Australian and International Safety Standards – Designing the Future

By Wayne Pearse, Safety Consultant Rockwell Automation
FSExpert (TÜV Rheinland, #203/13, Machinery)
FSEngineer (TÜV Rheinland, #4850/12, Machinery)

Adopting safety standards can lead to improved flexibility, expanded markets, and better use of technology. Modern quantitative standards may not be as simple to use as their qualitative predecessors, but they give designers the tools to work with the current generation of complex machinery safety systems.

Safety systems have come a long way in recent times. They have evolved from simple mechanistic shut-down functions to technologies such as safety capable logic, which can react to machine conditions and improve productivity. To use modern safety systems effectively, designers need new tools.

Current Australian and international safety standards provide quantitative methods to calculate risk and reliability. This is a big shift from the simple qualitative approach of machine safety standard AS4024:1501 (EN 954), which did not require designers to assess the reliability of safety components.

To keep Australia and New Zealand in line with international standards, the series of machinery safety standards AS 4024:2006 which was made up of 26 parts based on International Standards has been revised and the new AS/NZS 4024:2014 series of machinery safety standards was released in July 2014. The parts are direct text adoptions of the international standard, meaning that all references in the parts represent international standard numbers.

There are many compelling reasons to adopt international safety standards. The most evident include meeting the requirements of a global market and to lay the groundwork for future expansion. For example, machines exported to Europe must comply with International Organisation for Standardization (ISO) 13849-1 or International Electrotechnical Commission (IEC) 62061 (also known as AS 62061-1:2005).

Manufacturers can also take advantage of the framework provided by safety standards to homogenise the operation of their plants around the world. This leads to cost savings in training and maintenance, as well as increased safety for workers and equipment.

The quantitative approaches of AS/NZS 4024:1503 (ISO 13849-1:2006)[1] and IEC/AS 62061:2005 are also useful for engineers seeking to explain the need for a particular safety system in an application, or to justify the cost of a safety upgrade in terms of actual risk reduction.

Safety standards allow companies to demonstrate compliance to customers, and give them confidence that their machines will operate safely, with reduced down-time resulting from component failures. This can be augmented by employing engineers, such as myself, who have been certified as a Functional Safety Engineers by industry bodies.

Horses for courses

Sometimes there are competing international standards governing an aspect of the design process. This is illustrated by the two competing safety standards in Europe.

Both of these standards contain a framework and tools to analyse the functional safety of a system— the parts of the control system that ensure the safety of plant and personnel. For designers, the choice of which standard to apply can be confusing.

The ISO and IEC recognise the problem, and are participating in a joint working group to merge ISO 13849-1 and IEC 62061:2005. The process began in 2011 and it is likely that it will take several years to complete. In the mean time, the main consideration for engineers is to choose a standard that they feel comfortable working with and select safety systems that meet the requirements of the operating environment and machine function.

The IEC standard already operates in Australia as AS 62061-1:2005. It applies to programmable devices, such as safety PLCs, and should be used for these applications. The standard describes risk, and the ability of the system to reduce it, in terms of Safety Integrity Levels (SIL). SIL 1 is the lowest risk and SIL 3 the highest.

[1] ISO 13849-1:2006 is the international equivalent of machine safety standard AS/NZ 4024:1503, http://infostore.saiglobal.com/store/

The IEC standard is useful for applications in the petro-chemical or power generation industry, as these industries are familiar with the concept of SIL. In the process industry, risks can exceed SIL 3, so IEC 61508, and the process specific standard, IEC 61511, include SIL 4.

ISO 13849-1:2006 is also applicable in Australia, and has recently been referenced and referred to in AS/NZS 4024:1503. It applies to electrical, mechanical, pneumatic and hydraulic systems. Under AS/NZS 4024:1503, mean time to dangerous failure ($MTTF_d$) for the system is calculated in years. Instead of SIL, risk and system performance are described using Performance Levels (PL). There are five levels, ranging from PL a to PL e, where PL e is the highest. Table 1 shows an approximate relationship between PL and SIL.

A key difference between these two international standards is the work involved in the calculations of system performance. Unlike AS/NZS 4024:1503, AS 62061-1:2005 does not consider mean time to failure in years, and uses considerably more complex methods to determine the probability of dangerous failure per hour (PFH_D).

A free software tool, called SISTEMA (Safety Integrity Software Tool for the Evaluation of Machine Applications), has been produced by the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) to perform automatic calculations of Performance Levels under ISO 13849-1. It can be downloaded from the IFA website: http://www.dguv.de/ifa/en/pra/softwa/sistema/index.jsp

Safety lifecycle

Integrating safety and machine functionality during the concept and design phase can deliver a system that minimises risk, meets functional specifications and reduces training requirements. Specific gains can be made though sharing components between the standard and safety parts of the application and using intelligent safety systems to enhance operations.

The safety lifecycle of a machine starts with a system risk assessment which then flows into the development of the functional requirements for the system. Once the risk assessment and functional specification are complete, it is time to put your chosen international standard to work in the design and verification process. The design flow of AS/NZS 4024:1503 will be used to discuss factors such as performance level, system reliability, diagnostic coverage and common cause failure.

Performance Level Structure (Categories)

Performance levels are the basis for quantifying the ability of the safety related parts of a system to respond to risk. They are based on the system architecture (category); the reliability of the system, represented by the mean time to dangerous failure ($MTTF_d$); and the effectiveness of the system in checking for faults using Diagnostic Coverage (DC) and Common Cause Failure (CCF).

Many engineers are familiar with the use of categories to describe control system architecture. This terminology is used in AS4024:1501 and the now obsolete EN954-1 but remains an integral part of AS/NZS 4024:1503. A graph relating Performance Levels to Categories and average mean time to failure is shown in Diagram 1 (below). In this diagram, DC_{avg} is the average diagnostic coverage which is a measure of the test quality applied to components of the system.

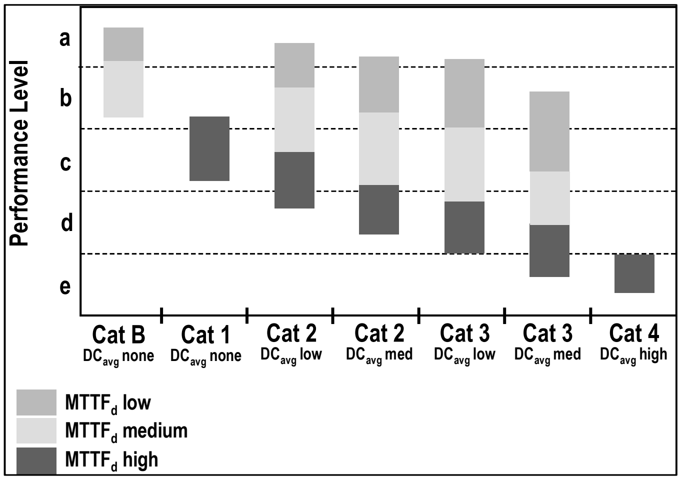

Diagram 1: Graphical determination of Performance Level

The risk graphs from AS/NZS 4024:1503 and AS 4024:1501 (EN 954-1) are shown in Diagrams 2 (right) and 3 (below right). In these diagrams, S1 refers to the risk of an incident resulting in a minor injury, such as a cut finger, and S2 to incidents with more serious outcomes. The main difference is that the S2 branch now subdivides, requiring more careful consideration of the safety measures for those systems have inherently lower risks.

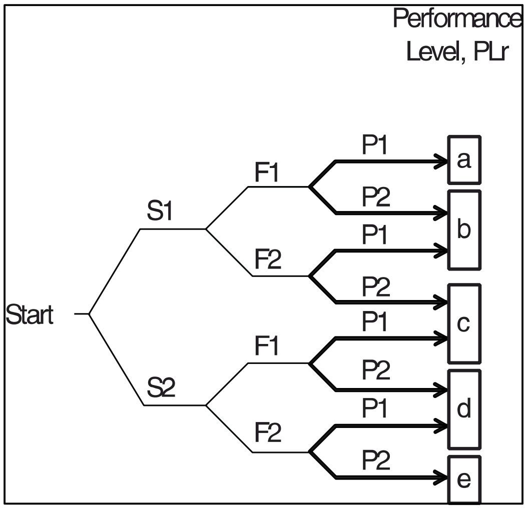

Diagram 2: Risk Graph from Annex A of EN ISO 1384-1

For a safety related control system, there are five categories: B, 1, 2, 3 and 4. The system behaviour for each of these categories is described in Table 2 (below).

Category B has no specific fault tolerance, but is the basis for the higher categories. In Category 1 systems, fault prevention is achieved through the use of simple design, and stable and predictable components and materials.

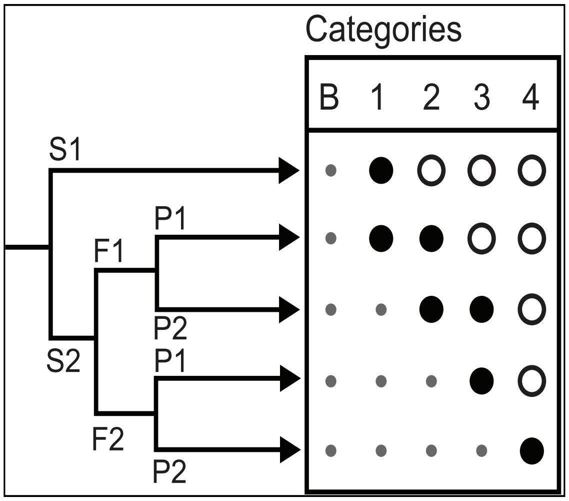

Diagram 3: Risk Graph from Annex B of EN 954-1

The three highest categories (2, 3 and 4) require that if faults cannot be prevented, they must be detected and the system must react appropriately. Redundancy, diversity and monitoring are the key concepts employed in reaching this outcome.

System reliability

As mentioned earlier, AS/NZS 4024:1503 uses $MTTF_d$ (years) as a measure of system reliability. The $MTTF_d$ of a single channel system or subsystem is the average of the $MTTF_d$ of each of its elements.

This value can be calculated using the simplified formula provided in the standard. For a dual channel system or subsystem, the $MTTF_d$ of each channel needs to be calculated separately.

Performance Level (PL)	Probability of dangerous failure per hour (PFHD)	Safety Integrity Level (SIL)
a	$\geq 10^{-5}$ to $<10^{-4}$	None
b	$\geq 3 \times 10^{-6}$ to $<10^{-5}$	1
c	$\geq 10^{-6}$ to $<3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ to $<10^{-6}$	2
e	$\geq 10^{-8}$ to $<10^{-7}$	3

Table 1: Approximate correspondence between PL and SIL (pp. 70, Safebook 4, Rockwell Automation, 2011)

Category	System Behaviour
B	When a fault occurs, it can lead to a loss of the safety function
1	As described for Category B, but with higher reliability of the safety function (less likelihood of failure)
2	Control system checks safety functions at machine start-up and then periodically. Faults can lead to the loss of safety functions between checks.
3	A single fault in any part of the system does not lead to loss of safety function. When the single fault occurs, the safety function is always performed. Not all faults will be detected. An undetected fault can lead to safety function loss.
4	When faults occur, the safety function is always performed. Faults will be detected in time to prevent safety system loss.

Table 2: System behaviour of safety related control systems (pp. 107, Safebook 4, Rockwell Automation, 2011)

Often, the PFH$_D$ of systems and subsystems are available from the manufacturer and can be entered directly into SISTEMA.

The MTTF$_d$ is limited by the standard to 100 years, although in some cases it may be higher. The average MTTF$_d$ of each system or subsystem is categorised as low, medium or high depending on its value, as shown in Table 3. This reliability range can then be used to determine PL as shown in Diagram 1.

Diagnostic Coverage

As discussed earlier, the different categories of safety system have varying levels of diagnostic testing. Diagnostic Coverage (DC) is the term used to describe the system's effectiveness in detecting faults.The failure rate within a system is expressed as Lambda (λ). DC is defined as the ratio of dangerous failures which are detected (λdd) to total dangerous failures (λd) expressed as a percentage ($DC= \lambda dd / \lambda d$). The failures that pose the greatest threat are the dangerous undetected hazards (λdu).

DC is divided into four basic ranges, as shown in Table 4 (below) and Diagram 1 (above).

Common cause failure

One of the important principles of AS/NZS 4024:1503 is the need for designers to determine whether the possibilities of faults in both channels of a dual channel system are separate and unrelated. If failure of a component in one system causes faults in other systems or components, this is considered a single failure.

Events which cause more than one component of the system to fail are called common cause failures (CCF). CCFs are many and varied, and it is necessary for engineers to employ a diverse arsenal of methods to combat them. The approach outlined in the standard is qualitative, and summarised in Table 5 (below).

Denotation of MTTF_d of each channel	**Range of MTTF_d of each channel**
Low	3 years <= MTTF_d < 10 years
Medium	10 years <= MTTF_d < 30 years
High	30 years <= MTTF_d < 100 years

Table 3: Levels of MTTF_d (pp. 83, Safebook 4, Rockwell Automation, 2011)

Denotation of Diagnostic Coverage (DC)	**Range of Diagnostic Coverage (%)**
None	< 60
Low	≥ 60 to < 90
Medium	≥ 99 to < 99
High	≥ 99

Table 4: Levels of Diagnostic Coverage (pp. 88, Safebook 4, Rockwell Automation, 2011)

No.	**Example of Measure Against Common Cause Failure (CCF)**	**Score**
1	Separation/Segregation	15
2	Diversity	20
3	Design/Application/Experience	20
4	Assessment/Analysis	5
5	Competence/Training	5
6	Environmental	35

Table 5: Scoring for Common Cause Failure (pp. 89, Safebook 4, Rockwell Automation, 2011)

Simply put, designers need to analyse the possible CCF of their application and mitigate the risk of them occurring. Annexe F of AS/NZS 4024:1503lists various measures—including the technological diversity of the design, physical separation of signal paths and electromagnetic compatibility—which can be taken to minimise CCF and assigns a score to each type. To demonstrate compliance with the standard, designers need to achieve a score of 65 or greater.

Safety standards not only support global markets and complex safety technologies. They give designers tools to quantify risk and provide a structured framework to implement integrated safety lifecycle design.

There is no right or wrong when choosing between AS/NZS 4024:1503and IEC/AS 62061:2005: engineers must do their research and decide which standard best suits their design parameters and provides the most workable tools for their application.

http://discover.rockwellautomation.com/_Safety_Solutions_Full.aspx

About Rockwell Automation

Rockwell Automation Australia and Rockwell Automation New Zealand are subsidiaries of Rockwell Automation, Inc.—a leading global provider of industrial automation and information solutions that helps manufacturers achieve a competitive advantage in their businesses. The company brings together leading global brands in industrial automation which include Allen-Bradley® controls and services and Rockwell Software® factory management software. Its broad product mix includes control logic systems, sensors, human-machine interfaces, drive controllers, power devices, and software.

Rockwell Automation, Inc. (NYSE:ROK), the world's largest company dedicated to industrial automation and information, makes its customers more productive and the world more sustainable. Headquartered in Milwaukee, Wis., Rockwell Automation employs about 22,000 people serving customers in more than 80 countries.

Rockwell Automation is the trademark of Rockwell Automation, Inc.