Session 2:

Machine Safety in Hazardous Areas

Ross De Rango
Hazardous Area Systems Manager
NHP Electrical Engineering Pty Ltd

Introduction – Icarus, Daedalus, and risk management

The ancient Greek story of Icarus and his father, Daedalus, tells of a master craftsman who made wings from feathers and wax, designed such that a man could wear them and fly. Daedalus made two sets of wings, for himself and his son, so that they could escape an island. Knowing the material properties of feathers and wax, Daedalus warned his son Icarus not to fly too high or too low, lest the wax be melted by the sun or the feathers clogged by sea-spray. Predictably, the son ignored the warnings, the wings failed, and Icarus fell and died. This myth is often taken as a parable on the dangers of pride and over-reach[1] – essentially making a point around the consequences of ambition.

Today in industry, however, we find a commercial environment in which ambition and over-reach are expected. A lack of willingness to reach beyond established capabilities is a lack of innovation – a sure sign of upcoming organizational decline. To counter the risks innovation brings in the environments we work in, we use risk management methodologies.

In our modern context, another interpretation of the Icarus myth is one of a failure of risk management. The risks of the system Daedalus built to the operators were known. What was missing was any attempt to mitigate those risks beyond a verbal instruction to the operator. The insufficiency of such warnings is a cornerstone reason for engineered safety systems, such as those this paper covers.

The overlap of AS4024 and AS/NZS60079

Disasters start in the absence of risk management. In this paper, we're concerned with the intersection of two kinds of risks, that are very well understood independently.

Machine Safety – AS4024

Machine safety, covered in Australia under AS4024, relates generally to mechanical injuries resulting from moving equipment. It starts with an hierarchical approach, mandating:

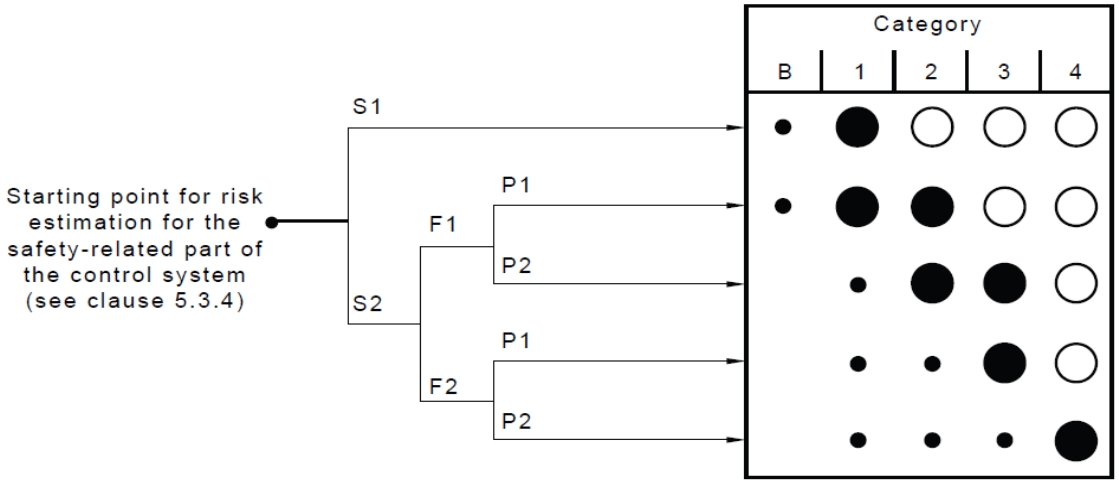
- Risk elimination where possible
- Substitution for less serious risks where elimination cannot be achieved
- Engineering controls where neither elimination or substitution can be achieved, and
- Personal protective equipment (PPE) as a last line of defence.

Within the engineering controls scope, another hierarchy is considered – this time, looking at keeping solutions as simple and as effective as possible. For example, light curtains should not be used if mechanical guards will suffice.

Once a determination has been made that engineering controls are required, a primary design consideration is how serious the risk is. Within the scope of AS4024, we use a basic risk estimation chart to consider:

- The severity of likely injury:
  - S1 being a non-serious 'first-aid kit' situation
  - S2 typically considered as non-reversible, significant recovery time, hospitalisation)
- The frequency and/or duration of exposure
  - F1 being less exposure
  - F2 being more exposure
- The probability of avoidance
  - P1 being a hazard the individual could reasonably evade
  - P2 being a hazard the individual would likely not be able to evade

This leads us to a category level that the engineering controls applied to the application need to meet, ranging from B to 4, with Category 4 being the most stringent in its requirements.



In practice, we often find implementation of Category 2 systems to be problematic. Category 2 includes a requirement to test functionality of devices in the system as part of system start up, during operation. If machine is not stopped/started regularly, and/or if the demand rate is low, periodic functional testing is required. For example, if the safety system included a level sensor to guard against tank overflow, a Category 2 rated system would need to include some means to routinely validate that sensor's performance – a practical challenge. For this reason, it is often more practicable to design to either Cat 1 or Cat 3; it can be seen from the chart above that this is provided as an option.

In this paper, we will focus on Category 3 and 4 safety systems. Note that to achieve Category 3 and 4, monitoring of the safety devices is required - where

reasonable to do so for Category 3, as an absolute requirement for Category 4. This is typically done through the use of safety relays or safety PLCs, which are shown in the application examples below.

Explosive Atmospheres – AS/NZS60079

Explosive atmospheres, covered for on-shore installations in Australia under AS/NZS 60079, relates to the risks presented by gases, vapours, and dusts. Again, we see an hierarchical approach, starting with risk elimination (remove equipment from the hazardous location), moving through substitution (place equipment in minimally hazardous zone), and then to engineering controls – personal protective equipment being less relevant to this type of risk. And, again, within engineering controls we see a wide range of different techniques, applicable to different application requirements.

Of principal interest for the purposes of this paper is zoning. Other considerations of course need to be taken into account to ensure that equipment installed is safe for the location, but it is zoning that has the most impact in the context of design choices for machine safety systems in hazardous areas.

The images below provide some clarity - in brief:

- in Zones 0 and 20 we expect to see a risk continuously present – the inside of a grain silo; the inside of a tank containing a liquid with a low flashpoint.
- In Zones 1 and 21, we expect to see a risk in normal operation of the equipment – connection/disconnection points, vents, immediate surrounds of conveyors, and so on.
- In Zones 2 and 22, we expect to see a risk in abnormal conditions – leaking flanges, unusual wind conditions, and the like.

The overlap

There are many workplaces still that do not apply either of these standards, in situations where they could be applied to make the workplaces safer. Consider as general examples:

- bucket elevators in agriculture

- open mixers for flammable liquids, which release vapour.
- crushing equipment for solid materials, which release flammable dusts

In all of these cases, an operator in close proximity to the equipment while it is in normal operation is at significant personal risk of serious mechanical injury. In all of these cases, we'd consider the area to be zoned hazardous, under the terms of 60079.

The approach taken here is to use as a frame of reference the safety category level, and the zone. A matrix is provided below, starting with Category 3:

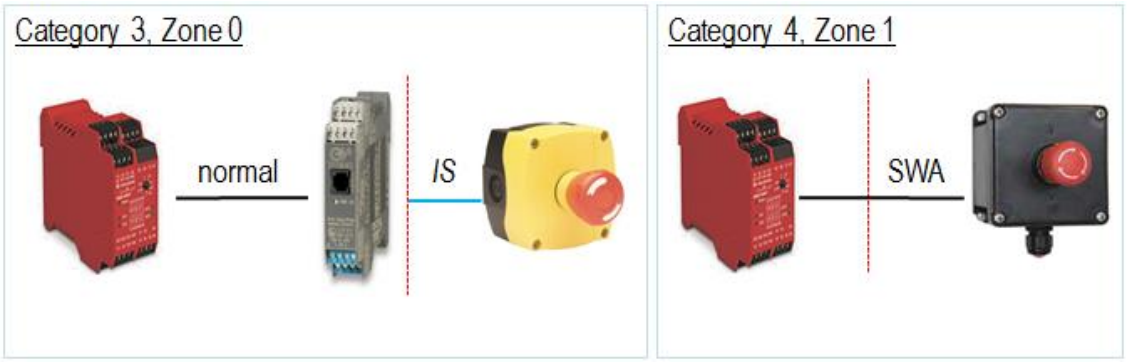
	Zone 1,2,21,22	Zone 0,20
Category 3	Yes	Yes
Category 4	Yes	Consider further

In the table above, by 'Yes' we're indicating that it's reasonable to routinely encounter these situations and design for them. By 'Consider further', we're indicating that while there are ways to engineer systems complying to Category 4 and zone 0, they should not regularly arise. If the explosive atmosphere is more or less continuously present (zone 0), ***and*** contains fast moving machinery capable of inflicting serious injury, humans should ideally not be there on a frequent or long-duration basis (category 4). In short, before starting system design on the engineering controls, review what the operator is doing there.

Happily, we are seeing an increased desire to implement systems which meet both sets of standards. This said, it is also apparent that amongst the engineering community, there is a knowledge gap around how to apply both sets of standards simultaneously, in cases where both types of risk are present. The purpose of this paper is to outline some specific techniques useful for achieving this.

Application example 1: E-stop buttons

We are all familiar with emergency stop buttons. The intent is to provide the operator with a means to immediately halt the machine. Pull-wire switches and dead-man switches, are similar in principle and in execution to the layouts below:



The Category 3, Zone 0 solution shown on the left uses a safety relay and a dual channel galvanic isolator (IS barrier) in the safe area, with intrinsic safe

wiring going from the galvanic isolator to a standard E-stop in the field. The emergency stop button is a simple device under 60079.11, clause 5.7, which permits its use with the galvanic isolator as part of an intrinsically safe circuit. The wiring between the galvanic isolator and the E-stop does not need to be Steel-wire armored (SWA) – though it does need to comply to intrinsic safe wiring rules. The limitation with this approach is that category 4 safety is not achievable – the use of galvanic isolators interferes with the ability to monitor for cross-channel faults, which is required to meet with Category 4. Zener barriers have the potential to resolve this challenge, but introduce the issue of managing earths more closely.

The Category 4, Zone 1 solution above is very common in hazardous area installations. Simply, an Ex-e or Ex-d rated enclosure with E-stop, wired direct back to the safety relay in the safe area. In this case, Category 4 becomes achievable, but zone 0 is not, as Ex-e and Ex-d protection methods are not suitable for zone 0.

Application example 2: Key exchange systems

This technique involves a safety relay wired to a captive key switch in the safe area, and a mechanical lock securing a movable guard or gate with a captive key actuation mechanism in the hazardous area – it allows Category 3 and Zone 0 to be achieved.

Zone 0 is achieved here through removing the electrical components from the zone entirely. This conforms to 60079.14, clause 4.1, which states:

“Electrical equipment should, as far as is reasonably practicable, be located in non-hazardous areas. Where it is not possible to do this, it should be located in an area with the lowest requirements”

This style of approach is suited to applications requiring occasional personnel access – securing movable guards and access gates.

In normal operation, the key is in the switch in the safe area, and the mechanical lock is keeping the gate shut. When the operator wishes to go through the gate, he removes the key from the switch in the safe area, which triggers the safety relay to create a ‘safe-state’ – typically machine power off, slow speed or ‘jog mode’, depending on the application. With the key in hand, the operator can now unlock the gate. When he’s done in the hazardous area, the operator re-locks the gate (note, it’s a captive key system – until the gate is locked, the key will not release), returns the key to the switch in the safe area, and turns it back to it’s normal position. This triggers the safety relay to return the system to normal operation.

Zone 0 here is achieved by using a purely mechanical device in the zoned area. This yields a significant installation advantage, in that no wiring needs to go into the zone – the lock is a standalone mechanical item. Category 3 derives from the way in which the key system is engineered – unique keys, captive to locations, makes the system robust and relatively hard to defeat.

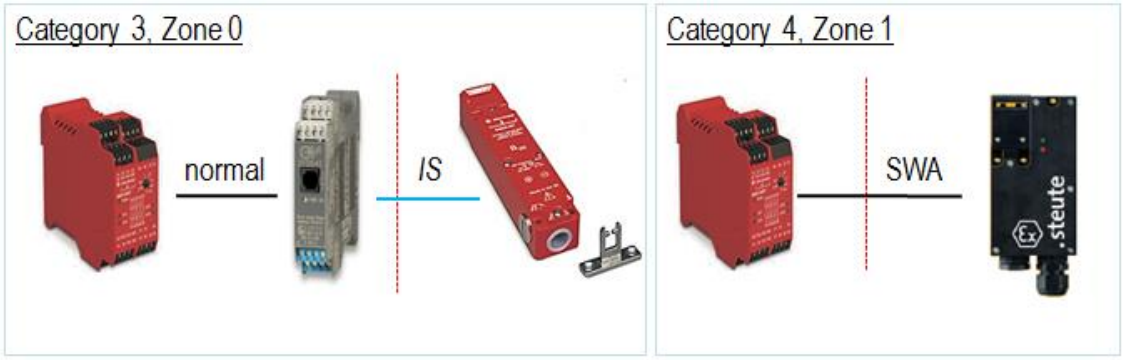
One limitation to this approach is scalability and key management. Managing a large number of unique keys can be problematic – clearly having spare keys readily available will defeat the purpose of the system, but if the operator drops one in a wheat silo (for example) there will be down time while someone either gets a new key or defeats the safety system some other way.

Another limitation is for systems that don't stop quickly – large inertial loads require run down time to come to a halt. Large cutting equipment, bucket elevators, and large mixers are examples of this.

Application example 3: Solenoid interlocks

This style of solution picks up where key exchange systems leave off.

What a solenoid interlock provides is for the safety relay to electronically unlock the gate for the operator, in response to the operator's request *combined with* other information, such as a run-down timer, a speed monitoring system, or similar. The intent is usually to ensure that whatever machinery is present behind the gate is in a safe state for the operator to be near it, *before* the gate is unlocked.



As with the E-stop example, two techniques are shown here – one using an intrinsically safe approach to provide for zone 0 requirements, and one using an Ex-de rated solenoid to provide for Category 4 requirements.

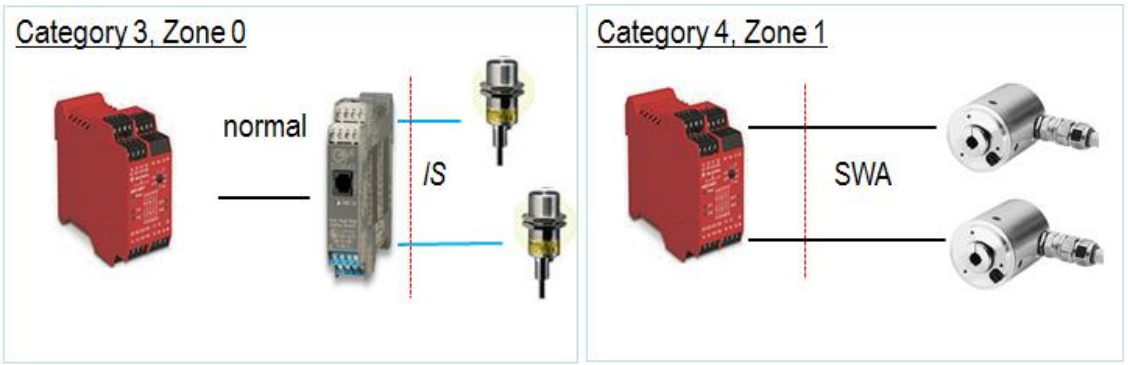
Distinct from the E-stop example, the solenoid interlock in the intrinsically safe example is ***not*** a simple device – it contains a coil, which means it will need to be Ex-i rated. Special attention needs to be paid to selecting appropriate barrier / solenoid combinations in these circumstances; it is often more practicable to use an Ex-de rated solenoid, and mount it somewhere other than zone 0.

The key downside from a trapped key system is that it is no longer a pure mechanical solution in the hazardous area; there are now live components in the zone, with wiring needing to go to them.

The key advantage of solenoid interlocks over key exchange systems is that the unlocking function is now more programmable. With a solenoid interlock, it's no longer the operator who unlocks the gate – it's the program.

Application example 4: Speed Monitoring

Speed monitoring has several usage cases. It is often used in combination with solenoid interlocks, above, to ensure that a machine is either stopped or moving sufficiently slowly before an operator can gain access. It is also used in cases where overspeed on a mechanical system may occur and create a potentially dangerous mechanical failure mode. Finally, speed monitoring can be useful in cases where system overload may occur – if a motor wired DOL is running significantly slower than expected, it may indicate that the conveyor it's driving is overloaded.



As with the solenoid interlock and E-stop example, two methods are shown here, using different protection techniques. Note that Category 3 is applicable to both – this is a function of relay operation; Category 4 is not commonly used in connection with speed monitoring.

Note that inductive proximity switches (pictured left, used with the galvanic isolator) are not simple devices. These need an Ex-i rating; inductive proxes of this nature are readily available.

On the right, Ex-de encoders are shown wired direct to the safety relay using SWA cable. For dust-zoned installations (21,22), Ex-t rated inductive proximity switches wired directly to the safety relay in the same fashion would provide similar function – it comes down to selection of a suitable safety relay at that point.

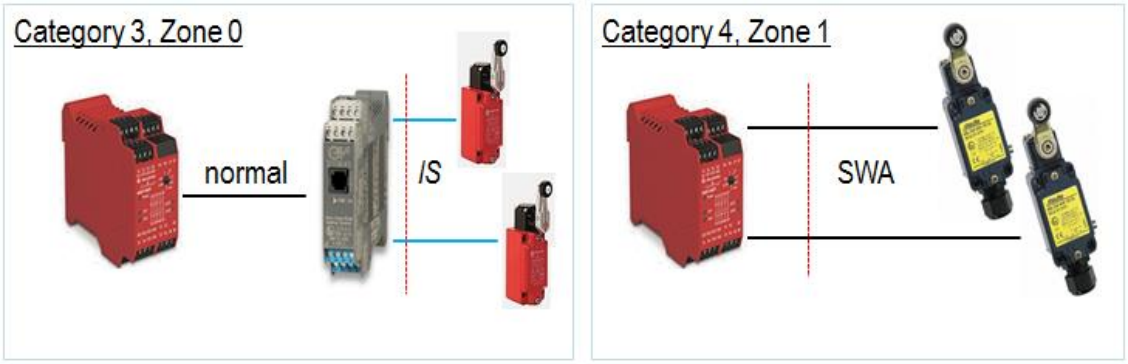
Note also the presence of dual field devices. From a safety category standpoint, there is an assumption that one device may fail, which would lead t the safety relay acting on bad information. To resolve this, safety relays designed for speed monitoring applications typically take dual inputs – in addition to looking at the incoming data, they cross-check to ensure they're seeing the same frequency from both devices within a fairly tight tolerance. Any significant deviation, and the relay engages the safe state.

Application example 5: Limit switches

The final application example in this paper covers limit switches. These are typically used for things like belt drift, machine travel limits, verifying that operators have correctly positioned things before taking other actions (stowing refueling hoses, lowering platforms on mobile equipment), and detecting positions of sliding guards.

Unlike the key exchange and solenoid interlocks shown above, limit switches do not prevent things gates and guards from opening – when used on sliding

guards, the intent is for the system to be immediately aware that the gate has been opened, and take whatever safety-related action is required.



As with E-stops, we are dealing with simple devices connected to the Galvanic Isolator shown in the Category 3, Zone 0 approach on the left. This means that while the limit switch still needs to be safety rated, it does not need to be Ex-i rated.

As with the speed monitoring example, for Category 3 and 4 safety systems we need to take into account the possibility of device failure in the field – typically, mechanical failure of the limit switch. To resolve this, dual field devices are the common approach.

Conclusion

This paper has shown a range of techniques applicable in situations requiring engineering controls to provide for machine safety in hazardous areas. The techniques shown are not in any way exhaustive; there are many ways to solve these types of challenge – they're simply methods that we have seen successfully used to meet the overlap.

Machine safety standards and hazardous area standards are rapidly evolving, and new innovative products in this space are coming to market even faster. This is all positive – better standards, and better equipment, work to increase the likelihood that we go home safe at the end of the working day.

Disclaimer

Techniques presented in this paper and the associated presentation should be considered in the context of the application. These techniques should not be applied without undertaking a risk assessment related to the specific installation. While some representative product images are used, the techniques are vendor neutral, subject to manufacturer's documentation and/or independent certification as applicable.

References

[1] Jacob E. Nyenhuis - Myth and the creative process: Michael Ayrton and the myth of Daedalus, the maze maker - 345 pages Wayne State University Press, 2003

AS/NZS 60079

AS4024