Changes in IEC 61511 Ed 2

YOKOGAWA Co-innovating tomorrow™

1 Introduction

As known IEC 61511 is the applicable standard for functional safety in the process industry. Defining the requirements for the specification, design, installation, operation and maintenance of a safety instrumented system (SIS), so that it can be confidently entrusted to achieve a safe state of the process. IEC 61511 is developed as a process sector implementation of IEC 61508, the so-called mother standard.

IEC 61511 is the leading standard for our clients, the process plant owners / operators, and for suppliers of Safety Instrumented Systems like our company Yokogawa .
In the beginning of 2016 a new version of the IEC 61511 standard was released. It is called “Edition-2”. Yokogawa is one of the voting members of the European IEC 61508 and IEC 61511 committees, represented by Ando Tadaaki, Elena Mauro and Arian Slagt.

This new edition is in general more precise than the old one. It gives a better description of tasks that must be done, and the way they should be done. This will help to understand the intention of the standard much better.

Many items are unchanged in the new version, like the relation with IEC 61508 and the safety lifecycle.

Also many of the changes are editorial or giving more explanation, e.g.

- The new version is more consistent with IEC 61508-Ed.2
- Safety Application “Software” is consistently renamed into “Application Programming”. When software is mentioned, internal software/firmware is meant.
- More emphasis is placed on functional safety assessments and audits

But there are also important other changes. These can be found in the following sections.

2 Management of functional safety

The requirements on competence are added. For Yokogawa this has no consequences as this subject is covered sufficiently by our internal procedures already. But end-users should carefully verify if they comply with this requirement. Each person must be proven competent for his function, and each function must be clearly specified.
There is more emphasis on assessments and audits. But again this is covered already within Yokogawa regarding engineering. In the sections on Operation and Maintenance this results in more requirements on the end-user to organize regular assessments and audits.

New is the requirement that vendors (also manufacturers of devices and/or sub-system) must have a Functional Safety Management system in place. Before only a quality system was required. The measurement of the achieved quality is referred to as Systematic Capability. This might imply that your vendor evaluation procedures must be re-checked.
The so-called Grandfather clause is included in the standard. This effects only existing plants: it is now required that the end-user shows that his existing plant is safe.

3 Safety lifecycle

The overall safety life cycle figure is moved into section 6: Safety life-cycle requirements. Also the life cycle figure for the application program is now moved into this section. It makes the definition of the safety life-cycle more logical and consistent.

4 Process Hazard and Risk assessment

During the Hazard and Risk Assessment now there is the requirement that cyber security risks must be included. It is end-user responsibility. In the Yokogawa Safety Validation Plan already a section is dedicated to this subject.

5 Safety Requirement Specification

In the section on the Safety Requirement Specification (SRS) a new section is added addressing the application program safety requirements. It states that depending on the SRS and the SIS architecture the requirements for the application program must be specified. It is not completely clear who must write these application requirements and when to do so, because these requirements might depend on the logic solver to be selected and also on the definition fo the safety functions.

6 SIS Design and Engineering

The most visible change in the Edition-2 is the table on the Hardware Fault Tolerance. The previous system using the Safe Failure Fraction for the logic solver is abandoned. Also the difference between prior-use and non-prior-use is removed. For all sub-systems there is only one table left, which is now the same as IEC 6108-Ed2 route 2H. Alternatively compliance with IEC 61508-Ed 2 route 1H can be used. For all used devices prior-use must be shown, or compliance with IEC 61508. Note that the requirements for prior-use still are not very precise. Note also that a logic solver for SIL3 cannot be claimed based on prior-use, it must be in accordance with IEC 61508 route 1H.

7 SIS Application program development

The section on application program development has been re-written completely. A significant change is the use of the wording “application program” instead of “software.” At Yokogawa, like all SIS suppliers, we do not design software for safety systems (although this word is often miss-used) but we design, test and deliver the safety application program. Resulting in either a source code list to be downloaded to the ProSafe-RS or a wiring list to wire the application logic of our ProSafe-SLS. So it’s good that the IEC 61511 standard now is using this wording consistently.
Also the way the application program has to be designed and tested is completely rewritten, and is much better described now.
All previous requirements for verification and validation are moved to another section.
FAT is no longer an option but a requirement. There are some changes in the text. When no integrated FAT in the office is conducted special care must be taken to comply with the requirements of the standard.

8 Operation and Maintenance

The standard pays much more attention to the operation and maintenance of the safety system during the normal use of the plant. It puts many requirements on the end-user regarding the way he operates his facilities, the procedures that must be in place, training of operators and maintenance engineers, testing that must be performed and many more issues. The end-user must have a well-organized Functional Safety Management system in place. Many, if not all, end-users will have to check if they are in compliance with this new standard. Of course Yokogawa can advise and assist them in this area for lifetime safety assurance, consultancy and education.

9 Conclusion

In practice the Yokogawa way of executing safety projects is well in line with the new IEC 61511 - Ed2 (2016) standard.
The end-user however should carefully check if his current way of operating and maintaining his plant is in compliance with the new standard.
When you have any question about the safety standards or functional safety in general, please contact one of the members of the safety assurance group via safety.assessments@nl.yokogawa.com or contact your local Yokogawa office.

Overview of changes in IEC 61511 - Ed2 Part 1

General		Many figures have a different number
		SIS life cycle is now Fig 7
Chapter	3	Abbreviations and Definitions
	--	More definitions
	3.2.42	Continuous mode better defined
Chapter	4	Conformance
	--	Almost unchanged
Chapter	5	Management of functional Safety
	--	Some changes
	5.2.2.3	Procedure for competency required
	5.2.5.2	Suppliers of devices must have FSM
Chapter	6	Safety lifecycle requirements
	6.2.4	Modification of earlier stage
	6.3	New: Application program SIS safety lifecycle
Chapter	7	Verification
	7.2.2	New: requirements on testing
	7.2.5	New: impact analysis on modifications needed
Chapter	8	Process Hazard and Risk assessment
	8.2.4	New: security risk
Chapter	9	Allocation of safety functions
	9.2.5/6	More restrictions on SIL4
Chapter	10	SIS safety requirement specification
	10.3.2	New: section on application program requirements
Chapter	11	SIS Design and Engineering
	11.3	Major changes
	11.4	HFT has only 1 table for logic solver and devices.
	11.5	Devices must be IEC 61508 or prior-use
	11.9	Calculation is required, nothing very special
Chapter	12	SIS Application program development
	--	Completely redesigned
	--	Much smaller (and better) now
	12.2	General requirements
	12.3	Application program design
	12.4	Application program implementation
	12.5	Application program verification
	12.6	Methodology and tools

Chapter	13	FAT
	--	FAT is also called Integration test
	13.2	The need for FAT shall be specified
Chapter	14	SIS installation and commissioning
	--	Expanded a little
Chapter	15	Safety validation
	--	Expanded a little
Chapter	16	SIS operation and maintenance
	--	More requirements (on the end-user)
Chapter	17	SIS modification
	--	More requirements (on the end-user)
Chapter	18	SIS decommissioning
	--	No major changes
Chapter	19	Information and documentation
	--	No major changes