ARTISAN®
TECHNOLOGY GROUP

Your **definitive** source for quality pre-owned equipment.

Artisan Technology Group
(217) 352-9330 | sales@artisantg.com | artisantg.com

Full-service, independent repair center
with experienced engineers and technicians on staff.

We buy your excess, underutilized, and idle equipment
along with credit for buybacks and trade-ins.

Custom engineering
so your equipment works exactly as you specify.

- Critical and expedited services
- In stock / Ready-to-ship
- Leasing / Rentals / Demos
- ITAR-certified secure asset solutions

Expert team | Trust guarantee | 100% satisfaction

All trademarks, brand names, and brands appearing herein are the property of their respective owners.

Find the *GE / Bently Nevada 3500/33-01* at our website: *Click HERE*

SIL Safety Manual

Bently Nevada* Asset Condition Monitoring



3500/32M_SIL and /33_SIL Relay

imagination at work

Document 115M5936
Rev. - (05/16)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

© 2016 Bently Nevada, Inc.
All rights reserved.

The information contained in this document is subject to change without notice.

*** Denotes a trademark of Bently Nevada, Inc., a wholly owned subsidiary of General Electric Company.**

Bently Nevada, Proximitor

The following are trademarks of the legal entities cited:

Printed in USA. Uncontrolled when transmitted electronically.

Contact Information

The following contact information is provided for those times when you cannot contact your local representative:

Mailing Address	1631 Bently Parkway South Minden, Nevada USA 89423 USA
Telephone	1.775.782.3611 1.800.227.5514
Fax	1.775.215.2873
Internet	www.GEmeasurement.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Additional Information

NOTE
This manual does not contain all the information required to operate and maintain the product. Refer to the following manuals for other required information.

3500 Monitoring System Installation and Maintenance Manual (part number 129766-01)

3500 Monitoring System Rack Configuration and Utilities Guide (part number 129777-01)

3500 Field Wiring Diagram Package (part number 130432-01)

3500 Monitoring System Computer Hardware and Software Manual (part number 128158-01)

3500/22M TDI Operation and Maintenance Manual (part number 161580-01)

3500/33 16-Channel Relay Module Manual (part number 162291-01)

3500/33 16-Channel Relay Module Data Sheet (part number 162301-01)

3500/32 and 3500/32M 4-Channel Relay Module Manual (part number 129771-01)

3500/32 and 3500/32M 4-Channel Relay Module Data Sheet (part number 141533-01)

3500 System: Functional Safety Data Sheet (part number 162242-01)

Product Disposal Statement

Customers and third parties, who are not member states of the European Union, who are in control of the product at the end of its life or at the end of its use, are solely responsible for the proper disposal of the product. No person, firm, corporation, association or agency that is in control of product shall dispose of it in a manner that is in violation of any applicable federal, state, local or international law. Bently Nevada, Inc. is not responsible for the disposal of the product at the end of its life or at the end of its use.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Contents

1. Purpose **1**
1.1 Abbreviations 1
1.2 IEC 61508-2 Annex D Requirements References 3
1.3 References 4
2. Hardware **5**
2.1 Rack Interface Monitor 6
2.2 System Power Supplies 6
2.3 Monitors 6
2.4 Relay Modules 7
2.4.1 3500/32M_SIL 4-Channel Relay Module 7
2.4.2 3500/33_SIL 16-Channel Relay Module 9
3. Constraints and SIL Requirements **12**
3.1 Skills Required to Commission and Maintain SIL Monitors 12
3.2 SIL 1 Requirements 12
3.2.1 Ordering requirements: 12
3.2.2 Hardware Requirements: 12
3.2.3 Software Requirements: 13
3.3 Recommendations 14
4. Functional Specifications **15**
4.1 Systematic Capability 15
4.2 Architectural/Random Constraints, Overview 15
4.2.1 Architectural/ Random Constraints, 1oo1 Configuration 15
4.2.2 Architectural/ Random Constraints, 1oo2 Configuration with Redundant Relay Paths 17
4.2.3 Architectural/Random Constraints, 1oo2 Configuration with Redundant Controller and Relay Paths 20
5. Failure Modes **23**
5.1 Failure modes of the 3500/32M_SIL and 3500/33_SIL Modules 23
5.2 Failure modes that are not detected by internal diagnostics 23

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

5.3 Failure modes that are detected by internal diagnostics 23
5.3.1 Diagnostic test interval 24
5.3.2 System Outputs 24
5.3.3 LED Fault Conditions 24
5.4 Failure modes of the diagnostics 24
5.5 External diagnostics 24
6. Periodic Proof Test 25
6.1 Choosing a Periodic Proof Test Interval 25
6.2 Periodic Proof test guide 25

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

1. Purpose

The purpose of this safety manual is to document all the information specifically related to the functional safety aspects of the 3500/32M_SIL and 3500/33_SIL Relay Modules. These modules are certified for use as a component in a functional safety system. This safety manual is required in order to enable the integration of the 3500/32M_SIL and 3500/33_SIL into a safety related system and to be in compliance with the requirement of IEC 61508-2 Annex D. This manual is focused on those details which specifically apply to the functional safety use case, and must be used in conjunction with the standard product documentation for these products.

1.1 Abbreviations

- ANSI/ISA – American National Standard Institute / International Society of Automation
- API - American Petroleum Institute
- ARM – armature
- β – common cause failure factor for undetectable dangerous faults
- β_D – common cause failure factor for detectable dangerous faults
- CE – Conformité Européenne (European Conformity)
- DC - diagnostic coverage
- FIT - failures in time
- FMEA - failure mode effect and analysis
- FS – functional safety
- HFT - hardware fault tolerance
- IEC – International Electro-technical Commission
- MRT - mean repair time
- MTBF - mean time between failure
- MTTF - mean time to failure
- MTTR - mean time to restoration
- NC - normally closed
- NDE - normally de-energized
- NE - normally energized
- NO - normally open
- PTC - proof test coverage
- PFD - probability of failure on demand
- SC - systematic coverage
- SFF - safe failure fraction
- SIF – safety instrumented function

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

- SIL – Safety Integrity Level
- TUV – Technischer Überwachungsverein (Technical Inspection)
- λ_s = safe failure rate
- λ_{sd} = safe detected failure rate
- λ_{su} = safe undetected failure rate.
- λ_d = dangerous failure rate.
- λ_{dd} = dangerous detected failure rate.
- λ_{du} = The dangerous undetected failure rate.
- λ- Common = common failures across all channels
- λ- Redundant = channel specific failures, which would take into account β's when used in redundant a 1oo2 configuration

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

1.2 IEC 61508-2 Annex D Requirements References

The table below provides a reference to which section of this document fulfills the 61508-2 Standard.

IEC 61508 requirements (part 2 annex D)	Reference
D2.1 a) a functional specification of the functions capable of being performed	Section 2.4.1 for 3500/32M_SIL Section 2.4.2 for 3500/33_SIL
D2.1 b) identification of the hardware and/or software configuration of the compliant item	Section 2.4.1 for 3500/32M_SIL Section 2.4.2 for 3500/33_SIL
D2.1 c) constraints on the use of the compliant item and/or assumptions on which analysis of the behavior or failure rates of the item are based	Section 3
D2.2 a) the failure modes of the compliant item due to random hardware failures, that result in a failure of the function and that are not detected by diagnostics internal to the compliant item	Section 5.2
D2.2 b) for every failure mode in a), an estimated failure rate	Section 4
D2.2 c) the failure modes of the compliant item due to random hardware failures, that result in a failure of the function and that are detected by diagnostics internal to the compliant item	Section 5.3
D2.2 d) the failure modes of the diagnostics, internal to the compliant item due to random hardware failures, that result in a failure of the diagnostics to detect failures of the function	Section 5.4
D2.2 e) for every failure mode in c), and d), the estimated failure rate	Failure rate for D.2.2 c) Section 4 Failure rate for D.2.2 d) Section 4
D2.2 f) for every failure mode in c) that is detected by diagnostics internal to the compliant item, the diagnostic test interval	Section 5.3
D2.2 g) for every failure mode in c) the outputs of the compliant item initiated by the internal diagnostics	Section 5.3
D2.2 h) any periodic proof test and/or maintenance requirements	Section 6
D2.2 i) for those failure modes, in respect of a specified function, that are capable of being detected by external diagnostics, sufficient information shall be provided to facilitate the development of an external diagnostics capability	Section 5.5
D2.2 j) the hardware fault tolerance	Section 4.2
D2.2 k) the classification as type A or type B of that part of the compliant item that provides the function (see 7.4.4.1.2 and 7.4.4.1.3)	Section 4
D.2.3 a) The systematic capability of the complaint item or that part of the element that provides the function	Section 4.1
D.2.3 b) Any instructions or constraints relating to the application of the compliant item, relevant to the function, that should be observed in order to prevent systematic failures of the compliant item	Section 3.2

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

1.3 References

IEC 61508, Parts 1 - 7:2010: Functional safety of electrical/electronic/programmable electronic safety-related systems

API Standard 670, 4th edition, Dec. 2000 Machinery Protection Systems

TÜV Certificate number 968/EZ 323.02/12 dated 2012-08-29

TÜV Certificate number 968/EZ 323.03/14 dated 2014-05-15

Schematic diagram 3500/33 & /32M Relay Control Module, Dwg. No: 149987

Schematic diagram 3500/33 16-Channel Relay IO Board, Dwg. No: 149993

Schematic diagram 3500/32 4-Channel Relay IO Board, Dwg. No: 125721

Statement of Compliance, BN26744C-18

System test procedures, No: 158792, Rev. NC, 28 Nov 1995

Copy of ISO 9001 certificate, issued by Det Norske Veritas, 11 Oct. 2001

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

2. Hardware

The 3500 system is a rack based machinery protection and condition monitoring system that provides information to protect and assess the mechanical condition of rotating and reciprocating machinery. The 3500 system continuously measures and monitors various protection and supervisory parameters and provides important information for early identification of machinery problems such as imbalance, misalignment, shaft crack, and bearing failures. The 3500 system is composed of monitors which accept inputs from transducers, condition the signals to provide various measurements, and compares the conditioned signals with user-programmable alarms. These alarm statuses are generated and broadcast onto the system alarming networks. Also in this system are relay modules that observe the alarming networks, and drive relays based on user programmable relay logic.

In SIL Certified systems, the safety function is supported by one or more SIL certified monitors which supply alarm and status information to one or more relay modules that consume the information to resolve machine trip logic and drive their relay output(s). These relay outputs are the monitoring system's safety output function. The relay outputs, are intended to be used in the greater Safety Instrumented Function (SIF) to bring the process to a safe state.

A basic 3500 system consists of a rack chassis, a backplane circuit board, redundant power supplies and a system interface module. This basic system supports a number of monitor/module slots where a variety of system monitors and modules can be installed in order to perform the machinery protection function required by the application.

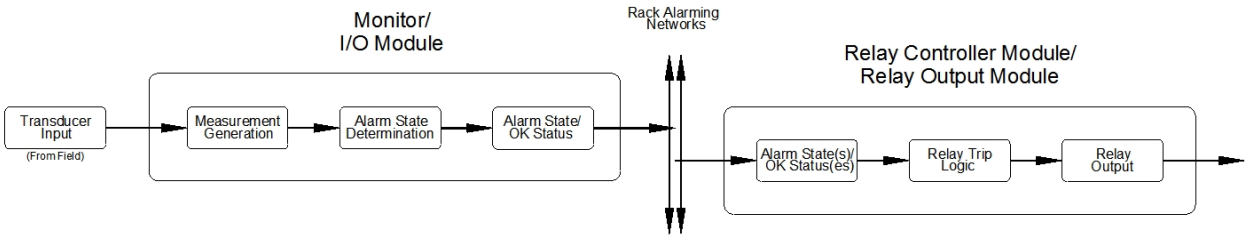


Figure 2 - 1: Basic 3500 Safety Element Architecture

A SIL certified 3500 system will be made up of one or more certified monitors interacting with one or more certified relay modules. Both the monitors and relay modules are designed specifically to function within the 3500 architecture and communicate with each other, and cannot be directly interfaced to external devices except as described above. The monitors and relay modules are

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

each certified independently to facilitate the flexibility of the system to be applied to a wide range of safety instrumented function applications.

2.1 Rack Interface Monitor

The 3500/22M Transient Data Interface Module (TDI) performs the interface functions to the 3500 system. It is used to configure the monitors and modules in the system as well as provide a Rack OK relay that provides an output of overall system health. Additionally, the module features a configuration control keyswitch that can be used as a physical mechanism to lock the configuration of the system to prevent unauthorized configuration changes. The TDI also includes password configuration protection measures that can be used as an additional software mechanism to prevent unauthorized configuration changes.

2.2 System Power Supplies

The 3500/15 System Power Supply accepts power from one of several possible power mains sources, and conditions the input into regulated internal rack power supplies that support internal power busses for the consumption of the monitors and modules installed in the system. Each 3500/15 Power Supply is fully capable of supporting all 3500 system functions. When two supplies are installed in a rack, the two supplies provide fully redundant system power mains capability which will automatically switch out the support of rack power load in the event that one supply or its power mains experiences a fault.

2.3 Monitors

The 3500 system monitors accept inputs from transducers in the field and condition the signal into measurements useful for machinery protection. The monitor constantly compares the measurements against configured alarm setpoints to generate alarm and channel OK statuses that are broadcast onto system alarming networks. The monitors are installed in any of the monitoring slots available in the system. Numerous SIL Certified monitors are available with the 3500 system, each providing different machinery protection capabilities. The different certified monitors can be combined and/or duplicated to achieve the required safety instrumented functionality.

A 3500 monitor is composed of a main card and an I/O module. The I/O module interfaces with the transducers producing the machinery-related signals, and condition the signals for the monitor main card. The main card is responsible for generating measurements from transducer information and generating the alarm and status messages.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

2.4 Relay Modules

The 3500 system relay modules consume the alarm and status information broadcast onto the system alarming networks and constantly compares these messages against the configured relay drive logic, to provide machinery protection trip output capability.

A 3500 relay module is a multi-channel module composed of a main card known as the relay controller and a relay output module. The relay controller interfaces with the 3500 system alarming network to process its configured relay drive logic and generate relay channel drive signals. The relay I/O module accepts the relay drive signals from the controller and contains the relay devices which provide the machinery trip contacts.

Each channel provides independent "Alarm Drive Logic" functionality which allows the user to develop complex logic strings using Boolean (AND and OR) logic elements. The logic acts on the alarm states (alert, danger) and validity states (Not OK) generated by monitors in the system which are available from the system alarming networks. Each channel's logic string drives its own relay output which is intended to be used as a machinery trip output.

The module's fundamental safety function is the relay output contact state change.

The module is configured using the 3500 Rack Configuration Software. All software configuration options and logic parameters available, are valid for use supporting the safety function without restriction. These parameters can be selected and arranged to suit the specific application requirements.

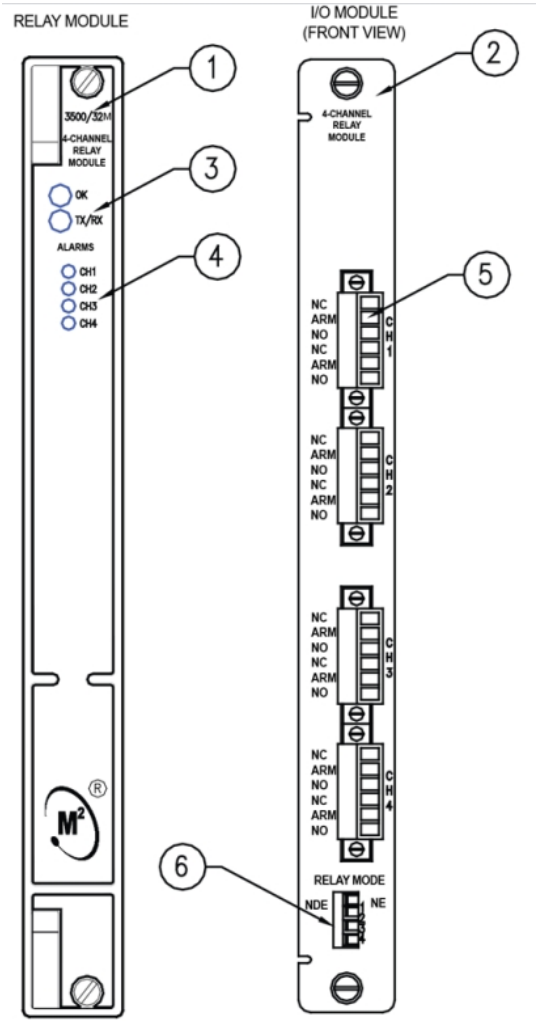
The Relay I/O contains three output contacts: Armature (ARM), Normally Open (NO), and Normally Closed (NC), which refer to the state of the contacts when the relay coils are de-energized. Also, each channel is independently configurable for Normally Energized (NE) or Normally De-energized (NDE) by means of DIP switches located on the back of the I/O module. The NE/NDE state refers to the state of the relay drive coil under normal (non-emergency) conditions.

2.4.1 3500/32M_SIL 4-Channel Relay Module

The 3500/32M_SIL is a four channel variant of the relay module which can be applied in either a one-out-of-one (1oo1), or a one-out-of-two (1oo2) architecture. A single path approach can be used to achieve a SIL 1 capable 1oo1 solution, while a dual path (redundant) approach can be used to achieve a SIL 2 capable, 1oo2 solution. Section 4.2 outlines the specific details that must be adhered to in order to correctly apply the relay module to achieve the two different SIL capable solutions.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Refer to the 3500/32 and 3500/32M Operation and Maintenance Manual (Part Number 129771-01) configuration section on how to properly configure the module using the 3500 Rack Configuration Software. For proper field wiring installation diagrams refer to the appropriate module section in of the 3500 System Field Wiring diagram package (Part Number 130432-01) for further information.



1. Relay module
2. I/O module
3. Status LEDs
4. Relay channel LEDs
5. Relay Contacts
6. Relay mode selection switch

Figure 2 - 2: 3500/32M_SIL Hardware Identification

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 2 - 1: SIL Certified 3500/32M_SIL Relay Modules

Part No.	Output Module (AXX)	Agency Approval Option (BXX)
3500/32M_SIL1 –A01 –BXX 3500/32M_SIL2 –A01 –BXX	01 - 4-Channel Relay Output Module	00 - None 01 - CSA/NRTL/C (Class 1, Div 2) 02 - ATEX.CSA (Class 1, Zone 2)

Table 2 - 2: 3500/32M_SIL Spare Part Numbers

Spare part number	Description	Hardware Revision	Firmware Revision
3500/32M_SIL1	3500/32M SIL1 4-Channel Relay Module	B	3.0
3500/32M_SIL2	3500/32M SIL2 4-Channel Relay Module	B	3.0
3500/32_SIL1-A01-BXX	3500/32 SIL1 4-Channel Relay I/O Module	AA	N/A
3500/32_SIL2-A01-BXX	3500/32 SIL2 4-Channel Relay I/O Module	AA	N/A

2.4.2 3500/33_SIL 16-Channel Relay Module

The 3500/33_SIL is a sixteen channel variant of the relay module which can be applied in either a one-out-of-one (1oo1), or a one-out-of-two (1oo2) architecture. A single path approach can be used to achieve a SIL 1 capable 1oo1 solution, while a dual path (redundant) approach can be used to achieve a SIL 2 capable, 1oo2 solution. Section 4.2 outlines the specific details that must be adhered to in order to correctly apply the relay module to achieve the two different SIL capable solutions.

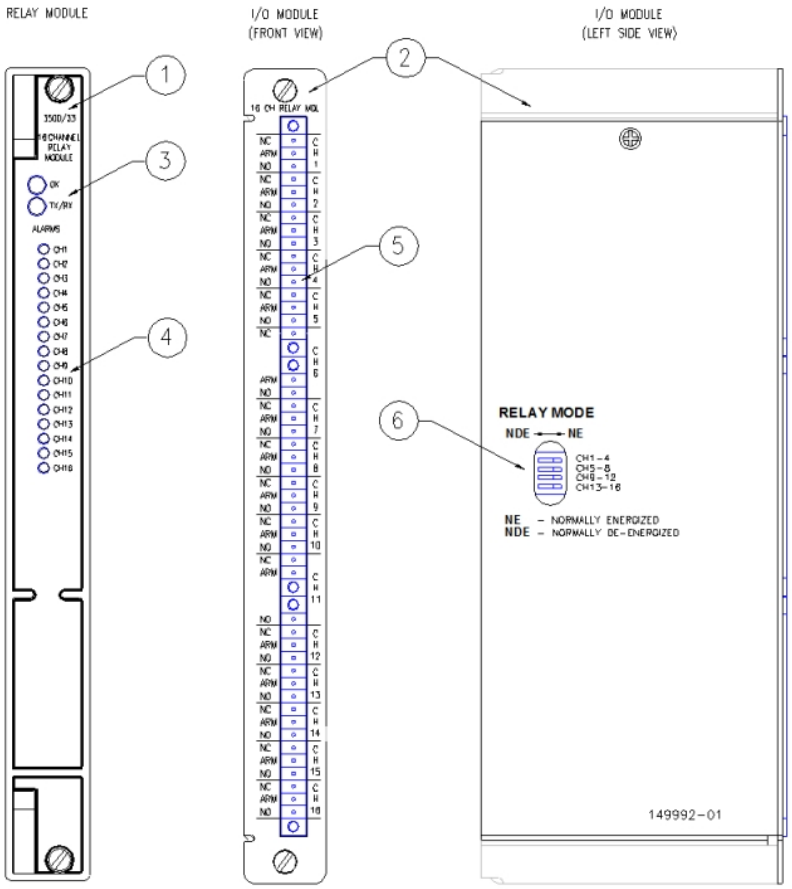
Refer to the 3500/33 Operation and Maintenance Manual (Part Number 162291-01) configuration section on how to properly configure the module using the 3500 Rack Configuration Software. For proper field wiring installation diagrams refer to the appropriate module section in the 3500 System Field Wiring diagram package (Part Number 130432-01).

The 3500/33_SIL relay module provides two options for the Relay I/O. It can be paired with either the standard I/O (3500/33-A01-BXX) or the “failsafe” I/O (3500/33-A02-BXX). The failsafe Relay I/O Module provides fail-safe behavior under a number of relay module fault conditions as described below:

- Removal of the main relay controller module from the front of the 3500 rack will cause all relays on its associated failsafe relay I/O module to go to the in alarm state.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

- When used with a failsafe Relay I/O module the microprocessor on the main relay controller module will drive the relays to the in-alarm state in the event that it detects a fatal error during its diagnostic checks or if a microprocessor execution exception occurs.



1. Relay module
2. I/O module
3. Status LEDs
4. Relay channel LEDs
5. Relay Contacts
6. Relay mode selection switch

Figure 2 - 3: 3500/33_SIL Hardware Identification

Table 2 - 3: SIL Certified 3500/33_SIL Relay Modules

Part No.	Output Module (AXX)	Agency Approval Option (BXX)
3500/33_SIL1 –AXX –BXX 3500/33_SIL2 –AXX –BXX	01 - 16-Channel Relay Output Module 02 - 16-Channel Failsafe Relay Output Module	00 - None 01 - CSA/NRTL/C (Class 1, Div 2) 02 - ATEX/CSA (Class 1, Zone 2)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 2 - 4: 3500/33_SIL Spare Part Numbers

Spare part number	Description	Hardware Revision	Firmware Revision
3500/33_SIL1	3500/33 SIL1 16-Channel Relay Module	E	3.0
3500/33_SIL2	3500/33 SIL2 16-Channel Relay Module	E	3.0
3500/33_SIL1-A01-BXX	3500/33 SIL1 16-Channel I/O Module	M	N/A
3500/33_SIL2-A01-BXX	3500/33 SIL1 16-Channel I/O Module	M	N/A
3500/33_SIL1-A02-BXX	3500/33 SIL1 16-Channel Failsafe I/O Module	D	N/A
3500/33_SIL2-A02-BXX	3500/33 SIL1 16-Channel Failsafe I/O Module	D	N/A

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

3. Constraints and SIL Requirements

The following are requirements and recommendations for the 3500/32M_SIL and 3500/33_SIL Functional Safety Certified products that must be considered in order for the product to be integrated into a safety-related system. These requirements and recommendations should be observed in order to achieve the necessary performance of the system and prevent systematic failures of the compliant product. For detailed information on conditions of use, refer to the certificates and test reports, contact Bently Nevada technical support, or visit http://www.GEmeasurement.com.

3.1 Skills Required to Commission and Maintain SIL Monitors

The 3500 system is highly configurable and flexible to accommodate a large number of machinery monitoring and protection applications. Due to this high level of configurability, only individuals that are familiar with the installation, operation and maintenance of the 3500 platform should configure, commission, and maintain the 3500 System.

3.2 SIL 1 Requirements

TÜV Rheinland of North America has determined that the 3500 Vibration Protection System 3500/32M_SIL and 3500/33_SIL Relay Modules meet the requirements for Safety Integrity Level 1 and 2 according to international standard IEC 61508. It can be used as a machinery protection system according to API 670 under the observance of the information in the Operating and Maintenance Manual and as described below.

3.2.1 Ordering requirements:

- When ordering a SIL certified 3500/32M module, the part number that is ordered must be 3500/32M_SIL1, or 3500/32M_SIL2.
- When ordering a SIL certified 3500/33 module, the part number that is ordered must be 3500/33_SIL1 or 3500/33_SIL2.
- Only those components contained within the TUV certified configurations can be used within a SIL. Refer to tables 2-1 and 2-3, or contact your local representative for details.

3.2.2 Hardware Requirements:

- The 3500/32M_SIL or 3500/33_SIL must be installed in a 3500 Rack that has a 3500/22 TDI Rack Interface Module and at least one SIL certified monitor card and I/O such as the

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

3500/40M_SIL or 3500/42M_SIL.

- The 3500 System that contains the 3500/32M_SIL or 3500/33_SIL modules must be supported by redundant 3500/15 Power Supplies.
- The system program keyswitch on the 3500/22M TDI must be set to the "RUN" position after the 3500/32M_SIL or 3500/33_SIL Relay Modules are configured, and the system commissioned.
- Removal of any component of the 3500 system that is part of the critical safety path will require a full proof test of the SIL system.
- The output relays must be configured for normally energized at the non-alarm condition (de-energize to trip).
- The wiring of the relay contacts must be such that the output circuit has continuity under non-alarm conditions, with the loss of circuit continuity indicating the unsafe state (the external circuit is de-energize to trip). Note that this is distinct and different from the relay drive coil normally energize/normally de-energized configuration.
- The system OK relay on the 3500/22M TDI must continuously monitored by an automated system to provide detection of system faults.
- The 3500/32M_SIL has a maximum contact rating of 2A and 30V.
- The 3500/33_SIL has a maximum contact rating of 5A and 30V.
- The 3500/32M_SIL and 3500/33_SIL are considered to be a system operating in low demand mode.

3.2.3 Software Requirements:

- The relay drive logic that supports the safety function, must accept only alarming parameters from SIL Certified Monitors.
- The monitoring card(s) used with the 3500/32M_SIL or 3500/33_SIL must be installed and configured per the applicable monitor's SIL safety manual.
- The system's configuration must be password protected.
- All relay module software configuration options and logic parameters available are valid for use supporting the safety function without restriction.
- After the relay module has had the configuration downloaded to it, the module configuration must be uploaded back to the host computer and the specified settings compared to verify the configuration was correctly received.
- The validation tests from the product manual must be performed. The behavior of the safety system in reference to particular failure conditions of the monitors (e.g. NOT OK status, no neuron communication) shall be evaluated at the system level.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

3.3 Recommendations

Bently Nevada, Inc. recommends having GE Bently Nevada Services inspect the components and system during validation/commissioning for proper installation, configuration and usage.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

4. Functional Specifications

Each channel provides independent “Alarm Drive Logic” functionality which allows the user to develop complex logic strings using Boolean (AND and OR) logic elements. The logic acts on the alarm states (alert, danger) and validity states (Not OK) generated by monitors in the system which are available from the system alarming networks. Each channel’s logic string drives its own relay output intended to be used as a machinery trip output.

Associated safety related elements such as Proximitors* and other 3500 Monitors (e.g. 3500/7X), have been independently assessed by the test institute and the results are documented under their individual test reports.

4.1 Systematic Capability

The 3500/32M_SIL and 3500/33_SIL techniques and measures to avoid and control systematic failures during the safety lifecycle phases were inspected by TÜV Rheinland, which resulted in a systematic capability of SIL 2 in accordance to IEC 61508: 2010, route 1S.

4.2 Architectural/Random Constraints, Overview

The 3500 SIL certified relay modules are available in four-channel and sixteen-channel variants, both of which are capable of being configured in 1oo1 or 1oo2 architectures to achieve a SIL 1 capable or a SIL 2 capable element, respectively. The following sections outline the architectural constraints for three different architecture configurations:

- 1oo1 - (SIL 1 capable)
- 1oo2 with redundant relay paths - (SIL 2 capable)
- 1oo2 with redundant controller and relay paths - (SIL 2 capable)

4.2.1 Architectural/ Random Constraints, 1oo1 Configuration

The calculation of the 3500/32M_SIL1 and 3500/33_SIL1 Relay Modules safety relevant parameters has shown that the requirements of SIL 1 to IEC 61508: 2010 are fulfilled in a 1oo1 configuration.

The component level FMEDA was carried out by TÜV Rheinland under consideration to the requirements of IEC 61508, parts 1-7:2010. Component failure rates were based on SN 29500, with a maximum ambient temperature of 65°C.

The safety related parameters are as follows:

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

- The relay channel must be configured for de-energize to trip.
- The safety-related circuit must be set up such that the opening of the relay contacts activates the safety function (de-energize circuit to trip) as shown in figure 4-1.
- Average probability of a dangerous failure on demand (PFD) < 10 E-1.
- The 3500/32M_SIL and 3500/33_SIL modules are considered to be a system operating in a low demand mode.
- The 3500/32M_SIL and 3500/33_SIL modules have a hardware safety integrity route of 1H.
- The 3500/32M_SIL and 3500/33_SIL modules have a systematic safety Integrity route of 1S.
- The rated life time of the 3500/32M_SIL and 3500/33_SIL modules is 10 years.
- The 3500/32M_SIL and 3500/32_SIL Relay Controller Module are Type B safety related elements with a Safe Failure Fraction (SFF) of 60% to <90%.
- The 3500/32M_SIL and 3500/32_SIL Relay Output Modules are Type A safety related elements with a Safe Failure Fraction (SFF) of <60%.
- The 3500/32M_SIL and 3500/33_SIL modules have a Hardware Fault Tolerance (HFT) of 0 when used in a 1oo1 configuration.
- The MTTR and MRT for the 3500/32M_SIL and 3500/33_SIL modules is 168 hours or 1 week**.

**MTTR and MRT were assigned as 168 hours for the purposes of generating the PFDAVE calculation. This figure may be adjusted to suit application specific considerations as long as the specific value is also used to adjust the PFD_{AVE} calculation specific to the safety-related installation.

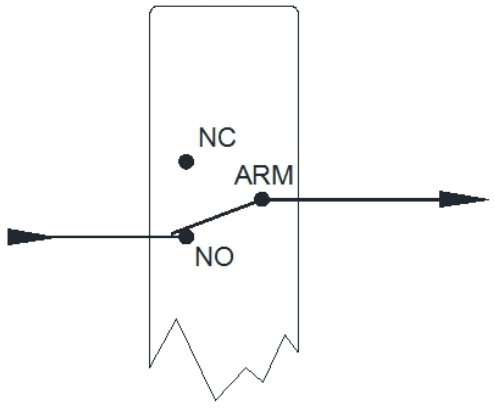


Figure 4 - 1: 1oo1 Relay Configuration

As shown in the safety block diagram, Figure 4-2, the 3500/32M and 3500/33 Relay Controller Modules are classified as Type B devices, and the 3500/32 and 3500/33 Relay Output Modules are

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Type A. The failure rates when used in the 1oo1 configuration are shown in Table 4-1. These failure rates are based on the 1oo1 safety block diagram in Figure 4-2.

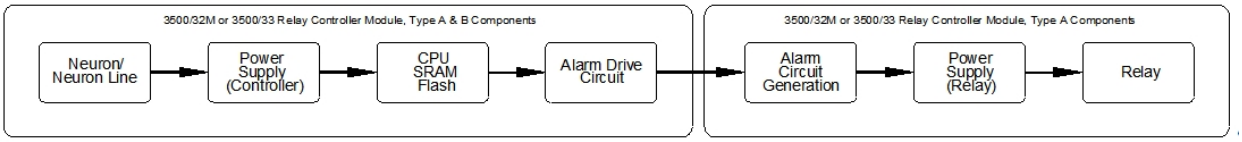


Figure 4 - 2: Safety block diagram, 1oo1 configuration

Table 4 - 1: 1oo1 Configuration Failure Rates

1oo1 Relay Failure Modes	Controller Module	Relay Module
Safe failure rate λ_s	451 FIT	585 FIT
Dangerous failure rate λ_d	397 FIT	568 FIT
Dangerous undetected failure rate λ_{du}	82 FIT	498 FIT

The following values were calculated by TÜV Rheinland of North America for the 3500/32M and 3500/33.

The review of the SFF (safe failure fraction) requirements in reference to IEC 61508, parts 1-7:2010 has shown that the Relay Controller Module achieves 60% to <90% and the Relay I/O Module when used in the 1oo1 configuration shown in Figure 4-2 is <60%.

$PFD_{AVG} = 2.7\ E^{-3}$, with the following assumptions:

- 1 year proof test interval
- MTTR = 168 hours

4.2.2 Architectural/ Random Constraints, 1oo2 Configuration with Redundant Relay Paths

The calculation of the 3500/32M_SIL2 and 3500/33_SIL2 Relay Modules safety relevant parameters has shown that the requirements of SIL 2 to 61508: 2010 are fulfilled in a redundant, 1oo2 configuration, as shown in Figure 4-3.

The component level FMEDA was carried out by TÜV Rheinland under consideration to the requirements of IEC 61508, parts 1-7:2010. Component failure rates were based from SN 29500, with a maximum temperature of 65°C.

The safety related parameters are as follows:

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

- The relay channel must be configured for de-energize to trip.
- The safety-related circuit must be set up such that the opening of the relay contacts activates the safety function (de-energize circuit to trip) as shown in figure 4-3.
- Average Probability of a dangerous failure on demand (PFD) < 10 E^{-2}.
- The 3500/32M_SIL and 3500/33_SIL modules are considered to be a system operating in a low demand mode.
- The 3500/32M_SIL and 3500/33_SIL modules have a hardware safety integrity route of 1H.
- The 3500/32M_SIL and 3500/33_SIL modules have a systematic safety Integrity route of 1S.
- The rated life time of the 3500/32M_SIL and 3500/33_SIL modules is 10 years.
- The 3500/32M_SIL and 3500/33_SIL Relay Controller Modules, and a Relay Output Modules are Type B safety related elements with a Safe Failure Fraction (SFF) of >90%, with a Hardware Fault Tolerance (HFT) of 0.
- The 3500/32M_SIL and 3500/33_SIL Relay Output Modules are Type A safety related elements with a Safe Failure Fraction (SFF) of <60%, with a Hardware Fault Tolerance (HFT) of 1 when used in a 1oo2 configuration. The signal path of an individual relay channel contained on the Relay Output Module is a Type A safety related element with a β_D =5%, and β =10%
- The MTTR and MRT for the 3500/32M_SIL and 3500/33_SIL modules is 168 hours or 1 week**.

**MTTR and MRT were assigned as 168 hours for the purposes of generating the PFD_{AVE} calculation. This figure may be adjusted to suit application specific considerations as long as the specific value is also used to adjust the PFD_{AVE} calculation specific to the safety-related installation.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

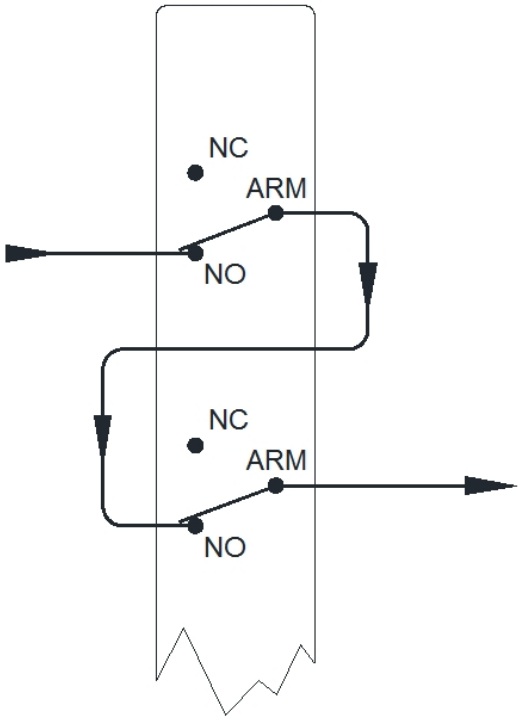


Figure 4 - 3: 1oo2 Relay Configuration

As shown in the 1oo2 safety block diagram, Figure 4-4, the 3500/32M and 3500/33 Relay Controller Modules are classified as Type B devices, and the 3500/32 and 3500/33 Relay Output Modules are Type A. The failure rates when used in the 1oo2 configuration are shown in Table 4-2. These failure rates are based on the 1oo2 safety block diagram in Figure 4-4.

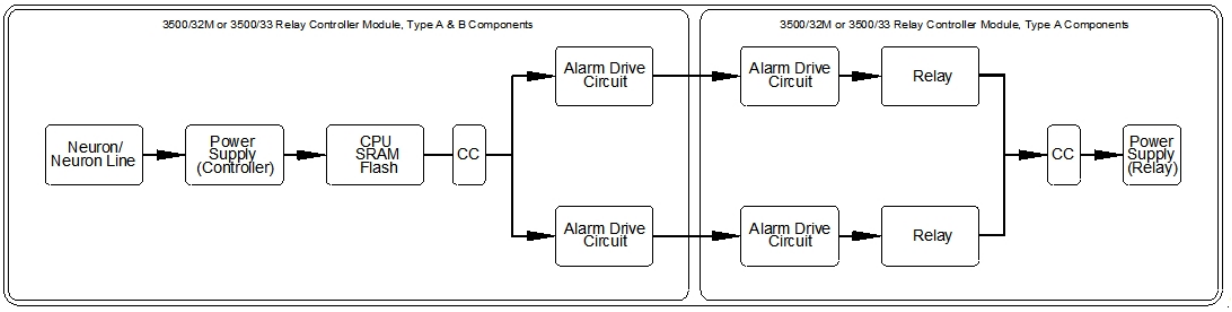


Figure 4 - 4: Safety block diagram, 1oo2 configuration - redundant relay paths

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 4 - 2: 1oo2 Configuration Failure Rates

/32M and /33 Internal 1oo2 Relay Failure Modes	Controller Module	Relay Module
Safe failure rate $\lambda_{s\ Common}$	411 FIT	81 FIT
Safe failure rate $\lambda_{s\ Redundant}$	40 FIT	503 FIT
Dangerous failure rate $\lambda_{d\ Common}$	356 FIT	60 FIT
Dangerous failure rate $\lambda_{d\ Redundant}$	41 FIT	509 FIT
Dangerous undetected failure rate $\lambda_{du\ Common}$	66 FIT	6 FIT
Dangerous undetected failure rate $\lambda_{du\ Redundant}$	16 FIT	492 FIT

The following values were calculated by TÜV Rheinland of North America for the 3500/32M and 3500/33.

$PFD_{AVG} = 6.38\ E^{-4}$, with the following assumptions:

- 1 year proof test interval
- MTTR = 168 hours
- βD =5%, and β =10%

4.2.3 Architectural/Random Constraints, 1oo2 Configuration with Redundant Controller and Relay Paths

The calculation of the 3500/32M_SIL2 and 3500/33_SIL2 Relay Modules safety relevant parameters has shown that the requirements of SIL 2 to 61508: 2010 are fulfilled in a redundant, 1oo2 configuration, as shown in Figure 4-5.

The component level FMEDA was carried out by TÜV Rheinland under consideration to the requirements of IEC 61508, parts 1-7:2010. Component failure rates were based from SN 29500, with a maximum temperature of 65°C.

The safety related parameters are as follows:

- The relay channel must be configured for de-energize to trip.
- The safety-related circuit must be set up such that the opening of the relay contacts activates the safety function (de-energize circuit to trip) as shown in figure 4-5.
- Average Probability of a dangerous failure on demand (PFD) < $10\ E^{-2}$.
- The 3500/32M_SIL and 3500/33_SIL modules are considered to be a system operating in a low demand mode.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

- The 3500/32M_SIL and 3500/33_SIL modules have a hardware safety integrity route of 1H.
- The 3500/32M_SIL and 3500/33_SIL modules have a systematic safety Integrity route of 1S.
- The rated life time of the 3500/32M_SIL and 3500/33_SIL modules is 10 years.
- The 3500/32M_SIL and 3500/33_SIL Relay Controller Modules are Type B safety related elements with a Safe Failure Fraction (SFF) of 60% to <90%. The Relay Controller Module has a β_D =5%, and β =10%.
- The 3500/32M_SIL and 3500/33_SIL Relay Output Modules are Type A safety related elements with a Safe Failure Fraction (SFF) of <60%. The Relay Output Module has a β_D =5%, and β =10%.
- The 3500/32M_SIL and 3500/33_SIL modules have a Hardware Fault Tolerance (HFT) of 1 when used in a 1oo2 configuration.
- The MTTR and MRT for the 3500/32M_SIL and 3500/33_SIL modules is 168 hours or 1 week**.

**MTTR and MRT were assigned as 168 hours for the purposes of generating the PFD_{AVE} calculation. This figure may be adjusted to suit application specific considerations as long as the specific value is also used to adjust the PFD_{AVE} calculation specific to the safety-related installation.

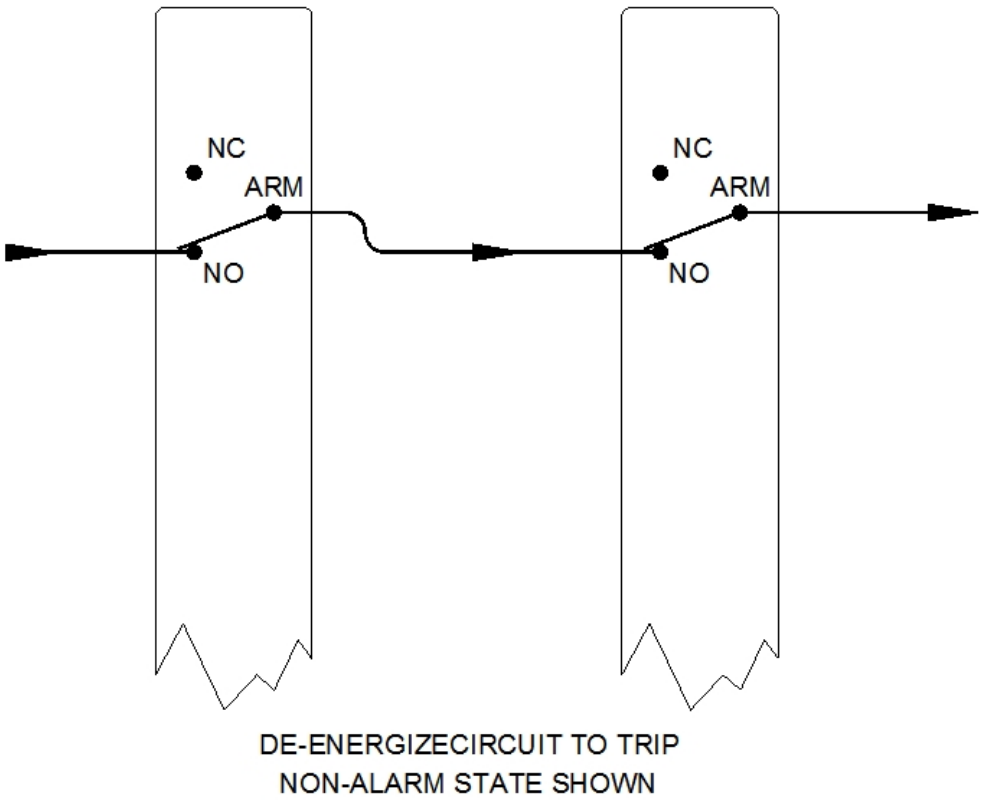


Figure 4 - 5: 1oo2 Relay Configuration

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

As shown in the 1oo2 safety block diagram, Figure 4-6, the 3500/32M and 3500/33 Relay Controller Modules are classified as Type B devices, and the 3500/32 and 3500/33 Relay Output Modules are Type A. The failure rates when used in the 1oo2 configuration are shown in Table 4-3. These failure rates are based on the 1oo2 safety block diagram in Figure 4-6.

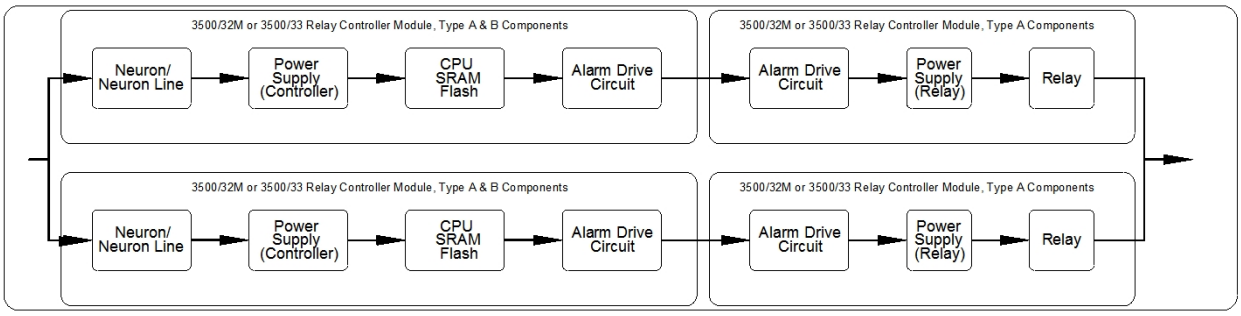


Figure 4 - 6: Safety block diagram, 1oo2 configuration - redundant controller and relay paths

Table 4 - 3: 1oo2 Configuration Failure Rates***

/32M and /33 Internal 1oo2 Relay Failure Modes	Controller Module	Relay Module
Safe failure rate $\lambda_{sCommon}$	451 FIT	585 FIT
Dangerous failure rate $\lambda_{d\ Common}$	397 FIT	568 FIT
Dangerous undetected failure rate $\lambda_{du\ Common}$	82 FIT	498 FIT

***λvalues listed are for a single path of the redundant system.

The following values were calculated by TÜV Rheinland of North America for the 3500/32M and 3500/33.

$PFD_{AVG} = 2.76\ E^{-4}$, with the following assumptions:

- 1 year proof test interval
- MTTR = 168 hours
- β_D =5%, and β =10%

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

5. Failure Modes

This section covers the failure modes of the 3500/32M_SIL and 3500/33_SIL relay modules and their internal diagnostics system. The estimated failure rate for each of these failure modes are given after each subsection of the corresponding failure mode.

The failure rates are driven by the following assumptions:

- Failure rates are based on Siemens standard SN 29500 and the outlined maximum temperature limits shown under the user manual of the relevant component.
- The failure rate is constant over time.
- The listed failure rates are in Failure in Time (FIT) = fit = [10-9 1/h].

5.1 Failure modes of the 3500/32M_SIL and 3500/33_SIL Modules

The specific failure modes of the 3500/32M_SIL and 3500/33_SIL modules are detailed in the FMEDA report, which is included in the SIL report which is available from GE Bently Nevada.

5.2 Failure modes that are not detected by internal diagnostics

When a failure mode occurs in a 3500/32M_SIL and 3500/33_SIL module that is not capable of being detected by the internal diagnostics of the module, the condition is not reported, there is no adjustment of the relay output states, and the Rack OK relay does not change state. This is the case whether the failure is safe or dangerous.

5.3 Failure modes that are detected by internal diagnostics

The 3500/32M_SIL and 3500/33_SIL modules feature internal diagnostics capabilities. When any failure is detected by the diagnostics, the module responds by annunciating the condition, and driving the Rack OK relay on the 3500/22M TDI to the “Not OK” state. In cases where a fault occurs that prevents the module from conducting its internal diagnostics and communicating with other system components, the 3500/22M TDI Module is capable of detecting the loss of communications, and responds by driving the Rack OK relay to the “Not OK” state.

When faults are detected by the module, the 3500/22M TDI records the failures in the 3500 System Event List. Refer to the "System Event List Messages" sections in the 3500/32M operation manual

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

(Part number 129771-01) or the 3500/33 operation manual (part number 162291-01) for a full list of failure codes that are detected by the internal diagnostic system.

5.3.1 Diagnostic test interval

The cycle interval between internal diagnostic checking is 1 hour maximum. In the vast majority of cases the interval is far less. The specified one hour interval is based on the fact that all of the diagnostics checks may take up to 1 hour to complete under worst-case conditions.

5.3.2 System Outputs

For any failure modes that are detected by the 3500/32M_SIL and 3500/33_SIL monitors by the internal diagnostic system, the Rack OK relay will drive to a NOT OK state.

5.3.3 LED Fault Conditions

Refer to the 3500/33 operation manual (Part number 162291-01) or the 3500/32M operation manual (part number 129771-01) for a list of the LED behavior under fault conditions.

5.4 Failure modes of the diagnostics

The failure modes of the 3500/32M_SIL and 3500/33_SIL diagnostic system are in the FMEDA report, which is included in the SIL report which is available from GE Bently Nevada.

5.5 External diagnostics

The 3500/32M_SIL and 3500/33_SIL are designed to be used in a 3500 system that includes at least one SIL certified monitor installed and used in conjunction with the SIL certified relay module (s). As described in sections 5.2 and 5.3, in addition to providing safety relay output functionality to the safety-related system, the 3500/22M TDI Module also provides a measure of external diagnostic capability to the module in the event that the monitor is rendered unable to communicate to the other system components. This external diagnostic functionality is established by simply installing the relay module in a properly constructed SIL 3500 system .

The 3500 system supporting the SIL certified monitor must have a 3500/22M TDI module installed. The Rack interface monitor performs diagnostics on all the monitors and I/O's installed in the Rack which are separate from the individual monitor internal diagnostics. When the Rack Interface Monitor senses a failure mode of one of the installed monitors, it changes the Rack OK relay to the Not OK state. Refer to the FMEDA report, which is available from GE Bently Nevada under the SIL Report, for all failure modes that drive the Rack OK Relay.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

6. Periodic Proof Test

The circuit boards and components inside 3500 modules cannot be repaired in the field. 3500 rack maintenance consists of testing module channels to verify that they are operating correctly. Monitors and modules that are not operating correctly should be replaced with a spare.

When performed properly, you may install the 3500/32M or 3500/33 controller module into or remove the module from the rack while power is applied to the rack, except when the rack is in a hazardous area. A hazardous area is defined by document BS EN 60079-0:2012 as an area in which an explosive atmosphere is present, or may be expected to be present, in quantities such as to require special precautions for the construction, installation and use of electrical apparatus. Refer to the Rack Installation and Maintenance Manual (part number 129766-01) for the proper procedure.

6.1 Choosing a Periodic Proof Test Interval

The proof test coverage provided by the internal diagnostic functionality of the 3500/32M_SIL and 3500/33_SIL monitors is 93%. Those dangerous failures that fall outside of the monitor's diagnostic capability are considered dangerous undetected failures which must be detected as part of periodic proof test activities.

GE Bently Nevada Recommends a periodic proof test interval of 1 year but by using the PFD_{AVE} equation from 61508-6 that is appropriate for the specific safety-related system, the effect on the PFD_{AVE} value can be determined for longer or shorter periodic proof test intervals.

6.2 Periodic Proof test guide

The test setup for verifying a Relay Module involves making connections to the monitor channels involved in the relay drive logic in order to simulate the monitor inputs. The inputs will be adjusted to exercise the SIF's relay logic, and verify that each of the relay contacts on the Relay Output Module are performing as intended. Note that if redundant relays are used, as shown in Figure 4-3 or 4-5, it is important to verify both sets of contacts. Reference the individual operation and maintenance manuals for each monitor used in the SIF's relay drive logic for the monitor-specific verification details.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group is an independent supplier of quality pre-owned equipment

Gold-standard solutions

Extend the life of your critical industrial, commercial, and military systems with our superior service and support.

We buy equipment

Planning to upgrade your current equipment? Have surplus equipment taking up shelf space? We'll give it a new home.

Learn more!

Visit us at **artisantg.com** for more info on price quotes, drivers, technical specifications, manuals, and documentation.

Artisan Scientific Corporation dba Artisan Technology Group is not an affiliate, representative, or authorized distributor for any manufacturer listed herein.

We're here to make your life easier. How can we help you today?

(217) 352-9330 | sales@artisantg.com | artisantg.com

ARTISAN® TECHNOLOGY GROUP