Results of the IEC 61508 Functional Safety Assessment

Project:
Faceboss Safety System

Customer:
Joy Global
Wigan, Lancashire
UK

Contract No.: Q14-06-014
Report No.: Joy 1406014 R001
Version V1, Revision R4, April 8, 2015
David Johnson
Management Summary

The Functional Safety Assessment of the Joy Global Faceboss Safety System development project, performed by exida consisted of the following activities:

- exida assessed the development process used by Joy Global through an audit and review of a detailed safety case against the exida certification scheme which includes the relevant requirements of IEC 61508. The investigation was executed using subsets of the IEC 61508 requirements tailored to the work scope of the development team.

- exida reviewed and assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.

- exida reviewed the manufacturing quality system in use at Joy Global.

The functional safety assessment was performed to the requirements of IEC 61508-3:2000 for SIL 1 and IEC 61508-1:2000 and IEC 61508-2:2000 for SIL 2. A full IEC 61508 Safety Case was reviewed, using the exida Safety Case tool, which was used as the primary audit tool. Hardware process requirements and all associated documentation were reviewed. Environmental test reports were reviewed. Also the user documentation (safety manual) was reviewed.

The results of the Functional Safety Assessment can be summarized by the following statements:


The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the Faceboss Safety System can be used in a low demand safety related system in a manor where the PFD$_{AVG}$ is within the allowed range for SIL 2 ($HFT = 0$) according to table 2 of IEC 61508-1 for safety function SF1 as defined in Table 1.

The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the Faceboss Safety System can be used in a high demand safety related system in a manor where the PFH is within the allowed range for SIL 1 ($HFT = 0$) according to table 2 of IEC 61508-1. This claim is limited to the list of SIFs in table 1 of this document that are listed as high demand.

The assessment of the FMEDA also shows that the Faceboss Safety System meets the requirements for architectural constraints of an element such that it can be used to implement a SIL 2 or SIL 1 safety function (with $HFT = 0$), according to Table 1 List of Safety Functions.

This means that the Faceboss Safety System is capable for use in SIL 1 or SIL 2 applications in Low or High Demand mode according to Table 1 when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual and when using the versions specified in section 3.1 of this document.
The manufacturer will be entitled to use the Functional Safety Logo.
# Table of Contents

Management Summary ........................................................................................................ 2

1 Purpose and Scope ............................................................................................................ 5
   1.1 Safety Function Summary ....................................................................................... 6
   1.2 Tools and Methods used for the assessment ............................................................ 7

2 Project Management ......................................................................................................... 8
   2.1 exida ......................................................................................................................... 8
   2.2 Roles of the parties involved ...................................................................................... 8
   2.3 Standards / Literature used ....................................................................................... 8
   2.4 Reference documents ............................................................................................... 8
      2.4.1 Documentation provided by Joy Global ............................................................. 8
      2.4.2 Documentation generated by exida ................................................................... 9
   2.5 Assessment Approach ............................................................................................... 9

3 Product Description ......................................................................................................... 10
   3.1 Hardware and Software Version Numbers ............................................................... 10

4 IEC 61508 Functional Safety Assessment Scheme ......................................................... 11
   4.1 Product Modifications .............................................................................................. 11

5 Results of the IEC 61508 Functional Safety Assessment ............................................... 11
   5.1 Lifecycle Activities and Fault Avoidance Measures ................................................ 12
   5.2 Safety Requirement Specification ............................................................................ 12
   5.3 Change and modification management .................................................................... 12
   5.4 System Design ......................................................................................................... 12
   5.5 Software Design ...................................................................................................... 12
   5.6 Hardware Design ..................................................................................................... 12

6 Software Verification ....................................................................................................... 12

7 Terms and Definitions ..................................................................................................... 13

8 Status of the document .................................................................................................. 14
   8.1 Liability .................................................................................................................... 14
   8.2 Releases .................................................................................................................... 14
   8.3 Future Enhancements ............................................................................................... 14
   8.4 Release Signatures .................................................................................................. 14
1 Purpose and Scope
This document shall describe the results of the IEC 61508 functional safety assessment of the Joy Global:

- Faceboss Safety System

by exida according to accredited exida certification scheme which includes the requirements of IEC 61508:2000.

The purpose of the assessment was to investigate the compliance of:
the Faceboss Safety System with the technical IEC 61508-2 and -3 requirements for a SIL 2 or SIL 1 safety function (with HFT = 0), according to Table 1 List of Safety Functions.

and

- the Faceboss Safety System development processes, procedures and techniques as implemented for the safety-related deliveries with the managerial IEC 61508-1, -2 and -3 requirements for SIL 1.

and

- the Faceboss Safety System hardware analysis represented by the Failure Mode, Effects and Diagnostic Analysis with the relevant requirements of IEC 61508-2.

The assessment has been carried out based on the quality procedures and scope definitions of exida.

The results of this assessment provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

The maximum quantities of RS20s system hardware permitted are as follows.

- SYNC - Quantity 1
- ACK - Quantity 1
- BARRIER - Quantity 345
- CORE - Quantity 350
- MIMIC - Quantity 700
- T-PIECE - Quantity 1390
- STU - Quantity 690
- DUAL SOLENOID – Quantity 4140

Note: If the system in use has two Mimics for every Core, then the maximum number of STU’s permitted must not exceed 500.
## 1.1 Safety Function Summary

<table>
<thead>
<tr>
<th>Safety Function</th>
<th>Maximum SIL</th>
<th>Demand</th>
<th>Summary</th>
</tr>
</thead>
</table>
| 1a 1b           | SIL2        | Low    | Emergency Stop – Dump Valve Direct Emergency Stop – Dump Valve ASB  
Hydraulic pressure shall be removed from the face when the emergency stop system is operated. This system shall operate in a fail-safe manner. |
| 2               | SIL1        | High   | Pre-Start Warning  
There shall be an audible and visual pre start warning before any out of sequence movement of a roof support which reduces the operator walkway.  
There shall be an audible and visual pre start warning when an operator instigates any valve sequences.  
There shall be an audible and visual pre start warning when an operator is detected in a shield and the operation will reduce the walkway. |
| 3               | SIL1        | High   | Adjacent Control  
The system shall only allow control of adjacent shield. |
| 4               | SIL1        | High   | Pause PRS Control  
To allow operators to safely traverse the face past operating shields there shall be a pause facility which pauses the current sequence. |
| 5 6             | SIL1        | High   | Free Run Control with Shearer Tracking (IR) Free Run Control with Shearer Tracking (SIRSA)  
The system shall allow operators to manually move shields in sequences which allow operators to keep away from moving shields. |
| 7               | SIL1        | High   | Faulty Sensor Detection  
The system shall be able to detect a non-operational or disconnected sensor. |
| 8 9             | SIL1        | High   | Shearer Initiation with Shearer Tracking (IR) Shearer Initiation with Shearer Tracking (SIRSA)  
The system shall allow operators to automatically move shields in sequences around the shearer which allows operators to keep away from moving shields. |
<table>
<thead>
<tr>
<th>Safety Function</th>
<th>Maximum SIL</th>
<th>Demand</th>
<th>Summary</th>
</tr>
</thead>
</table>
| 10 11           | SIL1        | High   | **Sprag Control with Shearer Tracking (IR)**
|                 | PFH < 1E-5  |        | **Sprag Control with Shearer Tracking (SIRSA)**
|                 |             |        | The system shall automatically extend and retract the Sprag around the Shearer, and report if operation was not successful. |
| 12a 12b        | SIL1        | High   | **Missing Mimic Detection (DS)**
|                 | PFH < 1E-5  |        | **Missing Mimic Detection (STU and DS)**
|                 |             |        | With systems having 2 or more PRS Mimics the system shall notify if a Mimic is missing and not allow the system to operate shields if two adjacent shields have missing Mimics. |
| 13              | SIL1        | Low    | **Emergency Stop – Solenoid Supply**
|                 | PFDav < 1E-1 |      | Actuating solenoids on the face shall be electrically isolated when the emergency stop system is operated. This system shall operate in a fail safe manner. |
| 14 15           | SIL1        | High   | **Proximity – Movement prevention via solenoid control**
|                 | PFH < 1E-5  |        | **Proximity – Movement prevention via Dump Valve control**
|                 |             |        | To prevent the movement of roof supports by disabling solenoids/Dump Valve operation under software control. |

Table 1 List of Safety Functions

1.2 Tools and Methods used for the assessment

This assessment was carried by using the **exida** Safety Case tool. The Safety Case tool contains the **exida** scheme which includes all the relevant requirements of IEC 61508.

For the fulfillment of the objectives, expectations are defined which builds the acceptance level for the assessment. The expectations are reviewed to verify that each single requirement is covered. Because of this methodology, comparable assessments in multiple projects with different assessors are achieved. The arguments for the positive judgment of the assessor are documented within this tool and summarized within this report.

The assessment was planned by **exida** agreed with Joy Global.

All assessment steps were continuously documented by **exida**
2 Project Management

2.1 exida

exida is one of the world’s leading accredited Certification Bodies and knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world’s top reliability and safety experts from assessment organizations and manufacturers, exida is a global company with offices around the world. exida offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. exida maintains a comprehensive failure rate and failure mode database on process equipment based on 100 billion hours of field failure data.

2.2 Roles of the parties involved

Joy Global Manufacturer of the Faceboss Safety System
exida Performed the hardware assessment
exida Performed the Functional Safety Assessment per the accredited exida scheme.

Joy Global contracted exida with the IEC 61508 Functional Safety Assessment of the above mentioned devices.

2.3 Standards / Literature used

The services delivered by exida were performed based on the following standards / literature.


2.4 Reference documents

2.4.1 Documentation provided by Joy Global

<table>
<thead>
<tr>
<th>Doc name / Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[D1] 0264-2 20150212 Fb Highway Comms Safety IEC61508 February 12, 2014</td>
<td>Analysis and Test results demonstrating the capacity to extend the maximum number of CORES</td>
</tr>
<tr>
<td>[D2] TELS0736-0413_Cert_rev02 March 2015</td>
<td>Operations and Maintenance manual. This describes the operating environment, and takes the place of a Safety Manual.</td>
</tr>
</tbody>
</table>
### 2.4.2 Documentation generated by exida

<table>
<thead>
<tr>
<th>Doc name / Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[R1] Joy 1406014 R001 Long Wall IEC61508 AssessmentV1R3.docx (this document)</td>
<td>Product Assessment Report (combines software and hardware)</td>
</tr>
<tr>
<td>[R2] Joy 12-02-087 R002 V2R1 Faceboss FMEDA April 14, 2014</td>
<td>Updated RS20s FMEDA on Faceboss hardware</td>
</tr>
<tr>
<td>[R3] JOY 08-11-21 R004 V2R1 PRS Software IEC61508 Assessment Sept 4, 2013</td>
<td>Previous Software Assessment Report</td>
</tr>
<tr>
<td>[R4] JOY 08-11-21 R003 V1R2 PRS Electronics IEC61508 Assessment Summary Oct 22, 2009</td>
<td>Previous Hardware Assessment Report</td>
</tr>
</tbody>
</table>

### 2.5 Assessment Approach

The certification audit was closely driven by requirements of the exida scheme which includes subsets filtered from IEC 61508.

The assessment was planned by exida and agreed with Joy Global.

The following IEC 61508 objectives were subject to detailed auditing at Joy Global:

- FSM planning, including
  - Safety Life Cycle definition
  - Scope of the FSM activities
  - Documentation
  - Activities and Responsibilities (Training and competence)
  - Configuration management
  - Tools and languages
- Safety Requirement Specification
- Change and modification management
- Software architecture design process, techniques and documentation
- Hardware architecture design - process, techniques and documentation
- Hardware design / probabilistic modeling
- Hardware and system related V&V activities including documentation, verification
  - Integration and fault insertion test strategy
- Software and system related V&V activities including documentation, verification
- System Validation including hardware and software validation
- Hardware-related operation, installation and maintenance requirements

The project teams, not individuals were audited.
The certification audit was done in Sellersville, PA February 27, 2015

3 Product Description

The Product is a mine longwall Powered Roof Support (PRS) system. During the mining process, longwall equipment and personnel are protected by hydraulically actuated roof supports which cover the length of the longwall face. The roof supports control the collapse of the overlying strata and help in stabilizing the coal face. Each roof support is connected to an Armored Face Conveyor (AFC) pan via a hydraulic ram which is used during longwall advancement. As the face advances longitudinally along the panel, the roof collapses under its own weight behind the roof supports. Controlling the collapse is critical to the efficiency and safety of the longwall mine.

![Diagram of Faceboss Safety System](image)

**Figure 1: Overview of the Faceboss Safety System**

3.1 Hardware and Software Version Numbers

This assessment is applicable to the following hardware and software versions of Faceboss Safety System:

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td>T070-65-14 - 5th February 2015</td>
</tr>
</tbody>
</table>
### 4 IEC 61508 Functional Safety Assessment Scheme

*exida* assessed the safety case, including a set of documents, against the functional safety management requirements of IEC 61508. This was done by a pre-review of the completeness of the related requirements and then a spot inspection of certain requirements, before the development audit. The safety case demonstrated the fulfillment of the functional safety management requirements of IEC 61508-1 to 3.

The detailed development audit (see [R1]) investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the Joy Global Faceboss Safety System.

The investigation was executed using the *exida* certification scheme which includes subsets of the IEC 61508 requirements tailored to the work scope of the development team.

The result of the assessment shows that the Product is capable for use in SIL 1 applications, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

#### 4.1 Product Modifications

The modification process has been successfully assessed and audited, so Joy Global may make modifications to this product as needed.

### 5 Results of the IEC 61508 Functional Safety Assessment

*exida* assessed the development process used by Joy Global during the product development against the objectives of the *exida* certification scheme which includes IEC 61508 parts 1, 2, & 3. The certification report referenced (see [R1]) describes the software portion of the certification and references documentation provided to support the certification.
5.1 Lifecycle Activities and Fault Avoidance Measures
Joy Global has an IEC 61508 compliant development process as assessed during the IEC 61508 certification. This compliant development process is documented in [R1].

5.2 Safety Requirement Specification
The objectives of the standard are fulfilled by the Joy Global functional safety management system.

5.3 Change and modification management
The objectives of the standard are fulfilled by the Joy Global functional safety management system.

5.4 System Design
The objectives of the standard are fulfilled by the Joy Global functional safety management system.

5.5 Software Design
The objectives of the standard are fulfilled by the Joy Global functional safety management system.

5.6 Hardware Design
The objectives of the standard are fulfilled by the Joy Global functional safety management system. The hardware certification report is identified in the detailed development audit (see [R2]).

6 Software Verification
Separate reports were written to certify the software and hardware. An additional report was written to perform an analysis on the maximum number of units that can be connected. This report is a combination of analysis of the design as well as testing of two existing systems. Graphs were created showing the correlation between the design analysis and the actual systems tested allowing a projection to a safe maximum number of units that can be part of a single system (see [D1]).

The report yielded the following conclusions:

- For different face lengths and for varying levels of highway communication activity, the theoretical times for data to access the highway have been compared with measured times and have found to be in agreement. This gives confidence that the highway communication model is accurate enough to predict what the worst case delays will be for the system declared in this IEC61508 assessment.
• The Joy document 0213 defines that the maximum number of System Cores and Barriers will be 350 and 345 respectively. Using the derived spreadsheet, the maximum delay time, for 100% communication capacity will be between 771ms and 1542ms. For communication messages requiring an acknowledge these times will need to be doubled so the worst case time for a Control/Acknowledge sequence is 3.084 seconds but the average time will be 2.313 seconds.

• The Append Refused mechanism in the cores has been physically tested and found to operate as predicted. All cores are shown to have equal access when placing packets on the face during an Append Refused cycle.

7 Terms and Definitions

Fault tolerance Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3)

FIT Failure In Time (1x10⁻⁹ failures per hour)

FMEDA Failure Mode Effect and Diagnostic Analysis

HFT Hardware Fault Tolerance

Low demand mode Mode, where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.

PFD_AVG Average Probability of Failure on Demand

PFH Probability of dangerous Failure per Hour

PVST Partial Valve Stroke Test

It is assumed that the Partial Stroke Testing, when performed, is automatically performed at least an order of magnitude more frequent than the proof test, therefore the test can be assumed an automatic diagnostic. Because of the automatic diagnostic assumption the Partial Valve Stroke Testing also has an impact on the Safe Failure Fraction.

SFF Safe Failure Fraction - Summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.

SIF Safety Instrumented Function

SIL Safety Integrity Level

SIS Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).

Type A element “Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2

Type B element “Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2
8 Status of the document

8.1 Liability

exida prepares reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. exida accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

8.2 Releases

Version History:
- V1, R1: Initial Release
- V1, R2: Minor corrections requested by Joy Global team
- V1, R3: Corrected references to previous assessment reports
- V1, R4: Minor corrections requested by Joy Global team

Authors: David Johnson
Review: Release status: Final

8.3 Future Enhancements

At request of client.

8.4 Release Signatures

David A. Johnson, Senior Safety Engineer

Michel Medoff, CFSE, CISA, Senior Safety Engineer