Issue #68 - November 2013

Technical News

Industrial Electrical and Automation Products, Systems and Solutions

The Impacts and Applications of Functional Machine Safety Standards

Written by Craig Imrie
Technology Specialist - Safety

ABSTRACT

In recent years the transition of international machine safety standards towards probability based design methods has occurred.

This has been a major challenge for much of the European industry and the Australian and New Zealand industries will be facing the same challenge over the coming years, as the requirements for probabilistic safety increase and their standards move in line with international standards.

This edition of Technical News explores the transition from Safety Categories to the probabilistic measurements of ISO 13849-1:2006 and explains how these probability methods build on the proven architectures of safety categories.

INTRODUCTION

In recent times the primary reference for machine safety in Australia has been AS 4024. AS 4024 is a collection of standards that cover many aspects of machine safety such as:

- Risk Assessment
- Ergonomics
- Design of safety control systems
- Design of Guards, etc

AS 4024 inherits from many European standards that cover these various topics, for example:

- AS 4024.1201 inherits from ISO 12100 for Basic Terminology and Methodology
- AS 4024.1301 inherits from ISO 14121 for Principles for Risk Assessment
- AS 4024.1501 inherits from EN 954-1 for General Principles for Design, etc

AS 4024 is organised into three parts:

1. **Part One (1000 series)** – Standards that can be used for any machine safety application, these standards address topics such as risk assessment, basic terminology, etc. Examples are:

   a) AS 4024.1101: Terminology – Terms and Definitions

   b) AS 4024.1201: General principles – Basic terminology and methodology

   c) AS 4024.1301: Risk assessment – Principles of risk assessment, etc

2. **Part Two (2000 series)** – Standards that address particular design considerations for safety systems and components. For example some of these standards offer guidance for particular devices such as two hand control units, light curtains, etc. If the standard is not relevant to your safety application there is no reason to reference the standard. Examples are:

   a) AS 4024.2801: Safety distances and safety gaps – Positioning of protective equipment with respect to the approach speed of parts of the human body

   b) AS 4024.2601: Design of controls, interlocks and guarding – Two-hand control devices – Functional aspects and design principles

3. **Part Three (3000 series)** – Standards that focus on specific types of machinery, to allow for better guidance for the equipment being protected. As with part two series, if the standard is not relevant to your application there is no reason to reference the standard. Examples are:

   a) AS 4024.3301: Robots for industrial environments – Safety requirements

   b) AS 4024.3001: Materials forming and shearing – Mechanical power presses

AS 4024 was designed in this way so it could be updated and revised in a simple manner. When an international standard is revised the relevant part of AS 4024 can be updated to reflect this without altering the other parts of the edition. The preface of AS 4024 parts reflects this idea by stating:

"When a new edition of a relevant Standard becomes available at the international level, it will be adopted and published within the framework of AS 4024 with a minimum delay, so ensuring continued international alignment."

Due to this desire to keep AS 4024 aligned with international standards, there is interest in the direction of AS 4024 in reaction to changing international safety standards. As mentioned previously AS 4024.1501 inherits from EN 954-1, this part of the standard is concerned with the design of safety-related control systems. In EN 954-1 systems are designed to the requirements of a particular safety category depending on the risk of the application.

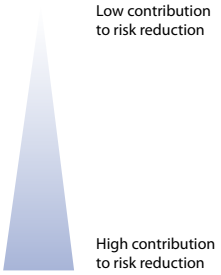
Europe has phased out EN 954-1 since the start of 2012. This means all European safety control systems are being designed in accordance to either ISO 13849-1:2006 or IEC 62061. As mentioned above it is preferable that Australian design standards are internationally aligned, so the inclusion of ISO 13849-1:2006 into AS 4024 could be witnessed as early as 2014.

With this in mind, this TNL edition will observe how the methods of ISO 13849-1 compare to the current AS 4024.1501. It will become clear that the method of ISO 13849-1 is built on Safety Categories and this standard is a useful bridge between the proven architectural requirements of Safety Categories to a probabilistic measurement called Performance Level (PL), which is directly related to the measurement of Safety Integrity Level (SIL).

WHAT IS A PERFORMANCE LEVEL (PL)?

Using the methods of design in ISO 13849-1, safety systems are designed to a designated Performance Level (PL). As with Safety Categories, the higher the risk of the application the higher the integrity of the required PL. PL is a measure of Probability of Dangerous Failure per Hour of operation (PFHd). As the risk increases, the PL moves from 'a' to 'e' and the PFHd reduces, this is demonstrated in Figure 1.

PL	Average probability of failure per hour
a	≥10-5 to < 10-4
b	≥ 3 x 10-6 to < 10-5
c	≥10-6 to < 3 x 10-6
d	≥10-7 to < 10-6
e	≥10-8 to < 10-7



Low contribution to risk reduction

High contribution to risk reduction

Figure 1 - Performance Level (PL)

The above figure seems very far removed from the architecture requirements of Safety Categories, however a PL is fundamentally based on these same architecture requirements. ISO 13949-1 addresses some of the short comings of safety categories and arrives at a probabilistic measure, which is compatible with SIL.

Some of the key reasons why safety categories were superseded in international standards were the following observations:

- Inability to consider all aspects of modern safety systems and components, for example poor guidance on software development
- Category selection method was ambiguous
- Low importance placed on component selection and quality
- Vague diagnostic requirements, especially in Category 3
- Poor guidance on Common Cause Failure (CCF) reduction

PL looks to address these issues by combining the architecture of Categories with the following measurements (refer Figure 2):

- Component quality - Mean Time To Dangerous Failure $MTTF_d$
- Diagnostics – Diagnostic Coverage DC
- Guidance to reduce CCF – CCF test

As well as the extra measures shown in Figure 2, ISO 13849-1 also provides a Software Design Lifecycle and improved PL selection method.

The following sections will look how these extra requirements compare to the requirements used for Safety Category design.

Figure 2 - Inner mechanics of a PL

SOFTWARE DEVELOPMENT LIFECYCLE

Modern safety systems may use programmable safety controllers, this software program becomes integral to the performance of the safety system. ISO 13849-1 provides great guidance on how to ensure the software component of the system is as reliable as the physical system.

The general concept used is based on a Software Development Lifecycle (Figure 3). This lifecycle starts with a Specification of the software, from this specification the program can be design, implemented, verified and finally validated. The activities and documentation produced throughout this lifecycle increase with the required PL. Refer to clause 4.6 of ISO 13849-1 for more information.

Compare this to the guidance for software development in AS 4024; guidance is given in AS 4024.1202 clause 5.11.8.3:

"The software…. shall be designed so as to satisfy the performance specification for the safety functions (See also AS 61508.3)"

The software lifecycle in ISO 13849-1 is based on the concepts of IEC 61508.3 but it is adapted specifically for machine safety applications. Detailed software development guidance is a major improvement delivered by ISO 13849-1

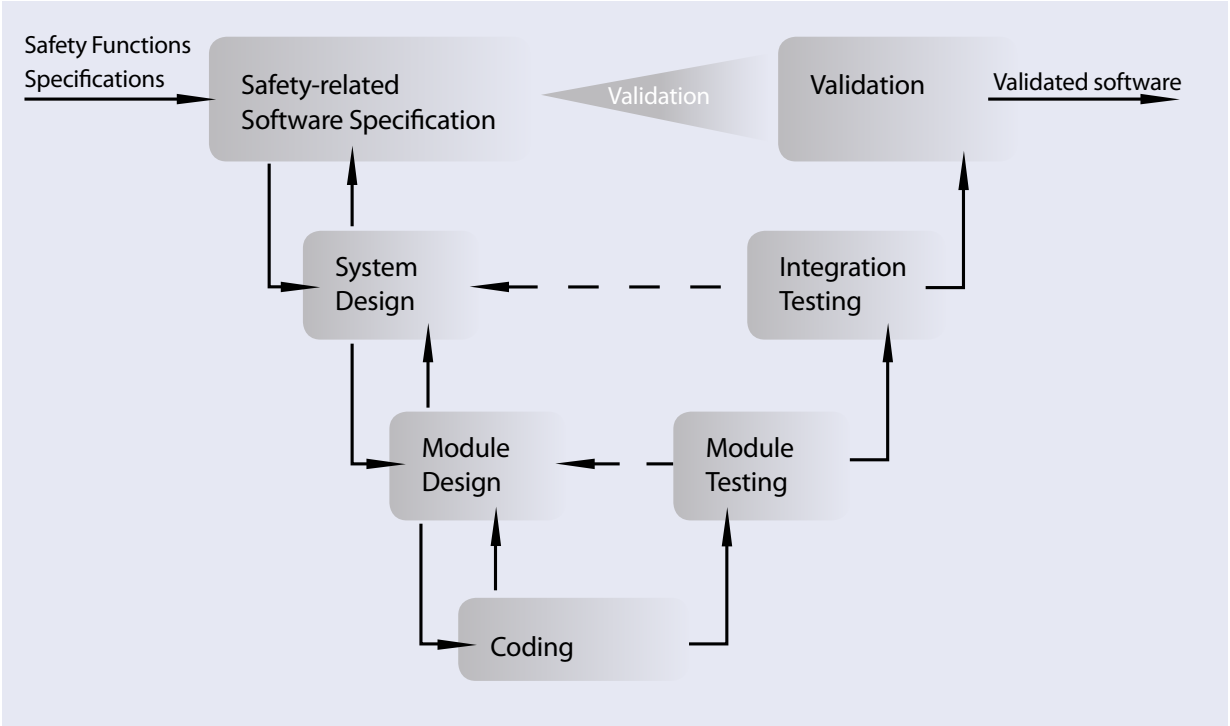


Figure 3 - Software Development Lifecycle used in ISO 13849-1

COMPONENT RELIABILITY

ISO 13849-1 requires the quality and selection of the components to be analysed. For each component in the safety system a Mean Time To Dangerous Failure ($MTTF_d$) needs to be calculated. This is then combined with the other components in the system to determine a $MTTF_d$ for the complete safety system.

The value is classified as Low, Medium or High, as can be seen in Table 1.

$MTTF_d$ Classification	Time Range
Low	3 years < $MTTF_d$ < 10 years
Medium	10 years ≤ $MTTF_d$ < 30 years
High	30 years ≤ $MTTF_d$ ≤ 100years

Table 1: $MTTF_d$ classification in IOS 13849-1

This aspect of PL ensures that the quality of components is an important part of designing a safety system. The design process in AS 4024 doesn't lay as much importance on the component quality because Safety Categories are generally more architecturally based. There are some requirements in Safety Categories to use well tried safety components and well-tried safety principles, however ISO 13849-1 formalises this requirement by quantifying the reliability of each component selected.

DIAGNOSTIC REQUIREMENTS

As like component reliability, ISO 13849-1 also quantifies the diagnostic ability of the safety system. The measurement used is Diagnostic Coverage (DC), this measurement represents what percentage of dangerous failures will be detected by the safety system.

The DC value is classified as None, Low, Medium or High, as can be seen in Table 2.

DC Classification	Time Range
None	DC < 60%
Low	60% ≤ DC < 90%
Medium	90% ≤ DC ≤ 99%
High	99% ≤ DC

Table 2: DC classification in ISO 13849-1

Safety Categories also have requirements for diagnostic levels, however the requirements can be vague in some cases. For example, in AS 4024.1501 the requirement for detection of failure in CAT 3 needs to be performed "whenever reasonably practicable." The introduction of the DC metric in ISO 13849-1 clearly defines what level of diagnostic coverage is required to achieve a given PL.

COMMON CAUSE FAILURE (CCF)

One major threat to a safety system with a redundant architecture is the possibility of common cause failures (CCF) Common cause failure would be a failure in 2 or more channels occurring due to the same event or cause. Some examples may be:

- Induced noise creating an erroneous signal on both channels
- Poor selection of components leading to redundant switches filling up with water due to incorrect IP rating

Due to CCF, ISO 13849-1 requires the designer to pass a CCF test for any architecture with redundant channels. The designer must implement measures to avoid CCF in the design of their system to an acceptable level, this may include techniques such as:

- Diversity – Using different technology or physical principles across redundant channels will reduce the chance of CCF
- Separation – Physical separation of channel will reduce the chances of CCF such as common noise.

ACHIEVING A PL

The above mentioned concepts combined with the system's architecture (CAT) achieve a PL. Table 3 indicates how the CAT, DC and $MTTF_d$ are used to determine the system's PL, this table assumes that CCF has been avoided to an acceptable level for redundant architectures.

Category	B	1	2	2	3	3	4
DCavg	None	None	Low	Medium	Low	Medium	High
$MTTF_d$							
Low	a	N/A	a	b	b	c	N/A
Medium	b	N/A	b	c	c	d	N/A
High	N/A	c	c	d	d	d	e

Table 3: Achieving a PL

CONCLUSION

In conclusion, most of the Australian industry is using the methods in AS 4024.1501 and designing their safety systems to achieve Safety Categories. AS 4024 will be updated to reflect international standards, which currently use probabilistic methods to design safety systems.

ISO 13849-1 provides an excellent transition method as it is built on top of the architectures of Safety Categories and achieves a probabilistic result. It is expected that ISO 13849-1 will be adopted into the AS 4024.1 as early as 2014, this would be the recommended transition path for designers who are familiar with the requirements of Safety Categories.

REFERENCES

AS 4024.1 – 2006

ISO 13849-1: 2006

NHP – YOUR SAFETY EXPERTS…

NHP has a long history in the safety industry and can be a trusted destination for all your safety application needs. Here are just a number of safety tools and training available…

NHP Safety Reference Guide

NHP's Safety Reference Guide includes a range of material to ensure you and your projects are safe!

Complete with technical information on NHP's extensive range of safety products, whitepapers on various safety applications and information documents on International/ Local Safety standards, the NHP Safety Reference Guide forms an invaluable resource for projects across all industries.

Combined with example system designs for achieving different safety categories and a glossary of typical safety terminology, registration for the NHP Safety Reference Guide is easy and FREE and is a must when it comes to the safety of your site.

To register for the free Safety Reference Guide, simply scan the QR code or search for 'Safety Reference Guide' on the NHP website.

NHP Safety Blog

NHP's Safety Blog is a communication forum that allows discussions to be held on various machine safety topics such as safety design, legislation, safety standards, risk assessment and much more.

The blog creates an opportunity for everyone involved in the machine safety industry to share their opinions and perspectives on safety topics as well as receive expert commentary from NHP's TUV Certified Safety specialists.

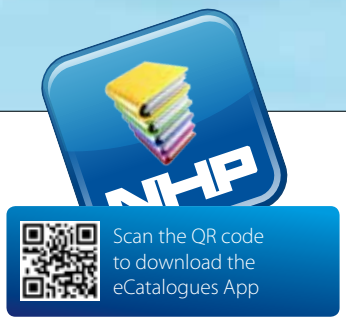
Join in the conversation today and be kept up to date with all the latest NHP and industry safety news. Simply scan the QR code or visit nhp.com.au/blog.

Safety Training

The Safety industry is a constantly changing landscape and it can be difficult to keep up with the latest news, information and standards. The only way to ensure your company and staff are abreast of these changes is to invest in continuous training.

NHP holds regular half and full-day safety workshops on a range of safety topics. Courses can range from machine safety standards and legislation to the design of machine safety systems, risk assessments and even an introduction into TUV certification.

For more information on specific courses, scan the QR code or simply search for 'Safety Training' on the NHP website.



If you would like previous copies of Technical News, simply visit **www.nhp.com.au/media** and navigate to 'Catalogues & Literature' or download the NHP eCatalogues App by scanning the QR code.

Editorial content: Please address all enquiries to marketing@nhp.com.au.

NHP Electrical Engineering Products Pty Ltd
A.B.N. 84 004 304 812

NTNL68 10 13

AUSTRALIA
nhp.com.au
SALES
1300 NHP NHP

Melbourne
Laverton
Albury/
Wodonga
Dandenong
Hobart
Launceston
Sydney*
Newcastle*
Wollongong*
Canberra
Brisbane*
Townsville
Rockhampton
Toowoomba*
Cairns
Adelaide
Perth
Darwin

NEW ZEALAND
nhp-nz.com
SALES
0800 NHP NHP

Auckland
Hamilton
Napier
New Plymouth
Wellington
Christchurch
Dunedin

* Rockwell Automation products not available from these locations

Authorised Distributor

Scan the QR code to download the eCatalogues App