Functional specification and risk assessment

Refuge Bay Emergency Indicator

DOCUMENT DETAILS

Project Title:	Refuge Bay Emergency Indicator
Document Number:	RBEI_FSRA_0_01
System/Subsystem Title:	
Document Issue Date:	2010/05/03
Client Reference:	NA

APPROVAL

Checked by	Name	Signature	Date
Author	Mr GPR van der Merwe		2010/05/05
QA:	Prof JEW Holm		2010/05/05
Technical Approval	Mr GPR van der Merwe		2010/05/05
Project Manager	Mr Martiens Visser		2010/05/05

Table of Contents

1 SCOPE

1.1 Purpose

This specification establishes the performance, design, test, manufacture, and acceptance characteristics and requirements for the Refuge Bay Emergency Indicator.

1.2 Identification

This document is comprised of the following sections:

1. Section 2: Product definition
2. Section 3: Quality assurance provisions
3. Section 4: Configuration control

2 PRODUCT DEFINITION

2.1 Product definition

The Refuge Bay Emergency Indicator is used to indicate the location of the refuge bay during emergency situations. The unit consists of four multicolour bezels, a siren and battery backup.

2.2 System primary functions

2.2.1 Primary mission

The primary mission of the refuge bay emergency indicator is to provide visual and audible indication of the refuge bay during emergency situations.

2.2.2 Secondary functions

Apart from indicating the location of the refuge bay, the following functions are supported by the system:

1. The refuge bay emergency indicator consists of a battery backup unit to ensure operation for at least 20 hours when no power is available;
2. Four multicolour bezels are used to provide efficient visual indication;
3. An multi-tone siren is used for audible indication;
4. The refuge bay emergency indicator provides a robust and water proof enclosure. The enclosure can also be locked to limit possible tampers to the system.

2.3 System and component arrangement diagrams

This sub-section incorporates the functional schematic and flow diagrams of the system. Applicable layout drawings that establish the general relationship of major components are included.

2.3.1 System arrangement

The refuge bay emergency indicator should be located just outside the refuge bay to indicate the location of refuge bays, especially during emergency situations.

2.3.2 System components

The system consists of a single module. This module is illustrated in figure 1.

FIGURE 1 – REFUGE BAY EMERGENCY INDICATOR

Figure 1 shows the graphical representation of the refuge bay emergency indicator. The unit consists of the following components:

1. Voltage specification: This shows the voltage requirement for the system. See section 2.4.1 for possible voltage specifications;
2. Square Key Lock: A square key is required to lock and open the enclosure;

3. Tamper Lock: The system can be locked to prevent tampering with the system;
4. Siren: The siren is used to sound during emergency situations;
5. Override switch: The override switch can be used to force the system into the emergency state, if the power is not tripped;
6. Power cable: A two meter long power cable is used to supply power to the system;
7. Mounting Bracket: The system can be mounted with this bracket;
8. Multicolour Bezels: Four multicolour (red / green) bezels are mounted on the sides of the refuge bay emergency indicator. These bezels indicate the states of the system.

2.4 Interfaces

A basic interconnection diagram (see Figure 2) below shows the interface arrangement of the refuge bay emergency indicator:

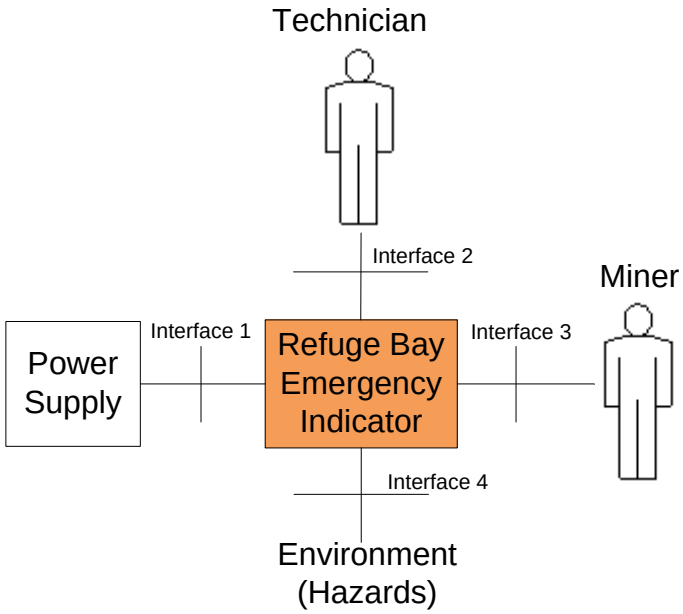

FIGURE 2 – REFUGE BAY EMERGENCY INDICATOR INTERFACES

The main interfaces are shown above. These are described as follows:

1. Interface 1 – An interconnecting power cable between the refuge bay emergency indicator and the power source;
2. Interface 2 – This is the interface between the technician and the RBEI system;
3. Interface 3 – This interface consists of the audible and visual indication to the miners in the area. The miner should also operate the override switch if necessary;
4. Interface 4 – This interface describes the environmental hazards that can affect the system.

Each of the interfaces shall be described in the following sections.

2.4.1 Interface 1 – Power cable

Various input voltages can be specified to power the system. These voltages are as follows:

- 110V AC;
- 220V AC;
- 525V AC;

These different configurations are possible but have to be defined and specified - the current product only covers the above ranges.

It is important that the correct power source specification is provided before a unit is supplied and installed. It is the responsibility of the mine to specify the required voltage.

2.4.2 Interface 2 – Maintenance performed by a technician

The system should be tested and maintained regularly in order to ensure proper operation. The outputs (bezels and siren) should be tested together with the status of the batteries. If the batteries are faulty, they should be replaced due to their limited lifetime.

2.4.3 Interface 3 – Miner indication and operation

Visual indication is provided by the four bezels, located on the four sides of the system. This allows for visibility in all directions. Audible indication is by means of a siren.

This interface also includes the override switch which should be activated (if the system is still in the safe state) by the first miner entering the refuge bay during an emergency situation. Generally the mains power will be tripped during emergency situations, which will force the system into the emergency state.

2.4.4 Interface 4 – Environmental hazards

The main hazard to the system would be direct fire, but should the system be installed at the correct location in order to minimize this hazard.

2.5 Characteristics

This section describes the functions of the refuge bay emergency indicator in terms of its operational modes. Where required, a function's performance, physical or other characteristics are given.

2.5.1 Functional characteristics

2.5.1.1 Modes of operation

The modes of operation for the refuge bay emergency indicator are shown in the following state diagram:

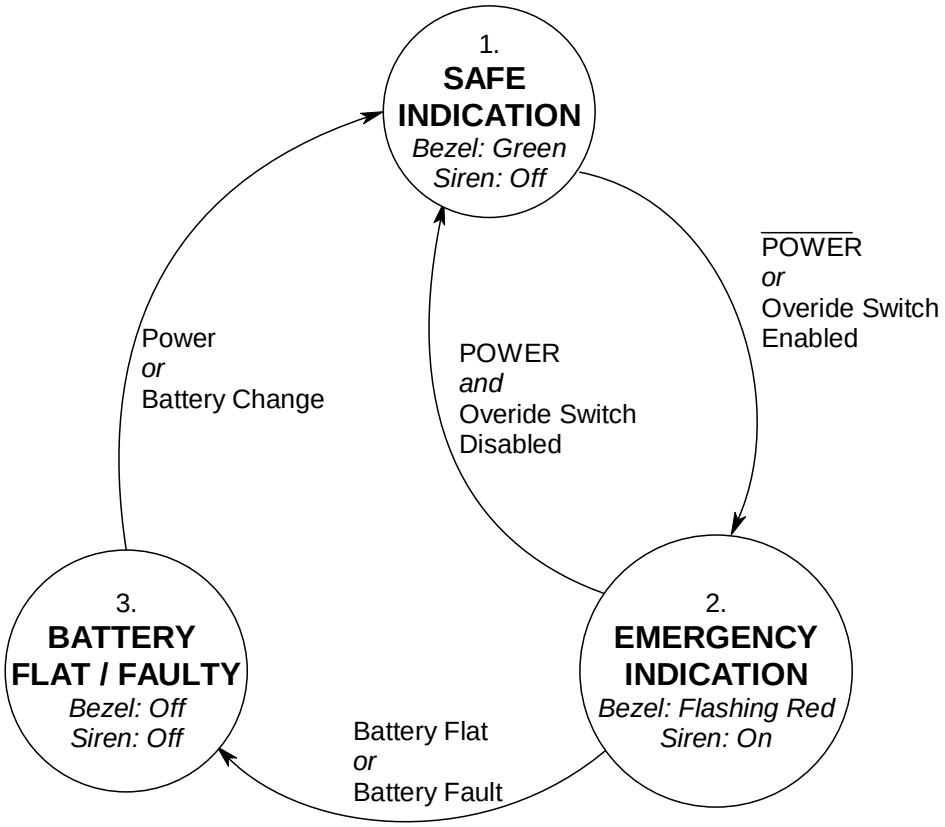

FIGURE 3 – REFUGE BAY EMERGENCY INDICATOR STATE DIAGRAM

1. **Safe indication:** When power is supplied to the refuge bay emergency indicator and the override switch (see unit 5, Figure 1) is disabled the system will be in this state. The four bezels will be GREEN while the buzzer will be off.

   During this state the backup batteries will also be charged. The batteries should charge to a maximum within 4 hours;

2. **Emergency indication**: If power is removed from the system or the override switch is enabled the system will exit the safe state and enters the emergency state. During this state the bezels will be flashing RED while the siren will sound.

   During this state the backup battery will be used to supply power to the system. This state will last at least 20 hours (if the batteries were fully charged) before the batteries will be flat and the system will enter state 3. The batteries will be automatically recharged once the system enters state 1 (Safe indication).

3. **Battery flat / faulty**: During this state no power is available to operate the system in state 2. In this state the bezels together with the siren will be off. The exit condition to this state would be when power is restored or when the batteries are replaced when necessary.

2.5.1.2 Failure modes

Different failure modes have been identified for the system. The effect of these failure modes can also be seen in the risk analysis done in section 2.6. These failure modes are as follows:

1. **External cable fault**: If the power cable is faulty, no power will be supplied to the system. The batteries will run out after which the system will fail. This is a total module failure;
2. **External over voltage**: If the incorrect voltage is supplied to a unit, the internal fuse will blow and needs to be replaced at the factory - this fault should only occur when very high voltage surges occur;
3. **Backup power failure**: Lead acid batteries are used to supply backup power. These batteries need to be maintained and replaced when necessary. The backup battery should be replaced at least every two years, depending on the charge / discharge cycles of the system.
4. **Bezel and Siren (Indicators)**: Both operational modes of the bezels (RED and GREEN) together with the siren should be tested regularly to ensure operation.
5. **Internal module fault**: This is a total module failure and can only be detected by testing the module before use.
6. **Visibility Failure (wrong installation)**: The location of the system installation should be of such to ensure maximum visibility of the system state to the surrounding areas.
7. **Environmental Hazard**: Possible environmental factors might affect the operation of the system. Direct fire might damage the system.

2.5.2 Performance characteristics

2.5.2.1 Durability

Various factors influence durability, including use factors. However, components in the system were designed to provide durability in a number of ways:

1. The mechanical design was done to provide a strong robust enclosure;
2. Electronics are conformally coated to provide protection against the ingress of water and other particles;
3. Electronics were designed with operational margins of more than 50% on input and output protection – the electrical power inputs are protected against over-voltage and over-current conditions.

2.5.2.2 Health and safety

Although all possible steps were taken from a design point of view to ensure safety, the following aspects are of high importance:

1. Procedures must be put in place to test for explosive gasses before any system is powered up;
2. Lead acid batteries are used within the system. The internal components of these batteries include lead and liquid electrolyte. The potential risks for these substances are as follows:
   - Electrolyte: Electrolyte is corrosive and contact may cause skin irritation and chemical burns. Electrolyte causes severe irritation and burns of eyes, nose and throat. Ingestion can cause severe burns and vomiting.
   - Lead: Direct skin or eye contact may cause irritation. Inhalation or indigestion of lead dust or fumes. This may also result in headache, nausea, vomiting, abdominal spasms, fatigue, sleep disturbances, anemia and leg, arm and joint pain.

   Note: These harmful substances internal to the batteries can be exposed during direct fire or explosion. Note that these batteries are located within the steel enclosure to limit possible exposure.

2.5.2.3 Maintainability and inter-operability

A swap-out policy was followed for unscheduled maintenance. The following specific guidelines should be followed:

1. No component should be opened for second-line repairs on the premises of the client;
2. The swap-out policy was designed into the system and facilitates a “drop-in” replacement of similar-type modules.

2.5.2.4 Transportability

The refuge bay emergency indicator units will be exposed to harsh conditions and were designed with the following requirements:

1. Humans will carry the units. Therefore the enclosure is light-weight and small;
2. All units are transported in protective cardboard boxes and are protected against shock and vibration.

2.5.2.5 Materials processes and parts

All materials used in the design were selected to withstand harsh underground conditions. Enclosures are manufactured from 3CR-12 stainless steel and powder coated to withstand all environmental conditions common to mines;

2.5.2.6 Modularity

Units were designed to be modular and interchangeable inasfar as possible. This is to facilitate swap out and replacement on site as well as to reduce the skills level requirements on maintenance personnel in operation.

2.5.2.7 Standards of manufacture

All electronic and mechanical sub-assemblies are manufactured / assembled in an ISO-9000 facility.

2.6 Quantified risk analysis

The quantified risk analysis for the refuge bay emergency indicator is done in the following section. The risk ratings used is defined in the following table:

Consequence Rating (CR)					
Rating	1	2	3	4	5
Explanation	Near miss injury / Damage	Disabling Injury	Serious Injury	Fatality	Catastrophic / multiple fatalities
Probability Rating (PR) - this is not a linear scale, please refer to the percentages.					
Rating	1 (<1%)	2 (1% - 5%)	3 (5% - 10%)	4 (10% - 50%)	5 (>50%)
Explanation	Practically Impossible	Not likely to happen	Could happen	Has happened	Common

Risk Rating (RR) = Consequence x Probability		
0 - 7	**8 - 15**	**16 - 25**
Low	**Medium**	**High**

TABLE 1 : RISK RATING DEFINITION

2.6.1 Refuge bay Emergency Indicator Risk Matrix

The risk matrix below indicates risk identified within the system. Please note that the current risk can be significantly reduced by implementing the recommended controls as shown with the reduced risk option.

Option 1 - Technical / Operational Risk									
Number	Failure mode	Consequence	CR	PR with control	RR without control	Additional controls	CR	PR with control	RR with control
1	Power cable fault	No power to the system - System failure.	4	1	4	Develop test specification to test the system regularly.	4	0.5	2
2	External over voltage condition	System failure	4	2	8	Implement protection – done in all units (as per design)	1	1	1
3	Backup battery failure	No power to the system for EM indication - System failure.	4	1	4	Develop test specification to test the system regularly. Replace battery every 2 years.	4	0.5	2
4	Battery theft	No power to the system for EM indication- System failure.	4	1	4	Ensure the system is locked to avoid tampers.	4	0.5	2
5	Bezel failure	No visual indication of the state of the system.	2	1	2	Four bezels are used, connected in parallel.	2	0.5	1
6	Siren failure	No audible indication of the state of the system.	2	1	2	Develop test specification to test the system regularly.	2	0.5	1
7	Incorrect installation	Minimal to limited visibility to the surrounding area.	3	1	3	Installation documentation and sufficient training.	3	0.5	1.5
8	Environmental Hazard (Direct fire)	System failure.	5	1	5	Ensure proper installation in a safe area.	5	0.5	2.5
9	Personnel training support system failure	System failure.	5	3	15	Ensure effective training documentation is available.	5	1	5
10	Maintenance and repair support system failure	System failure.	5	3	15	Schedule additional maintenance and keep stock of the system components.	5	1	5
		Unmitigated risk			**62**	***Mitigated risk***			**23**

3 QUALITY ASSURANCE PROVISIONS

3.1 Manufacturing

3.1.1 Documentation

All manufacturing, assembly, and test documentation was done to control quality during manufacturing. Quality design, procurement, manufacturing and assembly, and test and inspection procedures are documented and enforced.

3.1.2 Tests

The following tests are done during manufacture:

1. Component *inspection* before assembly;
2. Board-level *testing* is done to prevent infant mortality;
3. Assembly *inspection* is done;
4. Component-level *testing* is done;
5. Module-level *testing* is done;
6. Packaging *inspection* is done.

3.2 Installation, operation, and maintenance

3.2.1 Documentation

Installation, operational and maintenance documentation is available to ensure quality use of the system.

3.2.2 Tests

The following test procedures must be followed when utilizing the system:

1. Module *inspection* before installation;
2. First use *inspection* should be done on customer premises;
3. Replacement *inspection* and *testing*.

4 CONFIGURATION CONTROL

DOCUMENT HISTORY

Issue	Date	Status	Editor	Filename on disk
1	2010/05/05	Released	MSW	RBEI Product Functional Specification and Risk Assesment V1.doc

REVISION HISTORY

Issue	Date	Changes
1	2010/05/05	Creation

AUTHORISATION HISTORY

Issue	Date	Status	Reference
1	2010/05/05	Authorised	GPR van der Merwe