AS IEC 61131.6:2014

Australian STANDARD

Programmable controllers

Part 6: Functional safety

STANDARDS Australia

This Australian Standard® was prepared by Committee IT-006, Industrial Process Measurement, Control and Automation. It was approved on behalf of the Council of Standards Australia on 28 May 2014.
This Standard was published on 27 June 2014.

The following are represented on Committee IT-006:

- Australia Safety Critical Systems Association
- Australian Computer Society
- Australian Industry Group
- Australian Petroleum Production and Exploration Association
- Consult Australia
- Engineers Australia
- Institute of Chemical Engineers Australia
- Institute of Instrumentation, Control and Automation
- Process Control Society
- The University of Queensland
- Workplace Health and Safety Queensland

This Standard was issued in draft form for comment as DR 102270.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting www.standards.org.au

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard®

Programmable controllers

Part 6: Functional safety

First published as AS IEC 61131.6:2014.

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 978 1 74342 781 1

PREFACE

This Standard was prepared by the Standards Australia Committee IT-006, Industrial Process Measurement, Control and Automation.

The objective of this Standard is to specify product-specific requirements of AS 61508.1—2011, AS 61508.2—2011 and AS 61508.3—2011 for functional safety programmable logic controllers (FS-PLC) and their associated peripherals. Some aspects do not have a direct correlation with the AS 61508 series structure and are addressed somewhat differently. In part, this is due to addressing hardware, software, firmware, etc., in a single document.

This Standard should be read in conjunction with the other parts of the AS 61131 series.

This Standard is identical with and has been reproduced from IEC 61311-6, Ed.1.0 (2012) *Programmable controllers*, Part 6: *Functional Safety*.

As this Standard is reproduced from an International Standard, the following applies:

(a) Its number appears on the cover and title page, while the International Standard number appears only on the cover.

(b) In the source text, 'this part of IEC 61131' should read 'this Australian Standard'.

(c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

Reference to International Standard		*Australian or Australian/New Zealand Standard*	
IEC		AS	
60947-5-1	Low-voltage switchgear and controlgear—Part 5-1: Control circuit devices and switching elements—Electromechanical control circuit devices	60947.5.1	Low-voltage switchgear and controlgear—Control circuit devices and switching elements—Electromechanical control circuit devices
61508	Functional safety of electrical/electronic/programmable electronic safety related systems	61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
61508-1	Part 1: General requirements	61508.1	Part 1: General requirements
61508-2	Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	61508.2	Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
61508-3	Part 3: Software requirements	61508.3	Part 3:Software requirements
61508-6	Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3	61508.6	Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
IEC		AS IEC	
61131	Programmable controllers	61131	Programmable controllers
61131-1	Part 1: General information	61131.1	Part 1:General information
61131-2	Part 2: Equipment requirements and tests	61131.2	Part 2:Equipment requirements and tests
61131-4	Part 4: User guidelines	61131.4	Part 4:User guidelines

IEC		AS/NZS	
61000	Electromagnetic compatibility (EMC)	61000	Electromagnetic compatibility (EMC)
61000-4-5	Part 4-5: Testing and measurement techniques—Surge immunity test	61000.4.5	Part 4.5: Testing and measurement techniques—Surge immunity test
61000-4-8	Part 4-8: Testing and measurement techniques—Power frequency magnetic field immunity test	61000.4.8	Part 4.8: Testing and measurement techniques—Power frequency magnetic field immunity test
IEC		AS/NZS IEC	
61000	Electromagnetic compatibility (EMC)	61000	Electromagnetic compatibility (EMC)
61000-4-2	Part 4-2: Testing and measurement techniques—Electrostatic discharge immunity test	61000.4.2	Part 4.2: Testing and measurement techniques—Electrostatic discharge immunity test
61000-4-3	Part 4-3: Testing and measurement techniques—Radiated, radio-frequency, electromagnetic field immunity test	61000.4.3	Part 4.3: Testing and measurement techniques—Radiated, radio-frequency, electromagnetic field immunity test
61000-4-4	Part 4-4: Testing and measurement techniques—Electrical fast transient/burst immunity test	61000.4.4	Part 4.4: Testing and measurement techniques—Electrical fast transient/burst immunity test

Only normative references that have been adopted as Australian or Australian/New Zealand Standard have been listed.

The terms ‘normative’ and ‘informative’ are used to define the application of the annex to which they apply. A normative annex is an integral part of a standard, whereas an informative annex is only for information and guidance.

CONTENTS

Page

Page

Page

INTRODUCTION

General

IEC 61131 series consists of the following parts under the general title *Programmable controllers*:

Part 1: General information
Part 2: Equipment requirements and tests
Part 3: Programming languages
Part 4: User guidelines
Part 5: Communications
Part 6: Functional safety
Part 7: Fuzzy control programming
Part 8: Guidelines for the application and implementation of programming languages

This Part of IEC 61131 series constitutes Part 6 of a series of standards on programmable controllers and the associated peripherals and should be read in conjunction with the other parts of the series.

As this document is the FS-PLC product standard, the provisions of this part should be considered to govern in the area of programmable controllers and their associated peripherals.

Compliance with Part 6 of IEC 61131 cannot be claimed unless the requirements of Clause 4 of this part are met.

Terms of general use are defined in Part 1 of IEC 61131. More specific terms are defined in each part.

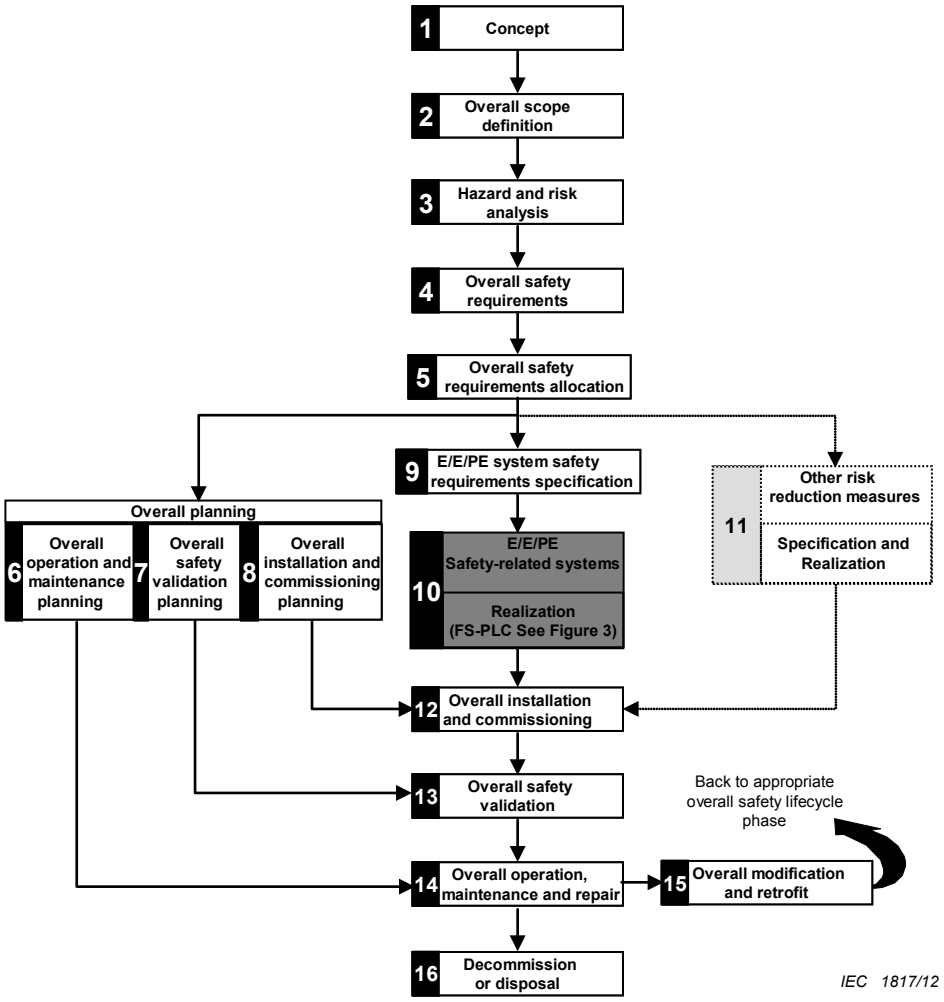
In keeping with 1.1 of IEC 61508-1:2010, this part encompasses the product specific requirements of IEC 61508-1, 61508-2 and 61508-3 as pertaining to programmable controllers and their associated peripherals.

This document's intent is to follow the IEC 61508 series structure, in principle. But some aspects do not have a direct correlation and thus need to be addressed somewhat differently. In part, this is due to addressing hardware, software, firmware, etc. in a single document.

Framework of this part

IEC 61508-1:2010, Figure 2 is included here, and is designated Figure 1. It has been adjusted to show how an FS-PLC fits into the overall E/E/PE safety-related system safety lifecycle. Though Figure 1 box 10 includes sensors, logic subsystem and final elements (e.g. actuators), from the viewpoint of IEC 61508-1, the FS-PLC is given emphasis here by including a reference to Figure 3.

As such, the Realization Phase, Figure 1, box 10, embodies only the logic subsystem, from this part's perspective.



NOTE 1 Activities relating to verification, management of functional safety and functional safety assessment are not shown for reasons of clarity but are relevant to all overall, E/E/PE system and software safety lifecycle phases.

NOTE 2 The phases represented by box 11 is outside the scope of this standard.

NOTE 3 IEC 61508-2 and IEC 61508-3 deal with box 10 (realization) but they also deal, where relevant, with the programmable electronic (hardware and software) aspects of boxes 13, 14 and 15.

NOTE 4 See IEC 61508-1, Table 1 for a description of the objectives and scope of the phases represented by each box.

NOTE 5 The technical requirements necessary for the overall operation, maintenance, repair Modification, retrofit and decommissioning or disposal will be specified as part of the information provided by the supplier of the E/E? PE safety-related system and its elements and components.

Figure 1 – FS-PLC in the overall E/E/PE safety-related system safety lifecycle phases

The areas included in this part are FS-PLC safety lifecycle management, functional safety requirements allocation, and development planning; with the major emphasis on the Realization Phase (Box 10) of the overall safety lifecycle, shown in Figure 1. The assumption of this part is that the FS-PLC is utilized as a logic subsystem for the overall E/E/PE system.

The Figure 1, Realization (box 10), includes:

- the allocation of the FS-PLC safety aspects to FS-PLC hardware, software or firmware, or any combination,
- FS-PLC hardware architectures,
- verification and validation activities at the FS-PLC level,
- FS-PLC modification requirements,
- operation and maintenance information for the FS-PLC user,
- information to be provided by the FS-PLC manufacturer for the user.

AUSTRALIAN STANDARD

Programmable controllers

Part 6: Functional safety

1 Scope

This Part of the IEC 61131 series specifies requirements for programmable controllers (PLCs) and their associated peripherals, as defined in Part 1, which are intended to be used as the logic subsystem of an electrical/electronic/programmable electronic (E/E/PE) safety-related system. A programmable controller and its associated peripherals complying with the requirements of this part is considered suitable for use in an E/E/PE safety-related system and is identified as a functional safety programmable logic controller (FS-PLC). An FS-PLC is generally a hardware (HW) / software (SW) subsystem. An FS-PLC may also include software elements, for example predefined function blocks.

An E/E/PE safety-related system generally consists of sensors, actuators, software and a logic subsystem. This part is a product specific implementation of the requirements of the IEC 61508 series and conformity to this part fulfils all of the applicable requirements of the IEC 61508 series related to FS-PLCs. While the IEC 61508 series is a system standard, this part provides product specific requirements for the application of the principles of the IEC 61508 series to FS-PLC.

This Part of the IEC 61131 series addresses only the functional safety and safety integrity requirements of an FS-PLC when used as part of an E/E/PE safety-related system. The definition of the functional safety requirements of the overall E/E/PE safety-related system and the functional safety requirements of the ultimate application of the E/E/PE safety-related system are outside the scope of this part, but they are inputs for this part. For application specific information the reader is referred to standards such as the IEC 61511 series, IEC 62061, and the ISO 13849 series.

This part does not cover general safety requirements for an FS-PLC such as requirements related to electric shock and fire hazards specified in IEC 61131-2.

This part applies to an FS-PLC with a Safety Integrity Level (SIL) capability not greater than SIL 3.

The objective of this part is:

- to establish and describe the safety life-cycle elements of an FS-PLC, in harmony with the general safety life-cycle identified in IEC 61508-1, -2 and -3;
- to establish and describe the requirements for FS-PLC HW and SW that relate to the functional safety and safety integrity requirements of a E/E/PE safety-related system;
- to establish evaluation methods for a FS-PLC to this part for the following parameters/criteria:
  - a Safety Integrity Level (SIL) claim for which the FS-PLC is capable,
  - a Probability of Failure on Demand (PFD) value,
  - an average frequency of dangerous failure per hour value (PFH),
  - a value for the safe failure fraction (SFF),
  - a value for the hardware fault tolerance (HFT),
  - a diagnostic coverage (DC) value,
  - a verification that the specified FS-PLC manufacturer’s safety lifecycle processes are in place,

