

# IEC61508

# CERTIFICATE OF COMPLIANCE **NAUTITECH™** SHUTDOWN SYSTEM

This document is issued as a summary of the hardware failure data affecting the application of the equipment as a sub-system being part of a Safety Function intended to conform with the requirements of IEC61508 - Functional Safety of Electrical/Electronic/Programmable Logic Safety Systems. The hardware has been subjected to a Failure Modes Effects and Diagnostics Analysis (FMEDA) to determine the specific failure modes and failure rates with the relevant results presented herein.

## Oil Pressure Shutdown Safety Function

The oil pressure shutdown safety function utilises the standard hardware platform from Nautitech consisting of the following items/products:

Item	Product Code	Character Display	Graphics Display
Oil Pressure Sensor	Type 5001 series	✓	✓
ECU Logic	PL500120	✓	✓
Character Display (*)	PL118503	✓	
Graphics Display (*)	ME5350-1-99-260		✓
PMU	PL500102	✓	✓

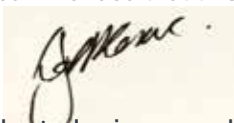
Notes (\*) Display units are interchangeable

## Product Failure Rates

Oil Pressure Shutdown Function	Character Display	Graphics Display
SIL Capability	1	1
Sub-System Type	B	B
Hardware Fault Tolerance (HFT)	0	0
Safe Failure Fractions (SFF)	85.6%	85.1%
PFH1oo1	$6.27 \times 10^{-6}$	$7.19 \times 10^{-6}$
PFD1oo1 (2 year proof-test interval)	$5.50 \times 10^{-2}$	$6.30 \times 10^{-2}$
MTBF	22922 hrs	20696 hrs

## Notes

- Reliability data for this analysis is taken from MIL-HDBK217F Notice 2 and Siemens SN29500 Reliability Data Handbook.
- Proof testing must be carried out according to the application requirements, however it is recommended that this be carried out atleast once every two years.



Analyst: Josias van der Merwe  
Date: 1st Nov 2016

Signed on behalf of Nautitech



Verification: Marcus Punch Pty. Ltd.  
Date: 1st Nov 2016