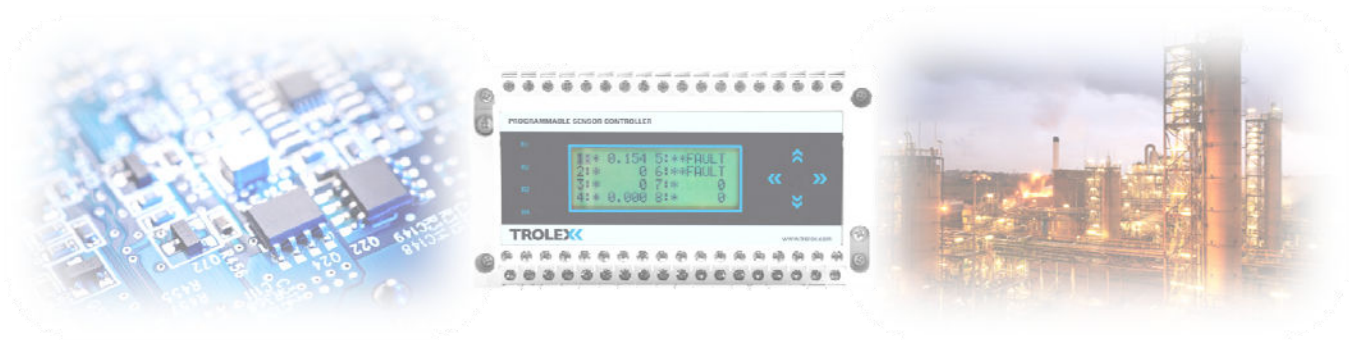




Functional Safety Assessment Report

Product assessed: TX9042 Programmable Sensor Controller
Manufacturer: Trolex Ltd
Report number: RPT14007-1CA
Report revision: Rev 1.0
Date of issue: 8th October 2014
Confidentiality status: Open



Assessor:

Paul Reeve BEng CEng MIET MInstMC
Silmetric Ltd

This is an abridged version (intended for open disclosure) of the full report RPT14007-1C, rev 1.0 (42 pages, client confidential). It may only be reproduced in its entirety and without change

I N D E P E N D E N T F U N C T I O N A L S A F E T Y A S S E S S M E N T

1 Scope of assessment

This report is a summary of an independent assessment of the TX9042 Programmable Sensor Controller against the requirements of IEC 61508-2:2010 according to the 'Route 2_H' and the 'Route 2_S' approach (also known as 'proven in use') from this Standard. The objective of meeting these requirements is to qualify the product for use in representative applications performing safety functions assigned with a Safety Integrity Level (SIL). The information in this document is extracted from the full product assessment report RPT14007-1C, rev 0.1 (41 pages, client confidential).

The evaluations included:

- Hardware and systematic safety integrity of the TX9042 based on analysis and statistical inference from field failure data for a large number of units gathered from end-users over several years of service in specific subsystem configurations
- Associated product documentation (e.g., the safety manual) to support the unit's selection and integration into safety-related systems in similar applications and environments
- Functional safety management within Trolex to support the ongoing monitoring and validity of the product's reliability performance and integrity applicable to future sales of the unit

The assessment has been carried out with reference to the *Conformity Assessment of Safety-related Systems (CASS)* methodology (www.cass.uk.net).

2 Compliance statements

Results of the assessment confirm that:

- 1) The versions and configurations of the TX9042 identified in this report comply with the relevant requirements of IEC 61508-2:2010
- 2) The stated safety function of this product when configured in the manner described in this report is suitable for use in safety instrumented functions up to and including:
 - **SIL 2** when used in a 'Low Demand' safety function ^[1] with proof test interval of 3 months
 - **SIL 1** when used in a 'Low Demand' safety function ^[1] with proof test interval of 12 months
 - **SIL 1** when used in a 'High Demand' safety function ^[1]

The functional safety data (below) must be taken into account by integrators and end-users, including compliance with the restrictions in use (below) and all other provisions in the Safety Manual.

System integrators and end users responsible for other lifecycle phases (system specification, integration, installation, commissioning, operation, maintenance, etc) need to perform assessments on the complete scope of their activities to ensure the overall safety function is achieved and maintained.

^[1] Low Demand and High Demand modes of operation are defined in IEC 61508-4, 3.5.16

3 Summary of the verified functional safety data

The product, configuration and safety manual that have been assessed are shown in Table 1.

PRODUCT INFORMATION	DETAILS
Product identification	TX9042.55 Programmable Sensor Controller
Product specification	Contained in the TX9042 User Manual, TX9042-UM-EN-01
Product configuration	4-20mA or 0.4-2V input cards fitted; Neither the display nor the RS-485 data link are part of the specified safety function.
System configuration	Monitoring of signals from devices configured as 2/3-wire current loop devices, 4-wire current inputs with separate power connection, or voltage inputs.
Element Safety Function	To de-energise an output channel relay (open relay contacts) if either the input signal transitions a pre-determined alarm threshold or an internal fault is indicated
Safety Manual	TX9042 User Manual (section 3), TX9042-UM-EN-01

Table 1: Basic element information

Modifications to the product or its documentation (e.g., Safety Manual) shall require re-assessment in order not to invalidate the compliance statements in this report.

The hardware failure data for the TX9042 element safety function based on the analysis of field failure data, using the single-sided χ^2 (chi-square) estimation method at 90% confidence, is shown in Table 2.

PARAMETER	VALUE
Dangerous failure rate (λ_D)	2.3E-06
Safe failure rate (λ_S)	N/R ^[1]
Safe failure fraction (SFF)	N/R ^[1]
Element type	Type B
Hardware fault tolerance (internal architecture)	0
Diagnostic coverage (DC)	60%
Diagnostic test interval	N/A ^[2]
Probability of Failure on Demand (PFD_{AVG}) ^[1 year proof test; 24hr MTTR]	1.0E-02 ^[2]
Probability of Failure on Demand (PFD_{AVG}) ^[3mth proof test; 24hr MTTR]	2.6E-03 ^[2]
Probability of dangerous Failure per Hour (PFH)	2.3E-06

Table 2: Hardware failure data

[1] Not required by Route 2_H

[2] To be conservative, no credit has been taken for the diagnostics

4 Additional information relevant to the assessment

Hardware safety integrity	Meets the requirements for Route 2 _H (IEC 61508-2, 7.4.4.3) based on component reliability data fed back from end users, increased confidence levels and hardware fault tolerance for specified safety integrity levels
Systematic safety integrity	Meets the requirements for Route 2 _S (IEC 61508-2, 7.4.10) based on proven-in-use evidence in restricted and specified configurations; Meets systematic capability level: SC 2
Management of functional safety	This product is manufactured and supplied under a quality management system that includes the relevant aspects of functional safety management from IEC 61508 that apply to Route 2 _H /2 _S

5 Restrictions and conditions of use

Restrictions in use	<p>The Safety Manual shall be strictly complied with to ensure validity of the failure data and systematic safety integrity. The following <i>additional</i> restrictions and conditions apply when the unit used in SIL applications:</p> <ol style="list-style-type: none">1. The TX9042 must be repaired within the MTTR assumed in the PFD calculations shown in the table above if an internal fault is detected in the unit2. If the MTTR or the proof test interval (T_1) is different from those assumed in this document, then the PFD_{AVG} must be re-calculated and the SIL capability re-verified accordingly (refer to Safety Manual)3. The display is for indication only and is not part of the safety function; likewise the RS-485 communications are not part of the safety function4. The environmental limits are restricted to: +20 to +40 deg C; relative humidity < 90%5. IEC 61508-2, 7.4.4.3.1c limits use to SIL 1 in high or continuous mode of operation when used in a non-redundant configuration
----------------------------	---

Proof Testing	Periodic proof tests of the element safety function must be performed to identify any dormant dangerous failures, particularly when used in 'low demand' safety functions – refer to the TX9042 User Manual, section 3. Faults identified by this test must be repaired within the MTTR and the unit returned to full working order. Details of the proof test are contained in the safety manual.
----------------------	--

SILMETRIC is a registered trade mark of Silmetric Ltd

I N D E P E N D E N T F U N C T I O N A L S A F E T Y A S S E S S M E N T