HIGH INTEGRITY ISOLATION SYSTEM

Case Study

Automated isolation systems are becoming widely used to provide high integrity isolation solutions that improve productivity and reduce manual handling.

Traditional isolation procedures in underground coal mines require connection and disconnection of high voltage electrical cables to be carried out by trained and competent electricians who have obtained a switching permit to perform work. These personnel then need to travel to the isolation location, which is commonly remote from the work location, perform the isolation and confirm its success. Although the process provides a safe methodology for electrical isolation it comes at the cost of production and potential manual handling issues due to the size and weight of the cables.

To counteract these issues and increase efficiency, automated isolation systems are becoming widely used. These engineered solutions routinely employ automation to simplify and control plant operation and can be applied to procedural safety and operational management.

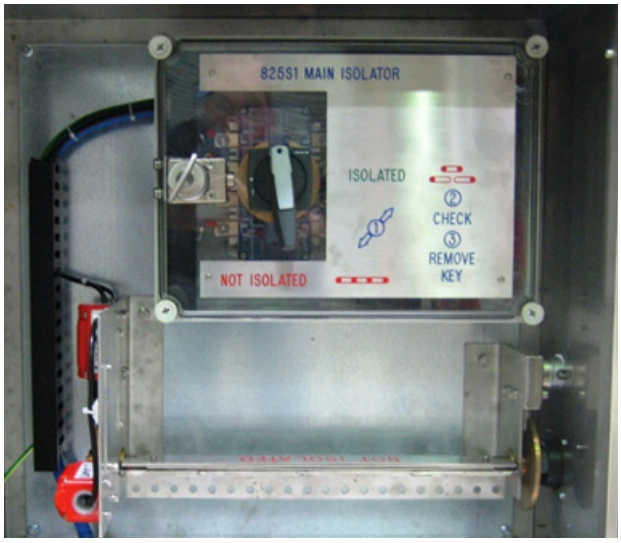
These automated systems provide immediate productivity improvements by removing the need to use a trained and competent electrician to complete the isolation, enabling isolations to be performed by operators and maintenance personnel, it also provides a decrease in manual handling of heavy cables and a minimisation of the time and travel associated with conventional manual isolation procedures.

High Integrity Isolation: A Case Study

This underground mine had a distributed Remote Isolation System, which allows for isolations to be initiated and onfirmed from numerous locations. This Remote Isolation System is used for minor short duration tasks.

Through a risk management process, the mine site determined that isolations could be effected using a specially designed High Integrity Isolation System (HIIS) for more complex, longer duration tasks.

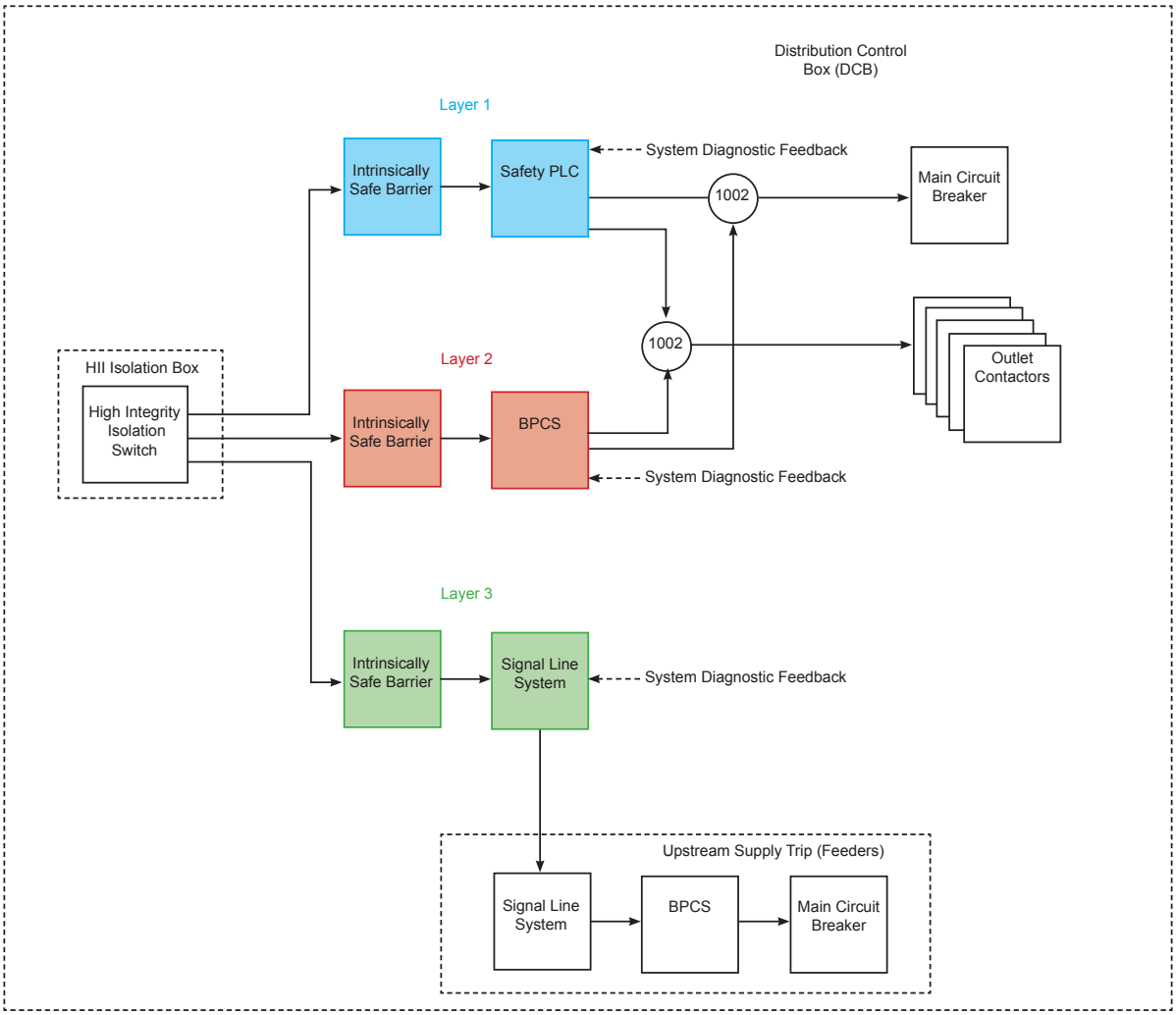
Ampcontrol designed a HIIS which opened multiple switch devices within the power circuit



to ensure an effective isolation and incorporated Electrical, Electronic, Programmable Electronic (E/E/PE) components in its control system. With this being the case, the HIIS was designed, tested, installed and commissioned in accordance with the functional safety principles and lifecycle outlined in AS/NZS61508.

This change in isolation philosophy provided a single high integrity isolation point, located near the 11kV longwall face conveyor, which effectively and safely isolates the face conveyor and associated drives and allows the fulfilment of multiple personal danger padlocks to secure the isolation.

The HIIS removes the requirement for electricians to perform isolations by physically removing heavy plugs. This allowed isolation and restoration of power to be performed by operators and maintenance personnel, saving valuable production time while achieving an effective and safe isolation.



The Scope of Work

The mine site developed a functional specification defining the system requirements including:

- The HIIS was to be a single isolation point for the face conveyor motors
- The requirement for a E/E/PE system (Electrical/Electronic/Programmable Electronic)
- Operational with the system energised or de-energised
- The maintenance tasks they wanted to undertake utilising the HIIS
- Their tolerable risk level
- That the system would be a High Demand system
- Maximum proof test interval

The System Design

After the scope was defined, Ampcontrol developed a detailed design following their Functional Safety Management Plan which aligns with the requirements of AS/NZS61508. This included facilitating a detailed hazard/ risk assessment and Layer of Protection Analysis with the mine site as part of the process to meet the target specification of a dangerous failure rate of 1 in 100,000 years. The Layer of Protection Analysis showed that to achieve the desired safety integrity level the design required multiple independent E/E/PE systems to provide sufficient redundancy to achieve this target.

The final design consisted of three separate monitoring and control system layers to achieve the target failure rate, as shown in the Function Block Diagram (below) and subsequent Fault Tree Analysis. With the first layer being a SIL3 system and the second and third layers both being SIL1.

The SIL3 system provides the primary level of safety protection which is operated by redundant inputs with fault detection from the High Integrity Isolation Switch. The PLC then disconnects power to the conveyor and longwall motors by opening the associated contactors and main circuit breakers via safety relays. The switching sequence and timing is utilised to ensure the isolation procedure has been effected properly in the required timeframe and the final step in the process is to affix personal danger padlocks securing isolation. The system includes many safety related products including an Allen Bradley Guardlogix PLC, safety relays, cable fault monitoring relays and controllers.

The secondary system is designed to SIL1 and operates in the same manner as the SIL3 system to provide redundancy. This system monitors the status of the input from the High Integrity Isolation Switch and disconnects power to the conveyor and longwall motors by opening the same contactors and main circuit breakers. To remove the possibility of common mode failures the components used in this layer are different from the SIL3 layer. This system consisted of Allen Bradley Controllogix PLC and Safety Relays, cable fault monitoring relays and controllers.

In the event both the primary and secondary levels were to fail, a tertiary system is designed to disconnect the supply to the whole longwall system by opening the main upstream supply circuit breaker. This tertiary system is designed to SIL1 and consists of a signal line/ remote isolation system communication line to disconnect power upstream in the event any of the longwall contactors and main circuit breakers remain closed when they were commanded to open.

Following design and installation in accordance with AS/NZS61508, the system design and calculations were independently assessed for compliance and a certificate was provided by the independent third party.

Confirmation of the system operating as expected under all normal and abnormal conditions was undertaken by Ampcontrol's trained staff using functional testing and the introduction of faults to confirm the adequacy of the design and manufacture and safe operation under all failure modes.

From these tests a list of any possible dangerous undetected faults were compiled into a proof testing document which was developed in such a way to allow for non-invasive proof testing at the periodic proof testing intervals as required by the SIL analysis to allow the mine to maintain the SIL claim.

This system is currently in operation and used for a range of maintenance tasks providing increased productivity and output by significantly decreasing isolation and restoration times at the mine site.

Functional Safety FAQs

What is a Safety Integrity Level (SIL)?

"A safety integrity level is one of four levels, each corresponding to a range of target likelihood of failures of a safety function. Note that a safety integrity level is a property of a safety function rather than of a system or any part of a system."

What is the difference between low demand and high demand or continuous mode of operation?

"Low demand mode, as defined in 3.5.16 of IEC 61508-4, is where the frequency of demands for operation made on a safety-related system is no greater than one per year.

High demand or continuous mode, as defined in 3.5.16 of IEC 61508-4, is where the frequency of demands for operation made on a safety-related system is greater than one per year. Continuous is regarded as very high demand."

Source: IEC International Electrotechnical Commission
http://www.iec.ch/functionalsafety/faq-ed2/