IEC 61508 Functional Safety Assessment

Project:

Safe-T-Pull

Customer:

Safe-T-Products Pty Ltd

18-19 Tambrey Way, Malaga WA 6090

Australia

Contract Number: Q24/03-114

Report No.: SAF 24/03-114 R002

Version V1, Revision R2, November 7, 2025

Jack Gao

Management Summary

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the Safe-T-Pull.

The functional safety assessment performed by *exida* consisted of the following activities:

- *exida* assessed the development process used by Safe-T-Products Pty Ltd 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* performed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* reviewed field failure data to verify the accuracy of the FMEDA analysis.
- *exida* reviewed the manufacturing quality system in use at Safe-T-Products.

The functional safety assessment was performed to the requirements of IEC 61508: ed2, 2010, SIL 3 for mechanical components. A full IEC 61508 Safety Case was prepared using the *exida* Safety Case tool 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 as:

The audited development process as tailored and implemented by the Safe-T-Products Pty Ltd Safe-T-Pull development project, complies with the relevant safety management requirements of IEC 61508 SIL 3, **SC 3 (SIL 3 Capable).**

The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the Safe-T-Pull can be used in a safety related system in a manner where the PFH / PFD_{avg} meets the requirements of table 2 or table 3 of IEC 61508-1.

The assessment of the FMEDA also shows that the Safe-T-Pull has a Safe Failure Fraction above 90%.

This means that the Safe-T-Pull is capable for use in SIL 3 applications, 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

1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the Safe-T-Products Pty Ltd:

- Safe-T-Pull

by *exida* according to accredited *exida* certification scheme which includes the requirements of IEC 61508: ed2, 2010.

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

The results of this 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.

1.1 Tools and Methods used for the assessment

This assessment was carried out 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 Safe-T-Products Pty Ltd.

All assessment steps were continuously documented by *exida* (see [R1] to [R3])

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 500 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 400 billion hours of field failure data.

2.2 Roles of the parties involved

Safe-T-Products Pty Ltd	Manufacturer of the Safe-T-Pull
exida	Performed the hardware assessment
exida	Performed the IEC 61508 Functional Safety Assessment per the accredited *exida* scheme.

Safe-T-Products contracted *exida* in April 2024 for the IEC 61508 Functional Safety Assessment of the above-mentioned devices.

2.3 Standards and literature used

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

[N1]	IEC 61508:2010 (Parts 1 - 2)	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Normative Parts
[N2]	IEC 61508:2010 (Parts 4 – 7)	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Informative Parts

2.4 Reference documents

2.4.1 Documentation provided by Safe-T-Products Pty Ltd

Doc ID	Project Document Name	Version	Date
D001	ECP-QMS-001 Quality Management System Manual.pdf	Version 4	21/3/2024
D003			
D004			
D005	ECP-PRO-001 Non-Conformance and Corrective Action - Version 5.pdf	Version 5	6/6/2025
D006			
D007	ECP-PRO-009 Purchasing.pdf	Version 2	8/9/2024

D010	ECP-QMS-001 Quality Management System Manual.pdf	Version 4	21/3/2024
D012	ECP-PRO-001 Non-Conformance and Corrective Action - Version 5.pdf	Version 5	6/6/2025
D013			
D016	D016	Folder	Folder
D019	ECP-PRO-001 Non-Conformance and Corrective Action - Version 5.pdf	Version 5	6/6/2025
D023	D016	Folder	Folder
D023b	D023b	Folder	Folder
D026	ECP-PRO-002 Design - Version 8.pdf	Version 8	2/5/2025
D027			
D027b	EXIDA - STP Device and Hardware Matrix - With Notes.pdf	Nil	Nil
D029	D029 Verification Plan	Folder	Folder
D030	STP - Net Sales Quantities for FY2019-2024.pdf	Nil	23/8/2024
D031	D031	Folder	Folder
D032	D032 Job Descriptions and Competency Levels	Folder	Folder
D033	ECP-PRO-006 Skills Recognition.pdf	Version 6	18/4/2024
D034			
D036	Safe-T-Products-9001-2015.pdf	6565-2366-01	1/11/2027
D038	SIL - List of Design Tools.docx	Version 1	27/5/2024
D040	D040	Folder	Folder
D047	D047 Mechanical Drawing	Folder	Folder
D054	D054	Folder	Folder
D069	D069	Folder	Folder
D073	ECP-PRO-001 Non-Conformance and Corrective Action - Version 5.pdf	Version 5	6/6/2025
D074	Testing of Safe_T_Pull Electrical Emergency Stop devices_AS_NZS_IEC 60947_5_5 _E250001Ex01_Final.pdf	E250001 Ex/01	23/5/2025
D078	PUB. No. TD_STP V4.6.pdf	V4.6	6/6/2025
D079			
D080			
D081	D081	Folder	Folder
D083	D083	Folder	Folder

2.4.2 Documentation generated by *exida*

[R1]	SAF 24-03-114 Pull Key FMEDA Report V1R1.pdf	FMEDA report, Safe-T-Pull
[R2]	SafeTProducts Audit Agenda_6-7Aug_MoM.xlsx	IEC 61508 Site Audit MoM, Safe-T-Products Pty Ltd
[R3]	SAF 24-03-114 V1R1 Safety Case.xlsm	IEC 61508 SafetyCaseWB for Safe-T-Pull
[R4]	SAF SafeTPull FFA R1.xlsx	PIU Analysis for Safe-T-Pull

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 upon by Safe-T-Products Pty Ltd.

The following IEC 61508 objectives were subject to detailed auditing at Safe-T-Products Pty Ltd:

- Functional Safety Management
- Safety Requirement Specification
- Change and modification management
- Hardware architecture design - process, techniques and documentation
- Hardware design
- Hardware V&V activities including Integration testing, documentation, verification
- Hardware-related operation, installation and maintenance requirements

3 Product Descriptions

Safe-T-Pull is a Final Element, Actuator, Electric Spring Return – It is an Emergency Stop Pull Wire Device. Activation of the Pull Wire will disable power to a conveyor system, stopping it.

3.1 Hardware Version Numbers

This assessment is applicable to the following hardware versions of Safe-T-Pull:

EXIDA - STP DEVICE AND HARDWARE MATRIX

	SIL SYSTEM	DEVICE FAMILY	MATERIAL	NUMBER OF MICROSWITCHES	INSTALLED ACTUATORS	ACGS	STROBE	RI
DEVICE	COMPULSORY	STP	-P	-2	(BLANK - DUAL)	(BLANK - NOT INSTALLED)	(BLANK - NOT INSTALLED)	(BLANK - NOT INSTALLED)
			-A	-4	-LH	-ACGS	-S2	-RI
			-SSB		-RH		-S3	
							-S4	
							-S6	
							-S7	
							-S8	

	SIL SYSTEM	HARDWARE FAMILY	MATERIAL	
HARDWARE	COMPULSORY	STL-10	-V	Safe-T-Lanyard
			-SS	

	SIL SYSTEM	HARDWARE FAMILY	MATERIAL	
HARDWARE	COMPULSORY	STG-FGK	(BLANK-SS ONLY)	First Guide Supports

	SIL SYSTEM	HARDWARE FAMILY	LENGTH	COVER	MATERIAL	
HARDWARE	COMPULSORY	STG	-200	(BLANK - NOT INSTALLED)	-SS	Safe-T-Guide - Standard Guide
				-C		

	SIL SYSTEM	HARDWARE FAMILY	MATERIAL	
HARDWARE	RECOMMENDED	STG-ES	-P	Safe-T-Guide - Signs
			-SS	

	SIL SYSTEM	HARDWARE FAMILY	MATERIAL	
HARDWARE	COMPULSORY	STP-E60	(BLANK-SS ONLY)	Compensation Spring

	SIL SYSTEM	HARDWARE FAMILY	NUMBER OF SPRINGS	MATERIAL	
HARDWARE	RECOMMENDED	STP-SH	-1 (SINGLE)	(BLANK - MILD STEEL)	STP Spring Holder
			-2 (DUAL)	-SS	

	SIL SYSTEM	HARDWARE FAMILY	MATERIAL	
HARDWARE KIT	COMPULSORY	STP-SSK	-SS	Rope Clamp Kit
			-P	

Only required for deflections exceeding 15 degrees from the Pull Cord axis, or when Safe-T-Guides are extended beyond the standard 200 mm length.

	SIL SYSTEM	HARDWARE FAMILY	MOUNTING BRACKET	MATERIAL	
HARDWARE KIT	COMPULSORY	STG	-RC (WITH)	(BLANK-SS ONLY)	Roller Guide with Mounting Bracket

	SIL SYSTEM	HARDWARE FAMILY	CLAMP	MATERIAL	
HARDWARE KIT	COMPULSORY	STG	-ER (SINGLE)	(BLANK - MILD STEEL)	Roller Guide mounted on Extension Head
			-ERD (DUAL)	-SS	

	SIL SYSTEM	HARDWARE FAMILY	COVER/CLAMP	MATERIAL	
HARDWARE KIT	COMPULSORY	STG	-EGC (WITH COVER - SINGLE CLAMP)	(BLANK - MILD STEEL)	Plastic Pull Cord Guide mounted on Extension Head
			-EGCD (WITH COVER - DUAL CLAMP)	-SS	

	SIL SYSTEM	HARDWARE FAMILY	MOUNTING	MATERIAL	
HARDWARE	COMPULSORY FOR: STG-ER, STG-ER-SS, STG-ERD, STG-ERD-SS, STG-EGC, STG-EGC-SS, STG-EGCD, STG-EGCD-SS	STPM	-EBD (VERTICAL OR HORIZONTAL MOUNTING)	(BLANK - MILD STEEL)	Dual Clamp Foot
			-EBD90 (VERTICAL OR HORIZONTAL MOUNTING - 90 DEGREE ROTATION)	-SS	

4 IEC 61508 Functional Safety Assessment Scheme

exida assessed the development process used by Safe-T-Products Pty Ltd for this development project against the objectives of the *exida* certification scheme which includes subsets of IEC 61508 -1 to 2. The results of the assessment are documented in [R3].

4.1 Methodology

Functional safety assessment includes an assessment of all fault avoidance and fault control measures during hardware development and demonstrates compliance with IEC 61508 to the end-user. The assessment considers all requirements of IEC 61508. Any requirements that have been deemed not applicable have been marked as such in the full Safety Case report, e.g. software development requirements for a product with no software. The assessment also includes a review of existing manufacturing quality procedures to ensure compliance to the quality requirements of IEC 61508.

As part of the IEC 61508 functional safety assessment the following aspects have been reviewed:

- Development process, including:
  - Functional Safety Management, including training and competence recording, FSM planning, and configuration management
  - Specification process, techniques and documentation
  - Design process, techniques and documentation, including tools used
  - Validation activities, including development test procedures, test plans and reports, production test procedures and documentation
  - Verification activities and documentation
  - Modification process and documentation
  - Installation, operation, and maintenance requirements, including user documentation
  - Manufacturing Quality System
- Product design
  - Hardware architecture and failure behavior, documented in a FMEDA

The review of the development procedures is described in section 5.1. The review of the product design is described in section 5.2.

4.2 Assessment level

The Safe-T-Pull has been assessed per IEC 61508 to the following levels:

- SIL 3 capability

The development procedures have been assessed as suitable for use in applications with a maximum Safety Integrity Level of 3 (SIL 3) according to IEC 61508.

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by Safe-T-Products Pty Ltd for these products against the objectives of the *exida* certification scheme which includes IEC 61508 parts 1 and 2 see [N1]. The development of the Safe-T-Pull was done per this IEC 61508 SIL 3 compliant development process. The Safety Case was updated with project specific design documents.

5.1 Lifecycle Activities and Fault Avoidance Measures

Safe-T-Products Pty Ltd has a defined product lifecycle process in place. This is documented in the Quality Management System Manual [D001] and various Quality Procedures [D002-D023]. Every customer's job goes through the complete design process. A documented modification process is also covered in ECP-PRO-002 [D023]. No software is part of the design and therefore any requirements specific to software and software development do not apply.

The assessment investigated the compliance of the procedures and techniques as implemented for product design and development. The investigation was done using the *exida* certification scheme which includes subsets of IEC 61508 requirements tailored to the SIL 3 work scope. The result can be summarized by the following observations:

The audited Safe-T-Products Pty Ltd design and development process complies with the relevant managerial requirements of IEC 61508 SIL 3 .

5.1.1 Functional Safety Management

The Safe-T-Pull products manufactured by Safe-T-Products are not built for inventory. These Safe-T-Pull products are built-to-order. The basic designs are standardized, but each order can have trim and materials variations or specific customer requested proof tests.

FSM Planning

Safe-T-Products Pty Ltd has a defined process in place for product design and development. Required activities are specified along with review and approval requirements. This is primarily documented in section 6 of their Quality Management System Manual [D001] and in greater detail in procedures ECP-PRO-002. Templates and sample documents were reviewed and found to be sufficient. The modification process is covered by ECP-PRO-002. This process and the procedures referenced therein fulfill the requirements of IEC 61508 with respect to functional safety management for a product with simple complexity and well-defined safety functionality.

Version Control

ECP-QMS-001 [D001] requires that all documents be under document control. Use of this to control revisions was evident during the audit.

Training, Competency recording

ECP-QMS-001 [D001] and ECP-PRO-006 require the Human Resource department to maintain training records of education, experience, training and qualifications for all personnel. Department heads are responsible for identifying and providing the training needs for their department as well as proficiency evaluations. The procedures and records were examined and found up-to-date and sufficient. Safe-T-Products hired *exida* to be the independent assessor per IEC 61508 and to provide specific IEC 61508 knowledge.

5.1.2 Safety Requirements Specification and Architecture Design

For the Safe-T-Pull, the simple primary functionality of the product is the same as the safety functionality of the product (changes position, Close / Open). Therefore, no special Safety Requirements Specification was needed. The normal functional requirements were sufficient. As the Safe-T-Pull designs are simple and are based upon standard designs with extensive field history, no semi-formal methods are needed. General Design and testing methodology is documented and required as part of the design process. This meets SIL 3.

5.1.3 Hardware Design

The requirements in this area of the hardware design process are satisfied by proven-in-use.

5.1.4 Validation

Validation Testing is documented on the report from Simtars [D074]. The test plan includes testing per all standard and customer performance requirements. As the Safe-T-Pull are purely mechanical devices with a simple safety function, there is no separate integration testing necessary. The Safe-T-Pull perform only 1 Safety Function, which is extensively tested under various conditions during validation testing.

Items from IEC **61508-2, Table B.3** include functional testing, project management, documentation, and black-box testing (for the considered devices this is similar to functional testing). Field experience and statistical testing via regression testing are not applicable. This meets SIL 3.

Items from IEC **61508-2, Table B.5** included functional testing and functional testing under environmental conditions, project management, documentation, failure analysis (analysis on products that failed), expanded functional testing, and black-box testing.

This meets SIL 3.

5.1.5 Verification

The development and verification activities are defined in Section 6 of [D001]. For each design phase the objectives are stated, required input and output documents and review activities. This meets SIL 3.

5.1.6 Proven In Use

In addition to the Design Fault avoidance techniques listed above, a Proven in Use evaluation was carried out on the Safe-T-Products Safe-T-Pull. Shipment records were used to determine that the Safe-T-Pull have >30 million hours in use and they have demonstrated a field failure rate less than the failure rates indicated in the FMEDA reports. This meets the requirements for Proven In Use for SIL 3.

5.1.7 Modifications

Modifications are initiated per ECP-PRO-001 [D023] Non-conformance and Corrective Action procedure. All changes are first reviewed and analyzed for impact before being approved. Measures to verify and validate the change are developed following the normal design process.

The modification process has been successfully assessed and audited, so Safe-T-Products Pty Ltd may make modifications to this product as needed according to IEC 61508, it was expected that modifications to the product prior the assessment did not include a functional safety impact analysis. The modification process has been revised to include a functional safety impact analysis. The initial post assessment modification to the Safe-T-Pull shall be audited by *exida* to confirm that a functional safety impact analysis was performed according to Safe-T-Products's modification procedure.

- The *exida* scheme requires a periodic surveillance audit. The modification documentation listed below is submitted as part of the surveillance audit. *exida* will review the decisions made by the competent person in respect to the modifications made.
    - List of all anomalies reported
    - List of all modifications completed
    - Safety impact analysis which shall indicate with respect to the modification:
        - The initiating problem (e.g. results of root cause analysis)
        - The effect on the product / system
        - The elements/components that are subject to the modification
        - The extent of any re-testing
    - List of modified documentation
    - Regression test plans

This meets SIL 3.

5.1.8 User documentation

Safe-T-Products Pty Ltd creates product catalogs and a Safety Manual. The Safety Manual was found to contain the required information given the simplicity of the products. The Safety Manual references the FMEDA reports which are available and contain the required failure rates, failure modes, useful life, and suggested proof test information.

Items from IEC **61508-2, Table B.4** include operation and maintenance instructions, user friendliness, maintenance friendliness, project management, documentation, limited operation possibilities (Safe-T-Pull perform well-defined actions) and operation only by skilled operators (operators familiar with type of valve, although this is partly the responsibility of the end-user). This meets SIL 3.

5.2 Hardware Assessment

To evaluate the hardware design of the Safe-T-Pull Failure Modes, Effects, and Diagnostic Analysis's were performed by *exida*. These are documented in [R1].

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify failure modes and their effects, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration. An FMEDA (Failure Mode Effect and Diagnostic Analysis) is a probabilistic analysis done to predict failure rates for each failure mode, test coverage factors and useful life.

All failure rate analysis results and useful life limitations are listed in the FMEDA report [R1]. Tables in the FMEDA report list these failure rates for the Safe-T-Pull under a variety of applications. The failure rates listed are valid for the useful life of the device.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H. Therefore, the Safe-T-Pull can be classified as a 2_H device. When 2_H data is used for all of the devices in an element, the element meets the hardware architectural constraints up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) per Route 2_H.

The analysis shows that the design of the Safe-T-Pull can meet the hardware requirements of IEC 61508, SIL 3 for the Safe-T-Pull depending on the complete final element design. The Hardware Fault Tolerance and PFD_{avg} requirements of IEC 61508 must be verified for each specific design.

6 Terms and Definitions

Architectural Constraint	The SIL limit imposed by the combination of SFF and HFT for Route 1_H or by the HFT and Diagnostic Coverage (DC applies to Type B only) for Route 2_H
exida 2H criteria	A method of arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route with more detail and more requirements than specified in IEC 61508-2.
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
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.
Random Capability	The SIL limit imposed by the PFD_{avg} for each element.
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).
Systematic Capability	The SIL limit imposed by the capability of the products manufacturer.
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

7 Status of the Document

7.1 Liability

exida prepares reports based on methods advocated in International standards. *exida* accepts no liability whatsoever for the use of this report or for the correctness of the standards on which the general calculation methods are based.

7.2 Version History

Contract Number	Report Number	Revision Notes
Q24/03-114	SAF 24/03-114 R001 V1, R2	Updated D027b and the hardware versions in Section 3.1, JG, 7th November 2025
Q24/03-114	SAF 24/03-114 R001 V1, R1	Released, JG, 31st October 2025
Q24/03-114	SAF 24/03-114 R001 V0, R1	Draft for internal review, JG, 27th October 2025

Reviewer: Desmond Lee, exida, October 31, 2025

Status: Released, November 7, 2025

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Jack Gao

Jack Gao, CFSE, Senior Safety Engineer

Desmond Lee

Desmond Lee, CFSE, Senior Safety Engineer

END OF DOCUMENT