,[5] variable speed drives with IEC 61800-5-2,[6] and many other areas. These other standards help interpret the very broad scope of IEC 61508 for these more limited fields.

An important parallel standard not derived from IEC 61508 is ISO 13849,[7] which covers machinery that is derived from the obsolete European EN 954 standard.

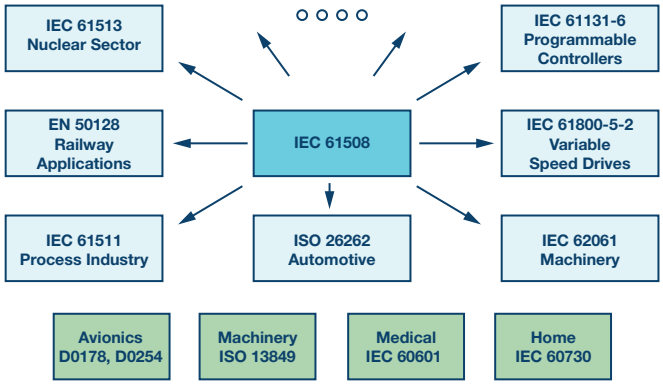

Figure 1. Sample of functional safety standards.

The more basic concept in functional safety is that of a safety function. A safety function defines an operation that must be carried out to achieve or maintain safety. A typical safety function contains an input subsystem, a logic subsystem, and an output subsystem. Typically, this means that a potentially unsafe state is sensed, and something makes a decision on the sensed values and, if deemed potentially hazardous, instructs an output subsystem to take the system to a defined safe state.

The time between the unsafe state existing to achieving a safe state is critical. A safety function might, for instance, consist of a sensor to detect that a guard on a machine is open, a PLC to process the data, and a variable speed drive with a safe torque off input that kills a motor before a hand inserted in a machine can reach the moving parts.

B. Safety Integrity Levels

SIL stands for safety integrity level and is a means to express the required risk reduction needed to reduce the risk to an acceptable level. According to IEC 61508, the safety levels are 1, 2, 3, and 4, with an order of magnitude increase in safety requirements as you go from one level to the next. SIL 4 is not seen in machinery and factory automation where generally no more than one person is typically exposed to a hazard. It is rather reserved for applications like nuclear and rail where hundreds or even thousands of people can be hurt. There are also other functional safety standards such as automotive, which uses ASIL (automotive safety integrity levels) A, B, C, and D, and ISO 13849. Its performance levels A, B, C, D, and E can be mapped to the SIL 1 to SIL 3 scale.

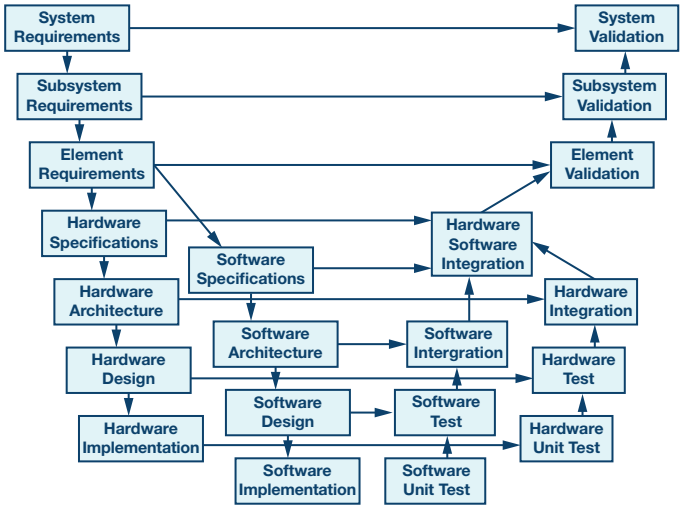

Figure 2. Example V model for a system-level design.

C. Sources of Failure

Functional safety standards generally recognize two types of failures and then propose the means to address them.

Random hardware failures are the easiest to understand in that they are caused by, as the name suggests, random unexpected failures in equipment. The probability of failure due to random failures is expressed as the PFH (average frequency of dangerous failure) for the system. The allowed PFH depends on the required SIL and ranges from 10^{-5}/h for SIL 1 to a minimum of 10^{-7}/h for SIL 3.

Systematic failures are those inherent in a design, in the sense that they can only be fixed by a design change. Insufficient EMC robustness can be considered a systematic error, as can deficiencies in requirements, insufficient verification and validation, and all software errors. Systematic errors are effectively weaknesses that exist in every item produced rather than being present in individual units. If the right set of circumstances arise, the failure will occur with 100% probability.

To be suitable for use in a situation requiring a SIL X safety function, both the random and systematic requirements given in the standard for that SIL level must be met. Compliance to the hardware requirements alone is not sufficient.

D. Dealing with Random Failures

No matter how reliable the equipment, everything has a finite chance of failing in any given hour. Techniques to combat random hardware failures include diagnostic coverage requirements and the use of redundancy. Depending on the SIL level for the safety function, there will be a minimum PFH or PFD (probability of failure on demand). Also, depending on the SIL, there will be a minimum required SFF (safe failure fraction) ranging from 60% to 99% as the SIL increases from SIL 1 to SIL 3. The standard allows a trade-off to be made between the diagnostics and the redundancy present in a system. Other techniques involve derating and the use of better quality components.

E. Dealing with Systematic Failures

Systematic failures are failures not related to a random hardware failure and can require a design change to avoid the failure.

Systematic failures are addressed by following a rigorous development process with independent reviews of the various work products. The process is often represented in V models of varying complexity. The required rigor of the reviews and the required independence of the reviewers increases with the SIL level.

In certain cases, systematic errors can be dealt with using diverse redundancy. This is because diverse systems are unlikely to fail in the same way at the same time. The diagnostics inserted to deal with random failures are also useful to detect systematic failures.

Much of the effort involves system engineering and good engineering practice. The expression used in some documents is “state of the art.” Documentation is vital and being able to prove safety was achieved is almost as important as achieving safety.

Industry 4.0

Industry 4.0[8] is known by other names, including Industrie 4.0, Industrial IoT (IIoT), made in China 2025, industry plus, smart factory, and others. The 4.0 in the name represents the claims that it represents the fourth industrial revolution following the third revolution from around 1970, when the widespread usage of electronics and IT began in automation.

While IoT for industry is a common topic in articles, conferences, and marketing efforts, it still lacks the killer application to bolster its adoption. Possible killer applications include predictive failure, adaptive diagnostics, and condition-based maintenance.

A key idea in Industry 4.0 is that of cyber-physical systems (CPS). A CPS consists of “smart machines, storage systems, and production facilities capable of autonomously exchanging information, triggering actions, and controlling each other independently.”[9] Put another way, everything is intelligent, instrumented, and interconnected. This definition has implications for networking and security among other concerns.

The key design principles of Industry 4.0 include

- Interoperability—everything is linked
- Virtualization—plant and simulation models available
- Decentralization—local intelligence
- Real-time capability—respond to the real world in real time
- Service orientation—services available via the internet
- Modularity—reconfigurable as required

With sensor fusion and data analytics, new insights will be gained, including preventative maintenance based on diagnostics gathered from smart instruments and its analysis in the cloud. Comparison of aging between systems can also allow for the switching in of redundant items to increase productivity. Machine health will be a key concern.

A. Networking

Older systems tended to use isolated islands of automation—typically using proprietary networks. Analog networking based on 4 mA to 20 mA circuits was and is still common and has many benefits including EMC robustness, a range up to 3 km, and it is intrinsically safe and synchronized but is not flexible or fast enough for Industry 4.0.

With Industry 4.0, the desire is to have everything connected and talking to everything else. Common terms include M2M (machine to machine) and P2M (process to machine). The connectivity can then be exploited to

- Increase manufacturing efficiency
- Increase manufacturing flexibility
- Increase operational knowledge
- Drive down production costs

Ethernet-based connectivity solutions are well placed to address the above requirements, but the safety and security requirements of such networks need to be addressed. With the new efficiencies, new services will become cost-effective.

B. Security

With the use of digital networks, security becomes an issue. Recent cases highlighted in film (for example, *Zero Days*) and the media include the Stuxnet and black energy viruses. If the network extends out into the cloud, then hacking one cloud provider could bring down many factories, whereas previously they would have to be hacked one at a time. This economy of scale makes them a much more attractive proposition for hackers. Some pundits have even claimed IoT really stands for "Internet of Threats."

IT security requirements are not generally suitable for application to industrial networks. IT security has several behaviors, including frequent software updates that are not suitable for manufacturing, where software changes are frowned upon due to the risk of unintended consequences stopping production. This abhorrence to change is even stronger when safety is involved due to the high cost of certifying functional safety systems and the required change management processes.

The proposed international consensus standard covering security requirements for industrial control is IEC 62443. IEC 62443[10] covers the design, implementation, and management of IACS (industrial automation and control systems).

C. Robots and Cobots

Robots used to be big scary machines that lived in cages. Cobots or collaborative robots are much less scary and take care not to hurt people. They are a fusion of sensors and software with no need to be separated from human workers. Cobots in an industrial environment could consist of an arm or pair of arms, such as the UR5 series from Universal Robots or ABB's YuMi®. In the factory of the future, cobots will assist the human operator and even know whether the person they are working with is right or left handed.

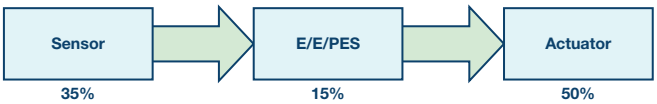

Figure 3. Error budget for a typical safety system.

AGV (automated guided vehicles) are mobile robots and could be considered a special kind of cobot. They provide an essential element for Industry 4.0 by moving product and materials around the manufacturing floor.

As new hazards arrive because of the dynamic environment, they must be addressed. For both cobots and AGV, the options are 1) to develop an inherently safe system because the forces are sufficiently low that no serious harm can occur, or 2) to engineer a solution based on the relevant functional safety standards. For AGV, collision avoidance can be based on vision, radar, lasers, or tracks embedded in the floor.

Functional Safety and Networking

A functional safety system typically consists of sensor, logic, and output subsystems. The three elements combine to implement a safety function and it is to the safety function as a whole that the SIL level, PFH, SFF, and HFT requirements apply. The communication between these subsystems is therefore safety related. IEC 61508 refers to IEC 61784-3, a fieldbus standard, for the functional safety requirements. These will include measures to deal with random and systematic error sources.

A commonly accepted error budget for the allocation of the maximum allowed probability of failure per hour is shown in Table 1. Refinements of this model often show 1% of the budget allocated to each of the interfaces shown in red. If the safety function is SIL 3, then the maximum allowed PFH is 10^{-7}/h, so the 1% allocation to the interfaces is 10^{-9}/h.

In total, the hazards related to communications that must be considered are shown in Table 1, which is contained in standards including IEC 61784, EN 50159, and IEC 62280.[11]

Each row in Table 1 must be addressed by at least one of the defenses. Further elaboration on the defenses is given in IEC 61784-3[9] and IEC 62280-1/EN 50159.[12] For instance, corruption might be dealt with by the use of a CRC with a Hamming distance dependent on the expected BER (bit error rate), SIL requirement, and number of bits transmitted per hour.

The requirements are further complicated by the fact that in an industrial environment, it is considered very advantageous if safety and nonsafety data can be communicated on the same network.

IEC 61508-2:2010 offers two options. Option 1) is the white channel approach, where the entire communication channel is developed to IEC 61508. Option 2) is the black channel approach, whereby no assumptions are made on the performance of the communications channel and safety is dealt with by a special layer in each safety device. This safety layer addresses the threats from Figure 2 with a set of defenses. These defenses are in addition to any defenses within the underlying fieldbus standard and might, for instance, include another CRC to detect bit corruption in addition to the CRC within the underlying communications protocol. The black channel approach is by far the more common. One example is PROFIsafe, which is a safety layer that sits on top of either PROFIBUS® or PROFINET®.

Functional Safety and Security

It is interesting that in many languages there is only one word for security and safety. However, in the industrial context, they both cover a different set of concerns that are sometimes in conflict. One definition of safety is that it prevents harm due to unintentional actions, while the corresponding definition of security is that it prevents harm due to intentional actions. Commonalities between the two include the fact that safety and security need to be considered at the architecture level. Otherwise they are very difficult to add in afterward. But the two conflict because the typical safety reaction to an unexpected event is to shut the system down—a feature that hackers can exploit through denial of service attacks, and which security is meant to protect against. Security features typically include passwords for authentication, but do you really want to slow down a safety reaction while somebody types in a password or lock the safety guy out if the password is entered wrong three times?

Revision two of IEC 61508 from 2010 contains almost no security requirements. It does state that security must be considered and references the as of yet unreleased IEC 62443 series for guidance. In addition, there are specific standards currently being written to address the relationship between functional safety and security in the machinery and nuclear domains.

Table 1. Threats and Defenses in a Network

Threats	Defenses							
	Sequence Number	Time Stamp	Time Out	Source and Destination Identifiers	Feedback Message	Identification Procedure	Safety Code	Cryptographic Techniques
Repetition								
Deletion								
Insertion								
Re-Sequence								
Corruption								
Delay								
Masquerade								

Similar to the SIL levels within IEC 61508, IEC 62443 defines SL (security level) where the levels are also 1 to 4. A system that meets SL 1 might be secure to a casual bystander, whereas a system that meets SL 4 might be secure to hacking attempts by state sponsored bodies. However, there is no direct mapping from SIL to SL.

IEC 62443 identifies seven fundamental requirements (FR) with IEC 62443-4-2 to give guidance on what is required for each FR to achieve a given SL. The seven FR are:

- Identification and authentication control (IAC)
- Use control (UC)
- System integrity (SI)
- Data confidentiality (DC)
- Restricted data flow (RDF)
- Timely response to events (TRE)
- Resource availability (RA)

SL 1 can then be represented as a security vector (1, 1, 1, 1, 1, 1, 1) where each item in the vector corresponds to one of the seven FR. Given that SL 1 represents casual attacks, that would seem the minimum requirement for a safety application where foreseeable misuse must be considered.[13] It can be argued that a suitable vector for safety applications with a SIL > 1 is (N_1, N_2, N_3, 1, 1, N_6, 1),[13] where it is recognized that data confidentiality, restricted data flow, and availability are of limited concern in industrial functional safety applications. However, there is no clear correlation between the values for N_1, N_2, N_3, and N_6 depending on whether the SIL level is 2, 3, or 4.

A key point to remember is that while not all security systems have functional safety requirements, security needs to be considered for all safety related systems.

Functional Safety and Robots

ISO 10218[14] is the standard covering the safety requirements for industrial robots including cobots. It covers safe stopping, teaching, speed, and separation monitoring, along with power and force limiting. ISO 10218-1:2011 clause 5.4.2 requires that safety-related parts of the control system be designed to comply with PL = D Category 3 as described in ISO 13849-1:2006 or SIL 2 with a HFT (hardware fault tolerance) of 1 as described in IEC 62061:2005. In effect, this means at least a 2-channel safety system with diagnostic coverage of at least 60% for each channel. Both standards (ISO 13849 and IEC 62061) defer to IEC 61508-3 for software requirements.

AGV are not well addressed in ISO 10218, and while driverless cars are addressed in the automotive standard, ISO 26262, the industrial usage is a special case of automotive given its far more restricted scope. The machinery directive scope includes AGV and, given the lack of a specific standard, the requirements of the generic IEC 61508 standard will apply.

Figure 4. Key benefit of software.

While networking will likely be Ethernet-based for fixed robots, it will be wireless for AVG, which will necessitate additional safety and security requirements.

Functional Safety and Software

The detailed requirements to implement high quality software are mostly the same regardless of whether you are dealing with safety or security. For instance, a software error by a programmer may lead to a system failure if the right set of circumstances arise to expose the error. It is hard to judge the probability of this, and some functional safety standards state the probability should be considered as 100%.[15] However, while it seems reasonable that a 99.99% bug free program will normally not cause a safety problem, a hacker will try to ensure that the 0.01% instance is always encountered. Therefore, the elimination of systematic errors is as important for security as for functional safety. However, it is true that 100% perfect safety related software could have gross security issues.

In the past, the use of software was not allowed in safety systems as it was deemed inherently untestable due to the number of different states it presents. The new standards offer a life cycle model that, if followed, allow a claim for safety to be made because the techniques advocated in those standards have been shown to produce safe systems in the past. Software is inherently attractive because it allows a general-purpose machine to be transformed into a very specific machine. However, this flexibility is also one of its weaknesses.

Documents such as ESDA-312[16] show that many of the techniques from IEC 61508 can be used to meet industrial security requirements. Following such a process leaves a paper trail of work products that can be used to demonstrate that safety has been achieved.

These techniques include doing design reviews, having a coding standard, planning the use of tools, verification at the unit level, requirements traceability, independent verification, and assessment. While software does not wear out, the hardware on which it runs can fail and the software needs to take care of this. For machines and robots, the use of redundant architectures such as Cat 3 or Cat 4 from ISO 13849 reduces the need to implement diagnostics at the IC level, but does raise the requirement to have diverse software.

Functional Safety and Integrated Circuits

Integrated circuits (ICs) are vital to smart systems. ICs can provide the means to track the items in a container rather than the container itself, track the position of robot arms rather than just the entire robot, track the health of even low value machines, and process data so that what is transmitted into the cloud is information rather than data. New motor control ICs can increase motor efficiencies and extend battery life.

ICs provide the brains and, especially out at the edge, the intelligence needs to be compact and low power. They also provide sensor technology; for instance, using radar, laser, magnetic, camera, or ultrasonic techniques. They can measure speed and position, and with new technologies such as AMR (anisotropic magnetoresistance), sensors can determine speed and position without external mechanical components. ICs implement both the physical interface and the MAC (media access control) layers in networks. With wireless communication, this implementation can all be done on an IC.

Similarly, integrated circuits can support security with PUF (physically unclonable functions), cryptographic accelerators, and tamper detection mechanisms. Given the level of integration now possible, what used to be system-level requirements in many cases have become IC level requirements.

However, there is little enough on integrated circuits in the present industrial functional safety standards and even less in the security standards. For automotive, the draft of ISO 26262-11 planned for 2018 is an excellent resource and much of it is useful for integrated circuits intended for industrial applications also. In revision 2 of IEC 61508, an ASIC lifecycle model is presented that is almost identical to that for software. In fact, the argument as to whether HDL code such as Verilog is software or just a representation of hardware is an interesting one. Annex E of IEC 61508-2:2010 deals with the requirements to claim on-chip redundancy if using a single piece of silicon, but is limited to digital circuits only, and for the case of duplication, except it does not cover diverse redundancy or analog and mixed-signal circuits. The informative Annex F of IEC

61508-2:2010 is extremely useful as it gives a list of measures to be taken during IC development to avoid introducing systematic errors. The requirements are given for each SIL, but once again it is limited to digital circuits with no specific guidance on analog or mixed-signal ICs.

The high level of integration available with an IC can be both a blessing and a curse. Individual transistors on an IC are extremely reliable when compared to individual components, with the most unreliable aspect of an IC often being the pins. For instance, if the Siemens SN 29500 standard is used for reliability prediction, then an IC with 500k transistors will have a FIT of 70, but this increases to only 80 if the number of transistors increases by a factor of 10 to 5 million. If instead two ICs, each with 500k transistors, are used, the FIT would be 70 for each, for a total of 140. The savings from 140 to 80 is before you also consider the savings in PCB area, PCB tracks, and external passives or that the on-chip antennas on an IC are so much smaller than on a PCB that EMI issues can be reduced. The curse part of the equation is that with a complex IC, determining the failure modes can be difficult. Simplicity is the friend of safety and it is more likely that two separately packaged microcontroller would be considered as simpler than an IC containing two microcontrollers. Annex E of IEC 61508-2:2010 gives some guidance. However, in claiming sufficient independence and in most safety standards, a β (measure of both channels failing at the same time for the same reason) of less than 10% is considered very good.

IC suppliers can help both their safety and security suppliers by supplying certified components, safety manuals, or safety data sheets for released parts, on-chip hardware accelerators, on-chip and off-chip diagnostics, and the means to separate critical and noncritical software (both safety and security critical). These safety and security features need to be designed in from the start. Trying to add safety and security after the ICs are designed will lead to extra system complexity and additional components.

There are several options for developing integrated circuits to be used in functionally safe systems. There is no requirement in the standard to only use compliant integrated circuits, but rather the requirement is that the module or system designers satisfy themselves that the chosen integrated circuit is suitable for use in their system. Having an independently assessed safety manual is one way to be satisfied, but not the only option.

The available options include:

- Develop the IC fully in compliance to IEC 61508 with an external assessment and safety manual
- Develop the IC in compliance to the IEC 61508 without external assessment but with a safety manual
- Develop the IC to the semiconductor companies standard development process but publish a safety data sheet
- Develop the IC to the semiconductor companies standard process

Note—for parts not developed to IEC 61508, the safety manual may be called a safety data sheet or similar to avoid confusion. The content and format in both cases will be similar.

Option 1 is the most expensive option for the semiconductor manufacturer, but it also offers potentially the most benefit to the module or system designer. Having such a component where the application shown in the safety concept for the integrated circuits matches that of the system cuts the risk of running into problems with the external assessment of the module or system. The extra design effort for a SIL 2 safety function can be on the order of 20% or more. The extra effort would probably be higher, except that semiconductor manufacturers typically already imply a rigorous development process even without functional safety.

Option 2 saves the cost of external assessment, but otherwise the impact is the same. This option can be suitable where customers are going to get the module/system externally certified anyway and the integrated circuit is a significant part of that system.

Option 3 is most suitable for already released integrated circuits where the provision of the safety data sheet can give the module or system designer access to extra information that they need for the safety design at the higher levels. This include information such as details of the actual development process used, FIT data for the integrated circuit, details of any diagnostics, and evidence of ISO 9001 certification for the manufacturing sites.

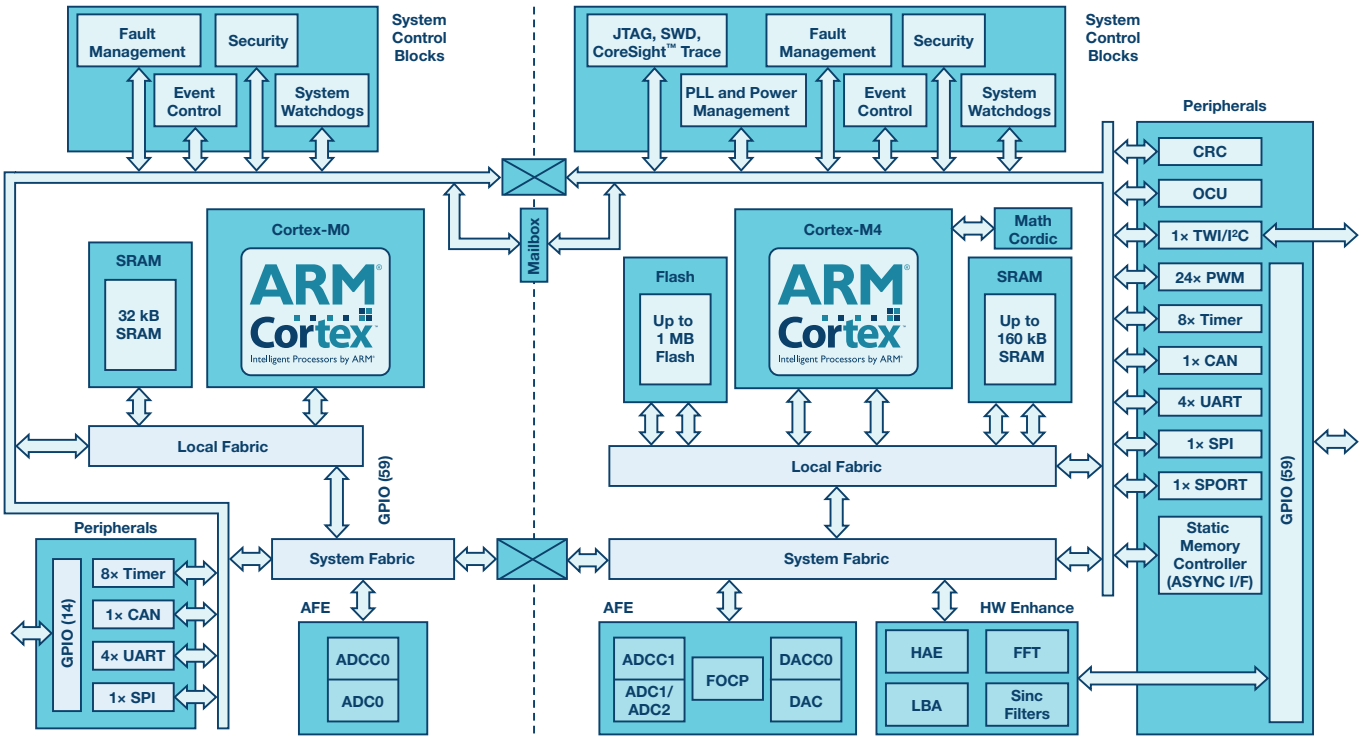

Figure 5. The ADSP-CM41x series from ADI with many safety and security features.

Option 4 will, however, remain the most common way to develop integrated circuits. Use of such components to develop safety modules or systems will require additional components and expense for the module/system design because the components will not have sufficient diagnostics requiring dual-channel architecture with comparison as opposed to single channel architectures. In addition, the diagnostic test intervals with such components will generally be suboptimal and the availability less as it will not be possible to identify which of the failing items has failed, which can have an impact on availability. Without a safety data sheet, the module/system designer will also need to make conservative assumptions treating the integrated circuit as a black box. This may reduce the reliability numbers that can be claimed.

To simplify implementing functional safety, IC manufacturers may wish to develop their own interpretation of IEC 61508. At Analog Devices, there is an internal company specification, ADI61508, which is the interpretation of IEC 61508 for an integrated circuit development. All seven parts of IEC 61508 are then interpreted in one document with the bits of IEC 61508 not relevant to an integrated circuit omitted and the remaining bits interpreted for an integrated circuit.

No matter which system level standards apply, ICs are developed to IEC 61508 with the one exception being automotive, where ISO 26262 can be used to develop ICs and software for automotive applications.

Summary

Industrial in general and Industry 4.0 are well served by various functional safety standards based on IEC 61508. These include standards for software, hardware, networking, security, and robotics. However, the information is currently spread across multiple standards, and Industry 4.0 has several unique features related to constant change that required due to the flexibility needed by Industry 4.0. It may be that a single focused standard for Industry 4.0 is warranted to simplify compliance using an interpretation of the basic safety standards for the new world. Perhaps this can be called "Safety 4.0" or "Smart safety"! Similarly, more IC-related information is required in the IEC 61508 standard to allow for sufficient safety to be demonstrated as well as achieved. Going forward, the opportunities and challenges before Industry 4.0 becomes a reality and a success will be interesting to behold.

Functional safety has a lot to offer Industry 4.0, not just because safety is an essential element of future factories, but also because functional safety has the techniques to enable higher reliability, diagnostics, resilience, and redundancy.

References

[1] IEC 61508 All Parts, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. International Electrotechnical Commission, 2010.

[2] ISO 26262 All Parts, Road Vehicles Functional Safety. International Organization for Standardization 2011.

[3] IEC 61511 All Parts, Functional Safety—Safety Instrumented Systems for the Process Industry Sector. International Electrotechnical Commission, 2016.

[4] IEC 61131-6 Programmable Controllers—Part 6: Functional Safety. International Electrotechnical Commission, 2012.

[5] IEC 62061—Safety of Machinery—Functional Safety of Safety-Related Electrical, Electronic, and Programmable Electronic Control Systems. International Electrotechnical Commission, 2005.

[6] IEC 61800-5-2 Adjustable Speed Electrical Power Drive Systems—Part 5-2: Safety Requirements—Functional. International Electrotechnical Commission, 2016.

[7] ISO 13849 All Parts, Safety of Machinery—Safety-Related Parts of Control Systems. International Organization for Standardization, 2015.

[8] "Recommendations of Implementing the Strategic Initiative Industrie 4.0: Final Report of the Industrie 4.0 Working Group." Forchungsunion and acatech, April 2013.

[9] IEC 61784-3 Industrial Communication Networks—Profiles— Part 3: Functional Safety Fieldbuses—General Rules and Profile Definitions. International Electrotechnical Commission, 2016.

[10] ISO/IEC 62443 All Parts, Security for Industrial Automation and Control Systems.

[11] IEC 62880, Railway Applications—Communication, Signaling, and Processing Systems—Part 1: Safety-Related Communication in Closed Transmission Systems. International Electrotechnical Commission, 2017.

[12] EN 50159, Railway Applications—Communication, Signaling, and Processing Systems—Part 1: Safety-Related Communication In Closed Transmission Systems. European Committee for Electrotechnical Standardization, September 2010.

[13] Jens Braband. "What's Security Level got to do with Safety Integrity Level?" 8th European Congress on Embedded Real-Time Software and Systems (ERTS 2016), January 2016.

[14] ISO 10218-1, Robots and Robotic Devices—Safety Requirements for Industrial Robots—Part 1: Robots. International Organization for Standardization, 2011.

[15] Chris Hobbs. *Embedded Software Systems For Safety Critical Systems.* Auerback Publications, October 2015.

[16] ISA Security compliance institute—EDSA-312—Embedded Device Security Assurance—Software Development Security Assessment. International Electrotechnical Commission, July, 2016.

About the Author

Tom is a 30-year veteran of Analog Devices and he holds a B.Eng. first class in electronics and an M.Sc. first class in applied mathematics and computing. Tom is the holder of eight U.S. patents and is a certified TÜV Rheinland functional safety engineer in the area of machinery. Tom is a member of various IEC working groups in the area of functional safety, including those related to IEC 61508-2, IEC 61508-3, and IEC 61800-5-2. He can be reached at *tom.meany@analog.com*.

Analog Devices, Inc.
Worldwide Headquarters

Analog Devices, Inc.
One Technology Way
P.O. Box 9106
Norwood, MA 02062-9106
U.S.A.
Tel: 781.329.4700
(800.262.5643, U.S.A. only)
Fax: 781.461.3113

Analog Devices, Inc.
Europe Headquarters

Analog Devices GmbH
Otl-Aicher-Str. 60-64
80807 München
Germany
Tel: 49.89.76903.0
Fax: 49.89.76903.157

Analog Devices, Inc.
Japan Headquarters

Analog Devices, KK
New Pier Takeshiba
South Tower Building
1-16-1 Kaigan, Minato-ku,
Tokyo, 105-6891
Japan
Tel: 813.5402.8200
Fax: 813.5402.1064

Analog Devices, Inc.
Asia Pacific Headquarters

Analog Devices
5F, Sandhill Plaza
2290 Zuchongzhi Road
Zhangjiang Hi-Tech Park
Pudong New District
Shanghai, China 201203
Tel: 86.21.2320.8000
Fax: 86.21.2320.8222