ENGINEERING SAFETY CONSULTANTS

*The Global Provider of Functional Safety Expertise and Technical Consultancy*

# IEC 61508 Random Hardware Reliability Certificate

## *Functional Safety of Safety-Related Programmable Electronic Systems*

The **Pneumatrol Ltd, Redundant Valve Manifold (RVM) Screw Isolation Low Flow and High Flow variants** have been assessed and are considered capable for use in a low demand Safety Function up to (and including) SIL 3, with respect to random hardware failures and architectural constraints.

The function of the RVM is to allow the pneumatic solenoid valves connected to the block to remove the pneumatic supply at the output of the of the block within the specified time. The function applies to use of pneumatic solenoid valves operating as De-Energise To Trip (DETT) or Energise To Trip (ETT).

The assessment was based on the assumptions, data provided, and recommendations given in:

- **Engineering Safety Consultants Ltd Report: G210_SV001 rev.5;**
- **Renewal Letter from Pneumatrol Ltd, signed by Jamie C Dummer, Managing Director, dated 20th January 2023.**

The product was assessed against the following failure modes:

- RVM Block with 4x solenoid valves in a DETT mode of operation (Low and High Flow variants);
- RVM Block with 4x solenoid valves in an ETT mode of operation (Low and High Flow variants).

The assessment was carried out to determine compliance with IEC 61508 (2010 Edition) with regards to:

- Random Hardware Failure:
  - DETT Mode: SIL 3 with a HFT = 1 via Route $1_H$ (Note: The RVM block is engineered to provide a fully redundant configuration (HFT=1) for execution of the safety function and to account for the inherent fault tolerance within the block);
  - ETT Mode: SIL 3 with a HFT = 1 via Route $1_H$ (Note: The RVM block is engineered to provide a fully redundant configuration (HFT=1) for execution of the safety function and to account for the inherent fault tolerance within the block).
- Architectural Constraints:
  - DETT Mode of Operation (Type A, SFF >60% <90%) for Low and High flow variants;
  - ETT Mode of Operation (Type A, SFF >60% <90%) for Low and High flow variants.

**IMPORTANT:** It should be noted that this assessment does not include confirmation of the response time of the device. For response times (along with any relevant assumptions) reference should be made to the Safety Manual of each device and the total SIF response time **MUST** be compared against the process safety time for the specific application.

Note 1: The SIL of a complete SIF (sensor, logic solver and final element subsystems) must be verified to calculate the required PFD / PFH, considering any redundancy, Proof Test Interval (PTI), Proof Test Coverage (PTC), Mission Time and Mean Time To Restoration (MTTR) for all elements included in the SIF. Each subsystem should be verified to ensure compliance with the minimum HFT requirements.

Managing Director: Simon Burwood
Assessment Date: September 2018
Renewal Date: February 2023, valid to February 2025
Certificate: G210_CT001 rev. 6

**ENGINEERING SAFETY CONSULTANTS LTD**
**2nd Floor, Exchequer Court, 33 St. Mary Axe,**
**London, EC3A 8AA UK**
**Telephone/Fax: +44 (0)20 8542 2807**
**E-Mail: info@esc.uk.net Web: www.esc.uk.net**
**Registered in England and Wales: 7006868**
**Registered Office: 33 St. Mary Axe, London EC3A 8AA**