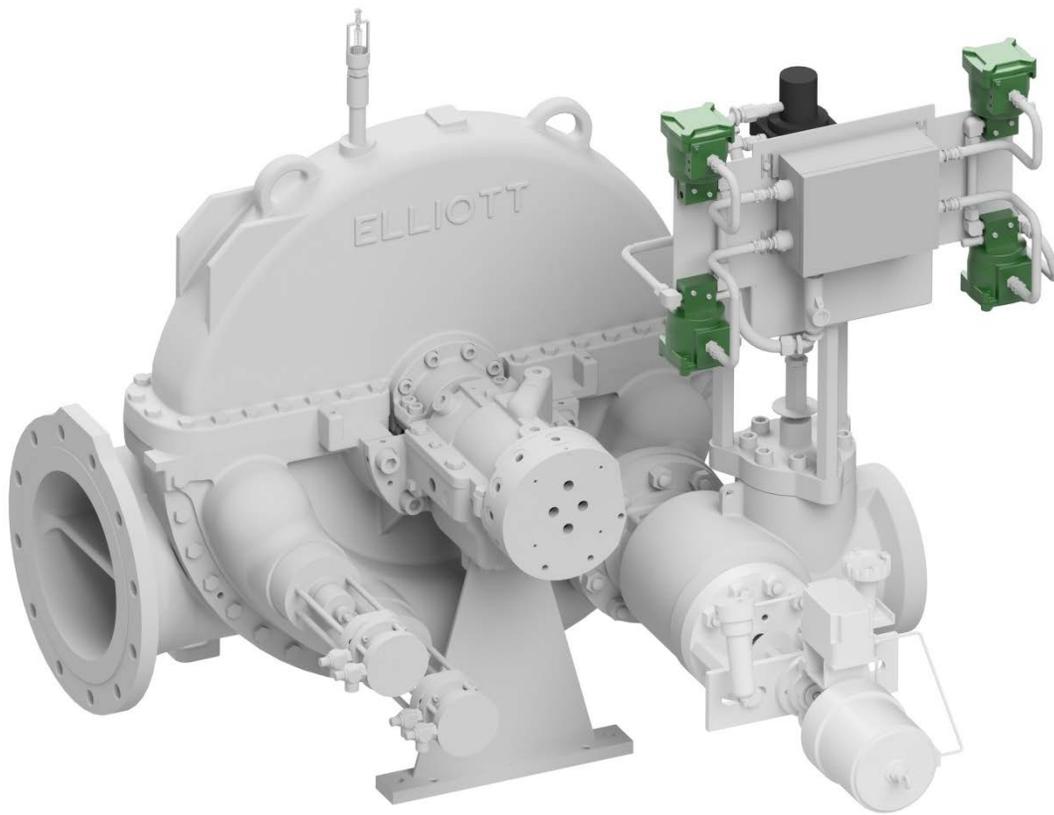


Direct Acting Pneumatic Trip with Partial Stroke

Safety Manual

In Accordance with IEC 61508

T H E W O R L D T U R N S T O E L L I O T T



C O M P R E S S O R S ■ T U R B I N E S ■ G L O B A L S E R V I C E

Elliott Company, 901 North Fourth Street, Jeannette, PA 15644
Document number 5046521

Rev No.	Issued By	Issued Date	Remarks
0	James Walsh	8/30/2017	Draft
0.1	James Walsh	9/6/2017	Initial Release
0.2	James Walsh	9/8/2017	
0.3	James Walsh	9/11/17	Update Elliott logo, minor formatting

Table of Contents

1	Introduction	3
1.1	Terms and Abbreviations.....	3
1.2	Acronyms	4
1.3	Product Support	4
1.4	Related Literature	4
1.5	Reference Standards	5
2	Product Description	5
2.1	Hardware Versions	6
3	Designing a SIF Using a Manufacturer Product.....	6
3.1	Safety Function	6
3.2	Environmental Limits	7
3.3	Application Limits & Restrictions	7
3.4	Design Verification.....	7
3.5	SIL Capability.....	7
3.5.1	Systematic Integrity	7
3.5.2	Random Integrity.....	7
3.5.3	Safety Parameters	8
3.6	Connection of the Direct Acting Pneumatic Trip System to the SIS Logic-Solver	8
3.7	General Requirements.....	8
4	Installation and Commissioning.....	9
4.1	Installation	9
5.1	Proof Test without Automatic Testing.....	9
5.2	Repair and Replacement.....	10
5.3	Useful Life	10
5.4	Manufacturer Notification.....	11

1 Introduction

This Safety Manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the Direct Acting Pneumatic Overspeed Trip System for Elliott YR steam turbines. The Direct Acting Pneumatic Trip System has the option of incorporating a Partial Stroke Actuation System.

This manual provides necessary user information and requirements for meeting the IEC 61508 and/or IEC 61511 functional safety standards.

A Failure Modes, Effects, and Diagnostics Analysis report for the Pneumatic Trip System is available upon request. See Section 1.3 for Product Support information.

1.1 Terms and Abbreviations

Safety	Freedom from unacceptable risk of harm.
Basic Safety	The equipment must be designed and manufactured such that it protects against risk of damage to persons by electrical shock and other hazards and against resulting fire and explosion. The protection must be effective under all conditions of the nominal operation and under single fault condition.
Functional Safety	The ability of a system to carry out the actions necessary to achieve or to maintain a defined safe state for the equipment / machinery / plant / apparatus under control of the system.
Safety Assessment	The investigation to arrive at a judgment - based on evidence - of the safety achieved by safety-related systems.
Element	Part of a subsystem comprising a single component or any group of components that performs one or more element safety functions.
Fail-Safe State	The State of the process when safety is achieved: De-energized on fault detection.
Fail Safe	Failure that causes the Pneumatic Trip System to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	Failure that does not permit the SIF to respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by automatic diagnostics, such as the Partial Valve Stroke Testing (PVST).
Fail Dangerous Detected	Failure that is dangerous, but is detected by automatic diagnostics, such as the Partial Valve Stroke Testing.
Fail No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
Low demand mode	Mode where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year and no greater than twice the proof test frequency.

1.2 Acronyms

EUC	Equipment Under Control
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HFT	Hardware Fault Tolerance
MOC	Management of Change - Specific procedures to follow for any work activities in compliance with government regulatory authorities or requirements of a standard.
MTTR	Mean Time to Repair
PFDavg	Average Probability of Failure on Demand
PFH	Probability of Failure per Hour
PVST	Partial Valve Stroke Testing
SFF	Safe Failure Fraction - The fraction of the overall failure rate of an element that results in either a safe fault or a diagnosed dangerous fault.
SIF	Safety Instrumented Function - A set of equipment intended to reduce the risk due to a specific hazard (a safety loop).
SIL	Safety Integrity Level - Discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems where Safety Integrity Level 4 is the highest level and Safety Integrity Level 1 is the lowest.
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. An SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).

1.3 Product Support

Product support can be obtained from:

Elliott Company
Industrial Products
901 North Fourth Street
Jeannette, PA 15644
724-527-2811
www.elliott-turbo.com

1.4 Related Literature

Hardware Documents:

- Direct Acting Pneumatic Trip System Installation, Operation, and Maintenance Instructions
- Direct Acting Pneumatic Trip System Installation with Partial Stroke Actuation, Operation, and Maintenance Instructions

Guidelines/References:

- Practical SIL Target Selection – Risk Analysis per the IEC 61511 Safety Lifecycle, ISBN 978-1-934977-03-3, exida
- Control System Safety Evaluation and Reliability, 3rd Edition, ISBN 978-1-934394-80-9, ISA
- Safety Instrumented Systems Verification, Practical Probabilistic Calculations, ISBN 1-55617-909-9, ISA

1.5 Reference Standards

Functional Safety

- IEC 61508: 2010 Functional safety of electrical/ electronic/ programmable electronic safety-related systems
- IEC 61511:2003 Functional Safety – Safety Instrumented Systems for the Process Industry Sector (or ISA 84.00.01 if it is more appropriate)

2 Product Description

The Direct Acting Pneumatic Trip System is an overspeed trip system for steam turbines with an integral trip valve. A single spring-loaded pneumatic cylinder acts directly on the trip valve. The cylinder is pressurized to open the valve and depressurized to close the valve. Two redundant and independently controlled solenoids control the actuation of the pneumatic cylinder and are de-energized to trip. A quick release valve is used to increase the speed of the cylinder discharge.

Two solenoid configurations are available:

1oo2 – The independently controlled solenoids are pneumatically configured to be in series. Only one solenoid needs to de-energize for the system to trip and close the trip valve.

2oo2 – The independently controlled solenoids are pneumatically configured to be in parallel. Both solenoids need to de-energize for the system to trip and close the trip valve.

The Partial Stroke Actuation operates independently by pressurizing the opposing side of the pneumatic cylinder in a controlled manner to exercise the valve without tripping the turbine. The Partial Stroke Actuation does not interfere with the overspeed trip function. The Partial Stroke function can be activated by a local selector switch, or it can be connected to a DCS for remote activation.

See Installation, Operation, and Maintenance Manual for additional setup and configuration details.

2.1 Hardware Versions

Table 1 – Pneumatic Trip Assemblies

Assembly	Elliott Drg Numbers	
	UL/FM	ATEX/IEC
Pneumatic Trip/ 1oo2	3011403	3011402
Pneumatic Trip w/ Partial stroke /1oo2	3010890	3006936
Trip w/ PT, 1oo2, 8" valve	3021748	3016609
Pneumatic Trip/ 2oo2	3021749	3021752
Pneumatic Trip w/ Partial stroke /2oo2	3021750	3021753
Trip w/ PT, 2oo2, 8" valve	3021751	3021754

Table 2 – Pneumatic Trip System Components

Device Description	Supplier	Model Number
Solenoid (S-1 & S-2)	ASCO	Series 32/8327G
Quick Exhaust Valve	Parker Pneumatic	OR50VB
Quick Exhaust Valve ³	Midland	2QEVSE122
Cylinder Actuator	ASCO	Numatics A-Series (Spring Return)
Emergency Trip Valve	Elliott Group	Series 676649-xx & 1055163

³ The Midland QEV replaces the Parker QEV for low temperature applications.

Table 3 – Pneumatic Trip System Partial Stoke Components

Device Description	Supplier	Model Number
Solenoid (S-3 & S-4)	ASCO	Series 32/8327G

3 Designing a SIF Using a Manufacturer Product

3.1 Safety Function

When internal dangerous faults are detected, the Direct Acting Pneumatic Trip System output moves to its fail-safe state.

When de-energized, the Direct Acting Pneumatic Trip System moves to its fail-safe position.

The Direct Acting Pneumatic Trip System, with or without Partial Stroke Actuation, is intended to be part of a SIF subsystem as defined per IEC 61508, and the achieved SIL level of the designed function must be verified by the designer.

The Direct Acting Pneumatic Trip System operates in low demand mode.

A proof test is required once per year (see section 5.1).

3.2 Environmental Limits

The designer of a SIF must check that the product is rated for use within the expected environmental limits. Refer to the Elliott Direct Acting Pneumatic Trip System Installation, Operation, and Maintenance (IO&M) Manual for environmental limits.

3.3 Application Limits & Restrictions

The Direct Acting Pneumatic Trip System is intended for use with Elliott YR steam turbines or steam turbines of similar design for an overspeed trip shut-off valve.

3.4 Design Verification

A detailed Failure Mode, Effects, and Diagnostics Analysis (FMEDA) report is available from Elliott Group. This report details all failure rates and failure modes as well as the expected lifetime. Assumptions made during the FMEDA are listed in the FMEDA report.

The achieved Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) design must be verified by the designer via a calculation of PFDavg or PFH, considering safety architecture, proof test interval, proof test effectiveness, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements. The exida exSILentia® tool is recommended for this purpose as it contains accurate models for the Direct Acting Pneumatic Trip System and its failure rates.

The failure rate data listed in the FMEDA report are only valid for the useful lifetime of Direct Acting Pneumatic Trip System. The failure rates will increase sometime after this time period. Reliability calculations based on the data listed in the FMEDA report for mission times beyond the lifetime may yield results that are too optimistic, i.e., the required Safety Integrity Level will not be achieved.

An appropriate MTTR shall be selected based on Elliott and/or plant operation and maintenance procedures.

3.5 SIL Capability

3.5.1 Systematic Integrity

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer. A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than the statement without “prior use” justification by the end user or diverse technology redundancy in the design.

3.5.2 Random Integrity

According to IEC 61508-2, the architectural constraints of an element must be determined. This can be done by following the 1H approach according to 7.4.4.2 of IEC 61508-2 or the 2H approach according to 7.4.4.3 of IEC 61508-2, or the approach according to IEC 61511:2016 which is based on 2H.

The 1H approach involves calculating the Safe Failure Fraction for the entire element.

The 2H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508.

The failure rate data used for this analysis meets the exida criteria for Route 2H which is more stringent than IEC 61508. Therefore, the Pneumatic Trip System meets the hardware architectural constraints for up to SIL 2 @ HFT=0 (or SIL 3 @ HFT=1) when the listed failure rates are used.

As an alternative to establishing architectural constraints via Route 1H or Route 2H, the user of the Pneumatic Trip System may establish the architectural constraints for an element using the Pneumatic Trip System per 11.4.5 of IEC 61511-1:2016. In which case the architectural constraints are SIL 2 @ HFT=0 (or SIL 3 @ HFT=1).

The architectural constraint type for the Pneumatic Trip System is A. The hardware fault tolerance of the device is 0. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL.

3.5.3 Safety Parameters

For detailed failure rate information, refer to the Failure Modes, Effects, and Diagnostic Analysis Report for the Direct Acting Pneumatic Trip System.

3.6 Connection of the Direct Acting Pneumatic Trip System to the SIS Logic-Solver

The Direct Acting Pneumatic Trip System is to be used in conjunction with a Woodward Protech GII overspeed trip control or equivalent, and the Woodward 1680-2030 or equivalent Sensor.

3.7 General Requirements

The system's response time shall be less than the process safety time. The Direct Acting Pneumatic Trip System will move to its safe state in less than 0.25 seconds under specified conditions.

All SIS components, including the Direct Acting Pneumatic Trip System, must be operational before process start-up.

User shall verify that the Direct Acting Pneumatic Trip System is suitable for use in safety applications by confirming the Direct Acting Pneumatic Trip System's nameplate is properly marked.

Personnel using and performing maintenance and testing on the Direct Acting Pneumatic Trip System shall be competent to do so. Results from the proof tests shall be recorded and reviewed periodically.

Steam quality is assumed to be consistent with Table 4. If the steam quality is less than specified in Table 4, then the reliability of the valve actuation upon demand is reduced due to potential scale build up. Steam quality less than specified will have a detrimental effect on the steam valve and valve stem in terms of useful life, and can effect operation upon demand. The Proof Test interval should be reduced when steam quality is not as specified.

Clean and dry compressed air, as per ANSI/ISA 7.0.01-1996 is required for reliable operation. The Direct Acting Pneumatic Trip is supplied with a filter/regulator. The filter regulator should be cleaned and maintained as need. Failure to provide clean, dry compressed air can have a detrimental effect on the pneumatic components of the system in terms of useful life, and can effect operation upon demand.

Table 4 – Steam Purity Limits

The steam purity limits for both start-up and continuous operation of steam turbines are defined in the following table, adapted from Table 9-2 of NEMA SM23-1991 with Chlorine comment added:

	CONTINUOUS	STARTUP
CONDUCTIVITY - MICROMHS/CM AT 25°C		
DRUM	0.3	1.0
ONCE THROUGH	0.2	0.5
SiO ₂ (PPB, MAX.)	20	50
FE (PPB, MAX.)	20	50
CU (PPB, MAX.)	3	10
NA + K (PPB, MAX.)		
UP TO 800 PSIG (5516 KPAG)	20	20
801 TO 1450 PSIG (5517 TO 9998 KPAG)	10	10
1451 TO 2400 PSIG (9999 TO 16548 KPAG)	5	5
OVER 2400 PSIG (OVER 16548 KPAG)	3	3
CHLORINE (PPB, MAX.)	10	10-30

Notes:

1. TDS (total dissolved solids) 100 ppm, max.
2. Other contaminants should be advised by Purchaser and reviewed by Elliott on an individual basis.

4 Installation and Commissioning

4.1 Installation

The Direct Acting Pneumatic Trip System must be installed per standard practices outlined in the Installation Manual. The environment must be checked to verify that environmental conditions do not exceed the ratings.

The Direct Acting Pneumatic Trip System location and placement must be accessible for physical and/or visual inspection and allow for manual proof testing.

4.2 Connections

Compressed air provided to the Direct Acting Pneumatic Trip System must be clean dry instrument quality air as per ANSI/ISA 7.0.01-1996.

5 Operation and Maintenance

5.1 Proof Test without Automatic Testing

The objective of proof testing is to detect failures within the Direct Acting Pneumatic Trip System that are not detected by any automatic diagnostics of the system. Of main concern are undetected failures that prevent the Safety Instrumented Function (SIF) from performing its intended function.

The frequency of proof testing, or proof test interval, is to be determined in reliability calculations for the safety instrumented functions for which the Direct Acting Pneumatic Trip System is applied. The proof tests must be performed at least as frequently as specified in the calculation in order to maintain the required safety integrity of the safety instrumented function.

The following proof test is recommended. The results of the proof test should be recorded, and any failures that are detected and that compromise functional safety should be reported to Elliott.

Table 5 – Recommended Proof Test

The suggested Proof Test consists of a full stroke of the Pneumatic Trip System

Step	Action
1	Disconnect driven load from turbine.
2	Send a signal to the Pneumatic Trip System to force the Actuator/Valve assembly to the Fail-Safe state and confirm that the Safe State was achieved (See Note 1).
3	Inspect the Direct Acting Pneumatic Trip System for any visible damage or contamination.
4	Record any failures in your company's SIF inspection database.
5	Close steam pressure isolation valve and allow steam pressure to bleed off.
6	Reconnect driven load and reset Pneumatic Trip Valve.

Note 1. For the test to be determined as effective, the turbine must reduce the speed to 500 RPM within 15 minutes.

This test will detect 95% without PVST and 93% with PVST of possible DU (Dangerous Undetected) failures in the Direct Acting Pneumatic Trip System.

The person(s) performing the proof test of a Direct Acting Pneumatic Trip System should be trained in SIS operations, including bypass procedures, valve maintenance and company Management of Change procedures.

It is recommended that a physical inspection (Step 3 from Table 5) be performed on a periodic basis with the time interval determined by plant conditions. A maximum inspection interval of one year is recommended.

5.2 Repair and Replacement

Repair procedures in the Direct Acting Pneumatic Trip System Installation, Operation, and Maintenance manual must be followed.

5.3 Useful Life

The useful life of the Direct Acting Pneumatic Trip System is three to five years.

5.4 Manufacturer Notification

Any failures that are detected and that compromise functional safety should be reported to Elliott customer service.

Elliott Company
Industrial Products Division
901 North Fourth Street
Jeannette, PA 15644
724-527-2811
www.elliott-turbo.com