Abstract
Following recent local and international changes in machine safety standards, there is a state of flux within the Australian machine safety sector, and some confusion over which is the best option to use for machine safety. AS 4024 and AS 62061 provide different techniques for the machine safety process, further complicated by the addition last year of AS 4024.1503, which is an adoption of ISO 13849. This now offers two methodology options within the Australian machine safety standard.

The objective of this paper is to clarify this situation and provide a better understanding of how these standards can be used to achieve effective machine safety solutions for Australian industry.

Introduction
Machine safety is now an integral component of manufacturing in Australian industry, with all states and territories enforcing legislation for the provision of safe workplaces. Most states and territories have now adopted the new harmonised Work Health and Safety legislation. Only Victoria and Western Australia have yet to adopt this new harmonised legislation and continue to operate under their respective existing Occupational Health and Safety legislation.

Regardless of the legislation being enforced, the requirement to provide a safe place of work is equally applicable throughout Australia and is relevant to all machinery, regardless of age.

As stated above, the standards available to Australian industry to provide the guidance for achieving a safe place of work with machinery have entered a state of flux with three different methodologies now available to the machine safety sector. The difficulty in many situations is in understanding which of these three methodologies is the best one to be applied in a particular situation.

Discussion
The starting point in developing this knowledge, is in understanding how the standards applicable to machine safety have evolved within Australia, and globally.

AS 4024.1 Safeguarding of machinery, Part 1: General principles was first introduced as an interim standard in 1992, becoming a full Australian Standard in 1996. Prior to 1992, the only Australian standards relating to machine safety
Session Two: Machinery and automation safety – safety categories vs. performance levels vs. safety integrity levels: which is best?

were those that applied to specific types of machinery, so the introduction of a standard which applied to all machinery in 1992 was a major step forward for Australian industrial safety.

At around the same time as AS 4024.1—1996 became a full Australian Standard, EN 954.1 was also published as a European Standard for safety related control systems, addressing electrical, mechanical, hydraulic and pneumatic systems. EN 954.1, however, only dealt with the definitions and assignment of safety categories (Cats) for safety control systems, identical to the definitions and assignment criteria detailed in AS 4024.1501—1996. These safety categories are primarily defined according to the structure of the safety control system.

AS 4024.1—1996 added some confusion as, in addition to the safety categories, there were also definitions for interlocking categories. In 2006, the revised version of AS 4024.1 was published, minus the interlocking categories. The revised version, AS 4024.1—2006, is comprised of 26 individual standards which provide a strong alignment with the European model for machine safety standards. By publishing AS 4024.1—2006 in this way, it would be easier to update individual sections (standards) within AS 4024.1—2006, without having to re-publish the complete standard.

While the machine safety sector was evolving, the process industry was making similar progress with the introduction of IEC 61508 in 1998. This standard introduced Safety Integrity Levels (SILs) for the definition and assignment of safety control systems, which put increased emphasis on the reliability of the safety control system, in addition to the structure. IEC 61508 was adopted as an Australian Standard, becoming AS 61508.

One drawback for AS 61508 in the machine safety sector, was that it involves a substantially more complex process in determining the overall reliability of a safety control system, in some situations being overly complex for a machine safety control system.

AS IEC 62061 was published, as a daughter standard derived from AS 61508, in 1995, providing a reduced level of complexity for the machine safety sector while utilising the Safety Integrity Level methodology.

In 1999, a new functional safety standard was introduced in Europe – ISO 13849.1. The 1999 version of the standard effectively duplicated the safety category methodology of EN 954.1 and AS 4024.1501—2006. When ISO 13849.1 was revised and republished in 2006, the new version introduced Performance Levels (PLs) as the means for defining and assigning levels of safety control systems, but employing a less complex methodology than AS 61508/62061.

Last year saw the review of AS 4024.1—2006, with several of the individual standards which make up this series being updated, now AS 4024.1—2014. This review included the addition of a new standard, AS 4024.1503—2014, which is an adoption of ISO 13849.1 into the Australian machine safety standard series.

This addition introduces the PL methodology into the existing Australian standard, effectively providing the parallel options of either Cat, or PL, within the same standard series. This situation mirrors the recent situation in Europe
where EN 954.1 and ISO 13849.1 ran in parallel for several years before the ultimate withdrawal of EN 954.1 in 2011.

The Australian manufacturing industry now has three different methodologies, which are applicable in determining machine safety requirements, which comes back to the original question of which standard is the best one?

The starting point for all machine safety systems is the risk assessment, as this provides the “foundation block” from which the safety system can be developed.

Examination of the three standards/methodologies highlights some differences in the way that the risk assessment results are used to identify the required safety category, performance level (PL), or safety integrity level (SIL), however, the basic process behind all three methodologies is very similar as all three methodologies consider the severity of an incident, the level of exposure and possibility of being able to avoid the hazardous situation.

This similarity between the three methodologies for risk assessment indicates that this does not help in answering the question of which standard is the best one.

The next point of comparison is the means of defining safety levels within each methodology.

There is a direct correlation between the PL and SIL definitions, as these are defined in terms of Probability of Dangerous Failures per hour (PFH\textsubscript{D}) and there is a direct correlation between some levels of each methodology. Figure 1 shows this correlation between the PL and SIL PFH\textsubscript{D} ranges.

It should be noted that there is no SIL equivalent to PLa and that SIL 1 is equivalent to the combined PFH\textsubscript{D} ranges of PLb and PLc. Also, SIL 4 is not applicable in AS 62061, as this level is typically applicable to extreme risk levels, exceeding the risk levels considered to be possible for machinery, i.e. nuclear reactors.

An additional factor to note in this comparison is that AS 62061 only considers high demand rates, whereas AS 61508 also considers low demand rates but low demand rates are not considered to be applicable for machinery applications. Therefore, SIL 3 is the highest level that is considered in AS 62061, correlating to PLe in AS 4024.1503 (ISO 13849.1)
When looking for a correlation between the Cats and functional safety methodologies, there is no direct correlation between the Cats and SILs. There is, however, some correlation between the Cats and the PLs as the Cat structure is a fundamental component of the PL determination. There are additional factors which are considered in the PL determination, and the Cats are correlated against multiple PLs, so it is still not possible to establish a direct correlation between the two methodologies. Figure 2 shows the correlations between the Cats and PLs.

Determination of a safety control system level using the PL methodology, incorporates additional relevant factors, these being the diagnostic coverage (DC) and Mean Time to Dangerous Failure (MTTF\textsubscript{d}) of the safety control system. Figure 3 shows the correlation between Cat and PL, including the DC and MTTF\textsubscript{d} factors.

It is clear that comparison of the methodologies for determining safety control system levels does not provide a means of establishing which standard/methodology is the best one, so further investigation is necessary.

The next area to examine is the structures, or architectures, of each methodology.

The Cat system is defined purely based on the physical structure of the safety control system, considering the redundancy of the system (single channel vs. dual channel) and the level of monitoring of the input/output devices by the safety controller. This provides a basic, but rigid, means of identifying each Cat.

The PL system starts by identifying the safety system structure, utilising the structures developed in the Cat system, however, as previously identified, the structure alone is not sufficient to determine the PL and requires the additional consideration of diagnostic coverage (DC), common cause failure (CCF) and reliability (MTTF\textsubscript{d}) of the components used in the system.

The SIL system shows similarities to the PL system but considers the architecture (structure) of the sub-systems which make up a safety control system, but also requires inclusion of the reliability (PFH\textsubscript{D}), diagnostic coverage (DC), safe failure fraction (SFF) and common cause failures (CCF).

It is clear that this methodology is significantly detailed in comparison to the Cat and PL methodologies, however, this still does not provide a simple answer as to which methodology is the best one to use.

An area not investigated yet in this paper, is the variety of technologies which each methodology can accommodate. This provides interesting comparisons
as the most complex methodology (SIL) is the most restricted in terms of technologies. This is actually apparent in the title of the standard, “Functional safety of safety-related electrical, electronic and programmable electronic control systems”. It is possible to consider electro-mechanical and mixed technologies within a SIL system but this can only be done if these technologies are addressed using the PL methodology and the resulting PFH\textsubscript{D} data is input into the SIL calculations. Therefore, the SIL methodology has significant technology restrictions. It is, however, the only methodology which is designed for complex electronic systems.

The PL methodology can be used for all technologies, but has some restrictions for electro-mechanical, mixed and complex electronic technologies. For complex electronic technologies, it is necessary to use the SIL methodology and use the resulting PFH\textsubscript{D} data in the PL assessment.

The Cat methodology is the simplest of the three methodologies and is capable of handling all technologies, with the exception of complex electronic systems for which there is no mechanism.

Figure 4 shows these capabilities of the three different methodologies to accommodate the various technology options.

The final aspect to be considered in this paper is the overall content covered by each of the standards/methodologies, relevant to machine safety.

Following the recent review and update of AS 4024.1-2014, the Cat and PL methodologies are now within the same group of standards and should be considered as being equivalent, in terms of the overall requirements for machine safety.

The SIL methodology (AS 62061), however, is primarily only concerned with the intricacies of the safety control system being examined and does not address any considerations outside of this sector, while the 25 individual standards which go to make up AS 4024.1—2014 cover a wide sector of ergonomics and other machine safety aspects which are not addressed in the functional safety standard.

Previously, the same situation was applicable with ISO 13849.1, however, since the adoption of this standard within AS 4024.1—2014 it cannot be viewed as a separate entity and must be considered in conjunction with all other sections of the machine safety standard series.
Conclusion

In conclusion, it becomes clear that a comparison of the three methodologies should not be considered to be a comparison of the three machine safety standards, but rather to be only a comparison of the aspects relating directly to the evaluation of the safety control systems. The reality of the situation is that regardless of whether the Cat, PL, or SIL, methodology is employed in assessing a machine safety control system, it is also necessary to consult AS 4024.1—2014 for guidance on all of the other aspects which relate to machine safety.

As for the question of which methodology is best, the obvious conclusion is that all three methodologies are best, depending upon the particular machine safety situation being considered:

The Cat methodology, while simple and rigid, is perfectly applicable to simple machine safety systems which do not require intensive examination;

The PL methodology provides more flexibility than the Cat methodology by including the additional factors of reliability and diagnostic coverage, but has limitations when complex electronic systems are involved;

The SIL methodology has the most rigorous examination of the machine safety system and is required for complex electronic systems, but also has strict limitations when non-electrical/electronic devices/systems are involved, so even though it may be the most rigorous methodology, it is effectively also the most restricted.

This highlights the importance of understanding the requirements of a machine safety system and the limitations of each methodology, to be able to determine which methodology is actually the best one, based on the requirements for each machine safety system taken on an individual basis. In this area, it is clear that there is no one methodology that “fits best” for every situation.

On top of this, it has also been highlighted that AS 4024.1—2014 should be incorporated on every machine safety system review, regardless of the methodology being employed, as this standard covers the additional aspects which are not addressed by AS 62061.

There is, however, some light at the end of the tunnel in the quest for a simplified, rationalised methodology for the machine safety sector, with a working group currently evaluating the merits of AS 62061 and ISO 13849.1 with the objective of producing a single standard with a single methodology. This will not be a simple process to achieve and current indications show a target date for completion and introduction of the new standard around 2016.
References

AS 4024.1—2014 Safety of machinery (series)

ISO 13849.1: 2009 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

ISO 13849.2: 2012 Safety of machinery – Safety-related parts of control systems – Part 2: Validation


AS 61508—2011 Functional safety of electrical/electronic/programmable electronic safety-related systems (parts 1-7)