



**Industry &  
Investment**

# **TECHNICAL REFERENCE**

**EES008-1**

**Electrical Engineering Safety**

**Design of powered winding  
systems**

**General requirements and  
registration**

**Produced by Mine Safety Operations Branch**

**Industry and Investment NSW**

**March 2011**

### **Public comment period**

Please note that this technical reference is published in draft form for the purpose of obtaining public comment.

Your feedback is welcomed and will assist with reviewing and improving the document. A feedback form is provided in the appendices for your convenience.

The closing date for public comment is Friday 20 May 2011.

DRAFT

## DISCLAIMER

The compilation of information contained in this document relies upon material and data derived from a number of third party sources and is intended as a guide only in devising risk and safety management systems for the working of mines and is not designed to replace or be used instead of an appropriately designed safety management plan for each individual mine. Users should rely on their own advice, skills and experience in applying risk and safety management systems in individual workplaces.

Use of this document does not relieve the user (or a person on whose behalf it is used) of any obligation or duty that might arise under any legislation (including the Occupational Health and Safety Act 2000, any other act containing requirements relating to mine safety and any regulations and rules under those acts) covering the activities to which this document has been or is to be applied.

The information in this document is provided voluntarily and for information purposes only. The New South Wales Government does not guarantee that the information is complete, current or correct and accepts no responsibility for unsuitable or inaccurate material that may be encountered.

Unless otherwise stated, the authorised version of all reports, guides, data and other information should be sourced from official printed versions of the agency directly. Neither Industry & Investment NSW, the New South Wales Government, nor any employee or agent of the Department, nor any author of or contributor to this document produced by the Department, shall be responsible or liable for any loss, damage, personal injury or death howsoever caused. A reference in this document to "the Department" or "Industry and Investment NSW" or "I&I NSW" is taken to be a reference to the Department of Industry and Investment.

Users should always verify historical material by making and relying upon their own separate enquiries prior to making any important decisions or taking any action on the basis of this information.

This publication contains information regarding occupational health, safety, injury management or workers compensation. It includes some of your obligations under the various workers compensation and occupational health and safety legislation that Industry & Investment NSW administers. To ensure you comply with your legal obligations you must refer to the appropriate legislation.

In the event of inconsistency with a provision of any relevant Act or Regulation the provision prevails over the guideline.

This publication may refer to NSW legislation that has been amended or repealed. When reading this publication you should always refer to the latest laws. Information on the latest laws can be checked at:

[www.legislation.nsw.gov.au](http://www.legislation.nsw.gov.au)

Alternatively, phone (02) 4931 6666.

## Foreword

Industry and Investment NSW (I&I NSW) has a vision for electrical engineering safety, which is:

“A mining and extractive industry that has eliminated death and injuries from electrically powered and electrically controlled equipment.”

Electrical engineering safety encompasses:

- Prevention of electric shock and burns, (electrocution, death or injury as a result of a shock, radiation burns, flash burns, burning particles and plasma)
- Prevention of electrical arcing and surface temperatures that have sufficient energy to ignite gas and/or dust
- Prevention of fires caused by the malfunction of electrical equipment
- Prevention of injury and death from unintended operation, failure to stop or failure to operate, of electrically powered and electrically controlled equipment
- Use of electrical technology to provide safe-guards and monitoring for non-electrical hazards and electrical hazards with a safety integrity level appropriate for the risk.

Supporting this vision is a philosophy of operation outlined in the Strategic and Operational Plan for Electrical and Engineering Safety in NSW Mines, which can be viewed at [www.dpi.nsw.gov.au](http://www.dpi.nsw.gov.au). The philosophy of operation embraces a **System Safety Approach**, applying the **Hierarchy of Risk Controls** and the **Risk Reduction Precedence**, and fostering a **Positive Safety Culture**.

Satisfactory electrical engineering safety has to be achieved in the context of the mining industry's increasing electricity consumption and its use of electrical technology, with resulting increases in size (power rating) and complexity. With this comes a changing risk profile. To adequately manage the safety risks posed by electrical equipment and technology the hazards, risks and risk controls need to be thoroughly understood. This understanding must be at an engineering level, so electrical engineers within the management structure of coal or mining operations will be responsible for development, periodic review and day to day implementation of the Electrical Engineering Safety aspects of a powered winding system.

This document is one of a series dealing with powered winding systems. These documents are consistent with the above philosophy of operation and are a key element in realising the vision and points 4 and 5 for electrical engineering safety listed above.

The documents in the series are:

- EES008.1 Design of Powered Winding Systems - Electrical Engineering Safety – General Requirements & Registration
- EES008.2 Design of Powered Winding Systems - Electrical Engineering Safety – Definitions and types of winders
- EES008.3 Design of Powered Winding Systems - Electrical Engineering Safety – a prescriptive approach
- EES008.4 Design of Powered Winding Systems - Electrical Engineering Safety – a Functional Safety approach
- EES008.5 Life-Cycle Management of Powered Winding Systems - Electrical Engineering Safety Requirements

Current legislation is consistent with this philosophy. In particular Clauses 107 and 113 of the Occupational Health and Safety Regulation 2001 recognise the high risk nature of mine winders, so legislation requires that the Director General design register and item register powered winding systems.

The purpose of this document is to facilitate, within an electrical engineering safety context, the design registration of powered winding systems and to assist coal and mine operators to maintain powered winding systems in a safe state.

Use of this document will:

- Enhance the management of safety risks associated with powered winding systems through good and safe electrical engineering practice
- Contribute significantly toward the prevention of unintended operation of mine winders and preventing any unintended operation from injuring personnel.

Use this technical reference to assess your Powered Winding Systems.

Use this technical reference as an aid to the design of Powered Winding Systems.

This technical reference will be used by Mine Safety Operations to assess powered winding systems for design registration purposes and routine assessment activities.

**John Francis Waudby**

Senior Inspector of Electrical Engineering – Special Projects

# Table of Contents

Foreword.....	4
Table of Contents.....	6
1. Establishment .....	8
1.1 Title.....	8
1.2 Purpose .....	8
1.3 Scope .....	8
1.4 Authority .....	8
1.5 Definitions.....	8
1.6 Applicable legislation.....	9
1.7 Referenced Gazette Notices .....	9
1.8 Referenced Standards and Guidelines .....	9
1.9 Acronyms .....	10
1.10 Who is affected by this Technical Reference? .....	10
2. Background – registration and approval .....	11
2.1 1984 Legislation .....	11
2.2 1999 Legislation .....	11
2.3 Non-mining Legislation.....	11
2.4 2006 Coal Legislation and 2007 Mining Legislation .....	11
3. Powered winding system safety requirements.....	13
3.1 Plant safety.....	13
3.2 Essential safety outcomes.....	14
3.3 Hardware requirements.....	14
3.4 Software requirements .....	15
3.5 Safety compliance approach .....	15
3.6 Prescriptive compliance approach .....	17
3.7 Functional safety approach .....	17
4. Information and registration .....	19
4.1 Plant safety information.....	19
4.2 Powered winding system plant safety information .....	19
4.3 Design registration information – electrical engineering safety file.....	20
4.4 Design registration – verification .....	21
5. Electrical engineering safety design review / certification.....	23
5.1 Assessment details .....	23
5.2 Process description .....	24

5.3 Process review .....	26
6. Example description of the Powered Winding System .....	31
6.1 Example – Mine Winder System Configuration.....	31
6.2 Example – Summary of the winder control.....	31
6.3 Example – functional description : cage winding control .....	33
6.4 Example – overview of the safety approach.....	35
6.5 Example – description of the safety functions .....	36
6.6 Example – overspend envelope .....	42
6.7 Example – program structure .....	43
7. Appendices .....	44
7.1 Feedback Sheet .....	44
7.2 I&I NSW Contact details.....	45

DRAFT

# 1. Establishment

## 1.1 Title

This is the Mining Industry Technical reference – *Electrical Technical Reference for Design of Powered Winding Systems Electrical Engineering Safety – General Requirements & Registration.*

## 1.2 Purpose

This document is intended to assist designers and manufactures of powered winding systems, including shaft sinking winders, by indicating parameters which will be considered in the assessment for design registration. It will also aid coal and mining operators to obtaining item registration. It also provides specific information on the content of any submission for design registration. Full details of how to obtain design registration is given in Guidance Note GNC-005 NSW DPI Guidance Note – *Registration of Plant Designs.*

**Note:**

Registration does not limit the responsibility of the designer, manufacturer and operator to ensure that the powered winding system is safe to operate.

This technical reference describes acceptable arrangements that can be tailored to suit the particular needs of an operation. It identifies some control measures relevant to electrical circuitry. It is intended to protect the safety of workers, others in the workplace and property.

## 1.3 Scope

This technical reference extends to all underground coal and mining operations in NSW that use a powered winding system. This technical reference is intended to provide guidance for any person designing, implementing, managing or reviewing a powered winding system installation.

## 1.4 Authority

This is an Electrical Engineering Safety Technical Reference and is recommended by Mine Safety Operations, Industry and Investment NSW.

## 1.5 Definitions

**Conveyance (EUC):** Any car, carriage, cage, skip, kibble, or stage in which persons, minerals or materials are wound through a shaft/drift or any counterweight. The terms conveyance and EUC are used interchangeably throughout this series of documents.

**Powered Winding System:** Refer to the Gazette Notice for Powered Winding systems

**Other Definitions:** Refer to - EES008.2 Design of Powered Winding Systems - Electrical Engineering Safety – Definitions and types of winders.

## 1.6 Applicable legislation

Occupational Health and Safety Act 2000  
Occupational Health and Safety Regulation 2001  
Coal Mine Health and Safety Act 2002  
Coal Mine Health and Safety Regulation 2006  
Mine Health and Safety Act 2004  
Mine Health and Safety Regulation 2007

## 1.7 Referenced Gazette Notices

Gazette Notice for Powered Winding systems

## 1.8 Referenced Standards and Guidelines

AS 4024.1 Series - Safety of machinery  
AS 61508 Series - Functional safety of electrical/electronic/programmable electronic safety-related systems  
AS 62061 Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems  
EES008.2 Design of Powered Winding Systems - Electrical Engineering Safety – Definitions and types of winders  
EES008.3 Design of Powered Winding Systems - Electrical Engineering Safety – a prescriptive approach  
EES008.4 Design of Powered Winding Systems - Electrical Engineering Safety – a Functional Safety approach  
EES008.5 Life-Cycle Management of Powered Winding Systems - Electrical Engineering Safety Requirements  
EN 954-1, Safety of machinery - Safety related parts of control systems - Part 1  
Guidance Note GNC-005 *NSW DPI Guidance Note – Registration of Plant Designs.*  
Guidance Note GNC-006 *NSW DPI Guidance Note – Registration of Item of Plant*  
ISO 13849.1 Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design

## 1.9 Acronyms

**EUC:** Equipment under control

**Other Acronyms:** Refer - EES008.2 Design of Powered Winding Systems - Electrical Engineering Safety – Definitions and types of winders

## 1.10 Who is affected by this Technical Reference?

This Technical Reference is relevant for all operators of coal or mining operations in New South Wales where there is a powered winding system.

DRAFT

## **2. Background – registration and approval**

Due to the very high risks associated with powered winding systems regulators have required that some regulatory review of winder design be undertaken. Traditionally this has been done by requiring that mine winders must be approved by the Chief Inspector. Under previous coal mining legislation particular approval requirements were specified in the 1984 and 1999 Regulations.

### **2.1 1984 Legislation**

Clause 7 of the Coal Mines Regulation Act (Shafts and Roadways – Underground Mines) regulation 1984 required that a mechanically operated winding apparatus or mechanically operated rope haulage apparatus used at a mine for transporting persons through any shaft or roadway be approved by the Chief Inspector.

Clause 9(1) and Clause 11 of the Coal Mines Regulation Act (Shafts and Roadways – Underground Mines) Regulation 1984 required that conveyances used at coal mines for transporting persons through a shaft or roadway, be of a type which has been approved for the purpose by the Chief Inspector.

Clause 6(6) of the Coal Mines Regulation (Approval of Items) Regulation by way of notice required that all slope drift rope haulage systems be approved by the Chief Inspector.

### **2.2 1999 Legislation**

Part 3 Transport, Division 3 Powered winding systems, Clause 58, of the Coal Mines (Underground) Regulation 1999 required that a powered winding system must not be used at a mine unless it is approved.

### **2.3 Non-mining Legislation**

Non-mining regulators have also recognized that high risk plant needs to be subject to regulatory activity and requires high risk plant to be both design and item registered.

### **2.4 2006 Coal Legislation and 2007 Mining Legislation**

With the latest regulatory review there has been an alignment of non-mining and mining safety legislation. As a result, coal mine winders are no longer required to be approved; however, they do have to be design and item registered. This registration requirement has also been extended to metalliferous mines. For mining plant, which includes powered winding systems, the registration is performed by the Director General (or delegate) of Industry and Investment, NSW.

Clause 107 Occupational Health and Safety Regulation 2001 as amended requires powered winding systems (being any plant Gazetted as such or a lift that provides access to the underground workings of a mine) used in underground mines (coal and metalliferous) to be design registered.

Clause 113 Occupational Health and Safety Regulation 2001 as amended requires: "Powered winding systems used in underground mines" to be item registered.

Effectively this means that powered winding systems currently in use and any new powered winding system have to be design and item registered.

Details for obtaining both design and item registration are given in Guidance Note GNC-005 *NSW DPI Guidance Note – Registration of Plant Design* and Guidance Note GNC-006 *NSW DPI Guidance Note – Registration of Item of Plant*.

Specific details of 'electrical' information required for powered winding system registration are given in Chapter 4.

DRAFT

## 3. Powered winding system safety requirements

### 3.1 Plant safety

Powered Winding Systems are a major item of plant. As a result, they must incorporate ALL plant safety requirements specified in legislation, specifically Chapter 5 of the OH&S Regulation. Powered Winding Systems are covered by these requirements and they need to be integrated within the arrangements for managing Electrical and Mechanical Engineering Safety. The Electrical and Mechanical Engineering Safety Management arrangements will need to include checks to establish that designers, suppliers, manufacturers, trade agents and hirers of powered winding systems have fulfilled their obligations.

Also the operator of power winding systems needs to be sure their obligations have been fulfilled. For example, an operator who contracts out the design of a powered winding system must ensure that the person who is engaged to design the powered winding system is provided with all relevant information about matters that may affect health and safety.

All people and organisations in the supply chain have responsibilities. An end user should be able to establish that any foreseeable hazards that may arise during the life-cycle of the powered winding system have been identified, risks assessed, risks eliminated or controlled, information has been provided and powered winding systems are not used in conditions likely to give rise to hazards.

The life-cycle management of Powered Winding Systems is an integral part of a coal or mining operation's arrangements for managing plant safety within an Electrical & Mechanical Engineering Safety context.

With regard to Powered Winding Systems the purpose of these arrangements include, but are not limited to:

- Preventing unintended operation of plant.
- Providing electrical and mechanical safeguards for electrical, mechanical and other non-electrical hazards with an appropriate safety integrity level.
- To generally provide the means by which the safety of electrical and mechanical plant is managed including requirements of the relevant Acts and this Regulations and relevant plant safety requirements under the *Occupational Health and Safety Regulation 2001*.

In achieving the above purpose the essential safety outcomes specified in 3.2 shall be achieved.

## 3.2 Essential safety outcomes

- 3.2.1 The conveyance shall operate between pre-defined travel limits.
- 3.2.2 When the conveyance operates outside the pre-defined limits, it shall be automatically brought safely to rest.
- 3.2.3 The conveyance shall operate between pre-defined speed limits.
- 3.2.4 When the conveyance operates outside the pre-defined speed limits, it shall be automatically brought safely to rest.
- 3.2.5 The conveyance shall operate within pre-defined acceleration and deceleration limits.
- 3.2.6 When the conveyance operates outside the pre-defined acceleration and deceleration limits, it shall be automatically brought safely to rest.
- 3.2.7 The conveyance shall not move while people are entering or leaving the conveyance.
- 3.2.8 The conveyance shall only be capable of access or egress at predefined locations. (When the conveyance is located at a predefined location, only then can access gates or doors on the conveyance, shaft collar and shaft entries be opened).
- 3.2.9 The conveyance shall have facilities that provide for signaling, operating or communicating to the winder control system or operator.
- 3.2.10 The conveyance shall not require any part of the body to protrude from the conveyance to signal, operate or communicate to the winder control system or operator.
- 3.2.11 The conveyance shall be capable of initiating it being automatically brought safely to rest in an emergency.
- 3.2.12 In the event of any safety related device, feature, component, circuit or the like failing in such a manner that it becomes incapable of operating on demand, the conveyance shall be automatically brought safely to rest.

## 3.3 Hardware requirements<sup>1</sup>

- 3.3.1 Ensure that all mechanically-actuated position switches are actuated in the positive mode.
- 3.3.2 Ensure that all hardware is suitable for the environment in which it is to operate, in particular with respect to resistance to corrosive liquids, ingress of dust and the ability to withstand impact damage.
- 3.3.3 Provide additional measures to prevent/detect failure where magnetic and proximity type safety switches are used.
- 3.3.4 Employ redundancy and diversity to avoid common cause failure.

---

<sup>1</sup> *Standards which are relevant to the selection and use of electrical switches for safety related controls in mine shaft and winding systems HSL/2007/58 p.37, Health and Safety Laboratory, Buxton UK 2007*

## 3.4 Software requirements<sup>2</sup>

- 3.3.1 Ensure suitable measures are taken to prevent inadvertent or deliberate alteration if a safety related control system is capable of being re-programmed.

**Note:**

Notwithstanding the requirements of AS 4024.1, AS 61508 and AS 62061, any reprogramming shall be conducted by the manufacturer / supplier and shall be risk based to verify the integrity of any changes.

- 3.4.2 Ensure Safety related software is self-monitoring.

## 3.5 Safety compliance approach

As part of the operations risk management process appropriate risk analysis must be undertaken. To enable decisions to be made based on the risk analysis, risk targets need to be established in the context of the NSW mining industry's goal of zero harm. This requires that risks be reduced to a level demonstrably As Low As Reasonably Practicable (ALARP).

There are three approaches to achieving ALARP risk, essential safety outcomes and addressing electrical engineering safety aspects of powered winding systems. These are:

- Full compliance with the prescriptive requirements specified in EES008.3, or
- Credibly applying the functional safety approach specified in EES008.4, or
- Substantial compliance with the prescriptive requirements specified in EES008.3 and where non-compliances are identified, providing alternative risk controls that provide for a level of risk less than or equal to that achieved by full compliance to EES008.3. The alternative risk controls must be established using the functional safety approach as specified in EES008.4

Irrespective of the approach taken, it must be systematic and encompass the life cycle of the powered winding system from concept to disposal. It is also important to clearly define the safety requirements for the powered winding system in a safety requirements specification and to specify the systematic review of all risk controls at critical points of the life cycle. It is recommended that a layer of protection analysis (LOPA) be conducted and that the winder control system, 'non-electrical' risk controls and the safety circuits, in combination, provide the required amount of risk reduction. This means the winder motor drive control system provides some level of risk reduction, but if this system fails then the safety circuits provides a further level of risk reduction. There may also be some 'non-electrical' layers of protection that also reduce the risk. In total the risk must be demonstrably reduced to the tolerable and ALARP level. This is shown in Figure 1: LOPA and powered

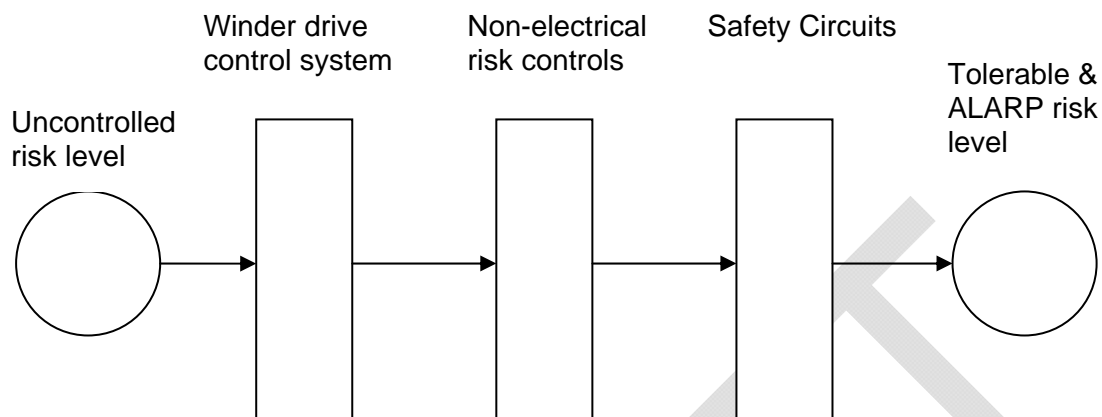
---

<sup>2</sup> Standards which are relevant to the selection and use of electrical switches for safety related controls in mine shaft and winding systems HSL/2007/58 p.37, Health and Safety Laboratory, Buxton UK 2007

winding systems.

DRAFT

**Figure 1: LOPA and powered winding systems**



Important elements in the safety approach are planning for every stage of the design and commissioning process and the verification and validation of the design. An example is given in Chapter 5.

### 3.6 Prescriptive compliance approach

Refer to EES008-3

This approach requires full compliance with EES008-3. Where it is required not to apply any element of the prescriptive requirements, then an alternative engineering control shall be implemented using a functional safety approach in accordance with EES008-4.

### 3.7 Functional safety approach

Refer to EES008-4.

This approach requires that AS61508, AS61511 or AS62061 be followed. This involves taking a holistic view of safety functions and places emphasis on systemic rigor, documentation, verification and audit. Consideration must be given to everything that is needed to ensure the safety function is successful when required to operate, eg input and sensing devices, logic/control devices and output devices (actuators).

The approach is risk-based and determines safety integrity requirements for risk controls. It uses safety integrity levels (SIL's) to specify reliability and fail-safe performance of safety functions. The SIL is a measure of risk reduction. To determine the amount of risk reduction requires the uncontrolled risk from the EUC to be determined; this is then compared against the specified tolerable & ALARP risk level.

**Note:** The tolerable and ALARP risk level will have to be specified by the operator.

This tolerable and ALARP risk specification will necessitate the calibration of the corporate safety risk matrix, particularly the likelihood. An example of a calibrated risk matrix is given in Figure 2<sup>3</sup>.

For mine winders unless the consequence can be reduced, which may be difficult in many circumstances, the likelihood has to be reduced. If the reduction of one level of likelihood equates to an order of magnitude reduction in risk, then effectively, a reduction in one level of likelihood implies an increase in the SIL of 1. Example: To reduce the risk from a high to a low category equates to a risk reduction factor (RRF) of 3 orders of magnitude = 1000 = SIL3.

Once the required amount of risk reduction has been decided, the amount of risk reduction to each risk control must be allocated. The risk controls in combination must achieve the required risk reduction. For a risk reduction factor of 1000 we can have one risk control with a RRF of 1000, or two risk controls (arranged to give probability multiplication), one with a RRF of 10 and another risk control with an RRF of 100 or any other combination that gives a total RRF of 1000. All of this then leads to a Safety Requirements Specification for the powered winding system.

**Figure 2 Calibrated risk matrix**

An extrapolation of the risk matrix specified in *MDG1010, Figure A.9.2* indicates that for a single fatality consequence, a “Low” risk would only be achieved with a hazardous event frequency less than 0.00001 / yr.

	1 x Medically Treatable Injury (MTI)	1 x Compensible Injury (CI) or 10 x MTI's	10 x CI's	1 x Permanent Disablement (PD)	1 x Fatality	10 x Fatalities
Frequent: ≥1 per year	Medium (100)	High (1,000)	Very High (10,000)	Severe (100,000)	Severe (1,000,000)	Severe (10,000,000)
Possible: < 1 per year (but ≥ 0.1 per year)	Medium/Low (10)	Medium (100)	High (1,000)	Very High (10,000)	Severe (100,000)	Severe (1,000,000)
Unlikely: < 0.1 per year (but ≥ 0.01 per year)	Low (1)	Medium/Low (10)	Medium (100)	High (1,000)	Very High (10,000)	Severe (100,000)
Very Unlikely: < 0.01 per year (but ≥ 0.001 per year)	Low (0.1)	Low (1)	Medium/Low (10)	Medium (100)	High (1,000)	Very High (10,000)
Barely Credible: < 0.001 per year (but ≥ 0.0001 per yr)	Low (0.01)	Low (0.1)	Low (1)	Medium/Low (10)	Medium (100)	High (1,000)
10 <sup>-4</sup> per year				Low (1)	Medium/Low (10)	Medium (100)
10 <sup>-5</sup> per year					Low (1)	Medium/Low (10)
10 <sup>-6</sup> per year						Low (1)

**Note:** For very simple winding systems the AS4024 approach may be used to determine the relevant category (CAT) and then relate that CAT to a SIL by using AS62061. If within the design a programmable system (PES) is used then it will need to conform to AS61508. Further guidance on establishing a quantifiable relationship between CAT and SIL can be found in ISO 13849-1:2006 Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design.

<sup>3</sup> Truck Loading / Rejects Bins, Functional Safety Study Report, Marcus Punch, May 2009

## 4. Information and registration

### 4.1 Plant safety information

The information must be sufficient to establish full compliance with legislation. As such Chapter 5 of the OH&S Regulation must be extensively referenced when developing powered winding system specifications. The information must encompass:

- All available information concerning health and safety about the powered winding system provided by the manufacturer
- Testing or inspections to be carried out
- Installation, commissioning, operation, maintenance, inspection, cleaning, transport, storage and, if it is capable of being dismantled, dismantling
- Systems of work necessary for the safe use
- Knowledge, training or skill necessary for persons undertaking inspection and testing
- Emergency procedures
- Any document relating to the testing and inspection.

### 4.2 Powered winding system plant safety information

The information relating to powered winding systems will be extensive. It will incorporate all the information generated from the concept phase to the disposal phase. It will basically serve two purposes:

- Information for on-going life cycle management, and
- Information for registration purposes.

The information needs to be managed so that the design and ongoing management of the powered winding system has a continual traceable history. The design registration information is just one of many avenues for accessing any of that information.

To facilitate the management of this information a 'Winder Library' should be established.

**Note:**

Alternative terms may be used for the 'Winder Library' such as 'Full Technical File' or 'Safety File'.

A 'Design Registration File' should be created within the library. This contains the essential and required information (mechanical and electrical) to obtain design registration. A sub-section of the Registration File is the 'Design Registration Electrical Engineering Safety File'. Where programmable systems are used it is essential that a 'Winder Software File' is established. This particular file will contain ALL software changes that are made.

The 'Winder Library' will be an essential component of the operation's Occupational Health and Safety Management System (OHSMS). For example the OHSMS may set the tolerable and ALARP risk levels and specify the hazard identification and risk analysis approach that is used within the powered winding system acquisition process.

### 4.3 Design registration information – electrical engineering safety file

The information supplied as part of the design registration is called the design registration electrical engineering safety file. Information supplied must be in accordance with Guidance Note GNC-005 *NSW DPI Guidance Note – Registration of Plant Designs*. It should be a distinct entity and be part of a Powered Winding System Library. A copy of this file shall be submitted in support of any application for design registration. The contents shall include:

- A list of all documents in the Powered Winding System Library.
- A list of all documents in the Powered Winding System Library which demonstrate compliance with this document and EES008-3 or 4 as appropriate or its predecessors (MDG2005).
- An index nominating precisely where each document in the "Design Registration Electrical Engineering Safety File" has been drawn from within the Powered Winding System Library.
- A clear description of the powered winding system including:
  - An electrical general arrangement drawing (system configuration), detailing major components (controller, switchgear, prime mover etc.) from the power source to the prime mover. A modified example (original example courtesy of ABB) is given in Section 6.1.
  - A summary of the winder control approach. A modified example (original example courtesy of ABB) is given in Section 6.2.
  - A functional description of the winder. A particular modified example (original example courtesy of ABB) is given in Section 6.3.
  - An overview of the safety approach taken. An example courtesy of ABB is given in Section 6.4.

**Note:**

Where the prescriptive approach is taken the relationship between the ultimate, primary and secondary safety circuits shall be clearly defined and the independence of each safety circuit shall be demonstrated.

- A clear description of the safety functions and the safety requirements specification, a modified example (original example courtesy of ABB) is given in Section 6.5.
- Over speed envelope and retardation profile, an example courtesy of ABB is given in Section 6.6.
- For programmable systems – a particular reference within the winder library that contains the program structure, an example of program structure, courtesy of ABB is given in section 6.7.

- An electrical block diagram outlining the primary and secondary safety circuits (if installed the ultimate safety circuit) or showing the realisation of the safety requirements specification.
- A general arrangement drawing showing the location of safety devices (refer to EES008.2 for typical examples).
- A summary of the standards, guidelines and technical references used in the design.
- A brief statement of compliance, variation, or reason for non-compliance with the essential safety outcomes specified in section 3.2.
- A brief statement of compliance with EES008-3 or 4. Where there is a variation to compliance, the reason for each non-compliance on a clause by clause basis.
- Results of the commissioning tests and associated statement of compliance.
- A specific section shall be maintained containing modifications or changes to any part of the winder control system carried out after the original registration of the winder.  
Changes shall be listed in chronological order.  
This section shall also contain each 5 yearly audit document including any changes following the outcome of each audit.

**Note:**

All changes shall be verified by the winder manufacture and/or a Qualified Engineer.  
All software changes shall be verified by the winder manufacturer.  
Any change to the winder control system shall be submitted to the Department for amendment to the registration document.

- Specific issues:
  1. **Shaft Sinking Powered Winding Systems:**  
The nature of shaft sinking and / or the repair or maintenance of shafts generally involves differing configurations of the shaft sinking equipment. For the purposes of design registration it will be necessary to submit documentation relating to each of the intended design / operation configurations.  
Information showing the arrangements and procedures established to address the provision of under travel protection as the depth of the shaft increases.
  2. **Explosion Protection Techniques** - For fixed winders installed in upcast shafts and for shaft sinking winders approaching coal seams, information demonstrating the explosion protection techniques (including any procedures) adopted to safely operate the winding installation in this environment.

#### 4.4 Design registration – verification

Design verification requirements are specified in gazette notices relating to powered winding systems at:  
<http://www.dpi.nsw.gov.au/minerals/safety/legislation/gazettals/occupational-health-and-safety-act-gazette-notices>

The gazette notice requires that from an Electrical Engineering Safety perspective, a qualified practicing engineer(s) registered on the National Professional Engineers Register (administered by Engineers Australia) or a qualified practicing engineer acceptable to the chief inspector must undertake the following:

- Confirm that the design of the powered winding system, as identified by a series of drawings, test certificates and other documents, meets the requirements of EES008 parts 1 to 4 (or MDG2005) as appropriate.
- Identify and state any technical specifications as required for the manufacture, assembly, testing and commissioning of the powered winding systems and its components, to meet the above requirements.

Irrespective of the approach taken in designing the powered winding system, any Functional Safety assessment to verify that the specified SIL's have been realised, shall be undertaken by a person (natural or corporation) that has internationally recognised Functional safety qualifications, for example with post nominal's "CFSE".

The installation and commissioning of the powered winding system must be carried out under the supervision of a qualified mechanical and electrical engineer.

An opportunity must be provided for witnessing of the commissioning process by an engineering representative of the Senior Inspector of Mechanical Engineering and Senior Inspector of Electrical Engineering of Mine Safety Operations.

## 5. Electrical engineering safety design review / certification

### 5.1 Assessment details

#### Electrical Design Certification Review

<b>Client:</b>	Coal Pty Ltd
<b>Project:</b>	Colliery Men and Materials Drift Winder
<b>Job Number:</b>	
<b>Folder Number:</b>	
<b>Context:</b>	Powered Winding System – Electrical Design Certification
<b>Description:</b>	<p>Certification in accordance with Notice under Clause 112A of NSW Occupational Health and Safety Regulation 2001 is required as part of design registration for powered winding systems.</p> <p>This document outlines the process used by ..... to assure itself that appropriate assessments and reviews are conducted before the certificate is issued.</p>
<b>Date:</b>	
<b>Author:</b>	
<b>Objectives of assessment:</b>	To provide traceable evidence of design, installation, commissioning and handover process. The process commences with design requirements (arising from risk assessments, MDG 2005 etc.), then follows the requirements through the functional specification to final commissioning, including intermediate verification and validation checks by designers and suppliers. Final independent validation checks against MDG 2005 and other requirements, clause by clause, noting the relevant support document references.
<b>Agreed scope, boundaries, limitations:</b>	The scope of this design certification is limited to the electrical safety systems modified as part of the upgrade project.
<b>Key stakeholders:</b>	Mine operator, mine employees, NSW Department of Industry and Investment.
<b>Note:</b>	
<b>Disclaimer:</b>	

## 5.2 Process description

### Description of items examined as part of the design certification review

<b>1. Assess risk, determine risk reduction needed from winder safety circuits</b>	<ul style="list-style-type: none"> <li>• Use fault trees, internal corporate risk evaluation methods or look-up tables per AS IEC 61508.</li> <li>• Tolerable risk level: Apply MDG 1010, UK HSE or NSW HIPAP No 4 (1990) guidelines.</li> <li>• Alternatively, mine operators often accept the published standards, guidelines or technical references.</li> </ul>
<b>2. Allocate risk reduction to various means, including safety circuits</b>	<p>Generally no other means are available, so mine operators either use their own assessments from Step 1 or apply the published standards, guidelines or technical references.</p>
<b>3. Design and operational risk assessment</b>	<ul style="list-style-type: none"> <li>• Conducted at the design stage. Starting point for systematic safety integrity.</li> <li>• Mine operators provided with clear definitions of systematic failures vs. random hardware failures.</li> <li>• Outlines design techniques for avoiding systematic failures, eg design for maintainability. See Advitech summary of AS IEC 61508 requirements, 22 Aug 08.</li> <li>• Identifies site-specific risks not necessarily addressed by the published standards, guidelines or technical references. eg. slack rope recovery procedures; using EUC as work platform in shaft or drift; switching between operating modes; range of operation of motion detection.</li> <li>• Issues raised at design and operational risk assessment act as inputs to functional specification.</li> </ul>
<b>4. Independent Failure Modes and Effects Analysis (FMEA)</b>	<ul style="list-style-type: none"> <li>• Aimed at identifying random hardware failures of components used in the safety systems, including sensors, logic solvers and final elements.</li> <li>• Components listed under subheadings:             <ul style="list-style-type: none"> <li>- Sensors (limit switches, E-stop buttons, over speed tachos, etc)</li> <li>- Logic solvers (relays, PLCs, I/Os, voltage comparators, etc)</li> <li>- Final elements (mechanical braking components, prime mover motor contactors, etc)</li> <li>- Cables and data communications (hard wiring, multiplexors, DeviceNet, etc) - Included with logic solvers</li> </ul> </li> <li>• Proportion of safe and dangerous failure modes listed, together with expected failure rates (based on published general reference data).</li> <li>• Published failure rates factored to allow for harsh environmental conditions encountered in mining applications.</li> <li>• All data sources referenced. Where no information found, conservative estimates used.</li> <li>• Data used as inputs for reliability engineering calculations in safety file.</li> </ul>
<b>5. Test for architectural constraints</b>	<ul style="list-style-type: none"> <li>• Components and their architecture (layout and interconnections) tested as per AS IEC 61508. Components classed as simple (Type A) or complex (Type B).</li> <li>• No further reliability engineering calculations made unless architectural constraint test met. If not met, redesign is requested.</li> </ul>
<b>6. Test for Average Probability of Failure on Demand (PFDA<sub>v</sub>)</b>	<p>Based on proof test intervals of the published standards, guidelines or technical references, random hardware failure rates of components and systems are recalculated as PFDA<sub>v</sub> to determine whether the values lie within the target SIL range as shown in the functional specification.</p>

<b>7. Functional specification of proposed system</b>	<ul style="list-style-type: none"> <li>• Important stage for systematic safety integrity. Incorporates inputs from the published standards, guidelines or technical references, design and operational risk assessment and other issues such as may be raised by DII audits, incidents and the like.</li> <li>• Provides design specification for application software development (if programmable electronic systems used).</li> </ul>
<b>8. Internal user validation checks of functional specification</b>	<ul style="list-style-type: none"> <li>• Important stage for systematic safety integrity. Incorporates inputs from the published standards, guidelines or technical references, design and operational risk assessment and other issues such as may be raised by DII audits, incidents and the like.</li> <li>• Provides design specification for application software development (if programmable electronic systems are used).</li> <li>• Mine operator conducts two-level internal validation check to confirm that functional specification has captured all issues thus far. (“Validate: To ensure that something is soundly-based.”)</li> <li>• Item by item requirement of the published standards, guidelines or technical references marked as being addressed by specific item in functional spec.</li> </ul>
<b>9. Independent validation checks of functional specification</b>	<ul style="list-style-type: none"> <li>• Item by item requirements of the published standards, guidelines or technical references, previous risk assessments and any other relevant matters marked as being addressed by line item in functional specification.</li> </ul>
<b>10. Application software verification</b>	<ul style="list-style-type: none"> <li>• Important stage for systematic safety integrity. Application software developer confirms that software is in accordance with functional specification. (“Verify: To prove something to be true; to confirm or substantiate.”)</li> <li>• Developer confirms that application software designed and tested according to principles of AS IEC 61508</li> </ul>
<b>11. Integration factory acceptance testing</b>	<ul style="list-style-type: none"> <li>• Important stage for systematic safety integrity. Application software integrated with embedded software and hardware of programmable electronic system, and then tested for functionality.</li> <li>• Input and output relationships verified against functional specification.</li> </ul>
<b>12. Commissioning testing and field validation</b>	<ul style="list-style-type: none"> <li>• Important stage for systematic safety integrity. Fully integrated system (sensors, logic solvers with embedded and application software, final elements) tested for functionality.</li> <li>• Input and output relationships checked against functional specification and overall safety requirements (ie a final verification and validation stage)</li> </ul>
<b>13. Control over changes during installation and commissioning</b>	<ul style="list-style-type: none"> <li>• Important stage for systematic safety integrity. Ensures that any changes from design intent are properly engineered and authorised.</li> <li>• FMEA and reliability engineering details in safety file recalculated as necessary.</li> </ul>
<b>14. As-built condition reflected in functional specification and related documentation</b>	<p>Check for “as built” status in all vendor documentation.</p>
<b>15. Lifecycle management instructions</b>	<ul style="list-style-type: none"> <li>• Important stage for systematic safety integrity. Ensures that vendor documentation contains instructions for user proof testing to maintain SIL status for safety circuits.</li> <li>• Vendor documentation includes residual risk areas and associated operating practices required to maintain risks at tolerable levels.</li> </ul>

### 5.3 Process review

Requirement	Source	Item	Preferred objective evidence	Available evidence	Adequate?	Qualification	Name signature date
Assess risk, determine risk reduction needed from winder safety circuits	OHS Reg	Specifies what SIL is required for risk reduction in total	Risk assessments	Document No. Report No. Reference in Mine Winder library	Y/N Or with qualification	Describes the qualification for the answer in the previous column	
Allocate risk reduction to various means, including safety circuits	AS IEC 61508	Specifies what SIL is required for each risk reduction measure	Risk assessments				
Design and operational risk assessment	Gazette 24	Outlines techniques for systematic failure avoidance at design stage. Identifies site-specific risks, as input to Functional Spec.	Report(s)				
Independent Failure Modes and Effects Analysis (FMEA)	EES008 series for new projects MDG 2005, for existing projects started prior to public'n of EES008 series	Identifies random hardware failure modes & rates for components used. Safe and dangerous failures identified.	FMEA report				
Test for architectural constraints	AS IEC 61508	Component suitability for SIL systems, according to fault tolerance	Safety file as per NIOSH best practice. This is also a requirement of MDG 2005 and EES008 series guidelines.				
Test for Average Probability of Failure on Demand (PFDAv)	AS IEC 61508	Subsystem calculations that show PFD is in target SIL range	Safety file as per NIOSH best practice. This is also a requirement of MDG 2005 and EES008				

			series guidelines.				
--	--	--	-----------------------	--	--	--	--

DRAFT

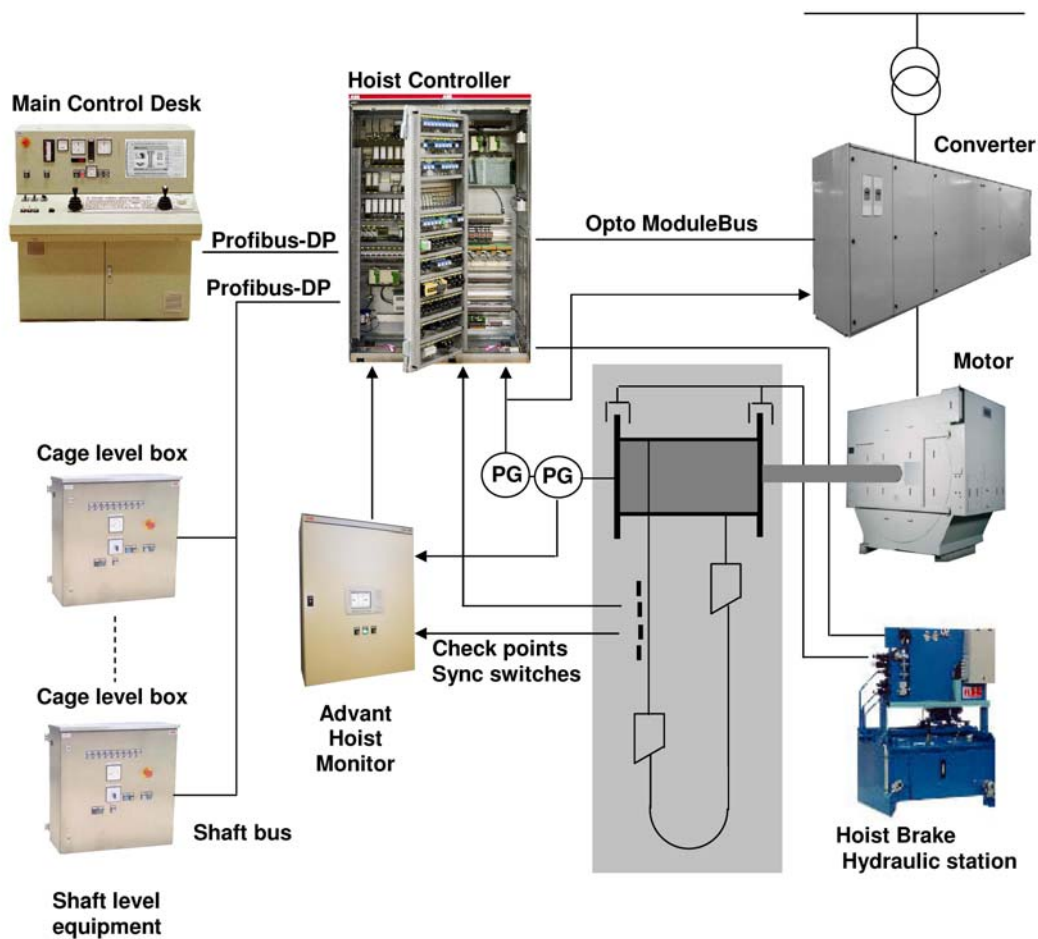
Requirement	Source	Item	Preferred objective evidence	Available evidence	Adequate ?	Qualification	Name, signature, date
Functional specification of proposed system	AS IEC 61508	Specification for application software development and / or relay logic	Functional Specification document, outlining system response on detection of safety command or fault (function by function). Two level sign-off for document.				
Internal user validation checks of functional specification	AS IEC 61508	To ensure Functional Spec meets safety requirements	Two level sign-off from user.				
Independent validation checks of functional specification	Prudent practice	To ensure Functional Spec meets safety requirements	Item by item list of MDG 200, EES008 series & other relevant requirements, each with applicable line item from Functional Spec				
Application software verification	AS IEC 61508	To ensure application software correctly reflects Functional Spec	Two-level sign-off from software developer, as per 61508.6 Annex E, Item E2.				
Integration factory acceptance testing	AS IEC 61508	To ensure application software, when integrated with Safety PLC hardware & its embedded software, meets the input/output relationships shown in the Functional Spec	FAT test plan & results. Two level sign-off for document.				

Requirement	Source	Item	Preferred objective evidence	Available evidence	Adequate ?	Qualification	Name, signature, date
Commission testing and field validation	AS IEC 61508	To ensure sensors, logic solvers (eg Safety PLCs or relays) & final elements meet the input/output relationships shown in the Functional Spec	Commission test plans & test results. Two level sign-off for document.				
Control over changes during installation and commission	Prudent practice	To ensure any changes from design intent are engineered & authorised	Field Engineering Change notices				
As-built condition reflected in functional specification and related documents	Prudent practice	Instructions for user proof testing to maintain SIL status. List of residual risks & associated operating practices required to maintain risks at tolerable level.	Operating instructions				
Lifecycle management instructions	AS IEC 61508 & OHS Regulation	Instructions for user proof testing to maintain SIL status. List of residual risks & associated operating practices required to maintain risks at tolerable level.	Issue of maintenance requirements				

Requirement	Source	Item	Preferred objective evidence	Available evidence	Adequate ?	Qualification	Name, signature, date
Maintenance Requirements	Manufacturers	To ensure all maintenance requirements have been established & manufacturers have provided sufficient information to enable adequate maintenance to be carried out	Issue of maintenance requirements				
Maintenance Procedures	Manufacturers / User	To ensure safety procedures are established to carry out maintenance, inspection & testing in a safe manner	Establishment of safe working procedures for the purpose of maintenance, inspection & testing				

## 6. Example description of the Powered Winding System

### 6.1 Example – Mine Winder System Configuration



Mine Hoist System Configuration

### 6.2 Example – Summary of the winder control approach

**Note:** This is a modified example (original example courtesy of ABB)

#### Control Concept

The mine winder (hoist) is designed for haulage of ore and waste and/or transportation of personnel to and from the different levels in the shaft.

The mine winder is provided with several advanced functions for winding, protection and supervision. This not only simplifies the maintenance, faultfinding and operation of the mine winder, but also enhances safety, availability, reliability, production and accuracy. In addition, the effect of increased precision and softness is reduced wear of the mechanical equipment. In order to meet the demand of safety for all involved personnel, the electrical equipment fulfils the demands required by the international and national standards and regulations.

### **Winder Operation**

The operator's (driver's or users) interface to the Winder Control, consists of conventional devices for manual operation, mounted in the control desk or in distributed control boxes, and a computer based monitoring system. The monitoring system shows, on different types of displays, information about system and objects for operation and maintenance, as well as production information.

### **Winder Control**

The winder is controlled in all modes of operation by a computer-based system. It includes functions for speed and position control, destination determination, automatic run and interface to Winder Operate, Drive and Brake. It also includes test functions and safety circuits for application of the safety brake.

### **Winder Safety**

Doubled hardware circuits which activate the Winder Brake for emergency stop or tripping of the safety brake on order from **Winder Control**, **Winder Drive** or **Winder Monitor** due to indicated faults. Winder Monitor is a separate independent safety system controlling all critical parameters during winding within acceptable limits. If outside the limits, the safety brake is applied. The Emergency stop trips the safety brake by using an emergency stop pushbutton.

### **Winder Drive**

Winder Drive is based on "xxxx" products for AC or DC converter and motor.

### **Winder Brake**

This is used for safe braking of the winder. It consists of brake callipers, hydraulic system and a control unit. Winder Brake controls both the service brake and the safety brake.

### **Winder Maintenance and Diagnostics**

For advanced faultfinding on site or remote via telecommunication. By using a personal computer containing monitoring system, tools and fast loggers, all data for monitoring and diagnostics of faults and normal maintenance can be reached.

## 6.3 Example – functional description : cage winding control

The winder is used for transportation of personnel and material between the top and bottom levels and also to and from the intermediate levels in the shaft served by the cage. Each level has a control box, block-release switch(es), gate closed(/locking) device(s), winder blocked lamp(s) and start signal buzzer for safe cage boarding and safe start of the winder.

The cage is controlled by the multilevel destination system, which allows the users of the cage to send level destination (including call) orders from the control boxes in the shaft. The system stores all received destination orders independent of the cage position and direction of movement.

### **Multilevel destination system:**

The system stores all calls and destinations given by the users at the different levels. All calls and destinations are stored in the up/down memories. The destination system works only in manual or automatic modes.

### **Emergency-driving mode (To be used in case of an accident in the mine):**

The destination system has an emergency-driving feature that can be ordered from all cage level boxes. Such order will cancel all other destinations and calls, and will in automatic mode send the cage to the called level. To inform that only the personnel who sent the order is allowed to use the winder, both light and sound signals are given on each level. The destination system still behaves as normal during this mode. The mode can be cancelled at the collar level (or other preferred level) when the cage has arrived to this level.

### **Cage attendant mode:**

The destination system has a key interlocked, cage attendant feature that can be ordered from all cage level boxes. In this mode it is only possible to set destinations. All other calls will be ignored by the system. The mode can be used when a cage attendant has full control of the cage.

### **Disconnection of cage levels (out of use):**

Disconnection of a level is made via an HSI-display. All destinations to the disconnected level are thereby cancelled and new destinations to the level cannot be set. Also all supervisions and start interlocks related to the level are bypassed.

### **Cage level functions:**

The equipment at the various levels served by the cage is connected to a local control box. It includes control devices for cage destination and for control of the cage near the level.

The local control boxes are powered by 230V AC. The control voltage is 24V DC, which is monitored against insulation (ground) fault. The control voltages are protected by MCBs and are distributed via distribution terminals in the box.

A pulsating watchdog monitors the bus communication to the local control boxes. The watchdog also monitors the control voltages.

Emergency stop pushbuttons and blocking-release switches are for safety reasons directly connected to the Winder Controller by conventional shaft cables. The cables include wires for the power supply to the remote I/O units, box heaters, analog depth value and telephone system. The cable from the top level includes wires for shaft overwinding and synchronize switches.

#### **Indication of level related winder supervisions:**

A tripped supervision related to a level is shown on the local control box. The fault is indicated as a fault number and is BC-coded by utilizing the normal signal lamps.

#### **Synchronizing magnet limit switch for 'at level' position:**

The cage will affect the switch just before the position 'at level' is reached. The switches (one per level) are supervised.

#### **Winder stopping sequence at level:**

The winder is stopped in a certain sequence procedure when the cage approaches the destination level in automatic mode and also when the cage approaches a level at creep speed in manual mode. The sequence steps: near level, in synchronizing zone, at level, trail brake order, low creep speed order and stop order are set by parameters which are compared against the cage position.

#### **Level functions for safe cage boarding and start:**

Each level is equipped with following functions/equipment:

- Block-release switch(es), reachable from the cage and from the level side.
- Blocked flashing light(s).
- Start signal buzzer (mounted on the control box).
- Gate closed switch(es)
- Gate locking device(s) including locked position switch.
- Proximity limit switch(es) for platform(s) in "up" position.
- Limit switches for chairing supports "out/retracted".

#### **Functions controlled from the local control box at the levels:**

The winder has a local 'Jogging' function. Jogging is Up/down control (hold-to run type) of the cage in a zone near the level. The jogging function can also be used for (rope) inspection by selecting the key-locked inspection mode on the control box. The near level zone condition is thereby bypassed.

### **Winder ready for start command, winder release time and winder blocked:**

With all shaft gates closed the start command is given from the level where the cage is located, when the block-release switch is turned to release position.

In automatic mode the winder will then start after a short delay, provided a destination order is set in the destination system.

In manual mode the lamp signal winder 'ready for start' is given to the driver, who must order a sound signal back to the cage level before the winder can be started.

If the cage stops at the destination level and nobody enters or leaves the cage, the winder will remain interlocked during a certain release time before it can start again. The winder blocked status (when any block-release switch is in block position) is shown on the control desk and on all control boxes in the shaft.

## **6.4 Example – overview of the safety approach**

### **Safety philosophy:**

The philosophy for the safety related electrical parts of the hoist control is based on European standard EN 954-1, *Safety of machinery - Safety related parts of control systems - Part 1*, and its normative references.

### **Risk assessment:**

A risk assessment is a series of logical steps to enable a systematic examination of the hazards associated with the winder control. The risk assessment includes analysis and evaluation.

### **Risk estimation, part of the risk analysis:**

The hoist is used in an industrial environment and by trained personnel. The hazards listed can create serious injury both for multiple persons and property. The hazards are frequent, with long time exposure and it is scarcely possible to avoid them. This is particularly so for hazards which can occur at high winding speed or at the shaft ends.

### **Risk reduction by design, part of the risk evaluation:**

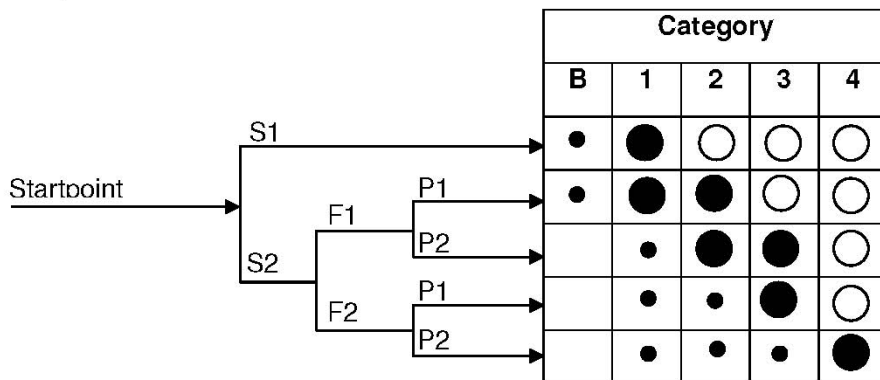
Risk reduction in the design can be achieved through use of well-known safety design principles, such as:

- Use of tested safety components (safety relay).
- Redundancy (active or passive)
- Diversification, different solutions/media at redundancy.
- Automatic (cyclical) monitoring.
- Positive action of mechanical components.
- Positively driven contacts (mechanically linked contact elements in relays).

- Overtating of contacts (in relays).
- Fail safe circuit design, interruption safe (closed circuit principle).
- Cross fault detection (different voltage potentials).
- Two-polarity switch-off (at isolated power system).
- Password/lock access to software in re-programmable electronic controller.
- Possibility to easily make a test of the ultimate protections/function (HSI-test display).

#### Fault resistance categories:

Standard EN 954-1 specifies five fault resistance categories for safety-related parts of control systems. These categories have been used for the design of the winder control system. The selection of category for a safety-related part in the hoist control system follows the figure below and the input to the selection criteria is taken from the risk assessment for that part.



#### Key

Severity of injury; S1= Slight injury, S2= Serious (irreversible) injury

Frequency and/or exposure time; F1= Seldom to quite often and/or short time, F2= Frequent and/or long time

Possibility of avoiding the hazard; P1= Possible under specific conditions, P2= Scarcely possible

Category selection ● = Preferred ● = Possible, additional ○ = Over dimensioned measures

## 6.5 Example – description of the safety functions

### Safety related parts in the hoist control system

The following parts in the hoist control system are considered as safety-related.

#### Insulation-monitoring device:

Control voltages used in safety related circuits that are physically spread out in the control system have an isolated type of power system and an insulation-monitoring device that detects symmetrical ground faults. The monitoring fulfils fault resistance category 2.

### **Safety circuit:**

Consists of a dual-circuit (24V DC) where all protections with fault resistance categories 3 or 4 are connected to the safety relay. De-energizing of the safety relay causes disconnection of the hoist motor driving or braking torque by static components and application of the safety brake by auxiliary safety contactor-relays.

Each protection is connected via two relays with positively driven contacts into the circuit and the two relays are monitored in the process controller. Protections that fulfil fault resistance category 3 and 4 are connected to the hardware part of the safety circuit.

Protections that fulfil fault resistance category B, 1 and 2 are connected to the software part of the safety circuit in the controller. The hoist protections can via the safety circuit retard and stop the hoist according to following tripping categories:

- **Immediate application of the safety brake:** The protection is connected to the hardware part of the safety circuit. The protections belong to fault resistance category 3 or 4.
- **Immediate application of the safety brake:** The protection is connected to the software part of the safety circuit, and is realized in a (single-channel) controller.
- **Immediate retardation of the hoist by the drive system and tripping of the safety circuit when the hoist is at standstill:** The protection is connected to the software part of the safety circuit, and is realized in a (single-channel) controller.
- **Tripping of the safety circuit when hoist is at standstill at the end of the winding cycle:** The protection is connected to the software part of the safety circuit and is realized in a (single-channel) controller.
- **The protection indicates an abnormal situation and gives a warning indication, (for instance for high temperature):** The safety circuit is not tripped (unless the trip limit is reached). The protection is realized in a (single-channel) controller.

### **Emergency stop circuit:**

Consists of two dual-circuits (110V DC) where the emergency stop pushbuttons are connected to two monitored contactor-relays. De-energizing of the contactor-relays will cause de-energizing of the safety circuit and disconnection the motor torque.

**Dual-circuit 1:** Emergency stop pushbuttons mounted in the control desk and in the hoist/electrical room disconnect the motor torque by electromechanical components only. Operation of any of these pushbuttons causes a Category 0 stop according to IEC Standard IEC 60204-1, *Safety of machinery – Electrical equipment of machines, Part 1*.

**Dual-circuit 2:** Emergency stop pushbuttons mounted in the shaft, as well as most of the protections which trip the safety circuit, disconnect the motor torque by static components. The emergency stop circuit fulfils fault resistance category 4

**Use of re-programmable electronic controllers:**

The controllers used for the winder control and protections are single-channel, re-programmable, electronic controllers. The controllers utilize proven hardware and firmware technology, and have comprehensive internal test and monitoring functions.

**Principles for using one controller (single-channel):**

Safety related parts in the hoist control system that belongs to fault resistance category B, 1 and 2 are realized in a single-channel controller. Safety related parts requiring dual inputs or outputs, thus fault resistance category 3 for the process interface, but not for the controller, is realized in the same single channel controller.

**Principles using two controllers (dual-channel):**

Safety related parts in the hoist control system that belongs to fault resistance category 3 is realized in a configuration of two independent single-channel controllers. The two controllers are independent of each other. - The two controllers are of the same type, but the solution of the safety related function is made in different ways in the two controllers. One of the controllers is used only for the safety related function and the setting of the parameters is done by a built-in HSI-device.

Both controllers have a built-in controller stall protection and all outputs are set to zero at stall. Both controllers are also monitored by a watch-dog that is independent of the controller and trips the safety circuit at fault. Both controllers have two trip outputs. Important process values relevant for the safety-related parts, are compared between the two controllers .

**Hoist speed and position determination:**

The speed and position determination is made in two independent controllers. Each controller has a pulse generator, connected to a pulse counting card and (at least one) synchronizing shaft limit switch (of latched type) per conveyance or counterweight. A failsafe position check against a shaft dependent checkpoint device is made just after start of the retardation at the shaft ends. The speed/position determination in the Hoist Controller is used both for control and supervision, whereas the speed/position determination in the Hoist Monitor is used only for supervision. The position value (and other values) is stored at least 672h in each controller. The position values are automatically compensated for wear of friction liners (using a shaft limit switch at top and at bottom level). The determination fulfils fault resistance category 3.

**Over- and under travel protection:**

The protection consists of two independent protection parts. One part is based on a dual-circuit (110V DC) where over- or under travel shaft limit switches are connected to two monitored contactor-relays. De-energizing of any of the contactor-relays causes tripping of the safety circuit. This protection part itself fulfils fault resistance category 4. The second part is software based in the Hoist Monitor and the position value is continuously compared against the position value in the Hoist Controller. The protection fulfils fault resistance category 4.

**Over speed protection:**

The protection consists of two independent protection parts. One part is software based in the Hoist Monitor. The second part is software based in the Hoist Controller. Each overspend protection part includes an Overspend envelope function (full speed zone, end-retardation zone, creep speed zone).

The Hoist Controller includes a speed check during end-retardation (~90% speed) by the shaft dependent checkpoint device. The protection fulfils fault resistance category 3.

**Automatic monitoring of the overspeed protection:**

Monitoring of actual speed and position values. Decrease check of the overspend envelope against a shaft dependent device, placed at the start of the retardation zone near the shaft top and bottom, is made in both controllers. Decrease check of the overspend envelope against a shaft dependent device just before the shaft end stop position.

**Motor torque disconnection circuit:**

Passive redundancy is used for the motor torque disconnection function. A second function overrides if the first function fails. At tripping of the safety circuit and at normal stop, the motor torque is disconnected by static components. This is done by zero setting of the converter run signal (first function), controlled by the controller outputs together with the safety relays contacts which open at tripped safety circuit. If the motor torque/current, which is monitored in the controller, does not disappear after this first signal the converter on signal (second function) is set to zero. The motor drive is thereby electromechanically disconnected by a breaker.

At emergency stop (by pushbuttons) and at stall of the controller (detected by watchdog) the disconnection of the motor torque is made by use of electromechanical components only.

The motor torque disconnection circuit (24V DC) fulfils fault resistance category 3 regarding redundant order given from a single controller.

### **Safety brake application circuit(s):**

The disc brake equipment consists of hydraulic brake callipers working on minimum two brake discs and a hydraulic station with oil pump and control valves. The control valves are used both for the service brake and the safety brake control. At tripping of the safety circuit both the control valves and the oil pump are disconnected by (opening of) the safety relays contacts. The safety brake is thereby applied for emergency retardation of the hoist. The control valves used for application of the safety brake are automatically tested each time the service brake is applied. This is possible as the valves are used both for application of the service and the safety brakes. The valve for the release of the accumulator at safety brake application is automatically tested every second hour when the hoist is at stand still.

### **Controlled retardation principle:**

The Brake Control Card together with a tachometer generator, driven by the pulley, is used for controlled retardation by the safety brake. The brake card controls the retardation to the set value, independent of the existing braking conditions (payload, position, direction and friction coefficient) within the set pressure limitations (maximum and minimum). This braking principle increases the margin to rope slip for friction hoists for all other conditions than full descending load.

The brake card has a passive redundancy function for the safety braking. The first function safety braking is controlled by a progressive increase of the braking force until the required (pre-set) retardation is reached. A proportional valve is used for this control. The second function, the brake card monitors the retardation during the safety braking, if the retardation is less than a pre-set value the card disconnects the proportional valve control and opens instead a backup valve of on/off type. The safety brake is thereby applied according to the constant braking force control principle. The controller also disconnects the backup valve via a non-failsafe order after a preset time. A battery with battery charger powers the brake card and the control valves, thus maintaining the safety brake function at power interruption. The brake card includes monitoring functions.

### **Constant braking force principle:**

The safety braking is, as already described, controlled by redundant (active) control valve circuits. The pressure value to obtain the required retardation of a full descending load is hydraulically set by pressure release and control valves, and the same braking force is used whenever the safety brake is applied. The use of the same braking force results in a retardation that is largely dependent on the existing conditions (payload, position, direction and friction coefficient). The safety brake application circuit (24V DC) fulfils fault resistance category 4.

**Hoist blocking circuit:**

Consists of a dual-circuit (110V DC) where the hoist-blocking devices and the pushbuttons at the shaft levels are connected to two monitored contactor-relays. De-energizing of the contactor-relays interlocks (by hardware) the run signal to the converter and prevents lifting of the service brake. This means that any start of the hoist is not possible. The hoist blocking circuit fulfils fault resistance category 4.

**Manual control commands, hoist up-down-stop and service brake lift-apply:**

Realization of manual control commands (lever, pushbutton) for hoist up-down-stop and service brake lift-apply are dependent of two signals. No up-down-lift order will thus take place if one of the two signals fails and stop-apply order occurs as soon one of the two signals is affected. These control commands from the devices are dependent of two digital input signals to the controller. The up-down command is based on the hold-to-run control principle. The hoist up-down-stop and service brake lift-apply order circuits (24V DC) fulfil fault resistance category 3 regarding redundant order given to a single controller.

**Motor torque generation circuits:**

Motor torque generation at hoist start is controlled from the controller by two (double) outputs and relays. The converter run signal is built-up by contacts from the two relays together with contacts on the safety relays, the controller monitors the two outputs/relays. Generation of motor torque will not start if there is a failure in one of the two outputs or relays. The motor torque is disconnected if one of the outputs/relays is affected. The motor torque generation circuits (24V DC) fulfil fault resistance category 3 regarding redundant order given from a single controller.

**Service brake lifting-application circuits:**

Lifting/application of the service brake is dependent of two outputs (relays/AO). The service brake will not be lifted, but remain applied, if a failure on one of the two outputs (relays/AO) occurs. Furthermore, the service brake will be applied if one of the output/relay fails after start. The controller controls and monitors the two brake lift outputs/relays and also an analog brake lift reference signal. The digital brake lift signal is built-up by contacts from the two relays together with contacts on the safety relays. The signal is connected to the brake control valves in the hydraulic station. The analog (voltage) brake-lifting signal is connected via a brake control card, which converts the voltage signal to a current signal, used for the proportional control valve. The proportional valve is also controlled by safety relay contacts. A torque-proving signal is also required before lifting of the service brake is possible when the hoist is started. The service brake lifting/application circuits (24V DC) fulfil fault resistance category 3 regarding redundant order given from a single controller.

## 6.6 Example – overspend envelope

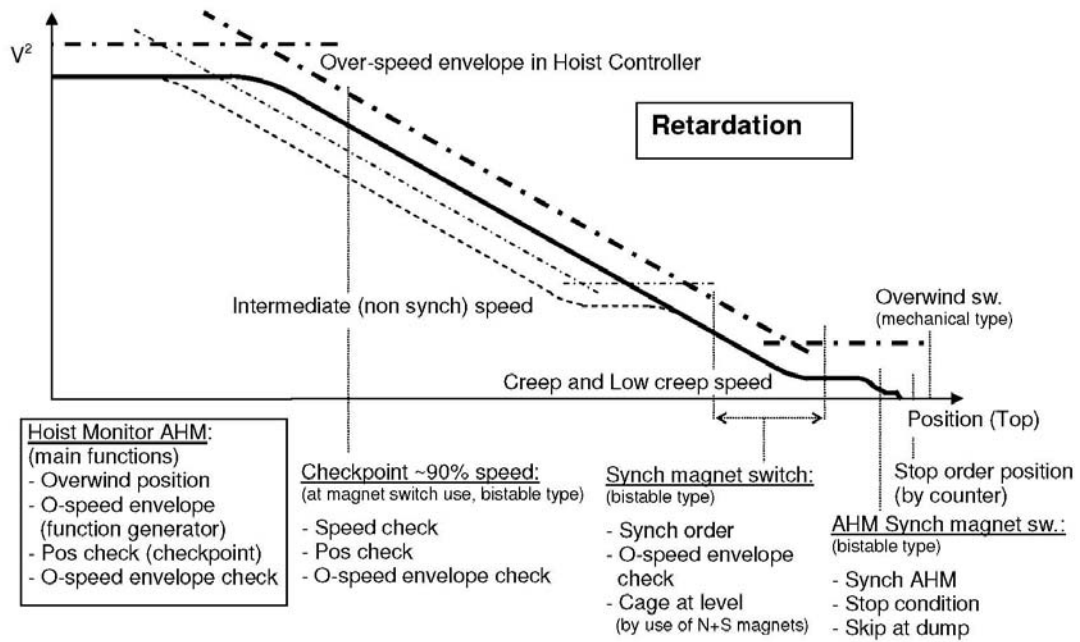
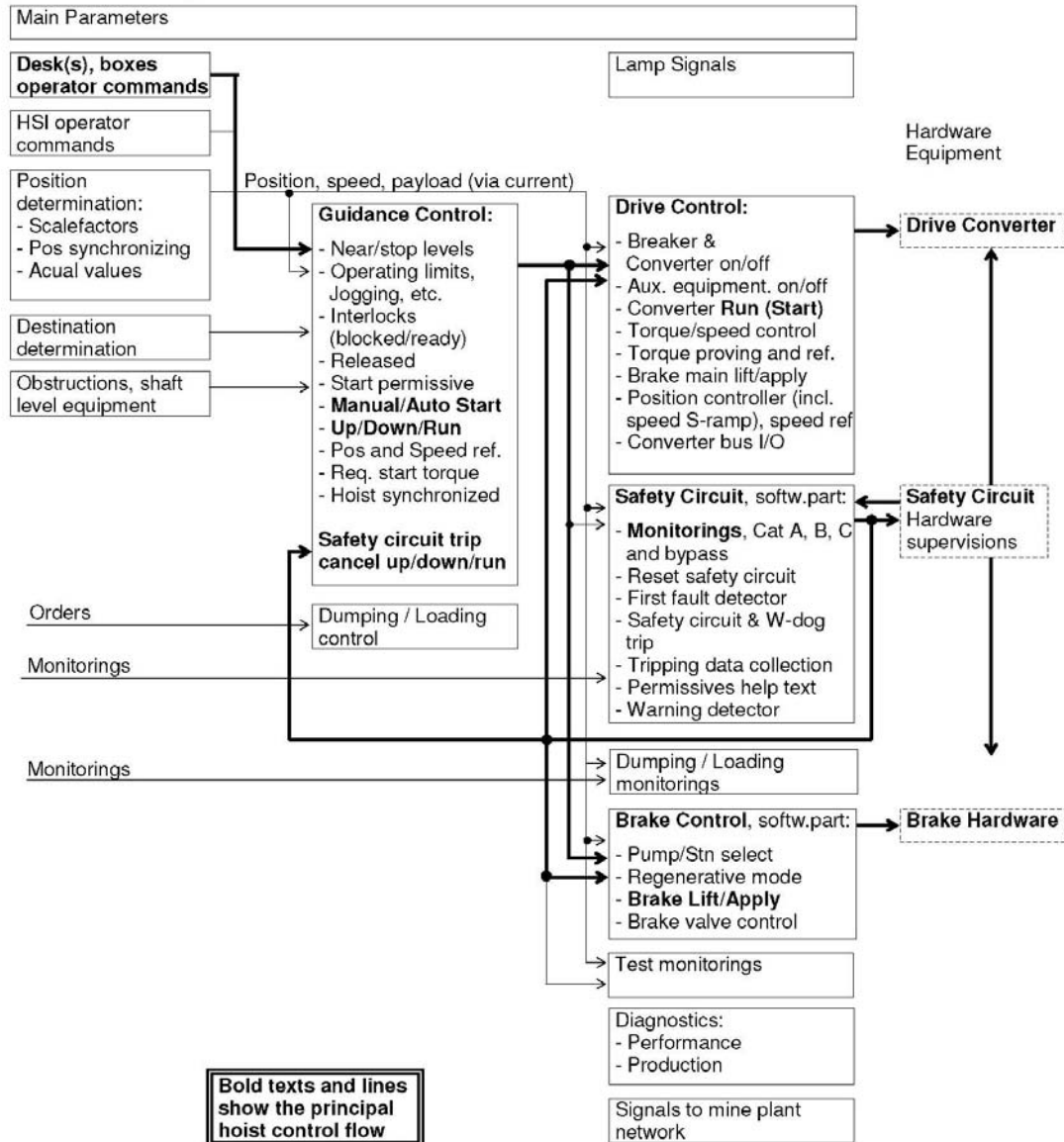


Figure: Speed curve at retardation with main control and monitoring functions.

## 6.7 Example – program structure

### 6.2.1.2 Program structure in the Hoist Controller



Block diagram showing the main functions in the Hoist Controller program.

## 7. Appendices

### Feedback Sheet

Your comment on this Technical Reference is essential for its review and improvement.

Please make a copy of this Feedback Sheet and send your comments to:

The Senior Inspector of Electrical Engineering  
Mine Safety Operations  
Industry and Investment NSW  
PO Box 344  
Hunter Region Mail Centre NSW 2310  
Phone: (02) 4931 6641  
Fax: (02) 4931 6790

<b>How did you use (or intend to use) this Guideline?</b>	
<b>What did you find most useful about the Guideline?</b>	
<b>What did you find least useful about the Guideline?</b>	
<b>Do you have any suggestions to improve the Guideline?</b>	

Thank you for completing and returning the Feedback Sheet.

## I&I NSW Contact details

I&I NSW offices located in coal mining regions.

North East Area	South East Area
<b>Maitland</b>	<b>Lithgow</b>
516 High Street Maitland NSW 2320 PO Box 344 Hunter Regional Mail Centre NSW 2310 Phone: (02) 4931 6666 Fax: (02) 4931 6790	Suite 1, 1 <sup>st</sup> Floor, 184 Mort Street Lithgow NSW 2790 Phone: (02) 6350 7888 Fax: (02) 6352 3876
<b>Singleton</b>	<b>Wollongong</b>
Level 1, 1 Civic Avenue Singleton NSW 2330 PO Box 51 Singleton NSW 2330 Phone: 02 6572 1899 Fax: 02 6572 1201	Level 3, Block F, 84 Crown Street Wollongong NSW 2500 PO Box 674 Wollongong NSW 2520 Phone: (02) 4222 8333 Fax: (02) 4226 3851