Functional Safety for the Mining and Machinery-based Industries

An integrated framework using AS(IEC)61508, AS(IEC)62061, AS(IEC)61511, ISO13849 and AS4024.1

Marcus Punch

2nd Edition

Cover: Kirstin Farr

2nd Edition

ISBN 978-0-9807660-2-8 (paperback)

RRP $AUD88.00 (including GST), plus postage and handling.

Published by:
Marcus Punch Pty. Ltd.
Tenambit NSW
Australia

Email: marcus@marcuspunch.com
Web: www.marcuspunch.com
Phone: +61 (0)432 168849

This text is intended to provide general information concerning the concepts and applications of functional safety in the mining and machinery-based industries. The examples shown and the principles discussed are particular to each situation. Whilst the author, contributors and publisher expect the text to be useful to any reader, the author, contributors and publisher do not accept any responsibility for actions taken by others in using this material.

Foreword

"Functional Safety for the Mining and Machinery-based Industries" by Marcus Punch is a landmark text.

In risk management and safety literature this book on functional safety fills the void between the various standards and purely technical texts. It encompasses both the practical process and detail necessary to apply functional safety. This is a text that brings together the key standards that alone do not deliver an integrated safety framework.

This is not functional safety simplified, but functional safety clearly explained and referenced for engineers and managers in the mining and machinery-based industries. Detail is not left out nor is the content overwhelming. This is a text as relevant for knowledgeable practitioners as well as for those seeking functional safety information for the first time.

The publication of this book is useful and timely as Governments throughout Australia implement new national occupational health and safety legislation and nationally consistent mine safety legislation.

Marcus clearly explains the purpose of the safety lifecycle to establish safety requirements for plant, considering the specific circumstances and risks in which it will be used, and then to achieve and maintain those requirements for the duration of the plant's life.

The objectives of this book are therefore to provide the reader with:

- an appreciation of the background and reasons why the functional safety and machinery safety approaches should be applied to mining and other plant,
- an overview of the contents of the AS(IEC)61508, AS(IEC)62061, AS(IEC)61511, ISO13849 and AS4024.1 standards, the standards for Functional Safety of Electrical / Electronic/ Programmable Electronic (E/E/PE) safety-related systems and Safety of Machinery,
- an overall framework and stand-alone guideline which integrates and applies these standards to machinery applications in a mine or other facility, and
- an interpretation of the standards, guidance and practical examples

By explaining the integrated safety life-cycle process Marcus guides the reader through the approach to make equipment as safe as possible for people to use. He explores safety integrity level and tolerable risk and the standards that may be applied. All applicable standards are listed and put in context with the working environment of mines and other facilities, the requirement for competent people and safe systems of work to deliver equipment that is fit for purpose throughout its life cycle – the functional safety approach.

Marcus steps the reader through the project life cycle stages of concept, scope, hazard and risk analysis, overall safety requirements, safety requirements allocation, design for operations and maintenance, validation, planning installation and commissioning, safety-related systems, "other technology" safety-related systems, risk reduction facilities, installation and commissioning, operations and maintenance, modification and retrofit and decommissioning.

His style is energetic, clear and knowledgeable.

This book adds significantly to the resources any organisation or individual requires to manage machinery risks and improve safety.

With this book you are equipped to make lasting improvements in the safety of your mining operations.

Rob Regan
Director Mine Safety Operations, NSW
Chief Inspector of Mines and Coal Mines

February 2013.

Table of Contents

List of Tables and Figures

1. Introduction - Why I Wrote This Book…..Again!

"Part of the overall safety relating to the Equipment Under Control (EUC) and the EUC control system that depends on the correct functioning of the Electrical / Electronic / Programmable Electronic (E/E/PE) safety-related systems and other risk reduction measures".[1]

Why did I write this book? Because the subject matter, the terminology and the myriad requirements of the various machinery safety and functional safety standards continue to be a source of confusion for many in industry. Consider for a moment what the prevailing suite of functional safety and machinery standards actually cover...

AS(IEC)61508-2011[2]: Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems

- Consists of eight (8) parts and about 600 pages
- Is based on a sixteen (16) phase 'whole-of-life', or 'cradle-to-grave' safety lifecycle process
- Provides detailed requirements for specifying, designing, validating, operating, modifying and decommissioning electrical / electronic / programmable electronic safety-related systems for all industries
- Uses the Safety Integrity Level (SIL) concept to describe four (4) classes of safety integrity (ie. reliability) – SIL1, 2, 3 and 4. SIL1 describes the lowest level of safety integrity and SIL4 describes the highest. The SIL concept takes account of 'low', 'high' and 'continuous' demand modes of operation of safety-related systems[3].
- The design of "other technology" (ie. mechanical, hydraulic, pneumatic etc...) safety-related systems is not within its scope
- The design of "other risk reduction measures" (ie. guards, barriers, procedures etc...) is not within its scope

AS(IEC)62061-2006: Safety of Machinery – Functional Safety of safety-related Electrical, Electronic and Programmable Electronic Control Systems

- Consists of one (1) part and about 90 pages
- Only covers the 'realisation' (ie. specification, design, installation, testing and commissioning and validation) phases of the 16-phase safety lifecycle process
- Uses the Safety Integrity Level (SIL) concept to describe three (3) classes of safety integrity – SIL1, 2 and 3, as per AS(IEC)61508. However, SIL4 is not within its scope. The SIL concept only takes account of 'high' and 'continuous' demand modes of operation of safety-related systems.
- Refers to AS(IEC)61508 requirements throughout
- Provides detailed requirements for designing electrical / electronic / programmable electronic safety-related systems for machinery-based industries

[1] The definition of 'functional safety' provided in AS61508.4.
[2] I have referred to AS61508 and AS62061 throughout this book as AS(IEC)61508 and AS(IEC)62061 for the sole purpose of expressing their origin and equivalence to the IEC standards.
[3] See Appendix A for the AS(IEC)61508.4 definitions for the demand modes.

- The design of "other technology" (ie. mechanical, hydraulic, pneumatic etc...) safety-related systems is not within its scope
- The design of "other risk reduction measures" (ie. guards, barriers, procedures etc...) safety-related systems is not within its scope

AS(IEC)61511-2004: Functional Safety – Safety Instrumented Systems for the Process Industry

- Consists of three (3) parts and about 200 pages
- Is based on the AS(IEC)61508 sixteen (16) phase 'whole-of-life' safety lifecycle process
- Provides detailed requirements for specifying, designing, validating, operating, modifying and decommissioning electrical / electronic / programmable electronic safety-related systems for process-based industries
- Uses the Safety Integrity Level (SIL) concept to describe three (3) classes of safety integrity – SIL1, 2 and 3, as per AS(IEC)61508. However, SIL4 is not within its scope. The SIL concept takes account of 'low', 'high' and 'continuous' demand modes of operation of safety-related systems.
- The design of "other technology" (ie. mechanical, hydraulic, pneumatic etc...) safety-related systems is not within its scope
- The design of "other risk reduction measures" (ie. guards, barriers, procedures etc...) is not within its scope

ISO13849-1:2006 / ISO13849-2:2012 Safety of Machinery: Safety-related Parts of Control Systems

- Consists of two (2) parts and about 200 pages
- Only covers the 'realisation' (ie. specification, design, installation, testing and commissioning and validation) phases of the 16-phase safety lifecycle process
- Uses the Performance Level (PL) concept to describe five (5) classes of safety integrity – PLa, b, c, d and e. PLa describes the lowest level of safety integrity and PLe describes the highest. The PL concept only takes account of 'high' and 'continuous' demand modes of operation of safety-related systems.
- Stated to be compatible with AS(IEC)62061
- Refers to AS(IEC)61508 requirements throughout
- Provides detailed requirements for designing electrical / electronic / programmable electronic safety-related systems for machinery-based industries
- The design of "other technology" (ie. mechanical, hydraulic, pneumatic etc...) safety-related systems is stated to be within its scope
- The design of "other risk reduction measures" (ie. guards, barriers, procedures etc...) safety-related systems is not within its scope

AS4024.1-2006 Safety of Machinery

- Consists of twenty-six (26) parts and about 600 pages.
- Only covers the 'analysis' (ie. hazard identification, risk analysis, safety requirements allocation) and 'realisation' (ie. design, installation, testing and commissioning) phases of the 16-phase safety lifecycle process

- Provides general requirements for specifying and specific requirements for designing and validating "other technology" (ie. mechanical, hydraulic, pneumatic etc...) and electrical / electronic safety-related systems for machinery-based industries
- Uses the Safeguarding Category (CAT) concept to describe five (5) classes of safety integrity – CATB, 1, 2, 3 and 4. CATB describes the lowest level of safety integrity and CAT4 describes the highest. The CAT concept does not classify the demand modes of operation of safety-related systems.
- The design of programmable electronic safety-related systems is not within its scope
- The design of some "other risk reduction measures" (eg. guards, barriers, etc...) safety-related systems is within its scope

Now consider the range of plant that may be encountered in a typical mine or industrial facility...

Machinery-based?	→ Yes[4]
Involves electrical / electronic safety-related systems?	→ Yes
Involves programmable electronic safety-related systems?	→ Yes
Involves "other technology" safety-related systems?	→ Yes
Involves "other risk reduction measures" (eg. guards, barriers etc...)?	→ Yes

Therefore:

- We can't just use AS(IEC)61508 alone. Whilst it provides a 'whole-of-life' safety lifecycle process, it does not cover the design of "other technology" safety-related systems or "other risk reduction measures"
- We can't just use AS(IEC)62061 alone as it does not cover the design of "other technology" safety-related systems or "other risk reduction measures" and it only covers part of the safety lifecycle.
- We can't just use AS(IEC)61511 alone. Whilst it provides a 'whole-of-life' safety lifecycle process, it only covers 'process-like' applications and it does not cover the design of "other risk reduction measures".
- We can't just use ISO13849 alone as it does not cover the design of "other risk reduction measures" and it only covers part of the safety lifecycle
- We can't just use AS4024.1 alone as it does not cover the design of programmable electronic safety-related systems and some "other risk reduction measures" and it only covers part of the safety lifecycle

Confusing?... Frustrating?...

Put simply, none of the above standards are able to provide both a stand-alone safety lifecycle framework and the guidelines necessary for the realisation of a diverse range of safety system applications and technologies that are likely to be encountered in a mine or industrial plant.

[4] But some parts or systems can be process-based, or the machinery is part of a process – See Section 4.3.

Clearly, AS(IEC)61508 provides an appropriate 'whole of life' safety lifecycle process, but what is lacking is a stand-alone guideline which integrates the approaches of AS(IEC)61508, AS(IEC)62061, AS(IEC)61511, ISO13849 and AS4024.1 for the realisation of safety-related systems based on electrical, electronic, programmable electronic and other technologies.

Therefore, this book has been written to draw together the relevant parts of the standards and provide a straight-forward, stand-alone guideline for the application of functional safety in the mining and machinery-based industries.

Whilst the focus is on mining applications, the content is equally applicable to other machinery-based industries.

The objectives of this book are therefore to provide the reader with:

1. An appreciation of the background and reasons why the functional safety / machinery safety approaches should be applied to mining or other plant
2. An overview of the contents of the AS(IEC)61508, AS(IEC)62061, AS(IEC)61511, ISO13849 and AS4024.1, standards
3. An understanding of the key concepts and requirements
4. An overall framework and stand-alone guideline which integrates and applies the AS(IEC)61508, AS(IEC)62061, AS(IEC)61511, ISO13849 and AS4024.1 standards to machinery applications in a mine or other facility
5. Interpretation of the standards, as well as guidance and practical examples

In addition the following resources are provided as appendices to the book:

Appendix A: Glossary of Terms

Appendix B: Project Safety Lifecycle Checklist