AADvance Controller

Catalog Numbers T9100, T9110, T9300, T9310, T9401/2, T9431/2, T9451, T9481/2

Allen-Bradley
by ROCKWELL AUTOMATION

Safety Manual

Original Instructions

Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

WARNING: Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.

ATTENTION: Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.

IMPORTANT Identifies information that is critical for successful application and understanding of the product.

Labels may also be on or inside the equipment to provide specific precautions.

SHOCK HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.

BURN HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.

ARC FLASH HAZARD: Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

About This Publication

This technical manual defines how to safely apply AADvance® controllers for a Safety Instrumented Function. It sets out standards (which are mandatory) and makes recommendations to make sure that installations satisfy and maintain their required safety integrity level.

In no event will Rockwell Automation be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment. The examples given in this manual are included solely for illustrative purposes. Because of the many variables and requirements related to any particular installation, Rockwell Automation does not assume responsibility or reliability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, with respect to use of information, circuits, equipment, or software described in this manual.

All trademarks are acknowledged.

Disclaimer

It is not intended that the information in this publication covers every possible detail about the construction, operation, or maintenance of a control system installation. You should also refer to your own local (or supplied) system safety manual, installation and operator/maintenance manuals.

Revision And Updating Policy

This document is based on information available at the time of its publication. The document contents are subject to change from time to time. The latest versions of the manuals are available at the Rockwell Automation Literature Library under "Product Information" information "Critical Process Control & Safety Systems".

Rockwell Automation Support

Any required support can be accessed through the Rockwell Automation Support Website at rok.auto/support.

Registration for Automatic Product Safety Advisories and Product Notices from Rockwell Automation, which are available by email, is obtained by using the Technical Support Center link (available on the above web-page) and signing in with either a TechConnect Account or free Rockwell Automation Member Account. Account holders can subscribe to important product updates, including Product Safety Advisories and Product Notices.

All repair actions for AADvance products are tracked against a SAP ticket number and customers can request a Root Cause Fault Analysis (RCFA) report.

Downloads

The product compatibility and download center is rok.auto/pcdc.

Select the Find Downloads option under Download.

In the Product Search field enter "AADvance" and the AADvance option is displayed.

Double click on the AADvance option and the latest version is shown.

Select the latest version and download the latest version.

AADvance Release

This technical manual applies to AADvance system release 1.41 and these software:

- AADvance® Workbench software version 1.4
- AADvance Workbench software version 2.1
- AADvance®-Trusted® SIS Workstation software version 1.2

NOTE AADvance system release 1.41 identifies the product family release. Each hardware, firmware and software component has its own version within this family release and the details of those versions can be found in the **AADvance System Requirements for version 1.41** in the PCDC Release Notes, which can be accessed from the Product Compatibility and Download Center at rok.auto/pcdc.

Latest Product Information

For the latest information about this product review the Product Notifications and Technical Notes issued by technical support. Product Notifications and product support are available at the Rockwell Automation Support Center at rok.auto/knowledgebase.

At the Search Knowledgebase tab select the option "By Product" then scroll down and select the ICS Triplex® product AADvance.

Some of the Answer ID's in the Knowledge Base require a TechConnect℠ Support Contract. For more information about TechConnect Support Contract Access Level and Features, click this link: Knowledgebase Document ID: IP622 - TechConnect Support Contract - Access Level & Features.

This will get you to the login page where you must enter your login details.

IMPORTANT A login is required to access the link. If you do not have an account then you can create one using the "Sign Up" link at the top right of the web page.

Purpose Of This Manual

This technical manual defines how to safely apply AADvance controllers for a Safety Instrument Function. It sets out standards (which are mandatory) and makes recommendations to verify that installations meet their required safety integrity level. To do this, it addresses how such installations are designed, built, tested, installed and commissioned, operated, maintained and decommissioned. It defines the requirements to be met during the life-cycle stages of safety-related systems design and commissioning so the safety objectives of the system are achieved during operation.

There are requirements for quality systems, documentation and competency in this technical manual; these are additional requirements for an operating company's or integrator's quality systems, procedures and practices.

Who Should Use Manual

⚠ **WARNING:** This manual is intended primarily for System Integrators. The information contained in this manual is intended to be used in conjunction with (and not as a substitute for) expertise and experience in safety-related systems. In particular, it is expected that the reader has a thorough understanding of the intended application and safety system principles and can understand the generic terms used within this manual and the terminology specific to the integrator's or project's application area.

⚠ **WARNING:** The System Integrator remains responsible for the generation of procedures and practices applicable to its business, and shall ensure that these are in accordance with the requirements defined herein. The application of such procedures and practices is also the responsibility of the system integrator, and these are mandatory for systems used for SIL 3 applications.

Environmental Compliance

Rockwell Automation maintains current product environmental information on its website at rok.auto/pec.

Download Firmware and Associated Files

Download firmware and associated files (such as OPC and DTM), and access product release notes from the Product Compatibility and Download Center at rok.auto/pcdc.

Summary of Changes

This publication contains the following new or updated information. This list includes substantive updates only and is not intended to reflect all changes.

New or enhanced features

This table contains a list of topics changed in this version, the reason for the change, and a link to the topic that contains the changed information.

Subject	Reason
AADvance Release on page 4	Updated AADvance system release and software information.
AADvance Features on page 15	Added Black Channel I/O bus.
Reference Documents on page 17	Changed ANSI ISA 84.00.01:2004 (IEC 61511-2 Mod) to ANSI/ISA 61511-1:2018.
Compiler Verification Tool Safety Requirement on page 78	Updated Attention table.

Additional Resources

These documents contain additional information concerning related products from Rockwell Automation.

Resource	Description
AADvance Controller System Build Manual, ICSTT-RM448	This technical manual describes how to assemble a system, switch on and validate the operation of your system.
AADvance Controller Configuration Guide Workbench 1.x, ICSTT-RM405	This software technical manual defines how to configure an AADvance controller using the AADvance Workbench software version 1.x to satisfy your system operation and application requirements.
AADvance Controller Configuration Guide Workbench 2.x, ICSTT-RM458	This software technical manual defines how to configure an AADvance controller using the AADvance Workbench software version 2.x to satisfy your system operation and application requirements.
AADvance-Trusted SIS Workstation Software User Guide, ICSTT-UM002	This publication provides how-to instructions for AADvance-Trusted SIS Workstation software configuration and use.
AADvance Controller OPC Portal Server User Manual, ICSTT-RM407	This manual describes how to install, configure and use the OPC Server for an AADvance Controller.
AADvance Controller PFH and PFDavg Data, ICSTT-RM449	This document contains the PFH and PFD_{avg} Data for the AADvance Controller. It includes examples on how to calculate the final figures for different controller configurations.
AADvance Controller Solutions Handbook, ICSTT-RM447	This technical manual describes the features, performance and functionality of the AADvance controller and systems. It provides guidance on product selection to satisfy your application requirements.
AADvance Controller Troubleshooting and Maintenance Manual, ICSTT-RM406	This technical manual describes how to maintain, troubleshoot and repair an AADvance Controller.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, rok.auto/certifications.	Provides declarations of conformity, certificates, and other certification details.

You can view or download publications at rok.auto/literature.

Chapter 1

Introduction

Chapter 2

Functional Safety Management

Chapter 3

AADvance System Architectures

Chapter 4

AADvance Functional Safety System Implementation

Chapter 5

Checklists

Introduction

This chapter provides an introduction to the AADvance® Safety Manual and to the AADvance system.

Verification of the Safety Manual

The AADvance system and the user Safety Manual are certified by an independent certification body to meet the requirements of IEC 61508 SIL 3.

Competency

The achievement of functional safety requires the implementation of the safety lifecycle whilst ensuring that persons who are responsible for any safety lifecycle activities meet the required competency levels in functional safety.

All persons involved in any safety lifecycle activity, including management activities, shall have the appropriate training, technical knowledge, experience and qualifications relevant to the specific duties they have to perform. The suitability of persons for their designated safety lifecycle activities shall be based on the specific competency factors relevant to the system application and shall be defined and recorded for each individual.

The following competence factors should be addressed when assessing and justifying the competency level of persons to carry out their duties:

- Engineering experience appropriate to the application area
- Engineering experience appropriate to the technology
- Functional safety engineering experience appropriate to the technology
- Knowledge of the legal and safety regulatory framework
- The consequences of failure of the safety-related system
- The safety requirements class of the safety-related systems
- The novelty of the design, design procedures or application
- Previous experience and its relevance to the specific duties to be performed and the technology being employed

In all of the above, the higher risk will require increased rigor with the specification and assessment of the competence.

Terminology

Vocabulary and Conventions

The terms **certification** and **certified** are used widely within this Manual, these terms refer principally to the functional safety certification of the AADvance system to IEC 61508 SIL 3 and other relevant standards.

This Manual contains rules and recommendations:

- **Rules** are mandatory and shall be followed if the resulting application is to be compliant with IEC 61508 up to and including SIL 3. These are identified by the term 'shall'.
- **Recommendations** are not mandatory, but if they are not followed, extra safety precautions shall be taken in order to certify the system. Recommendations are identified by the term '**it is highly recommended**'.

Process Safety Time

The generally accepted understanding of process safety time is the period a dangerous condition can exist in the process before a hazardous event occurs without a safeguard. This process safety time is used to determine the response time for the SIF implemented in the SIS.

Use the Process Safety Time configuration parameter in AADvance® Workbench software or AADvance®-Trusted® SIS Workstation software to:

- Enforce the safe state when a dangerous failure is detected.
- Verify that the Process PST is not exceeded.

This configuration parameter only applies to the logic solver portion of the process safety time, so its value must be configured taking into account both the sensor and final element response times.

Fault Tolerance in Safety Applications

For safety applications you shall define how the control system will respond in the presence of faults. Fail Safe configurations are designed to enforce a 'safe state' when dangerous faults are detected.

Fault tolerant configurations are designed to allow continued operation of the process without any loss of Safety Integrity when a dangerous fault is detected (as long as the fault is repaired within the MTTR).

Internal diagnostics combined with redundancy provide the fault tolerance capability. The AADvance system diagnostics will detect hidden faults so that users can repair the system within the MTTR (used for the PFD calculations) and maintain the SIF's integrity level.

The AADvance Controller

The AADvance Controller is specifically designed for functional safety and critical control applications, it provides a flexible solution for smaller scale requirements. The system can be used for safety implemented functions as well as applications that are non-safety but still critical to a business process. This controller offers you the ability to create a cost-effective system including but not limited to any of the following applications:

- critical process control
- fire and gas protection systems
- rotating machinery control systems
- burner management

- boiler and furnace control
- distributed process monitoring and control.

The AADvance Controller is a logic solver and I/O processing device that contains processor modules, I/O modules and field termination assemblies that can easily be assembled and configured. Build a system from one or more controllers, a combination of I/O modules, power sources, communications networks and application software. The type of applications to use depends on the configuration of the system.

An AADvance Controller is particularly well suited to emergency shut down and fire and gas detection protection applications by providing a system solution with integrated and distributed fault tolerance. It is designed and validated to international standards and is certified by an independent certifying body for functional safety control installations.

The benefits of the AADvance Controller are its performance and flexibility. Designed to IEC 61508 (Type B), it has the following attributes:

- up to and including SIL 3 application capability
- The product has met systematic capability requirements for SIL 3 (SC 3).
- can be configured for de-energize to trip (DTT) and energize to action (ETA)
- can cope with high and low demand, mixed SIL rated applications.

The number of modules required are summarized in the table below:

Table 1 - Table summarizing module configuration for SIL compliance

Application Type	Input	Processor	Output
SIL 2, Low Demand, DTT	1	2	1
SIL 2, High Demand, DTT	1	2	1
SIL 3, Low Demand, DTT	1	2	1
SIL 3, High Demand, DTT	1	2	1
SIL 2, Low Demand, ETA	1	2	1
SIL 2, High Demand, ETA	2	2	2
SIL 3, Low Demand, ETA	1	2	2
SIL 3, High Demand, ETA	2	2	2

1. Fault tolerance may be implemented by configuring dual or triplicated modules for each module type.

NOTE There is no provision for configuring triplicated output modules

2. AADvance digital output modules contain an element of redundancy and are therefore tolerant to some faults. Within each output module channel there are a pair of series switches that enable redundant behavior for de-energize to trip applications (output SIL 3); they remain non-redundant for execution of energize to action (output SIL 2).
3. Modules reporting dangerous failures must be replaced within the Mean Time To Repair (MTTR) assumed by the Probability of Failure on Demand (PFD). The application must be designed to shut down the safety instrumented functions if a module reporting a dangerous failure has not been replaced within the MTTR assumed by the PFD, unless compensating measures are defined in the Safety Requirements Specification (SRS) and documented in operating procedures.

All of the configurations are readily achieved by combining modules and assemblies without using special cables or interface units. System architectures are user configurable and can be changed without major system modifications. Processor and I/O redundancy is configurable so you can choose between fail safe and fault tolerant solutions. This scalability is user configurable, therefore, there is no change to the complexity of operations or programming if you choose to add redundant capacity to create a fault tolerant solution.

A controller is built from a range of compact plug-in modules that are straightforward to assemble into a system. They can be mounted onto DIN rails in a cabinet (see photograph) or directly mounted onto a wall in a control room. They do not require forced air cooling or special environmental control equipment. However, certain consideration to the cabinet type must be applied when used in hazardous environments.

A secure network communications protocol, developed by Rockwell Automation for the AADvance system, permits distributed control and safety using new or existing network infrastructure while ensuring the security and integrity of the data. Individual sensors and actuators can connect to a local controller, minimizing the lengths of dedicated field cabling. There is no need for a large central equipment room; administer the distributed system from one or more computers installed at different locations.

The AADvance system has comprehensive built-in diagnostics, while maintenance activities are straight forward operations which maximize system availability.

The AADvance controller is developed and built for IEC 61131 compliance and includes support for all five programming languages. Program access is secured by a removable "Program Enable" key. Simulation software lets you prove a new application before reprogramming and downloading, again maximizing system uptime.

AADvance Features

The AADvance system controls complex and often critical processes in real time — executing programs that accept external sensor signals, solving logic equations, performing calculations for continuous process control and generating external control signals. These user-defined application programs monitor and control real-world processes in the oil and gas, refining, rail transit, power generation and related industries across a wide range of control and safety applications. AADvance products have a useful lifetime of 20 years.

The main features of the AADvance system are as follows:

- Facilitates differing fault tolerant topologies — 1 out of 1 with diagnostics (1oo1D), 1 out of 2 with diagnostics (1oo2D) and 2 out of 3 with diagnostics (2oo3D)
- The Black Channel I/O bus facilitates the interconnection of mixed architectures consisting of both AADvance and AADvance Eurocard Technologies.
- Flexible modular construction using individual modules to build a system
- Operates as a stand-alone system or part of a larger distributed network
- Easily transformed from a simplex non-safety system to a fault tolerant safety related system
- IEC 61508 certified
- Scalable I/O module expansion without system interruption
- Supports secure SIL 3 rated 'Black Channel' external communication over Ethernet
- Supports industry standard protocols including MODBUS and HART
- Supports OPC

System Security

An AADvance system, with its computers and DCS interfaces, whether using Ethernet networks or Serial links is likely part of a larger corporate network which may expose the system to accidental or malicious infection, attack or less obvious security vulnerabilities. If appropriate (or defined in the SRS), a security risk assessment should be carried out and the appropriate level of risk mitigation applied.

The following general security steps should be used to verify that the system is secure:

- Network and computer security must set up when installing and setting up the system. As a minimum use the following security measures:
- AADvance system must not be connected to a network with open unsecured access to the Internet.
- A router firewall must be active on the computer, helping prevent access to the unused Ethernet ports on each communication interface.
- Anti-virus software must be installed and be kept updated.

IMPORTANT	Firewalls have been known to affect the operation of the AADvance Discover utility so it may be necessary to temporary disable the Firewall when using this tool.

- The computer must be password-protected.
- If using a laptop, keep the laptop locked when not in use.

- If the software uses a hardware license USB dongle, keep the USB dongle secure. The software will not run without the USB dongle.
- AADvance Workbench software or AADvance-Trusted SIS Workstation software projects must be password-protected by using the applicable software. You can also set a target password on the AADvance controller from the software.
- The controller running the application must be protected by using a Program Enable Key.

Communication Port Security

A network communications protocol suitable for safety systems, developed by Rockwell Automation for the AADvance system, permits distributed control and safety using new or existing network infrastructure while ensuring the integrity of the data. Individual sensors and actuators can connect to a local controller, minimizing the lengths of dedicated field cabling. There is no need for a large central equipment room; rather, the complete distributed system can be administered from one or more computers placed at convenient locations. AADvance has a Rockwell secure SIL 3 rated 'Black Channel' external communication over Ethernet.

The Ethernet transport layer ports (services) are supported by AADvance, some ports are always available others are only available when configured. When "always available" ports are not configured or unused they are open to unauthorized access.

The following transport layer ports (services) are supported by AADvance. Some ports are always available; others are only available when configured.

Table 2 - AADvance Communication Ports

Protocol	Port Number	Availability	Purpose
TCP	502	When configured	MODBUS Slave
TCP	1132	Always available	Application downloads, update, monitor, SoE, and so forth
TCP	10001- 10006	When configured (and the application is stopped)	Transparent Communications Interface (Serial Tunnelling)
TCP	44818	Always available	CIP™ Produce & Consume
TCP	55555	Always available	Telnet (diagnostic interface)
UDP	123	When configured	SNTP
UDP	1123,1124	Always available	SNCP bindings
UDP	2010	Always available	Discovery and configuration protocol (DCP, Rockwell Automation)
UDP	2222	When configured	CIP Produce & Consume IO
UDP	5000	When at least one P2P subnet is active on a controller	Trusted® peer-to-peer
UDP	44818	Always available	CIP Produce & Consume

When "always available", ports are not configured or unused, they are open to unauthorized access.

⚠ **WARNING:** Unused open ports that are not configured should be blocked, this can be done at the firewall settings. Refer to the appropriate AADvance Configuration Guide or the AADvance-Trusted SIS Workstation Software User Guide, publication ICSTT-UM002, for the instructions about blocking these ports.

WARNING: The telnet port is for diagnostics access and should only be used by Rockwell Technical Support.

Associated Documents

The following documents are associated with the safety requirements applicable to the AADvance system.

PFH and PFD_{avg} Data

The PFH and PFD_{avg} data is provided in a separate document - Publication No: ICSTT-RM449 "PFH and PFD_{avg} Data" for AADvance Controllers.

Table 3 - Reference Documents

Document	Title
IEC 61508:2010 Parts 1-7	Functional safety of electrical/electronic programmable safety-related systems
IEC 61511-1:2017 + A1:2017	Functional-safety: Safety instrumented systems for the process industry sector
ANSI/ISA 61511-1:2018	Functional Safety: Safety instrumented systems for the process industry sector.
EN 61131-2:2017	Programmable controllers – Part 2: Equipment requirements and tests
NFPA 72:2019	National fire alarm and signalling code
NFPA 85:2019	Boiler and combustion systems hazard code.
NFPA 86:2019	Standards for ovens and furnaces
EN 50156-1:2015	Electrical equipment for furnaces and ancillary equipment: Requirements for application design and installation
EN 54-2:1997, + AC:1999 + A1:2006	Fire alarm control panels
UL 508	Industrial control equipment

NOTE A good understanding of health and safety practices, functional safety principles is highly recommended; and the principles of these standards should be understood before generating procedures and practices to meet the requirements of this Safety Manual.

Controller Certification

Certification

AADvance is certified by an independent certifying body. Refer to the certificate for details of the standards included in the certification.

System Installation Environment

The installation environment can be a source of common cause failure so it is necessary that the installation assessment covers the environmental specification for the AADvance system and includes the following:

- the prevailing climatic conditions
- type of area, e.g. is it a hazardous or non-hazardous area
- location of power sources
- earthing and EMC conditions

In some customer installations parts of the system can be installed in differing locations; in these cases the assessment must include each location.

Power Sources and Heat Dissipation Calculations

It is highly recommended that module supply power and field loop power consumption calculations are done to find out the heat dissipation before designing a suitable enclosure and making a decision about the installation environment (see topic "System Design for Heat Dissipation").

Safety Related System Installation Process

For a Safety Related System the installation process must also be in line with the following:

⚠ **WARNING:** You must use the installation guidelines given in this manual and any installation and commissioning procedures that comply with applicable international or local codes and standards.

⚠ **CAUTION:** AADvance modules are suitable for use in Class I, Division 2, Groups A, B, C and D Hazardous locations or Non-hazardous locations only or equivalent.

⚠ **ATTENTION:** Pour les modules AADvance sont utilisables dans Class I, Division 2, A, B, C et D pour un environnement dangereux ou pour un environnement non dangereux ou équivalente

Environment Standards

The AADvance system has been investigated to United States National Standard (s) UL 508, 17th Edition and Canadian National Standard (s) C22.2 No 142, 1st Edition. The investigation covers the following modules and provides requirements for compliance to the standards for use in a non-hazardous and hazardous environments.

The AADvance controller has been investigated and approved by UL for use as Industrial Control Equipment in hazardous locations, Class I, Division 2, Groups A, B, C and D in North America.

The AADvance controller has been assessed for ATEX compliance. The UL Certification No. is DEMKO 11 ATEX 1129711X Rev 2; UL report number is 4786144521. The ATEX marking is Ex nA IIC T4 Gc.

Additionally the AADvance controller is approved under the IECEx certification scheme. The certificate number is IECEx UL 12.0032X

Installation Requirements for Non-Hazardous Environment

Investigation File Number E341697

Products Covered

The products investigated and approved:

Programmable Logic Controller Models:

- 9110 Processor Module
- 9401 Digital Input Module
- 9402 Digital Input Module, 16 Channel
- 9431 Analogue Input Module
- 9432 Analogue Input Module, 16 Channel
- 9451 Digital Output Module
- 9481 Analog Output Module
- 9482 Analogue Output Module, 8 Channel.

Listed Accessories for use with PLCs:

- 9100 Processor Backplane
- 9300 I/O Backplane
- 9801 Digital Input Termination Assembly, Simplex
- 9802 Digital Input Termination Assembly, Dual
- 9803 Digital Input Termination Assembly, TMR; 9831 Analogue input Termination Assembly, Simplex
- 9832, Analogue Input Termination Assembly, Dual
- 9833 Analogue Input Termination Assembly, TMR
- 9851 Digital Output Termination Assembly, Simplex and 9852 Digital Output Termination Assembly, Dual
- 9892 Digital Output Termination Assembly, Dual
- 9881 Analogue Output Termination Assembly, Simplex
- 9882 Analogue Output Termination Assembly, Dual.

Non-Hazardous Installation Requirements

Environmental

In a non-hazardous environment a system can be installed in an enclosure or on a support/wall; however, the enclosure or the area where it is installed must not be more than a Pollution Degree 2 or similar environment in accordance with IEC 60664-1:2007.

The surrounding air temperature ratings are:

- For the 9110 Processor module = 60 °C
- For all other I/O modules, base units and termination assemblies = 70 °C

NOTE For burner management applications, and to meet EN 298:2012, the AADvance controller must be fitted in an enclosure offering IP40 for indoor use and IP54 for outdoor use.

Pollution Degree Definition

For the purpose of evaluating creepage distances and clearances, the following four degrees of pollution in the micro-environment are established:

- Pollution Degree 1: No pollution or only dry pollution occurs. The pollution has no influence.
- Pollution Degree 2: Only non-conductive pollution occurs except that occasionally a temporary conductivity caused by condensation is to be expected.
- Pollution Degree 3: Conductive pollution occurs or dry non-conductive pollution occurs which becomes conductive due to condensation which is to be expected.
- Pollution Degree 4: Continuous conductivity occurs due to conductive dust, rain or other wet conditions.

Installation Requirements for Hazardous Environment

The AADvance controller has been investigated and approved by UL for use as Industrial Control Equipment in hazardous locations, Class I, Division 2, Groups A, B, C and D in North America.

The AADvance controller has been assessed for ATEX compliance. The UL Certification No. is DEMKO 11 ATEX 1129711X Rev 2; UL report number is 4786144521. The ATEX marking is Ex nA IIC T4 Gc.

Additionally the AADvance controller is approved under the IECEx certification scheme. The certificate number is IECEx UL 12.0032X.

Installation Requirements

To comply with the standards the following conditions must be applied to the installation:

⚠ **WARNING:** Special conditions for safe use

- Model 9110: The ambient temperature range is -25 °C to +60 °C (-13 °F to +140 °F).
- All other Models: The ambient temperature range is -25 °C to +70 °C (-13 °F to +158 °F).
- Subject devices are to be installed in an ATEX/IECEx Certified, IP54, tool accessible enclosure that has been evaluated to the requirements of EN 60079-0: 2012+A11:2013 and EN 60079-15:2010/IEC 60079-0 Ed 6 and IEC 60079-15 Ed 4. Enclosure is to be marked with the following: "Warning - Do not open when energized". After installation of subject devices into the enclosure, access to termination compartments must be dimensioned so that conductors can be readily connected. Grounding conductor should have a minimum cross sectional area of 3.31 mm^2.
- Subject devices are for use in an area of not more than pollution degree 2 in accordance with IEC 60664-1.
- Subject devices are to use conductors with a minimum conductor temperature rating of 85 °C.
- Subject devices are to be installed in the vertical orientation only.

AADvance meets the essential requirements of EN 60079-0:2012 + A11:2013 & EN 60079-15:2010 and IEC 60079-0 Ed 6 and IEC 60079-15 Ed 4.

File Number E251761

The AADvance controller investigation and approval is contained in the following file certifications:

- NRAG.E251761: Programmable Controllers for Use in Hazardous Locations Class I, Division 2, Groups A, B, C and D.

The products have been investigated using requirements contained in the following standards:

- ANSI/ISA 12.12.01-2013, Nonincendive Electrical Equipment for use in Class I and II, Division 2 and Class III, Division 1 and 2 Hazardous Locations.
- UL 508, Industrial Control Equipment, Seventeenth edition, with revisions through and including April 15, 2010.
- NRAG7.E251761: Programmable Controllers for Use in Hazardous Locations Certified for Canada; Class I, Division 2, Groups A, B, C and D.

The products have been investigated using requirements contained in the following standards:

- CSA C22.2 No 213-M1987, Nonincendive Control Equipment for Use in Class I, Division 2, Hazardous Locations.
- CSA C22.2 No 142-M1987, Process Control equipment, Edition 1 - Revision date 1990-09-01.

Products Covered

The products investigated and approved:

Programmable Logic Controllers Models:

- 9110 Processor Module
- 9401/2 Digital Input Module
- 9431/2 Analogue Input Module
- 9451 Digital output Module;
- 9482 Analogue Output Module.

Listed Accessories for use with PLCs:

- 9100 Processor Backplane
- 9300 I/O Backplane
- 9801 Digital Input Termination Assembly, Simplex
- 9802 Digital Input Termination Assembly, Dual
- 9803 Digital Input Termination Assembly, TMR
- 9831 Analogue input Termination Assembly, Simplex
- 9832, Analogue Input Termination Assembly, Dual
- 9833 Analogue Input Termination Assembly, TMR
- 9851 Digital Output Termination Assembly, Simplex.

Certifications for Safety System Applications in Hazardous Environments

ATEX Certificate

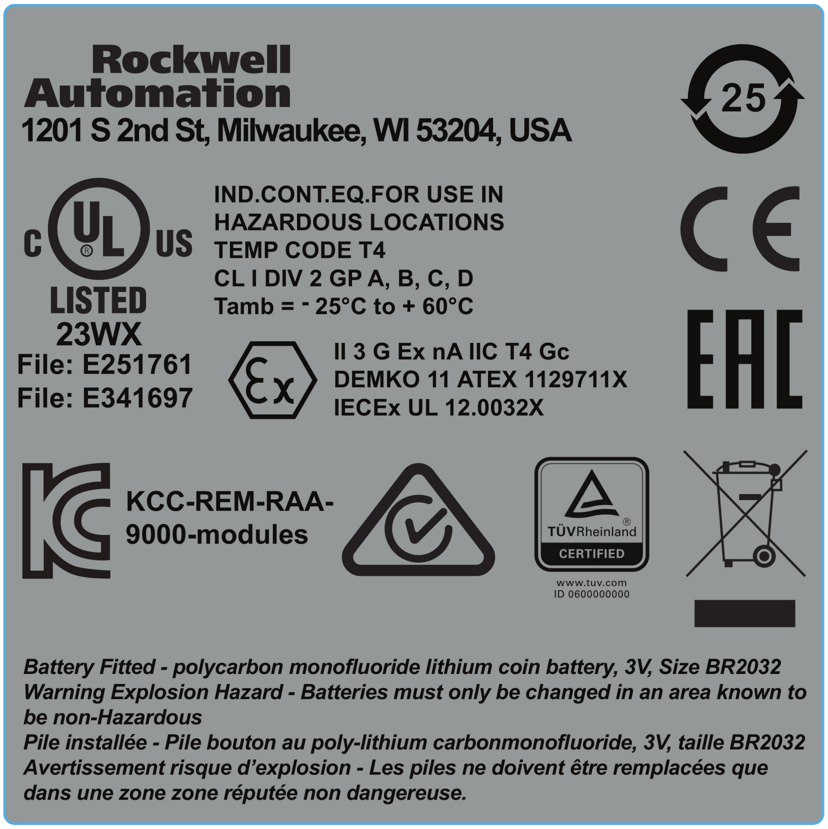
Refer to AADvance Series T9000 Programmable Control and Safety System - ATEX certificate, publication 9000-CT003.

IECEx UL Certificate

Refer to AADvance Series T9000 Programmable Control and Safety System - IECEx certificate, publication 9000-CT006.

Module Labels

Labels containing comprehensive safety information are attached to all modules. The following CPU label is illustrated as an example, but similar labels are produced for each module type.



Battery Fitted - polycarbon monofluoride lithium coin battery, 3V, Size BR2032
Warning Explosion Hazard - Batteries must only be changed in an area known to be non-Hazardous
Pile installée - Pile bouton au poly-lithium carbonmonofluoride, 3V, taille BR2032
Avertissement risque d'explosion - Les piles ne doivent être remplacées que dans une zone zone réputée non dangereuse.

KCC-EMC Registration

1. A급 기기 (업무용 방송통신기기): 이 기기는 업무용(A급)으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.
   - Translation: Class A device (Broadcasting Communication Device for Office Use): This device obtained EMC registration for office use (Class A), and may be used in places other than home. Sellers and/or users need to take note of this.

Functional Safety Management

This chapter explains the principles that should be applied to managing the safety related system.

The Safety Management System

A prerequisite for the achievement of functional safety is the creation and use of procedures and other measures as part of a safety lifecycle, collectively known as a Safety Management System. The Safety Management System defines the generic management and technical activities necessary to achieve and maintain functional safety in the product design and development. In many cases, the Safety Management and Quality systems will be integrated within a single set of procedures. The integrator should have an accredited quality management system.

The Safety Management System shall include:

- A statement of the policy and strategy for achieving and maintaining functional safety.
- A safety planning procedure, which shall result in the definition of the safety lifecycle stages to be applied, the measures and techniques to be applied at each stage, and the responsibilities for completing these activities.
- Definitions of the records to be produced and the methods of managing these records, including change control. The change control procedures shall include records of modification requests, the impact analysis of proposed modifications and the approval of modifications. The baseline for change control shall be defined clearly.
- Configuration items shall be uniquely identified and include version information. Examples of configuration items are system and safety requirements, system design documentation and drawings, application software source code, test plans, test procedures and test results.
- Methods of ensuring that persons are competent to undertake their activities and fulfill their responsibilities.

The Safety Life-cycle

The safety life-cycle is defined by the IEC 61508 standard. It is designed to structure a system's development into defined stages and activities as follows:

- Scope definition
- Hazard and risk analysis
- Functional and safety requirements specification
- System engineering
- Application programming
- System production
- System integration

- System installation and commissioning
- Safety system validation
- Operation and maintenance plan
- System modification
- Decommissioning

The definition of each life-cycle stage shall include its inputs, outputs and verification activities. It is not necessary to have separate stages within the life-cycle addressing each of these elements independently; but it is important that all of these stages are covered within the life-cycle. Specific items that need to be considered for each of these life-cycle elements are described in the following sub-paragraphs.

Scope Definition

The scope definition is the first step in the system life-cycle. You have to identify the boundaries of the safety related system and provide a clear definition of its interfaces with the process and with all third party equipment. This stage should also establish the derived requirements resulting from the intended installation environment, such as environmental conditions and power sources.

In most cases, the client will provide this information. The system integrator must review this information and gain a thorough understanding of the intended application, the bounds of the system to be provided, and its intended operating conditions.

Hazard and Risk Analysis

The hazard and risk analysis has three objectives:

- The first objective is to determine the hazards and hazardous events of the controlled system for all reasonably foreseeable circumstances, including fault conditions and misuse.
- The second objective is to determine the event sequences that may lead to a hazardous event.
- The third objective is to determine the risks associated with the hazardous event.

This risk analysis will provide basic information for identifying the safety-related requirements to mitigate risks.

System Functional and Safety Requirements

A set of system functions and their timing requirements will be specified. Where possible, the functions should be allocated to defined modes of operation of the process. For each function, it will be necessary to identify the process interfaces. Similarly, where the function involves data interchange with third party equipment, the data and interface should be clearly identified. Where non-standard field devices, communications interfaces or communications protocols are required, it is especially important that detailed requirements for these interfaces are established and documented at this stage.

The client should provide the functional requirements, where this information is not supplied the System Integrator should define the requirements and agree them with the client. It is, however, necessary to collate these requirements into a document, including any clarification of the requirements. It is recommended that logic diagrams be used to represent the required functionality and highly recommended that all requirements are reviewed, clarified where required and approved by the client.

During the system safety requirements stage the functional requirements are analyzed to determine their safety relevance. Where necessary, additional safety requirements shall be identified and documented to verify that the plant will fail-safe in the case of failures of the plant, safety-related system, external equipment or communications, or if the safety-related system's environment exceeds the required operating conditions.

The appropriate safety integrity level and safety-related timing requirements shall be defined for each safety-related function. For each function the required safety failure mode shall be determined. The client should supply this information or it should be defined and agreed with the client as part of this phase. The System Integrator shall ensure that the client approves the resulting safety requirements.

System Engineering

The system engineering stage realizes the design of the safety-related system. It is recommended that the engineering be divided into two distinct stages, the first defining the overall system architecture, and the second detailing the engineering of the individual architectural blocks.

The architectural definition shall define the safety requirements class for each architectural element and identify the safety functions allocated to each element. Additional safety functions resulting from the chosen system architecture shall be defined at this stage.

The detailed engineering design shall refine the architectural elements and culminate in detailed information for system build. The design shall be in a form that is readily understood and allows for inspection and review of each stage of the process and final design.

If the possibility of errors cannot be eliminated, the system integrator should make sure that procedural methods are devised and applied to detect them.

The system design should include facilities to allow field maintenance tasks can be performed.

Each installation shall be designed to ensure that the control equipment is operated in environments that are within its design tolerances. Therefore, the operating environment should provide the proper control of temperature, humidity, vibration and shock, as well as adequate shielding and earthing to minimize that exposure to sources of electromagnetic interference and electrostatic discharge.

Application Programming

Application programs are developed and monitored using the AADvance® Workbench software or the AADvance®-Trusted® SIS Workstation software.

The development of the application software shall follow a structured development cycle; the minimum requirements of which are:

- General Requirements: The application program shall be designed in accordance with this safety manual and the application program safety requirements.
- Design: Where both safety and non-safety functions are required, the design shall ensure that the non-safety functions cannot affect the safety functions. The design shall be structured to ensure traceability back to the application program safety requirements and for assessment during the FSA.
- Implementation: The implementation shall be modular to reduce complexity, improve testability and traceability.
- Verification: Verification shall be performed and documented using a combination of review, simulation and testing to ensure that the application program safety requirements have been met.

System Production

The system production stage implements the detailed system design. The production techniques, tools and equipment, including those used for production testing of the system, shall be appropriate for the specified safety requirements class.

System Installation Environment

The installation environment is a potential source of common cause failure, therefore it is vital that compatibility of the equipment with the environment is known. The environment for these purposes includes the prevailing climatic, hazardous area, power, earthing and EMC conditions. In many cases, there will not be a single installation environment. Elements of the system may be installed in differing locations; in these cases, it is important to know the environment for each location.

⚠ **WARNING:** You must use installation and commissioning procedures that comply with applicable standards of the country of installation. The applicable standards can include, for example, IEC 61511, NFPA 72 and ISA 84.00.01, depending on the location.

System Integration

The system integration stage shall integrate the application programs with the AADvance controller. Where multiple systems are used to meet an overall requirement, it is recommended that each sub-system undergoes application program and target system integration and testing before commencing overall system integration. To meet the requirements of the intended safety requirements class, the system integration shall result in full compliance of the software and hardware with the functional safety requirements.

System Commissioning

The commissioning stage is to prove the system installation and verify its correct 'end-to-end' functionality, including the connection between the AADvance controller and the requisite sensors and final elements. It is likely that groups of functions are commissioned in stages rather than the system as a whole, for example accommodation area functions before production functions. It is important to define the commissioning sequence and the measures to be taken to enable safe operation during such periods of partial commissioning. These measures shall be system specific and shall be defined clearly before starting any commissioning. It is also important to define that any temporary measures implemented for test purposes, or to allow partial commissioning, are removed before the system, as a whole, goes live.

Records shall be maintained throughout the commissioning process. These records shall include evidence of the tests completed, any problem reports and the resolution of problems.

Safety System Validation

Safety system validation shall test the integrated system to ensure compliance with the safety requirements specification at the intended safety requirements class. The validation activities should include those necessary to prove that the system implements the safety actions during normal start-up and shutdown and under abnormal fault modes.

The validation shall confirm that each functional safety requirement has been implemented at the specified safety integrity level, and that the realization of the function achieves its performance criteria, specifically that the process safety time requirements have been met.

The validation shall also consider the potential external common cause failures (power sources and environmental conditions) and confirm that the system will provide fail-safe operation when these conditions exceed its design capabilities.

Operation and Maintenance Plan

The provision of an Operation and Maintenance Plan verifies that functional safety can be maintained beyond the commissioning of the system. The in-service operation and maintenance is normally outside the responsibility of the system integrator, but the system integrator can provide guidance and procedures to verify that the persons or organizations responsible for operation and maintenance can verify that the system operates to the specified safety levels.

The Operating and Maintenance Plan shall include the following items:

- Clear definitions of power up and down sequences. These definitions shall ensure that the sequences cannot result in periods when the system is unable to respond safely whilst a hazard may be present.
- The procedures for re calibrating sensors and actuators. The recommended calibration periods shall also be included.
- The procedures for periodically testing the system, together with definitions of the maximum intervals between testing.
- Definitions of the overrides to be applied to be able to carry maintenance of the sensors and actuators.
- The procedures for maintaining system security.

Maintaining Functional Safety

Design changes will inevitably occur during the system life-cycle; to verify that the system safety is maintained, such changes shall be carefully managed. Procedures defining the measures for updating the plant or system shall be defined and documented. These procedures are the responsibility of the end user, but the system integrator shall provide sufficient guidance so that the procedures maintain the required level of functional safety during and after the changes.

Functional Safety Assessment

The functional safety assessment (FSA) is intended to confirm the effectiveness of the functional safety performance of the SIF's implemented by the SIS.

The FSA is to be carried out by an audit team that shall include at least one senior competent person independent from the project.

The FSA shall review the work associated with all applicable phases of the life-cycle to verify that the requirements have been met and the processes followed appropriately.

Safety Integrity Design

Safety Integrity

The architecture of the AADvance system has been designed to allow a scalable system to be configured using standard components. The configurations available range from simplex fail-safe to TMR fault tolerance.

The processor module has been designed to meet the requirements for SIL 2 with two or three processor modules and SIL 3 when two or three modules are fitted. Input and output modules have been designed to meet SIL 3 requirements with a single module in a fail-safe mode.

The processor module and the individual I/O modules have built in redundancy and have been designed to withstand multiple faults and support a fixed on-line repair by replacement configuration in dual and triple modular redundant configurations. The input and output modules support a number of architecture options; the affects of the chosen architecture should be evaluated against the system and application specific requirements.

Notes:

AADvance System Architectures

An AADvance® controller can be configured to manage non-safety up to SIL 3 safety related system requirements and low demand or high demand fault tolerant applications.

This chapter describes the different system architectures that can be configured for an AADvance controller to meet this variety of requirements.

NOTE Architectures are independent of I/O module capacity therefore 8 or 16 channel I/O modules can be used.

SIL 2 Architectures

SIL 2 architectures are recommended for fail-safe low demand applications. All SIL 2 architectures can be used for energize or de-energize to trip applications. In any configuration when a faulty processor or input module is replaced then the previous fault tolerance level is restored. For example in a fault tolerant input arrangement and one module is faulty then the system will degrade to 1oo1D, by replacing the faulty module the configuration is restored to 1oo2D.

In all SIL 2 architectures, when the processor modules have degraded to 1oo1D on the first detected fault, the system must be restored to 1oo2D by replacing the faulty processor module within the MTTR assumed in the PFD calculations; also, unless compensating measures are defined in the Safety Requirements Specification (SRS) and documented in operating procedures, the application program must be designed to shut down safety instrumented functions if a module failure due to a dangerous fault has not been replaced within the MTTR.

Configuration Backups

⚠ **CAUTION:** You must make a backup of the AADvance® Workbench software or AADvance®-Trusted® SIS Workstation software system and test the backup copy prior to storing it. Refer to the AADvance Configuration Guide or the AADvance-Trusted SIS Workstation Software User Guide, publication ICSTT-UM002, for information about these procedures.

Fail-safe Architecture

The following is a simplex fail-safe SIL 2 architecture, where I/O modules operate in 1oo1D under no fault conditions and will fail-safe on the first detected fault. The processor will operate in 1oo2D under no fault conditions, will degrade to 1oo1D on the first fault in either processor module and will fail-safe when there are faults on both processor modules.

NOTE Simplex output modules used for energize to action applications can only be used for low demand applications.

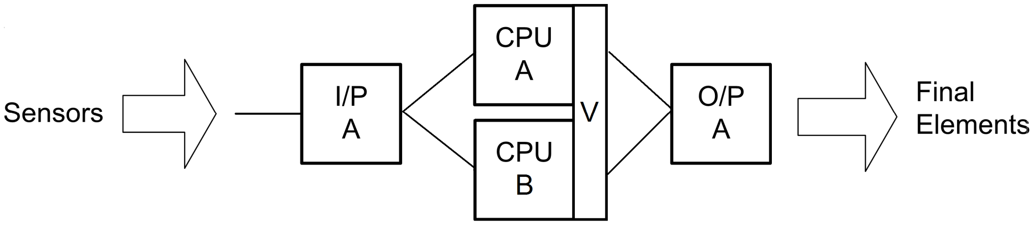


Table 4 - Modules for SIL 2 Fail-Safe Architecture

Position	Module Type
I/P A	T9401/2 Digital Input Module, 24V dc, 8/16 Channel + T9801 Digital Input TA, 16 Channel, Simplex. or T9431/2 Analogue Input Module, 8/16 Channel + T9831 Analogue Input TA, 16 Channel, Simplex T9300 I/O Base Unit
CPU A	2 x T9110 Processor Module, T9100 Processor Base Unit,
O/P A	T9451 Digital Output Module, 24V dc, 8 Channel, isolated + T9851 Digital Output TA, 24V dc 8 Channel, Simplex 1 x T9481/T9842 Analogue Output Module, 3/8 Ch, Isolated + T9881 Analogue Output TA, 8 Ch, Simplex

Fault Tolerant Input Architectures

A SIL 2 fault tolerant input architecture can have dual or triple input modules with a dual processor and single output modules. The illustration shows a dual input arrangement where the dual input modules operate in 1oo2D under no fault conditions, they degrade to 1oo1D on detection of the first fault in either module of the redundant pair, and when a fault occurs on the second module it will fail-safe.

The processor will operate in 1oo2D under no fault conditions, will degrade to 1oo1D on the first fault in either processor module and will fail-safe when there are faults on both processor modules. The output module operates in 1oo1D under no fault conditions and will fail-safe on the first detected fault.

When a triple input module arrangement is configured the group of input modules operate in 2oo3D under no fault conditions, degrade to 1oo2D on the detection of first fault in any module, then degrade to 1oo1D on the detection of faults in any two modules, and will fail-safe when there are faults on all three modules.

NOTE Simplex output modules used for energize to action applications can only be used for low demand applications.

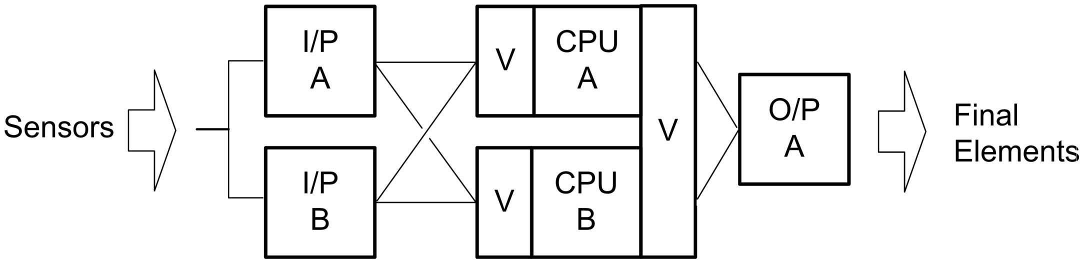


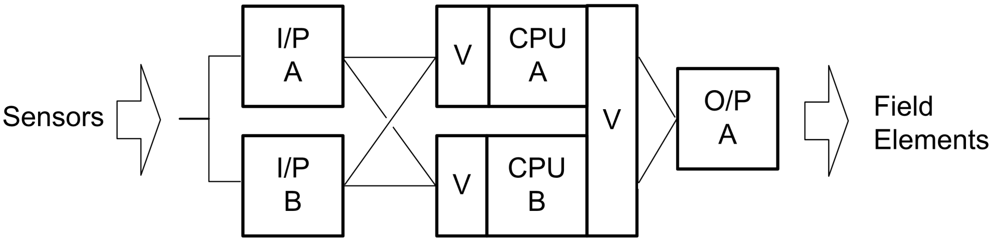
Table 5 - Modules for SIL 2 Architecture

Position	Module Type
I/P A and B	2 × T9401/2 Digital Input Module, 24V dc, 8/16 Channel + T9802 Digital Input TA, 16 Channel, Dual or 2 × T9431/2 Analogue Input Module, 8/16 Channel, Isolated, + T9832 Analogue Input TA, 16 Channel, Dual T9300 I/O Base Unit
CPU A	2 x T9110 Processor Module, T9100 Base Unit
O/P A	T9451 Digital Output Module, 24V dc, 8 Channel + T9851 Digital Output TA, 24V dc, 8 Channel, Simplex T9300 I/O Base Unit or 1 x T9481/T9842 Analogue Output Module, 3/8 Ch, Isolated + T9881 Analogue Output TA, 8 Ch, Simplex

Output Architecture

A SIL 2 output architecture has a single output module with dual processor and single or redundant input modules.

The illustration shows a SIL 2 single output arrangement where the output module operates in 1oo1D under no fault conditions and will fail-safe on the first detected fault. The processor will operate in 1oo2D under no fault conditions, will degrade to 1oo1D on the first fault in either processor module and will fail-safe when there are faults on both processor modules.



Digital Output

For Digital Output Modules the following applies:

- For energize to action high demand applications you must use dual digital output modules.

Analogue Output

For Analogue Output the Following applies:

- The fail-safe state current of the Analogue Output module is less than 2mA.
- For energize to action high demand applications you must use dual analogue output modules.

Table 6 - Modules for SIL 2 Fault Tolerant Output Architecture

Position	Module Type
I/P A	T9401/2 Digital Input Module, 24V dc, 8/16 Channel. + T9801 Digital Input TA, 16 Channel, Simplex or T9431/2 Analogue Input Module, 8/16 Channel + T9831 Analogue Input TA, 16 Channel, Simplex T9300 Base Unit
CPU A	2 x T9110 Processor Module, T9100 Processor Base Unit and 9300 I/O Base Unit
O/P A	1 × T9451 Digital Output Module, 24V dc, 8 Channel + T9851 Digital Output TA, 24V dc, 8 Channel, Dual or 1 x T9481/T9842 Analogue Output Module, 3/8 Ch, Isolated + T9881 Analogue Output TA, 8 Ch, Simplex

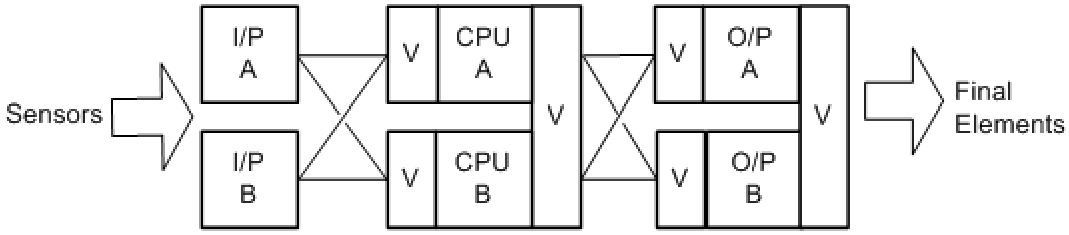
Fault Tolerant Input and High Demand Architecture

A SIL 2 fault tolerant "High Demand" architecture has dual input, dual processor and dual output modules. In a dual arrangement the input modules operate in 1oo2D under no fault conditions, degrade to 1oo1D on the detection of the first fault in either module, and will fail-safe when there are faults on both modules.

A triple input module arrangement can also be configured if it is required to increase the fault tolerance of the input. When a triple input module arrangement is configured the input modules operate in a 2oo3D under no fault conditions, degrade to 1oo2D on detection of the first fault in any module, then degrade to 1oo1D on the detection of faults in any two modules, and will fail-safe when there are faults on all three modules.

The processor will operate in 1oo2D under no fault conditions, will degrade to 1oo1D on the first fault in either processor module and will fail-safe when there are faults on both processor modules. For high demand applications, unless compensating measures are defined in the Safety Requirements Specification (SRS) and documented in operating procedures, the application program must be designed to shut down safety instrumented functions if a module failure due to a dangerous fault has not been replaced within the MTTR.

WARNING: For High Demand mode applications you must use a minimum of a dual processor configuration. High demand energize to action applications will require dual output modules. (Analogue Output Modules where the normal output current is less than 4mA are classed as energize to action applications).



WARNING: For Continuous Mode applications the measures defined in this section for High Demand applications must be applied.

Table 7 - Modules for SIL 2 Fault Tolerant High demand Architecture

Position	Module Type
I/P A	2 × T9401/2 Digital Input Module, 24V dc, 8/16 Channel + T9802 Digital Input TA, 16 Channel, Dual or 2 × T9431/2 Analogue Input Module, 8/16 channel + T9832 Analogue Input TA, 16 Channel, Dual 2 × T9300 I/O Base unit
CPU A & CPU B	2 x T9110 Processor,, T9100 Processor Base Unit
O/P A	2 × T9451 Digital Output Module, 24V dc, 8 Channel + T9852 Digital Output TA, 24V dc, 8 channel, T9300 Base Unit or 2 x T9481/T9842 Analogue Output Module, 3/8 Ch, Isolated + T9882 Analogue Output TA, 8 Ch, Dual

SIL 3 Architectures

SIL 3 architectures have at least two processor modules and are suitable for use with:

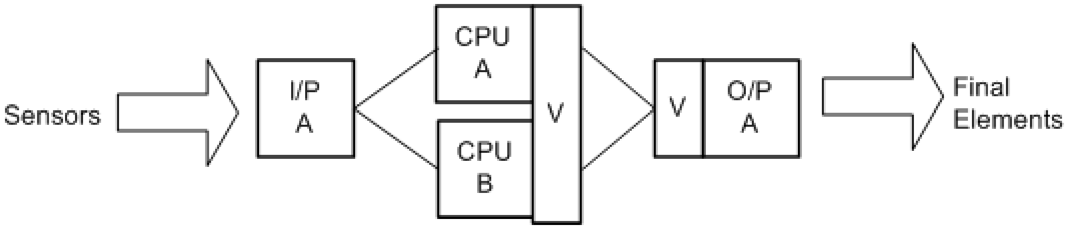
- SIL 3 de-energize to trip applications.
- SIL 3 energize to action applications which have dual digital/analogue output modules.

Faulted input modules in a SIL 3 arrangement may be replaced without a time limit; faulted output modules must be replaced within the MTTR assumed in the PFD calculations.

In all SIL 3 architectures, when the processor modules have degraded to 1oo1D on the first detected fault, the system must be restored to at least 1oo2D by replacing the faulty processor module within the MTTR assumed in the PFD calculations; also, unless compensating measures are defined in the Safety Requirements Specification (SRS) and documented in operating procedures, the application program must be designed to shut down safety instrumented functions if a module failure due to a dangerous fault has not been replaced within the MTTR.

Fail-safe I/O, Fault Tolerant Processor

A SIL 3, fail-safe I/O with a fault tolerant processor architecture has a simplex input and output arrangement with dual or triple processor modules. The dual processor modules operate in 1oo2D under no fault conditions and degrades to 1oo1D on detection of the first fault in either module. When there are faults on both modules the configuration will fail-safe.



If required you can configure triple processor modules as a variation of this SIL 3 architecture. Using this arrangement the processor modules operate in 2oo3D under no fault conditions and 1oo2D on the detection of the first fault in any module. They degrade to 1oo1D on the detection of faults in any two modules, and will fail-safe when there are faults on all three modules.

Digital Output Modules

- For de-energize to action operation one digital output module is sufficient for SIL 3 requirements. However, for energize to action operation, dual digital output modules are required.
- A digital output module fault must be repaired within the MTTR which was used in the PFD calculation.

Analogue Output Modules

- The fail-safe state current of the analogue output module is less than 2mA.
- For de-energize to action operation one analogue output module is sufficient for SIL 3 requirements. However, for energize to action operation, dual analogue output modules are required.
- An analogue output module fault must be repaired within the MTTR which was used in the PFD calculation.

Table 8 - Modules for SIL 3 Fail-safe I/O, Fault Tolerant Processor

Position	Module Type
I/P A	T9401/2 Digital Input Module, 24V c, 8/16 Channel + T9801 Digital Input TA, 16 Channel, Simplex or T9431/2 Analogue Input Module, 8/16 channel + T9831 Analogue Input TA, 16 Channel, Simplex T9300 Base unit
CPU A & CPU B	2 x T9110 Processor Module, T9100 Base Unit
O/P A	1 x T9451 Digital Output Module, 24V dc, 8 Channel + T9851 Digital Output TA, 24V dc, 8 Channel, Simplex or 1 x T9481/T9842 Analogue Output Module, 3/8 Ch, Isolated + T9881 Analogue Output TA, 8 Ch, Simplex

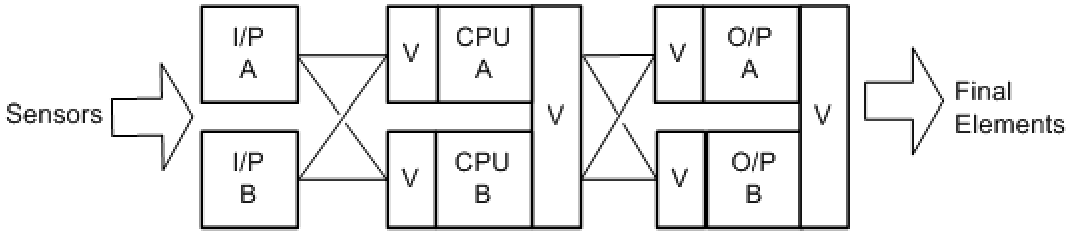
Fault Tolerant I/O Architectures

A SIL 3 fault tolerant processor and I/O is achieved by dual input and output module configurations with dual or triple processor modules. The processor modules operate in 1oo2D under no fault conditions, degrade to 1oo1D on the detection of the first fault in either module and fail-safe when there are faults on both modules.

Similarly the input modules operate in 1oo2D under non faulted conditions and 1oo1D on detection of the first fault in either module and will fail-safe when there are faults on both modules.

Unless compensating measures are defined in the Safety Requirements Specification (SRS) and documented in operating procedures, the application program must be designed to shut down safety instrumented functions if a module failure due to a dangerous fault has not been replaced within the MTTR.

WARNING: For SIL 3 applications you must use a minimum of a dual processor configuration.



Digital Output Modules

A digital output module fault must be repaired within the MTTR which was used in the PFD calculation.

Analogue Output Modules

An analogue output module fault must be repaired within the MTTR which was used in the PFD calculation.

Table 9 - Modules for SIL 3 Fault Tolerant Architectures

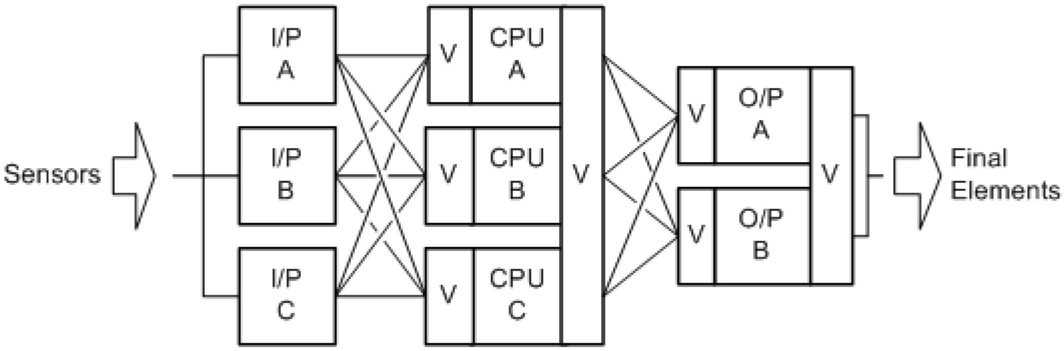
Postition	Module Type
I/P A and I/P B	2 × T9401/2 Digital Input Module, 24V dc, 8/16 Channel, + T9802 Digital Input TA, 16 Channel, Dual or 2 × T9431/2 Analogue Input Module, 8/16 Channel + T9832 Analogue Input TA, 16 Channel, Dual 2 x T9300 I/O Base Unit
CPU A & CPU B	2 × T9110 Processor Module, 9100 Processor Base Unit,
O/P A and O/P B	1 × T9451 Digital Output Module, 24V dc, 8 Channel + T9851 Single Digital Output TA, 24V dc, 8 Channel for de-energize to action. T9300 Base unit 2 x T9451 Digital Output Module, 24V dc, 8 Channel + T9852 Dual Digital Output TA for energize to action. or 2 x T9481/T9842 Analogue Output Module, 3/8 Ch, Isolated + T9882 Analogue Output TA, 8 Ch, Dual

TMR Input and Processor, Fault Tolerant Output

A SIL 3 TMR architecture offers the highest level of fault tolerance for an AADvance controller and consists of triple input modules, triple processors and dual output modules.

- The input and processor modules operate in a 2oo3D under no fault conditions, degrade to 1oo2D on detection of the first fault in any module, and degrade to 1oo1 on the detection of faults in any two modules and will fail-safe when there are faults on all three modules.

In the event of a failure in any element of a channel, the channel processor will still produce a valid output which could be voted on because of the coupling between the channels. This is why the triple modular redundant implementation provides a configuration that is inherently better than a typical 2oo3 voting system.



Digital Output Modules

A digital output module fault must be repaired within the MTTR which was used in the PFD calculation.

Analogue Output Modules

An analogue output module fault must be repaired within the MTTR which was used in the PFD calculation.

Table 10 - Modules for TMR Input and Processor, Fault Tolerant Output

Position	Module Type
I/P A	3 × T9401/2 Digital Input Module, 24V dc, 8/16 Channel + T9803 Digital Input TA, 16 Channel, TMR or 3 × T9431/2 Analogue Input Module, 8/16 Channel + T9833 Analogue Input TA, 16 Channel, TMR 2 × T9300 I/O Base Unit
CPU A & CPU B	3 × T9110 Processor Module, T9100 Processor Base Unit,
O/P A	2 × T9451 Digital Output Module, 24V dc, 8 Channel + 9852 Digital Output TA, 24V dc 8 Channel, Dual or 2 x T9481/T9842 Analogue Output Module, 3/8 Ch, Isolated + T9882 Analogue Output TA, 8 Ch, Dual

NOTE All configurations that use dual or triplicate processor modules are suitable for SIL 3 architectures with de-energize to trip outputs. Dual outputs are also required for SIL 3 energize to action outputs.

Certified Configurations

Table 11 - Central Modules

Modules	Certified Configuration	Conditions
Processor Module T9110	1oo2D, 2oo3D	Safety-related and can be used for safety-critical applications in SIL 2 with 2 modules fitted and SIL 3 applications with 2 or 3 modules fitted. **Note:** For both Low and High Demand applications you must use a minimum of two processors.

Table 12 - Central Modules

Modules	Certified Configuration	Conditions
Digital Inputs T9401/2, 24V dc, 8/16 Channel, isolated. + T9801/2/3 Digital Input TA, 16 channel, Simplex/Dual/TMR	1oo1D, 1oo2D, 2oo3D	De-energized to action (normally energized): SIL 3 with 1, 2 or 3 modules fitted. Energize to action (normally de-energized): with 1, 2 or 3 modules fitted **Note:** when the integrity level is at 1oo1D then the faulty module must be replaced to restore the integrity level back to 1oo2D.
Analogue Inputs T9431/2, 8/16 Channel, isolated + T9831/2/3 Analogue Input TA, 16 Channel, Simplex/Dual/TMR	1oo1D, 1oo2D, 2oo3D	Within the manufactures specified safety accuracy limits of 0.2mA. The safety state of the analogue input has to be set to a safe value which is a calculated value based on a count value of 0mA. (refer to the AADvance Configuration Guides, publications ICSTT-RM405 and ICSTT-RM458, or the AADvance-Trusted SIS Workstation Software User Guide, publication ICSTT-UM002, for more details) SIL 3 with 1, 2 or 3 modules fitted. **Note:** when the integrity level is at 1oo1D then the faulty module must be replaced within the MTTR assumed for the PFD calculations to restore the integrity level back to 1oo2D.

Table 13 - Output Modules

Modules	Certified Configuration	Conditions
Digital Outputs T8451, 24V dc, 8 channel. + T9851/2 TA,24V dc, 8 Channel, Simplex/Dual	1oo1, 1oo2 or 1oo2D	De-energize to action (normally energized): SIL 3 with 1 or 2 modules fitted. (1oo2D with dual output modules fitted). Energize to action (normally de-energized): SIL 2 with 1 module fitted and SIL 3 with 2 modules fitted. A faulty digital output module must be repaired or replaced within the MTTR which was used in the PFD calculation.
Analogue Outputs T9481/T9842 Analogue Output Module, 3/8 Ch, Isolated + T9881/T9882, TA, 8Ch, Simplex/Dual	1oo1, 1oo2 or 1oo2D	De-energize to action (normally energized): SIL 3 with 1 or 2 modules fitted. (1oo2D with dual output modules fitted). Energize to action (normally de-energized): SIL 2 with 1 module fitted and SIL 3 with 2 modules fitted. A faulty analogue output module must be repaired or replaced within the MTTR which was used in the PFD calculation.

Table 14 - Auxiliary Modules

Modules	Conditions
Processor Base T9100	Safety-related and can be used for safety critical applications in SIL 2 applications with 2 modules fitted or SIL 3 applications with 2 or 3 modules fitted.
I/O Base T9300 (3-way)	Safety-related and can be used for safety critical applications in SIL 3.

NOTE Revisions of modules are subject to change. A list of the released versions can be obtained from Rockwell Automation.

Internal Diagnostics

The AADvance controller embodies sophisticated internal diagnostic systems to identify faults that develop during operation and raise appropriate alarm and status indications. The diagnostic systems run automatically and check for system faults associated with the controller (processor and I/O modules), and field faults associated with field I/O circuits.

⚠ **WARNING:** Safety wiring principles shall be employed for field loops if it is necessary for the user to guard against short circuit faults between I/O channels (e.g. to comply with NFPA 72 requirements). The AADvance controller internal diagnostics do not detect external short circuits between channels.

The diagnostic systems report a serious problem immediately, but filter non-essential safe failures to avoid spurious alarms. The diagnostic systems monitor such non-essential items periodically, and need a number of occurrences of a potential fault before reporting it as a problem.

The internal diagnostics detect and reveal both safe and dangerous failures. A dual module arrangement, for example, diagnostics can address dangerous failures and help redress the balance between failure to respond and spurious responses. A dual system could therefore be 1oo2D reverting to 1oo1D on the first detected fault and reverting to fail-safe when both modules have a fault. A whole self-test cycle completes every 24 hours.

Safety Networks

AADvance provides two safety network functionality that will allow data exchanges across a SIL 3 rated safety communication across the Ethernet communications link:

- SNCP (Safety Network Control Protocol)
- Peer-to-Peer

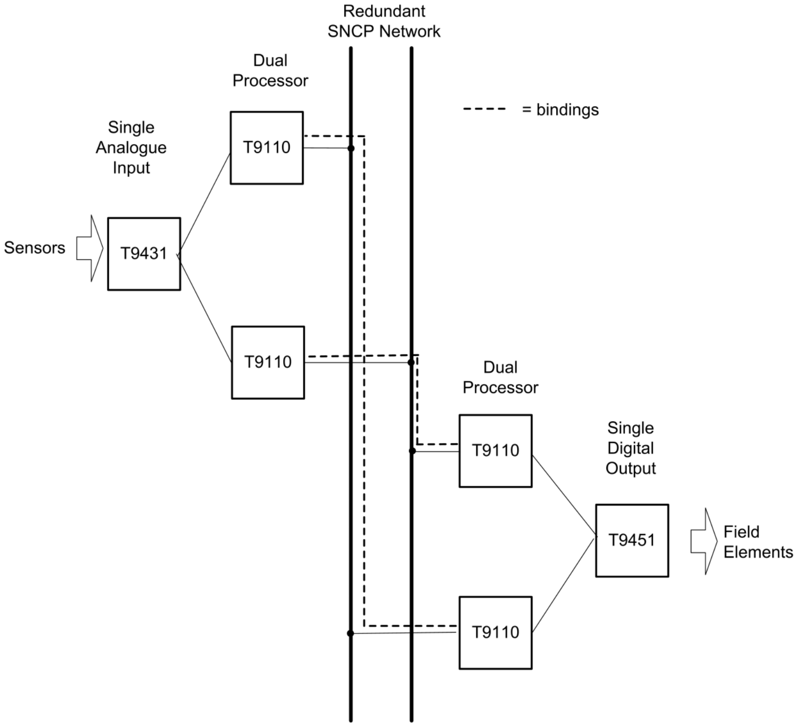
SNCP Safety Networks

SNCP (**Safety Network Control Protocol**) is the Safety Protocol that allows elements of an AADvance System to exchange data. AADvance SNCP is a SIL 3 certified protocol which provides a safety layer for the Ethernet network making it a "Black Channel". Data is exchanged by creating a relationship between variables in different AADvance controllers; this is called "Binding Variables". Once variables are bound between controllers the SNCP protocol provides a transparent SIL 3 Certified layer allowing safety related data to be passed between AADvance controllers.

The bindings are based on a producer/consumer model. The controller consuming the data establishes a binding link with the Controller producing the data, and manages the entire exchange of data, including scheduling the data exchange, providing the diagnostics, managing the safety response in the event of faults and managing the communications redundancy.

SNCP Networks can be configured as Simplex (Fail Safe) or Redundant (Fault tolerant), the choice of network configuration is dependent on the applications safety and availability requirements. The data exchange is independent of the physical; network configuration as the connection between the controllers is treated as a logical network.

The physical network is considered a "Black Channel" so the design of the Ethernet network and the equipment used does not impact the SIL rating of the communications interface, but the design of the network does affect the reliability of the network and does impact the spurious trip rate. SNCP Network data can be combined on a common network resulting in safety and non-safety data sharing in a common physical network; this does not compromise the SIL rating of the network but again does introduce failure modes and possibly security risks which can increase the spurious trip rate, careful consideration should be given to the network topology during the applications specification and design phase.



The SNCP protocol can be configured in the AADvance controller to provide a safety network; refer to the AADvance Configuration Guide(s), publications ICSTT-RM405 and ICSTT-RM458, or AADvance-Trusted SIS Workstation Software User Guide, publication ICSTT-UM002, for detailed configuration procedures.

WARNING: For SNCP bindings to be used in a Simplex Network configuration, SIL 3 can be achieved but the following conditions must be met:

- For de-energize to trip configurations, associated SIF outputs shall be configured to shutdown on loss of communications.
- For energize to trip configurations link failures shall be repaired within the MTTR.

NOTE Additional measures must be considered for ensuring that the process remains within its safe operating parameters during the repair time; these additional measures must be defined in the Operating and Maintenance procedures written for maintaining the SIF for the specific Plant or Process.

Configuring Variable Bindings

The bindings configuration includes the value of an age timeout (**MaxAge**). This timeout defines the maximum age of data that can be used by a consumer system. Data older than the defined timeout is discarded and the system continues using its last state value. Once disconnected the consumer attempts to re-establish a connection to the producer by sending a connection request at **ConnectTimeout** intervals. The consumer continues to send connection requests until a connection is established.

The configuration also includes a timeout value for a consumer **Bind Response Timeout** value for the binding data response from a producer. Failure to receive a valid response containing fresh data within this timeout causes the consumer to disconnect from the producer. The number of retries that are attempted before a consumer disconnects depends on the configured values for the parameter **MaxAge**.

The configuration also includes a timeout value **Bind Request Timeout**, which is used by a producer system to timeout binding data requests from a consumer system. Should a producer fail to receive a binding data request from a consumer within this timeout value, the link to the consumer system is closed. The consumer system, if still functional, will timeout the link from its end.

An **UpdateTimeout** value can also be configured. This timeout is used in both the consumer and producer resources during an on-line update. During an on-line update all binding connections are closed. The SNCP binding driver then restarts with the potentially new binding configuration. This timeout value is the time in which the consumer must re-establish its binding connections.

Timeout values should be set within the fault tolerant capabilities of the bindings network, so the system can still respond within the required PST. The network propagation time must be included in the timeout period calculations, and should be verified after each change to the network configuration.

Two function blocks are provided that make the overall status of the bindings communication subsystem available to the application — one indicates consumer status (KvbConsNetStatus) for a specific bindings link (identified by the Producers Resource Number and IP Address, the other producer status (KvbProdNetStatus) for a specific bindings link (Identified by the Consumers Resource Number and its IP Address). In addition to these, an error variable can be configured to report error codes for the bindings links to the application.

NOTE The Consumers Network bindings parameters (i.e. timeout values) are those located in Producing Resource if using AADvance Workbench software version 1.x, and in Communication View if using AADvance Workbench software version 2.x or AADvance-Trusted SIS Workstation software.

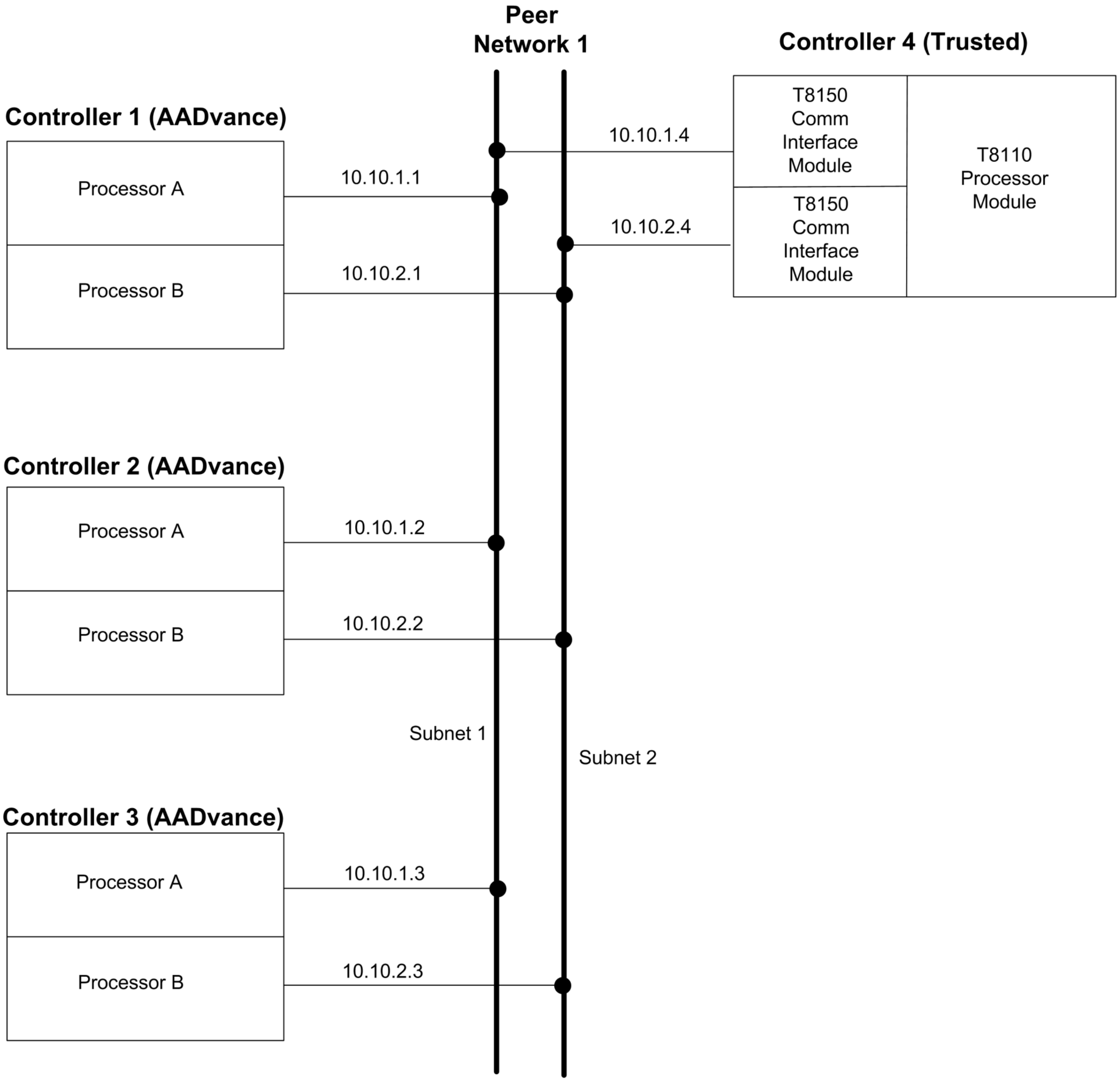
Peer-to-Peer

AADvance provides the capability for a SIL 3 certified Peer-to-Peer data connections, allowing safety data to be transferred between AADvance and Trusted® controllers. The Trusted Peer-to-Peer network protocol enables you to share safety data between AADvance systems or AADvance and Trusted systems across an Ethernet network. Data can be transferred between individual systems or from one to several systems at the same time using multicast network connections. Peer-to-Peer communication is configured by defining a peer network controller and I/O devices within the application program.

Note: AADvance currently supports multicast network connections on the left most port of each processor.

For safety related applications it is recommended that the Peer-to-Peer communications use redundant networks (for availability) and separate networks (from general purpose, for security and integrity). Any of the AADvance or Trusted ports can be used for Peer-to-Peer data connections see Example shown.

The Trusted Peer-to-Peer protocol is a master/slave interaction. For each peer communications subnet one system acts as a master while the others act as slaves. During the Peer-to-Peer communication cycle the master sends a command to the first slave to transmit its data. When the slave completes this task it acknowledges this back to the master. The master repeats this with the next and all slaves in turn. Finally the master transmits its own data then repeats the cycle with the slaves.



Safety Related Peer-to-Peer Configurations

The following Peer-to-Peer configurations are approved for use in a safety Related Function:

IMPORTANT The peer-to-peer configurations in this section only apply to AADvance Workbench software version 1.4.

For AADvance Workbench software version 2.1 users, refer to the AADvance Controller Configuration Guide WorkBench R2.x, publication ICSTT-RM458, and the software online help for information.

For AADvance-Trusted SIS Workstation software users, refer to AADvance-Trusted SIS Workstation Software User Guide, publication ICSTT-UM002, and the software online help for information.

Table 15 - Safety Related Peer-to-Peer Configurations

Peer-to-Peer Settings	Certified Configuration	Conditions
Software Board Definitions: Dxpdi16 Dxpdo16 Dxpao16 Dxpdi128 Dxpdo128 Dxpnc40	Certified for use over a single communication network or multiple networks	Certified as safety-related and can be used for safety critical communications in SIL 3 applications.
Software Board Definitions: Dxpai128 Dxpao128	Certified for use over a single communication network or multiple networks	Certified as safety-related and can be used for safety critical communications in SIL 3 applications provided two separate Dxpai128 & Dxpao128 board definitions are used for safety values, the safety values from the two Dxpai128 boards (or digital trip points from the values) shall have a 1oo2 vote within the receiving application.

Notes:

AADvance Functional Safety System Implementation

This chapter provides the implementation guidelines for an AADvance® safety related system.

General Design Measures for Functional Safety

I/O Modules

The AADvance system supports single module configurations, where it is acceptable to either stop the system or allow the signals corresponding to that module to change to their default fail-safe state. It also supports fault tolerant I/O configurations where it is required to enable continued system operation in the event of a fault.

All configurations may be used for safety-related applications; the choice between the configurations being dependent on the end-user's fault tolerance requirements.

The input modules can be configured as a simplex, dual or triple arrangement. Output modules can be configured as a simplex or dual arrangement. All I/O modules include line-monitoring facilities; it is recommended that these line monitoring facilities be enabled for safety-related I/O. For normally de-energized I/O these facilities shall be enabled.

NOTE Refer to the section Digital Field Loop Circuits for details of line monitoring circuits.

Both input and output modules undergo regular diagnostics testing during operation that is managed by the processor modules. The self-tests are coordinated between modules that are configured in a fault tolerant arrangement, to verify that the system remains on-line even in the case of a demand during the execution of the tests. I/O channel discrepancy and deviation monitoring further enhances the verification and fault detection of module or field failures.

The processor reports any detected I/O fault to the application running on the AADvance® Workbench software or AADvance®-Trusted® SIS Workstation software and provides an alarm signal for a central alarm indicator. Front panel LEDs on the faulty module will indicate a module or field fault. In all cases, even in the presence of a fault during this period, the system will continue to be able to respond when configured in a fault tolerant arrangement.

ATTENTION: When a channel is not capable of reporting a value within the safety accuracy specified for the module, 'safe' values are reported instead. Thus, an I/O channel fault condition results in a fail-safe state.

ATTENTION: The maximum duration for single-channel operation of I/O modules depends on the specific process and must be specified individually for each application:

- Input modules can operate in a simplex arrangement without time limit for SIL 3 and lower applications.
- Faulty Output modules must be replaced within the MTTR used for PFD calculations.
- Faulty Processor modules must be replaced within the MTTR used for the PFD calculations.
- Unless compensating measures are defined in the Safety Requirements Specification (SRS) and documented in operating procedures, the application program must be designed to shut down safety instrumented functions if a module failure due to a dangerous fault has not been replaced within the MTTR.

When a module is operating in a dual mode (or is degraded to a dual mode) and a state or value discrepancy occurs, then if no module fault is detected, the state or value reported to the application will always be the lower of the two states or values for a digital and analogue input module configurations.

ATTENTION: In safety applications channel discrepancy alarms shall be monitored by the application program and used to provide an alarm to plant operations personnel.

Energize to Action Configurations

Certain applications may require energize to action for inputs and/or outputs.

ATTENTION: Energize to action configurations shall only be used if the following restrictions apply:

- At least two independent power sources must be used. These power sources must provide emergency power for a safe process shutdown or a time span required by the application.
- Each power source must be provided with power integrity monitoring with safety critical input read back into the system controller or implicit power monitoring provided by the I/O modules. Any power failure shall lead to an alarm.
- Unless provided implicitly in the I/O modules, all safety critical inputs and outputs must be fitted with external line and load integrity monitoring and safety critical read back of the line-status signals. Any line or load failure shall lead to an alarm.
- Module configuration must comply with Table 1 on page 13 of Chapter 1 according to the required SIL and demand rate.

Controller Process Safety Time (PST)

The **Process Safety Time (PST)** setting defines the maximum time that the processor will allow the outputs to remain in the ON state in the event of certain internal diagnostic faults or systematic application faults. If the process safety time expires the system will go to its safe state. You have to specify the PST for the whole controller, this is a top level setting that you make once for the whole controller and is set at the processor module. I/O modules can be set at a lower PST but must not exceed this overall setting.

An AADvance controller adopts a default value for the PST = 2500ms. The system integrator can use the following method to confirm whether this is acceptable and adjust as necessary.

The value of PST for the Controller is governed by this equation:

$$\text{PST} \leq \frac{\text{PST}_{\text{euc}}}{2} - \left(\text{sensor delay} + \text{actuator delay}\right)$$

Where PSTeuc is the process safety time for the equipment under control.

As an example, consider a system function using one sensor and one actuator given the following parameters:

- PSTeuc: 10,000ms
- Sensor delay: 250ms
- Time for actuator (an ESD valve) to fully operate: 1750ms

In this example therefore, the setting of PST for the controller should be less than or equal to 3000ms.

Choosing Controller PST Settings

The response time allocated to a logic solver such as the AADvance controller needs to take account of delays within the operation of sensors and actuators. In addition, the system's scan time should be considerably less than the process safety time.

The value of the PST shall form part of the safety considerations for the system. The value is defined by the process design authority; the system integrator shall calculate and verify that the process safety time meets the stated requirements.

- In an AADvance system the PST value is assigned to the system and can be assigned to individual modules. The system PST value is enforced by the processor modules and has priority over the module PST values. When the system PST is not met the processor modules will fail-safe.
- The input PST is also enforced by the processor modules; when the PST is not met, the processors will present fail-safe input values to the application logic.
- Output PST is enforced by the output modules and when the output PST is not met, the output module will assume the fail-safe state.

NOTE The fail-safe state for all AADvance modules is de-energized.

You must specify the process safety time for the whole controller. If desired, you can specify additional process safety times for individual groups of I/O modules. The setting for the whole controller is a top level setting, which you make once for all the 9110 processor modules. Groups of I/O modules can inherit this setting or, if desired, use individual process safety times instead.

NOTE
- The minimum controller's PST must be at least twice the application scan time.
- If you choose to specify a process safety time for a group of I/O modules, the I/O modules use this setting instead of the top level setting.
- If you do not specify a process safety time for a group of I/O modules, the I/O modules use the top level setting.
- If you do not specify any process safety time, the controller will use a default value of 2,500ms throughout.

Industrial Functional Safety Standards

AADvance is designed to meet the following industrial safety system requirements:

NFPA 85 Requirements

NFPA 85:2015 provides minimum requirements for the design, installation, operation and maintenance of large commercial industrial boilers, heat recovery, heat recovery steam generators and related combustion systems. The AADvance system is certified for use with NFPA 85 compliant systems.

The systems should be integrated in accordance with NFPA 85. In particular the following shall be applied:

- independently and directly actuate the safety shutdown trip relay. At least one identified manual switch shall be located remotely from the boiler where it can be reached in case of emergency.
- The burner management system shall be provided with independent logic, independent input/output systems, and independent power supplies and shall be a functionally and physically separate device from other logic systems, such as the control system for the boiler or heat recovery steam generator.
- Logic sequences or devices intended to cause a safety shutdown, once initiated, shall cause a burner or master fuel trip, as applicable, and shall require operator action prior to resuming operation of the effected plant. No logic sequence or device shall be permitted that allows momentary closing and subsequent inadvertent reopening of the main or ignition fuel valves.
- Documentation shall be provided to the owner and operator, indicating that all safety devices and logic meet the requirements of the application.
- System response time shall be sufficiently short to help prevent negative effects on the application.
- The NFPA 85 certification is only applicable where the system is applied in accordance

NFPA 86 Requirements

NFPA 86:2019 provides comprehensive requirements for the safe design, installation, operation, inspection, testing and maintenance of Class A, B, C and D ovens, dryers and furnaces. The AADvance system is certified for use with NFPA 86 compliant systems.

The systems should be integrated in accordance with NFPA 86. In particular the following shall be applied.

- The supplier of the application software for the AADvance controller shall provide both the end user and the safety authority having jurisdiction with the documentation needed to verify that all related safety devices and safety logic are functional before the controller is placed in operation.
- In the event of a power failure, the AADvance controller (hardware and software) shall not prevent the system from reverting to a safe default condition. A safe condition shall be maintained upon the restoration of power.
- The control system shall have a separate manual emergency switch, independent of the AADvance controller, which initiates a safe shutdown.
- Any changes to hardware or software shall be documented, approved, and maintained in a file on the site.
- System operation shall be tested and verified for compliance with the NFPA 86 standard and the original design criteria whenever the AADvance controller is replaced, repaired, or updated.
- Whenever application software that contains safety logic or detection logic is modified, system operation shall be verified for compliance with the NFPA 86 standard and the original design criteria.
- The NFPA 86 certification is only applicable where the system is applied in accordance with this safety manual and NFPA 86 requirements.

NFPA 87 Requirements

NFPA 87:2015 provides comprehensive requirements for the safe design, installation, operation, inspection, testing and maintenance of Type F, Type G & Type H fluid heaters & related equipment. The AADvance system is certified for use with NFPA 87 compliant systems.

The systems should be integrated in accordance with NFPA 87. The following shall be applied:

- The supplier of the application software for the AADvance controller shall provide both the end user and the safety authority having jurisdiction with the documentation needed to verify that all related safety devices and safety logic are functional before the controller is placed in operation.
- In the event of a power failure, the AADvance controller (hardware and software) shall not prevent the system from reverting to a safe default condition. A safe condition shall be maintained upon the restoration of power.
- The control system shall have a separate manual emergency switch, independent of the AADvance controller, which initiates a safe shutdown.
- Logic sequences or devices intended to cause a safety shutdown, once initiated, shall require operator action prior to resuming operation of the effected heating system plant.
- Any changes to hardware or software shall be documented, approved, and maintained in a file on the site.

- Application software shall be labelled in order to make the identification and functions readily identifiable. A list of all applications and associated documentation should be available to end users.
- System operation shall be tested and verified for compliance with the NFPA 87 standard and the original design criteria whenever the AADvance controller is replaced, repaired, or updated.
- Whenever application software that contains safety logic or detection logic is modified, system operation shall be verified for compliance with the NFPA 87 standard and the original design criteria.
- The NFPA 87 certification is only applicable where the system is applied in accordance with this safety manual and NFPA 87 requirements.

EN 50156

EN 50156-1:2015 applies to the application design and installation of electrical equipment, control circuits and protective systems for furnaces which are operated with solid, liquid or gaseous fuels and their ancillary equipment. It specifies requirements to meet operating conditions for furnaces, to reduce the hazards of combustion and to protect the heated systems from damage. The AADvance controller is certified for use an EN 50156 compliant systems.

In particular the AADvance controller controls protective devices for:

- monitoring of flames and other safety conditions of the firing
- interrupting the flow of the fuel to the furnace for safety reasons
- ventilating the body of the furnace and the flue gas ducts
- monitoring of safety condition of the heated systems (e.g. water level limiter in steam boilers)

The EN 50156 certification is only applicable where the system is applied in accordance with this safety manual and EN 50156 requirements.

BS EN 54 Requirements

BS EN 54-2:1997 + AC:1999 + A1:2006 specifies the requirements for control and indicating equipment for fire detection and fire alarm systems installed in buildings. The AADvance system is certified for use with BS EN 54 compliant systems.

IMPORTANT The analogue output modules are not certified to EN 54-2.

The systems should be integrated in accordance with BS EN 54. In particular the following shall be applied.

- Where an alphanumeric display is used to display indications relating to different functional conditions these may be displayed at the same time. However, for each functional condition there shall be only one window, in which all of the fields relating to that functional condition are grouped.
- Unless BS EN 54 section 7.11 and/or 7.12 applies, the time taken by scanning, interrogation or other processing of signals from fire detectors, in addition to that required to take the fire alarm decision, shall not delay the indication of the fire alarm condition, or of a new zone in alarm, by more than 10 seconds.

- The control and indicating equipment shall enter the fire alarm condition within 10 seconds of the activation of any manual call point.
- The audible indication shall be capable of being silenced by means of a separate manual control at access level 1 or 2. This control shall only be used for silencing the audible indication, and may be the same as that used for silencing in the fault warning condition.
- The control and indicating equipment shall be capable of being reset from the fire alarm condition. This shall only be possible by means of a separate manual control at BS EN 54 defined access level 2. This control shall be used only for reset and may be the same as that used for reset from the fault warning condition.
- Unless BS EN 54 7.11 and/or 7.12 apply, the control and indicating equipment shall action all mandatory outputs within 3 seconds of the indication of a fire alarm condition.
- Unless BS EN 54 7.11 applies, the control and indicating equipment shall action all mandatory outputs within 10 seconds of the activation of any manual call point.
- The control and indicating equipment shall enter the fault warning condition within 100 seconds of the occurrence of the fault or the reception of a fault signal, or within another time as specified in BS EN 54.
- In the event of the loss of the main power source (as specified in EN 54-4), the control and indicating equipment may have provision to recognize and indicate the failure of the standby power source to a point where it may no longer be possible to fulfill mandatory functions of this European Standard. In this case at least an audible indication shall be given for a period of at least one hour.
- A system fault shall be audibly indicated. This indication may be capable of being silenced.
- The cabinet of the control and indicating equipment shall be of robust construction, consistent with the method of installation recommended in the documentation. It shall meet at least classification IP30 of IEC 60529:1991.
- All mandatory indications shall be visible at access level 1 without prior manual intervention such as the need to open a door.
- If the control and indicating equipment is designed to be used with a power supply (item L of figure 1 of EN 54-1) contained in a separate cabinet, then an interface shall be provided for at least two transmission paths to the power supply, such that a short circuit or an interruption in one does not affect the other.
- The EN 54-2 certification is only applicable where the system is applied in accordance with this safety manual and EN 54-2 requirements.

EN 54 section 7.12 Alarm Signal Dependencies

7.12.1 Type A dependency (option with requirement)

Following the receipt of a first alarm signal from a fire detector, the entry to the fire alarm condition may be inhibited until the receipt of a confirmation alarm signal from the same fire detector, or from a fire detector in the same zone. In this case, the first alarm state need not be indicated, and the following shall apply:

- the mode of operation shall be configurable at access level 3 for individual zones;

- reception of a confirmation alarm shall not be inhibited for more than 60s following the receipt of the first alarm signal. The manufacturer may specify a time shorter than 60 s. In this case, this specification shall be tested and verified;
- the first alarm state shall be automatically canceled within 30 min of the receipt of the first alarm signal;
- information on the values of the configured delay times shall be accessible at access levels 2 or 3.

7.12.2 Type B dependency (option with requirement)

Following the receipt of a first alarm signal from a fire detector, the entry to the fire alarm condition may be inhibited until the receipt of a confirmation alarm signal from the same fire detector, or from a fire detector in the same or a different zone. In this case, the first alarm state need not be indicated, and the following shall apply:

- the mode of operation shall be configurable at access level 3 for at least individual zones;
- the first alarm state shall be indicated by means of:
  - an audible indication as in 12.10 which may be the same as that in the fire alarm condition or fault warning condition;
  - a visible indication of effected zone, which may be the same as that for indication of zone in alarm as in 7.3. The general fire alarm indicator shall not be illuminated;
- it shall be possible to manually cancel the first alarm state at access level 2. This may be done with the same control as is used for reset from the fire alarm condition or fault warning condition;
  - the Control and Indicating Equipment (CIE) may have provision to automatically cancel the first alarm state after a time interval which shall not be less than 5 min;
  - if the mode of operation is configured to accept a confirmation alarm signal from the same fire detector, this shall not be inhibited for more than 4 min following the receipt of the first alarm signal.

Type C dependency (option with requirement)

Following the receipt of a fire alarm signal from a fire detector or a manual call point, the CIE shall enter the fire alarm condition, but may have provision to inhibit the activation of outputs until a second alarm signal is received from another fire detector or manual call point, which may be the same or another zone. In this case it shall be possible to configure the mode of operation at access level 3 to apply individually to each of the following (where provided):

- output to fire alarm devices
- output to fire alarm routing equipment
- output to fire protection equipment

UL 508

This standard defines the Safety Requirements for Industrial Control Equipment. It covers systems utilizing a programmable memory for storage of user-oriented instructions for specific functions such as logic, sequencing, counting and controlling various industrial equipment through digital or analog inputs or outputs.

The UL standards can also be used to investigate equipment for use in hazardous locations such as:

- The possible presence of an explosive atmosphere such as flammable gas, vapors or liquids (Class I), combustible dusts (Class II) or ignitable fibers (Class III); the likelihood that the explosive atmosphere is present when equipment is operating; or the ignition-related properties of the explosive atmosphere that is present.
- An area may also be considered "hazardous" for other reasons, such as the use of electrical equipment in the vicinity of water, the risk of personal injury from moving or falling parts, or even the presence of biological hazards.
- This approach to classifying hazardous locations is used by the United States (National Electrical Code), Canada (Canadian Electrical Code), Europe (CENELEC EN 60079-10) and throughout the world (IEC 60079-10).
- While hazards are associated with all of these conditions, areas are only considered hazardous (classified) locations under definitions defined by the NEC, CEC, IEC 60079-10, or CENELEC EN 60079-10, as applicable.

The AADvance controller has been investigated and approved by UL for use as Industrial Control Equipment in a general industrial environment and for use in hazardous locations, Class I, Division 2, Groups A, B, C and D.

Field Configurations

The following are recommended field loop circuits for line monitoring of digital/analogue inputs.

⚠ **ATTENTION:** Use cable monitoring and circuit integrity cable as appropriate for the application, as inter-channel short circuits cannot be detected by an AADvance controller.

Line Monitoring

This section provides recommended line monitoring circuits and resistor values. You can set-up line monitoring on the following modules:

- T9401 and T9402 Digital Input Modules
- T9431 and T9432 Analogue Input Modules

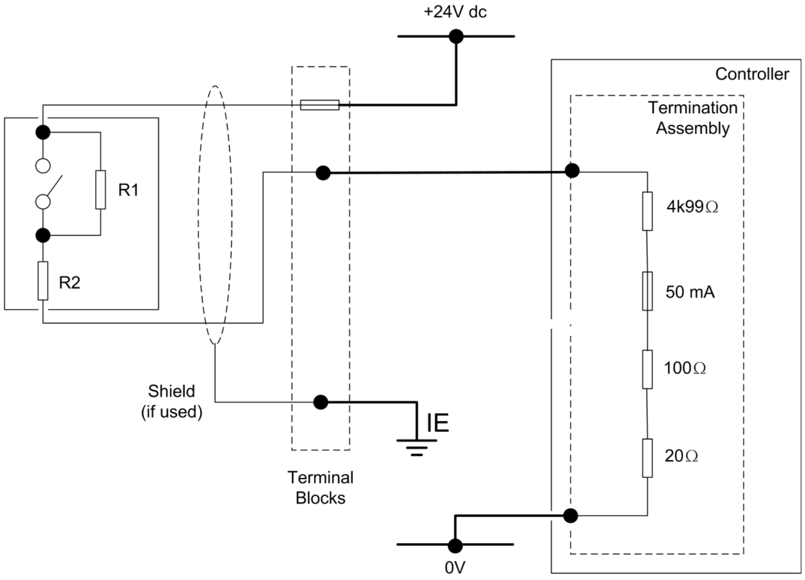
NOTE You must ensure that there is no crossover between channels.

Digital Input Field Loop Circuits

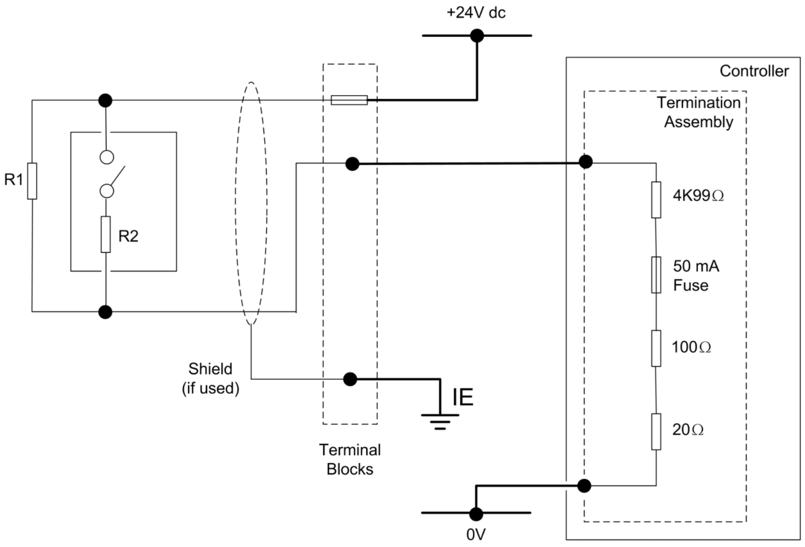
Recommended Field Loop Circuits

This section contains recommended field loop circuits for line monitoring digital inputs used in Emergency Shutdown or Fire & Gas applications.

Field Loop Circuit for Digital Input



Field Loop Circuit for Line Monitored Digital Input for Emergency Shutdown Systems (ESD)



The suggested values for R1 and R2 are as follows:

R1 = 15K Ω 1%, 1W (maximum power dissipated is 47mW at 26.4V)

R2 = 3K9 Ω 1%, 1W (maximum power dissipated is 182mW at 26.4V)

Suggested range of values for both of the above circuits are as follows:

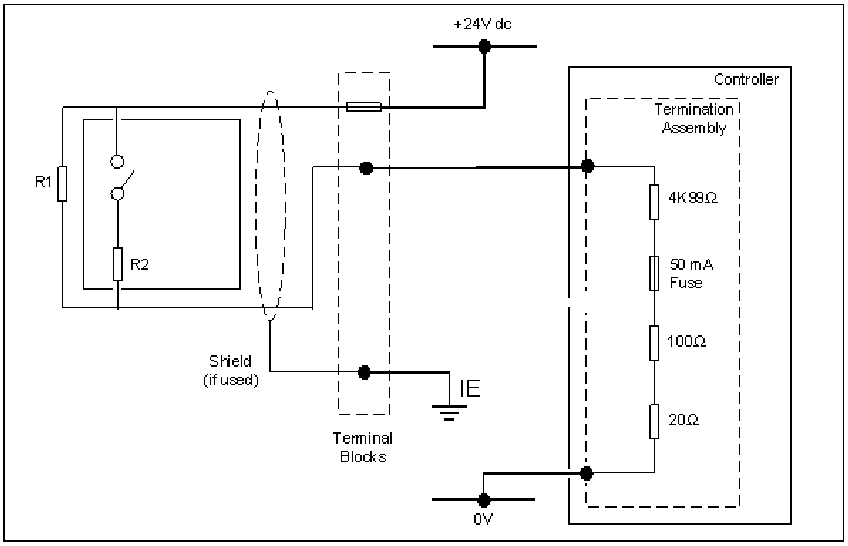
Range		Value (mV)
Maximum Allowed	=	32000
		SHORT CIRCUIT
High	=	19000
Low	=	18500
		ON (nominal 16V)
High	=	11000

Range		**Value (mV)**
Low	=	10500
		INDETERMINATE
High	=	6500
Low	=	6000
		OFF (nominal 8V)
High	=	3500
Low	=	3000
		OPEN CIRCUIT

Assumptions:

- Loop supply voltage = 24V ± 10%
- Maximum Field Cable Line Resistance: < 100 Ω total; this means < 50 + 50 Ω for the two cables.
- Minimum Isolation is 0.75M Ω between the field loop conductors.
- These values will allow the input to detect more accurately different voltage levels that represent OPEN CCT - OFF - ON - SHORT CCT and will also detect Over Voltage and an input which is neither ON nor OFF. The values verify that a line fault will be declared before it becomes possible for a false declaration of On and Off states due to a combination of resistor value drift and loop voltage variation.

Field Loop Circuit for Line Monitored Digital Input for Fire and Gas Systems (F & G)



- The F&G circuit will also allow two devices to be in alarm without reporting short circuit.
- All of the input circuits are suitable for simplex, dual and TMR configurations.
- The F&G circuit assumes that the devices are volt-free contacts.
- For further information, please refer to application note AN-T90001 Field Loop Configuration, which is located in the Rockwell Automation Knowledgebase Support Center. This also includes advice for fire detectors which are not simple volt free contacts.

Recommended Field Circuit for Digital Outputs

This circuit is suitable for simplex and dual configurations of digital output modules. The two 10A fuses shown are included on the termination assembly within the controller. The field power 5A fuses comply with UL 508 requirements see illustration below.

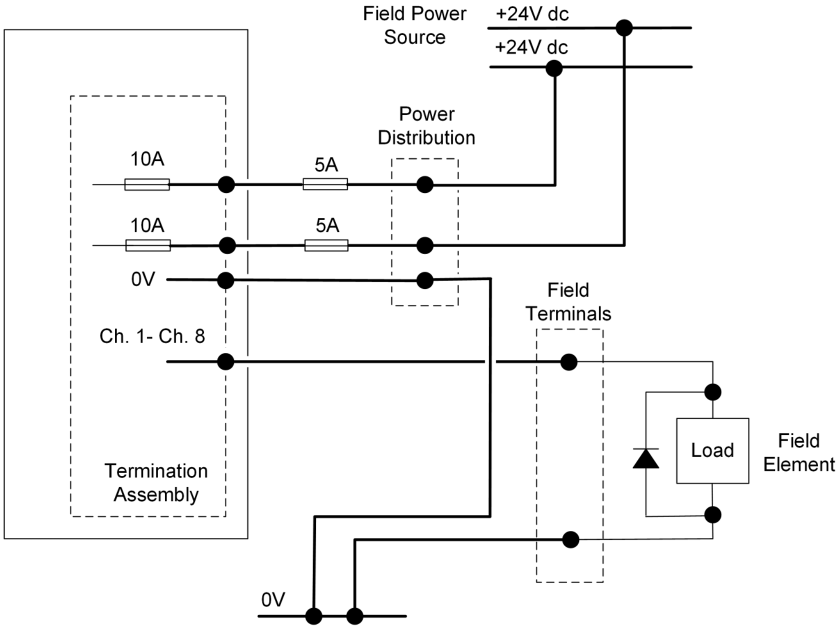
The 10A fuses are fitted into the termination assembly and are:

- T9902: SMF Omni-Block, Surface Mount Fuse Block 154 010, with a 10A, 125V Fast Acting Fuse, Littelfuse.

The field power input fuses are 5 A / 125 V, Slow Blow and comply to UL 248 - 14.

NOTE

1. Alternatively instead of fitting two 5A fuses you can use Class 2 power supplies for the +24V dc field voltage. Class 2 is defined by the NEC as providing less than 100 watts (at 24V).
2. The field power must be wired using 12 AWG wire.
3. The field power must be supplied with an isolating source.
4. The minimum current required for line monitoring is 20mA for a dual pair.



ATTENTION: For inductive loads, a back EMF protection diode shall be fitted at the load.

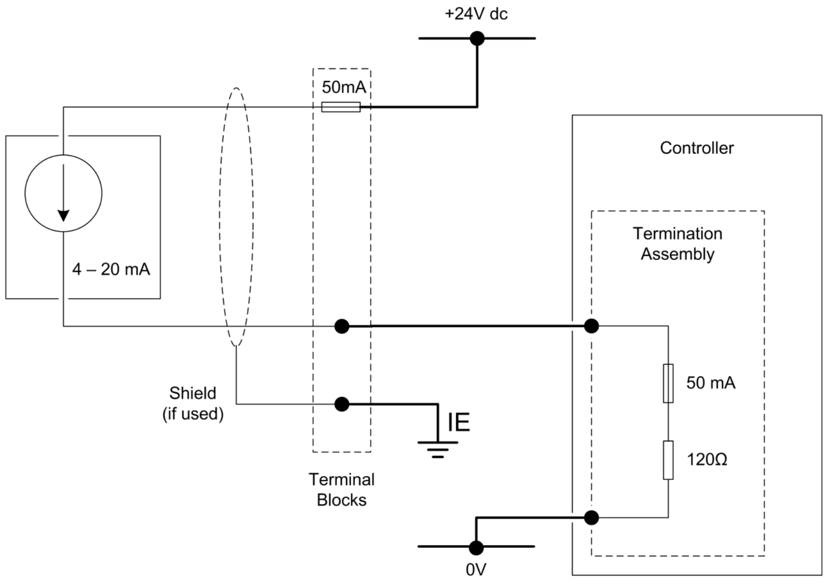
NOTE For details of how the AADvance digital output module detects field faults, see Knowledgebase Document ID: QA23147 AADvance/ bulletin 1715: Digital output channel diagnostic test.

Sign in to your Rockwell Automation account to view Knowledgebase articles.

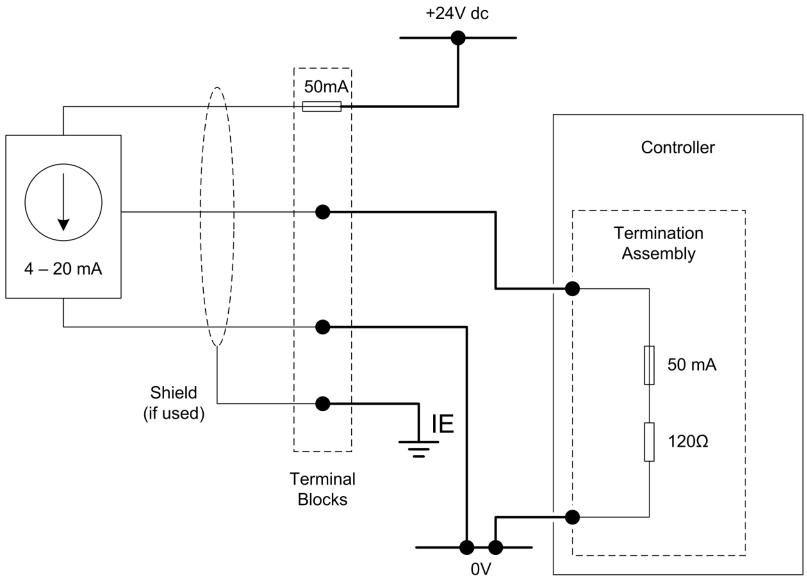
Analogue Input Field Loop Circuits

The recommended field loop circuits for analogue inputs are as shown below.

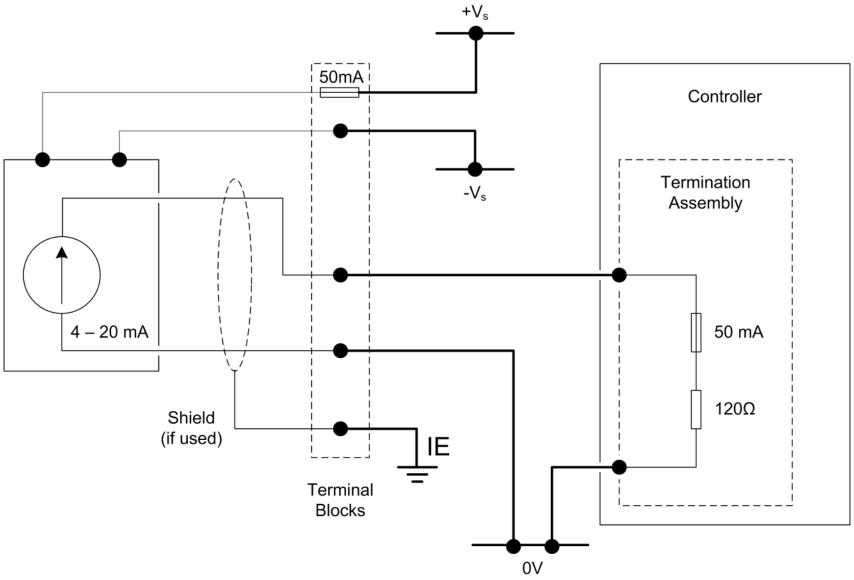
Field Loop Circuit for 2-Wire Analogue Input



Field Loop Circuit for 3-Wire Analogue Input



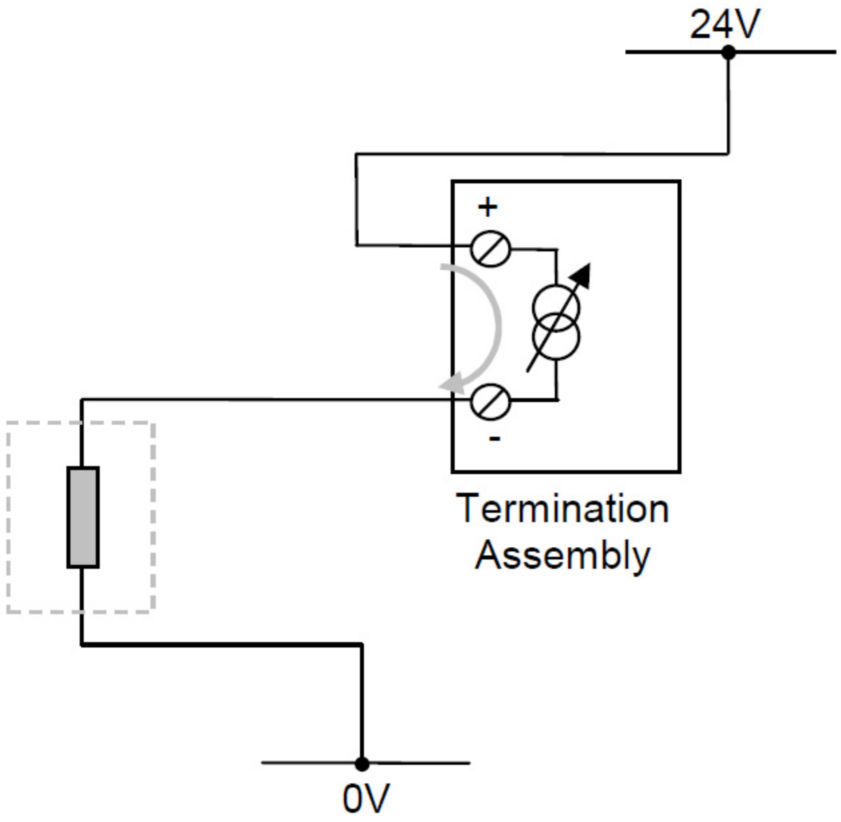
Field Loop Circuit for 4-Wire Analogue Input



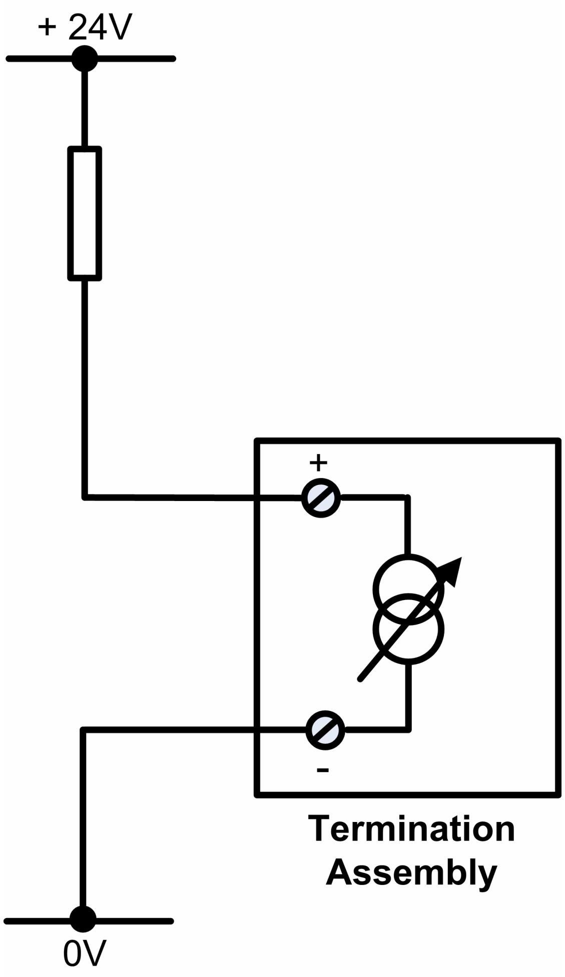
Recommended Circuit for Analogue Outputs

These circuits are suitable for simplex and dual configurations of analogue output modules. All channels are isolated from each other but may be bridged at the '+' terminal if fed by a common system mounted supply.

System powered devices

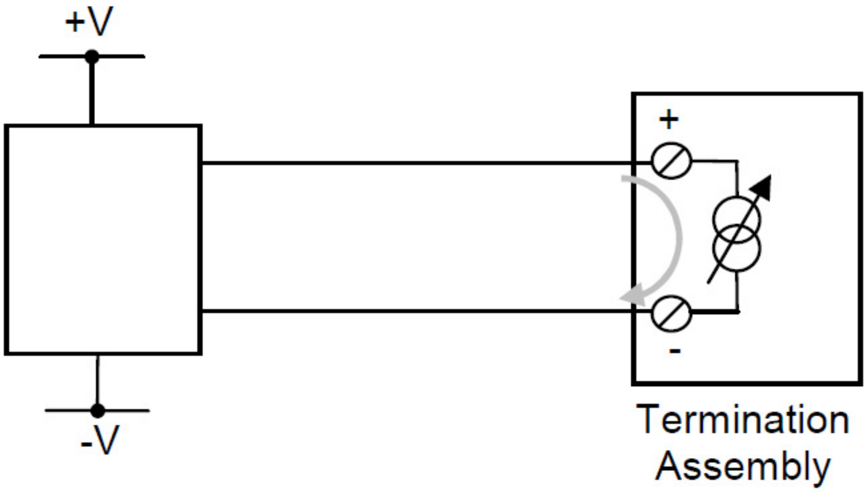


The above circuit is appropriate for devices that are powered by the system. The channel will pass a requested current between 0mA and 24mA. The field device could also be connected between the 24V supply and the Loop Plus terminal.



NOTE If the 0V or 24V supply is shared between channels or between modules, the field loops will not be isolated from each other.

Field powered devices



The above circuit is appropriate for devices that are powered locally and expect a current-controlled signal loop. Ensure that the loop is wired to pass current to the Loop Plus terminal and return it on the Loop Minus terminal.

Sensor Configurations

ATTENTION: In safety critical input applications using a single sensor, it is important that the sensor failure modes be predictable and well understood, so there is little probability of a failed sensor not responding to a critical process condition. In such a configuration, it is important the sensor be tested regularly, either by dynamic process conditions that are verified in the AADvance system, or by manual intervention testing.

The function of a signal shall be considered when allocating the module and channel within the system. In many cases, redundant sensor and actuator configurations may be used, or differing sensor and actuator types provide alternate detection and control possibilities. Plant facilities frequently have related signals such as start, and stop signals. In these cases it is important to ensure that failures beyond the system's fault-tolerant capability do not result in either inability to respond safely or in inadvertent operation. In some cases, this will require that channels be allocated on the same module, to verify that a module failure results in the associated signals failing-safe.

Sensor configurations should be considered. In most cases it will be necessary to separate the signals across modules. Where non-redundant configurations are employed, it is especially important to ensure that the fail-safe action is generated in case of failures within the system.

Field loop power should be considered in the allocation of signals to input channels and modules. For normally energized input configurations, field loop power failure will lead to the fail-safe reaction. As with the allocation of signals to modules, there may be related functions (for example start and stop signals) where loss of field power should be considered in the same manner as the signal allocation.

HART

The AADvance controller supports HART communications using dedicated HART modems on each analogue input and output channels allowing HART field device status, diagnostic data and process signal data to be integrated into the application logic, increasing the level SIF diagnostics significantly. The AADvance Analogue Input/Output modules use HART commands #03 to collect data from the field device as defined by Revision 5 of the HART specification.

The extra data available from HART enabled field devices is reported to the application in custom data structures.

The T9K_AI_HART and T9K_AI_HART_FULL structures provide the following information:

- Current in milliamps
- process measurement in engineering units
- errors on HART communication seen by device

- status of the field device
- time in milliseconds since the last update.

Typical uses of this data are:

- To compare the measured process value from the Analogue input channel with the process variable value transmitted over HART from the field device to detect discrepancies.
- To monitor the field device status and report device status and report diagnostic errors or manual configuration changes

NOTE The update rate for HART data from field devices is significantly slower than the update rate for the 4-20mA analogue signal itself, HART data may take up to 4 seconds to update, depending on the device type and configuration.

Precautions for HART in a Safety System

If using HART in a safety system, follow these precautionary guidelines:

ATTENTION: HART data shall not be used as the primary process value for Safety Functions as the HART protocol does not meet the required integrity levels for Safety Instrumented Functions.

ATTENTION: HART Pass-Through should be disabled if the field devices do not have locked configuration, or if the device status is not monitored and alarmed to help prevent accidental or unauthorized changes to field device configuration.

ATTENTION: HART devices have custom data which is provided in response to HART command #03, the specific data for each device type must be used in accordance with the device manufacturers published recommendations.

HART Pass-Through

AADvance also supports a HART Pass-Through feature. This gives AADvance the ability to pass HART data between an external Asset Management System (AMS) and Field Devices. This is strictly a pass-through mechanism using a dedicated AADvance HART DTM. This pass-through capability can however be enabled or disabled under application control.

ATTENTION: If HART Pass-Through is enabled on a safety loop, then either the field device shall have the facility to lock the configuration on the field device itself or the HART Pass-Through function shall be disabled by the application program during normal operation when HART communication is not required.

ATTENTION: The device status must be monitored and alarmed if HART Pass-Through is enabled.

ATTENTION: The software package used to monitor and configure the field device using HART Pass-Through shall be evaluated to ensure that it is suitable for use with safety devices.

Actuator Configurations

In safety critical applications using a single actuator, it is important that the actuator failure modes be predictable and well understood, so that there is little probability of a failed actuator not responding to a critical process condition.

In such a configuration, it is important that the actuator be tested regularly, either by dynamic process conditions that are verified in the AADvance system, or by manual intervention testing.

The function of a signal shall be considered when allocating the module and channel within the system. In many cases, redundant actuator configurations may be used, or differing actuator types can provide alternate control and mitigation possibilities. Plant facilities frequently have related signals; in these cases it is important to ensure that failures beyond the system's fault-tolerant capability do not result in either an inability to respond to safety demands or in inadvertent operation.

In some cases, this will require that channels be allocated on the same module, to verify that a module failure results in the associated signals failing-safe. However, in most cases, it will be necessary to separate the signals across modules. Where non-redundant configurations are employed, it is especially important to ensure that the fail-safe action is generated in case of failures within the system.

Field loop power should be considered in the allocation of signals to output channels and modules. For normally energized configurations, field loop power failure will lead to the fail-safe reaction. As with the allocation of signals to modules, there may be related functions where loss of field power should be considered in the same manner as the signal allocation. Where signals are powered from separate power groups, it is important that this separation be maintained when allocating the signals to modules, i.e. that inadvertent coupling between power groups, and particularly return paths, are not generated.

Calculations of Probability of Failure upon Demand,

For information regarding the calculation and for PFD/PFH numbers allocated for the AADvance system refer to the approved PFD calculation document (Publication No: ICSTT-RM449 AADvance PFH and PFD_{avg} Data) listed in the approved version list.

Processor Functional Safety Configuration

The T9110 Processor Module supports a limited set of configuration options; the system will verify the hardware configuration, such as the module locations against actual module types.

The processor module process safety time can be specified through the AADvance Workbench software or AADvance-Trusted SIS Workstation software and details are given in the appropriate AADvance Configuration Guide(s), publications ICSTT-RM405 and ICSTT-RM458, or AADvance-Trusted SIS Workstation Software User Guide, publication ICSTT-UM002.

Processor Safety Functions

The processor module is classified as safety critical and is responsible for the following safety functions:

- solving application logic
- external communication (Ethernet and serial)
- communication with I/O modules such as receiving input values, sending output values, coordinating diagnostics
- enforcement of system PST
- diagnostics, fault indications and degradation of the processor module
- enforcement of input PST
- diagnostics, fault indications and degradation of input modules
- initiating diagnostics, fault declaration and for some fault conditions the degradation of output modules
- recovery mode operation

Reaction to faults in the processor module

The processor module reports faults by front panel indicators and fault codes stored in the System Event log. **SYSTEM HEALTHY** and **HEALTHY** LEDs go RED when a fault is detected in the processor module. Fault indications are also sent to the user application by variables that you can set up during the system configuration process. These variables provide the following information:

- module presence
- module health and status
- channel health and status
- an echo of the front panel indications

For a single fault deemed by the system to be a "critical failure" the processor module enters the Recovery Mode.

Recovery Mode

Recovery Mode is a shutdown mode and uses a base level firmware. It is entered automatically when a critical firmware failure occurs or it can be entered manually by either pressing the processor **Fault Reset** button or by enabling the remote fault/reset join feature immediately after the module has booted up.

As an alternative firmware version it allows the following maintenance activities:

- Update the firmware using the **ControlFLASH**™ utility

- Program the processor IP Address with the AADvance Discover utility
- Extract diagnostic information

In Recovery Mode the **Ready**, **Run**, **Force** and **Aux** LEDs go Amber and the **Healthy** and **System Healthy** LEDs stay Green. The System Healthy and Healthy LEDs may go Red if a fault is detected while in the Recovery Mode.

NOTE When in Recovery Mode the I/O communications are disabled and the Application code is not running.

Processor Module Locking Screw safety Function

The module **locking screw** acts as a module retaining device and also as a switch that controls the module's operation. For the module to be fully operational the locking screw must be turned to the locked position. If the screw is turned to the unlocked position when a module is operational it will initiate a fault indication and the module will become non-operational.

Processor modules can be replaced or installed on-line without affecting the controller operation provided at least one is fitted and is fully operational. However, each module must be installed one at a time and allowed to educate before the next module is installed.

Processor Module Access Port

The front panel of the T9110 Processor Module has a concealed PS/2 style connector on the front panel behind a plastic cover. This connector is for Rockwell Automation use only and is used for factory settings during manufacturing. However, the plastic cover can be removed to replace the processor battery.

I/O Module Safety Functions

This section describes the I/O safety parameters.

I/O Module Safety Related Parameters

The AADvance Workbench software and AADvance-Trusted SIS Workstation software provide you with the capability to adjust these safety related parameters for an I/O module:

- Process safety time
- Shutdown action of a digital output module channel
- Fail-safe guard for the Analogue Output Module
- Shutdown action for the Analogue Output module

I/O Module Start-Up and Locking Screw Safety Function

I/O modules can be replaced or installed on-line without affecting the controller operation provided at least one is fitted in a dual/triple Termination Assembly and is fully operational. However, each module must be installed one at a time and allowed to educate before the next module is installed.

The module **locking screw** acts as a retaining device and also as a switch that controls the module's operational status. For the module to be fully operational the locking screw must be in the locked position.

When the first I/O module is installed and the locking screw set to the lock position, the startup and education process begins automatically. When the locking screw is set to the unlocked position then the module will switch off and the following indications will be displayed:

Status Indicator	Colors
Healthy	GREEN
Ready	GREEN ➔ OFF
Run	GREEN ➔ RED
Channels 1 to 8 or 1 to 16	OFF

NOTE If the above indications are not present when the locking screw is set to the unlocked position refer to the Troubleshooting and Repair Manual.

I/O Module Process Safety Time (PST)

This option allows the system integrator to configure the PST for an I/O module, independently from the system value set through the processor module. If no independent value is set for the module it will adopt, by default, the top level value of PST set for the processor module. When an input module exceeds the PST, (that is, the controller does not receive an update from the I/O module within the PST) then the I/O module is set to a fail safe state and returns safe values to the controller (refer to the topic - Input Modules Safety Accuracy).

Digital/Analogue output module PST

For a digital/analogue output module the PST represents the period of a watchdog timer that specifies the length of time the controller will allow the module to run without receiving updates from the application. If the module runs beyond this time without receiving any updates, it enters its shutdown state. The default PST is 2500 ms.

Protective ability and versatility of the input module

An input module is classified as safety critical and is designed to SIL 3 level as a single fail safe module. The input modules offer 8 or 16 isolated channels and reports input voltage levels to the processor, for the analogue input variant the

module will convert the field current into a voltage. Input values are updated at least once per application cycle. The same hardware is used for the 24 Vdc digital input modules and the
4-20 mA analogue input module.

I/O modules can be replaced or installed on-line without affecting the controller operation provided at least one is fitted and is fully operational. However, each successive module must be installed and allowed to educate before the installation of the next module.

The input module can be configured to operate in SIL 2 or SIL 3 configurations for energize to action and de-energize to trip applications. The module provides the following isolation:

- channel to channel galvanic isolation
- galvanic isolation between channels and the communication signals
- galvanic isolation between channels and power
- locking screw operational function

Reactions to faults in the input modules

When an input channel is not capable of reporting a voltage within the safety accuracy specified for the module, then the module returns safe values to the processor. Signals go to a safe state if the module scan time exceeds the PST (refer to "Input Module Safety Accuracy" for safe state details). All I/O modules provide front panel indications, store fault codes in the fault log and can also report via the AADvance Workbench software or AADvance-Trusted SIS Workstation software application variables. The following status information is provided:

- module presence
- module health and status
- channel health and status
- field faults
- an echo of the front panel indicators for each module

Availability of input modules

Input modules support redundancy when configured for dual or triple operation using the appropriate termination assembly. Redundant input modules may be inserted or removed at any time without any impact on the safety function of the system. Redundant input modules operate independently providing independent values of the input values to the processor module.

Termination Assemblies

The termination assemblies are safety critical and provide termination for 16 channels. They connect the field signals to the input modules. The simplex version connects each input channel to one input module, the dual TA routes them to two input modules and the triple TA to three input modules.

Digital and analogue input TA circuits both have fuse protection and a high reliability input load for each channel.

Input Module Safety Accuracy

The input modules determine the channel state and the line fault state by comparing the input reported values with user programmed threshold values. When triple analogue input modules are used and active, the system adopts the median value. When dual modules are used, the lowest reported value is used. The discrepancy between the redundant channels' measurements are monitored to determine if they are within the safety accuracy limit.

When the safety accuracy within a channel is detected outside the following limits then that channel is set to a fail-safe state.

- Digital Input Module = 1 v
- Analogue Input Module = 0.2 mA

When the safety accuracy between channels exceeds the following limits then a discrepancy alarm is set for the input channel

- Digital Input Module = 2 v
- Analogue Input Module = 0.4 mA

In both situations the following safe values are reported by the variables:

Digital input modules

- Input state FALSE
- Line fault TRUE
- Discrepancy TRUE
- Channel fault TRUE
- and the voltage value is 0mV

Analogue input module

- process value = a calculated value based on a count value of 0 (51 counts = 0.2mA) (PV)
- line fault TRUE
- Discrepancy TRUE
- Channel Fault TRUE
- Count value 0 (Raw Count)
- State

ATTENTION: In safety critical applications, the discrepancy alarms shall be monitored by the application program and be used to provide an alarm to the plant operations personnel.

Output Module Safety Functions

Digital Output Module Safety Functions

The digital output module is rated at SIL 3 as a fail-safe module. In dual redundant configurations it can be used for energize to action and de-energize to trip SIL 3 applications. Each module provides the following safety functions:

- output channel signals based on commands from the processor.
- redundant voltage and current measurements to the processor modules for monitoring and diagnostics.
- over current and over voltage channel protection.
- executing diagnostic tests (on command from the processor module) and reporting results back to the processor module.
- On power up or module insertion all output channels are set to the de-energized (fail-safe) state until command states are received from the processor. Each channel is driven individually according to the command state values.
- When the module is unlocked, all of its output channels (including any channels set to hold last state) always go to the de-energized state.
- the module enters a Shutdown Mode when the time between processor commands exceeds the PST.
- The PFH & PFD_{avg} data has been calculated on the basis that the shutdown state is configured to the OFF state. Therefore the OFF state shall be used for SIL 2 & SIL 3 applications.
- When a module fails then all the channels are set to the de-energized state.

Reactions to faults in output modules

When an output module goes faulty the following status information is reported:

- module presence
- module health and status
- channel health and status
- field faults
- an echo of the front panel indicators for each module

When any of the following internal conditions exist the output module will fail-safe:

- power feed combiner over temperature detection
- power supply rails out of tolerance

Process safety time faults

For a digital output module, the process safety time represents the period of a watchdog timer that specifies the length of time the controller will allow the module to run without receiving updates from the application. If the module runs beyond this time period without receiving any updates, it enters the Shutdown Mode.

Shutdown Mode

When in the Shutdown mode the Ready and Run indicators will go RED. You can configure the state of the outputs when the module is in the Shutdown Mode. You have to decide when you configure the module how you want the output channels to behave in the Shutdown mode. The output modules can be configured to provide the following channel values:

- De-energized (Off default fail-safe value)
- Hold Last State

ATTENTION: Careful consideration should be given to the affect on the process of using the 'hold last state' setting. The PFH & PFDavg data has been calculated on the basis that the shutdown state is configured to the OFF state. Therefore the OFF state shall be used for SIL 2 and SIL 3.

An installed module automatically transitions from the Shutdown mode to the Ready or Recover modes and hence to the Run mode when the RESET button on the processor is pressed and the application is running.

The following conditions will also cause a module to enter the Shutdown mode from the Ready, Recover or Run modes:

- Stopping the application for any reason
- Invalid calibration - the module will not be able to transition out of the Shutdown mode until the module has been re-calibrated (module calibration interval recommendation is describe in the Preventive Maintenance Schedule, Chapter 2 of The Troubleshooting and Maintenance manual; ICSTT- RM406-EN-P.

Disable line test

The digital output module incorporates line test functionality that can report and indicate 'no load' field faults. This functionality can be enabled or disabled. The settings are:

- **Yes** - disables reporting and indication of 'no load' field faults
- **No** - 'No load' field faults are reported and indicated

Availability of output modules

Output modules support redundancy when configured in dual operation using the appropriate termination assembly. One redundant module may be inserted or removed at any time without any impact on the safety function of the system.

DO Termination assembly

The DO termination assembly is safety critical, it comes in two sizes — simplex or dual. It has fuses for field output power and 8 field termination connections for the output signals.

Analogue Output Module Safety Features

Analogue Output Module Safety Applications

The Analogue Output Module can be used in the following safety related applications:

- The fail-safe state current of the analogue output module is less than 2mA.
- For energize to action high demand applications you must use dual analogue output modules.
- When the module is unlocked, all of its output channels (including any channels set to hold last state) always go to the de-energized state.

Analogue Output Module Safety Functions

The Analogue output Module is rated at SIL 3 as a fail-safe simplex module. And 1oo2D as a dual module. For high demand SIL 2 energize to action high demand applications you must use dual analogue output modules. This arrangement is also rated as SIL 3 for energize to action applications. Each module provides the following safety functions:

- Commanded Values and Scaling Factor (Command State)
- Fail-safe Guard Band
- Shutdown
- Module Status
- Diagnostics

Commanded Values and Scaling Factor

- User configurable value.
- The application cannot change the scaling factor; it can only be changed by an on-line update.

Fail-Safe Guard

- User configurable value.
- Fail-safe guard is user configurable and cannot be changed by the application; it can only be changed by an on-line update.
- The default value is 1% (0.2mA).

Shutdown

When in the Shutdown mode the Ready and Run indicators will go RED. You can configure the state of the outputs when the module is in the Shutdown Mode. You have to decide when you configure the module how you want the output channels to behave in the Shutdown mode. The output modules can be configured to provide the following channel values:

- De-energized (Off default fail-safe value)
- Custom shutdown value
- Hold Last State

ATTENTION: Careful consideration should be given to the affect on the process of using the ‘custom shutdown value’ or the 'hold last state' setting. The PFH & PFDavg data has been calculated on the basis that the shutdown state is configured to the OFF state. Therefore the OFF state shall be used for SIL 2 and SIL 3.

Reactions to faults in output modules

When an output module goes faulty the following status information is reported:

- module presence
- module health and status
- channel health and status
- field faults
- an echo of the front panel indicators for each module

When any of the following internal conditions exist the output module will fail-safe:

- internal software error detected by the FPGA
- power feed combiner over temperature detection

Input and Output Forcing

The AADvance Workbench software and AADvance-Trusted SIS Workstation software support forcing of individual inputs and outputs. The AADvance Workbench software and AADvance-Trusted SIS Workstation software use the term 'locking' to describe forcing.

ATTENTION: It is important the implications of forcing (or locking) of input and output points on the process and their impact on safety are understood by any person using these facilities. It is the plant operators' responsibility to ensure that if forced conditions are present that they do not jeopardize the functional safety.

Forcing requires the program enable key to be fitted to the 9100 Processor Base Unit and is intended only for the purposes of engineering, installation and commissioning activities. When the system is in-service, maintenance overrides for safety-related inputs and outputs should be implemented using the application program instead.

The Force LED on the front of the T9110 Processor Module indicates when one or more I/O points are forced. The application program can determine how many points are currently forced; it is highly recommended that this information be used to control an additional status display and/or for logging purposes.

ATTENTION: If the forcing facility is used when the system is in-service, a safety related input connected to an operator accessible switch shall be implemented to initiate the removal of the force condition.

A list of the currently locked points is read back from the AADvance system and made available within the AADvance Workbench software or AADvance-Trusted SIS Workstation software.

Maintenance Overrides

Maintenance Overrides set inputs or outputs to a defined state that can be different from the real state during safety operation. It is used during maintenance, usually to override input or output conditions in order to perform a periodic test, calibration or repair of a module, sensor or actuator.

To correctly implement a maintenance override scheme within the AADvance system, the override or 'bypass' logic shall be programmed within the Application Program, with a separate set of safety-related input points or variables enabling the bypass logic.

There are two basic methods to check safety-related peripherals connected to the AADvance system:

- External hard-wired switches are connected to conventional system inputs. These inputs are used to deactivate sensors and actuators during maintenance. The maintenance condition is handled as part of the system's application program.

- Sensors and actuators are electrically switched off during maintenance and are checked manually.

In some installations, the maintenance console may be integrated with the operator display, or maintenance may be covered by other strategies. In such installations, the guidance given in section “Input and Output Forcing” is to be followed. A checklist for the application of overrides is given in the Checklists chapter.

Application Program Development

The application program development shall follow a structured approach as defined in the AADvance Workbench software or AADvance-Trusted SIS Workstation software documentation.

ATTENTION: Development of application software consisting of program organization units (POUs), user-defined functions and user-defined function blocks must follow the requirements defined in IEC 61511 (ANSI ISA-84.00.01) for LVL languages and the requirements defined in IEC 61508 for FVL languages.

However, these requirements can be waived if the program organization units (POUs) used have previously been tested and validated according to IEC 61511 (ANSI ISA-84.00.01)/IEC 61508 and validation evidence is provided as part of the Project Test Documentation.

The stages defined in the following sub-sections shall additionally be applied for safety related applications.

AADvance Application Security

For project security, you can set access control using a password for projects, controllers, programs, libraries, and library functions and function blocks. Password definitions are limited to eight characters and can consist of letters and digits. When projects are password-protected, they cannot be opened for editing. Project sub-elements, can have their own level of access control. For example, a program having its own password remains locked and cannot be modified without entering its password.

ATTENTION: Appropriate security protection shall be implemented to help prevent access/change to the application programs. A Program Enable key that is inserted into the (KEY) socket on the T9000 processor base unit can be removed and help prevent access/change to the application program. The Controller is also able to hold a “Target Password”, which may be set to protect the following actions:

- Stopping the application from the debugger (connected mode)
- Downloading an application
- Online updating of an application
- Locking a variable
- Forcing a variable value

For further information see Knowledgebase Document ID: QA24038 AADvance: Target Password protects system against program changes.

Sign in to your Rockwell Automation account to view Knowledgebase articles.

Language Selection

The AADvance Workbench software and AADvance-Trusted SIS Workstation software offer many programming tools to develop algorithms to meet the needs of virtually any real-time control application. The configuration and programming languages approved for use in SIL 3 safety related application are shown below.

- Function Block Diagram (FBD)
- Instruction List (IL) (AADvance Workbench version 1.4 only)
- Structured Text (ST)
- Ladder Diagrams (LD)
- Sequential Function Chart (SFC) (AADvance Workbench version 1.4 only)

Safety Related Languages

The AADvance controller supports a comprehensive set of certified functions. The certified function set includes the most commonly used functions. These tested functions may be used freely in the development of an application. Further functions may be used subject to completion of testing commensurate with the level used for the commonly used function

ATTENTION: IL (AADvance Workbench version 1.4 only) and ST include program flow control functions; these functions shall be used with caution to verify that infinite loop or omitted logic conditions do not result. Where these constructs are used, it is recommended that full branch and data coverage tests be performed on these sections of program. It is recommended that only Boolean conditions be used for these constructs to verify that a feasible set of tests can be applied.

ATTENTION: Application programmer generated function blocks may be created either on a project specific or library basis. Where these functions are to be used for safety-related applications, they shall be subject to exhaustive testing, commensurate with that used for the commonly used functions. Once the function block has been subject to this level of testing it may be used as for commonly used functions.

Sequential Function Chart

The SFC programming language cannot be used with the Compiler Verification Tool (CVT) enabled and is therefore not suitable for use in a safety related system.

It may be possible for an SFC application developed using an earlier version of the software to be used in a safety related system, provided that they have been tested and validated previously. It is the end user’s responsibility to ensure that validation evidence exists in the Project Test Documentation.

Testing of New or Previously Untested Functions

Each safety-related software block shall be 100% testable, such functions could be:

Burner flame supervision including temperature and air/gas pressure monitoring

- Burner gas-to-air ratio control/supervision
- Parts or whole of the start-up sequence of a batch reactor

The fewer the number of inputs, outputs and signal paths, the fewer the number of permutations that require testing. However, a single safety function should not be split into separate blocks; such a division is likely to lead to the introduction of errors during maintenance activities.

The interaction between the individual software blocks shall be minimized. Where interaction is necessary, it should be kept as simple as possible, for example a single shutdown initiation signal.

Each safety function shall be responsible for the control of the corresponding outputs. Sharing of outputs between functions shall not be permitted.

⚠ **ATTENTION:** The use of these function blocks in a safety certified system is only permitted once they have been tested for correct operation.

The new or previously untested function may be:

- a standard function block, included with the software, but has not previously been subject to the level of testing defined herein, or
- a user-defined function block, which is written to meet the needs of a particular feature within an application program, and may comprise a number of generic function blocks or other program functions.

Individual Safety Related Functions

The AADvance Workbench software and AADvance-Trusted SIS Workstation software allow definition of up to 65,536 program organization units (POUs) in a project. This facility should be exploited to enable the allocation of individual safety related functions to separate programs. Where such programs contain independent logic paths, these should be investigated to determine if they are separate safety functions. Where they are separate, it is recommended that these be further allocated to their own program, subject to conforming to the recommendation to minimizing the coupling between programs.

Cases should be looked for that allow the creation of individual logic paths by repeating small sections of logic rather than fanning out the resultant signal(s).

Partitioning the Application

It is impractical and unnecessary to apply the same degree of rigorous development and testing to all functions within the Application where some of those functions are not safety related.

The identification of safety functions is, in part, dependent on the specific safety philosophy. Examples of non-safety may include status indication, data reporting and sequence of events. It is important to establish that these elements are not safety related. For example, some safety cases rely on human intervention and therefore the correct operation of status indication.

ATTENTION: The safety related elements shall be implemented within separate programs to those of non-safety related elements. Where information passes between these elements, it shall be arranged that the direction of flow is from safety relevant to non-safety relevant only.

Defensive Measures

In defining the Application the programmer must consider the potential sources of error and apply reasonable defensive programming techniques. Where values are received from other programs or external communications interfaces, the validity of the values should be checked where possible. Similarly, values received from input interfaces should be checked where possible. In many cases, it will also be possible to monitor permutations of data, inputs and plant operating modes to establish the plausibility of the information and program measures to verify safe responses in case of implausible conditions.

ATTENTION: Safety related functions shall be latched when in their tripped state to help prevent intermittent field faults from removing the trip condition. This can be achieved with the application logic or with measures external to the logic solver. The application software shall be written to ensure that safety related functions are in their safe state during system startup.

Minimize Logic Depth

Where possible, the logic depth should be minimized. This helps reduce visual complexity, simplifies testing, minimizes the number of interconnects required and improves program efficiency.

Where there is nested logic, it shall be possible to establish the correct operation of all intermediate logic connections.

The use of memory (latch) components within the safety function shall be minimized. Similarly, the permutation of conditions that lead to their activation shall be minimized.

Compiler Verification Tool Safety Requirement

The Compiler Verification Tool (CVT) is a software utility that validates the output of the application compilation process. It is automatically enabled by default. This process in conjunction with the validated execution code produced by the AADvance Workbench software and AADvance-Trusted SIS Workstation software verifies that there are no errors introduced by the Compiler during the compilation of the application.

To achieve this CVT decompiles the application project file and then compares each individual application project (POU) source files with its decomposed version. The CVT analysis is displayed in the Output window.

ATTENTION: The following applies to all safety related applications:
- The CVT must be enabled for the final compilation of any application used for safety control. See KnowledgebaseDocument ID QA56957 ICS Triplex 9000 Series:TN30031-01 Compiler verification tool - mandatory use for safety applications.
- The CVT may return compiler errors or warnings. Compiler errors help prevent to download of an application to a controller, warnings do not.
- If there are any warnings that refer to non – recommended programming constructs, the constructs must be removed and new code constructed according to the coding guidelines in Knowledgebase article, KB 685793. See Knowledgebase Document ID QA27029 Coding guidelines to reduce AADvance CVT mismatch warnings.
- If any warnings still remain, contact Rockwell Automation customer support and maintenance (CSM) services.

Sign in to your Rockwell Automation account to view Knowledgebase articles.

Communications Interaction

The AADvance system provides a range of communications options to allow interaction with external systems. Where this communication is used for reporting (or out-going) communications, there are no specific safety requirements.

Data received from external equipment that either controls safety-related functions or affects their operation must be handled with caution. The Application Program shall handle the received data.

The received data should be such that it is limited to interactions which:

- Initiates safety operations, i.e. initiates shutdown sequences
- Resets signals, with the reset action only possible once the initiating conditions have been removed
- Initiate timed start-up override signals which are removed automatically either on expiration of the start period or once the associated signal has stabilized in the normal operating condition
- Adjust control parameters within defined safe operational limits, i.e. lowering of trip thresholds.

Where the interaction does not fall within these categories, the effects of incorrect values and sequences of values shall be considered and measures taken to verify that the system will respond safely in the event of erroneous data. Alternatively, measures may be implemented within the application to verify the integrity and validity of the data.

Remote Fault Reset

The AADvance controller offers the ability to remotely initiate a processor fault reset or standby join. These operations would normally require use of the processor Fault Reset button. The remote reset feature is enabled and configured as part of the application

ATTENTION: Consideration should be given to the affect on system safety of enabling the remote fault/reset join, as continuous fault resets can mask permanent fault conditions.
To minimize the affect on system safety, the following precautions should be taken:

- Do not enable the remote fault reset/join feature unless it is required.
- The application should not set the authentication key variables ("Allow Remote Fault Reset MSB" and "Allow Remote Fault Reset LSB") to the key value. It must be the remote client that provides the correct key value.
- The authentication key variables should only be set for the time required to perform a reset, then cleared.
- The authentication key should not be configured as an easy to guess value, for example 'hex speak' values such as DEADBEEF should not be used.

Program Testing

Even with a small number of inputs, it is possible to reach a point where the number of tests becomes unreasonable. Eliminating impossible or unlikely scenarios should be used to reduce the number of logic path tests that need to be performed. The selection of what constitutes a scenario that does not require testing can be performed only after a suitable hazard analysis.

The scenarios should include possible plant conditions, sequences of plant conditions, and system conditions including partial power conditions, module removal and fault conditions.

Where it is not possible to define a representative suite of test cases, all permutations of input conditions, i.e. all possible states on all possible inputs, shall be exercised. Where the logic includes memory or timing elements, additional tests shall be defined to exercise all the possible sequences of input permutations leading to their operation.

ATTENTION: All safety-related functions shall be tested and the results of the tests recorded. The tests shall include the system scan time, fault detection time, fault reaction time and throughput delay for shutdown logic. The system scan time, including Peer-to-Peer and bindings communications where appropriate, shall be less than ½ PST.

ATTENTION: Functional testing of all safety related programs is considered to be 100% if:

- All inputs are exercised through their entire allowable range
- All outputs are exercised through their entire program determined range
- All logic paths are exercised
- All timers have been tested regarding their timing characteristics without changing timing parameters
- All combinatorial permutations of digital signals, with the exception of 100% tested function blocks, are tested, including fault states.
- All combinatorial permutations of analogue signals, with the exception of 100% tested function blocks, are tested within the safety accuracy granularity.
- All timing properties of each safety loop have been verified

Cross Reference Checking

While the aim shall be to minimize the coupling and dependencies between individual programs, there will inevitably be occasions where, for example, a variable is used within two or more programs. It is important to ensure that any application program changes that affect these interactions do not jeopardize the functional safety.

On-line Modification

It is highly recommended that on-line changes are not performed unless absolutely necessary as it could reduce the safety integrity of the system while doing the changes. Where changes have to be carried out on-line alternative safety measures must be implemented for the duration of the change procedure.

Certain modifications can be performed without directly affecting the system's safety function, for example the physical installation of additional modules. Although these modifications will not affect the system's operation until the system configuration and application program have been modified, caution shall be exercised to ensure that the modifications do not affect other safety related functions.

The procedures to perform an on-line update are provided in the AADvance Configuration Guide(s), publications ICSTT-RM405 and ICSTT-RM-458, and AADvance-Trusted SIS Workstation Software User Guide, publication ICSTT-UM002.

On-line modifications must follow the end users' MOC process as required by the applicable industry safety standards. On-line modifications must include any specific checks recommended by Rockwell Automation for the product.

IMPORTANT For Releases 1.3x onwards you can change the I/O module configuration with an on-line update without having to stop the running application. However, if you are still using an earlier product release the I/O module configuration cannot be changed with an on-line update.

⚠ **ATTENTION:** Changes that affect the system's ability to respond safely, or that may cause other plant disruption shall not be performed on-line unless alternate protection measures can be implemented for the duration of such modifications.

Physical Installation

The installation environment is a potential source of common cause failure, therefore it is vital that compatibility of the equipment with the environment is known. The environment for these purposes includes the prevailing climatic, hazardous area, power, earthing and EMC conditions. In many cases, there will not be a single installation environment. Elements of the system may be installed in differing locations; in these cases, it is important to know the environment for each location.

⚠ **ATTENTION:** You must use installation and commissioning procedures that comply with the applicable international or local codes and standards.

⚠ **ATTENTION:** The AADvance controller equipment (base units and modules) is designed for use when it is installed upright, that is with the base units in a vertical plane and the ventilation slots on the modules at the top and bottom. This orientation is essential to verify that non-forced air cooling is effective and the controller meets the specified MTBF of the modules. This rule applies to all installations regardless of ambient temperature and any additional forced air cooling that may be applied.

Environmental Requirements

⚠ **ATTENTION:** HEAT DISSIPATION AND ENCLOSURE POSITION
System and field power consumption by modules and termination assemblies is dissipated as heat. You should consider this heat dissipation on the design and positioning of your enclosure; e.g. enclosures exposed to continuous sunlight will have a higher internal temperature that could affect the operating temperature of the modules. Modules operating at the extremes of the temperature band for a continuous period can have a reduced reliability.

It is recommended that the field power consumption calculations to determine the heat dissipation are done before designing the enclosure and deciding upon the installation environment.

Environmental Specifications

The following environmental specification defines the minimum recommended environmental conditions for an AADvance controller installation. Additional conditions apply to installations in a Hazardous environment.

Table 16 - Environmental Specification

Attribute	Value
Operating Temperature Range:	
For use in Hazardous Environments (UL Certification):	
Processor Modules	-25 °C to 60 °C (-13 °F to 140 °F)
I/O Modules and Assemblies	-25 °C to 70 °C (-13 °F to 158 °F)
For use in Non-Hazardous Environments:	
All Modules and Assemblies	-25 °C to 70 °C (-13 °F to 158 °F)
Storage and Transport Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Module Surface Temperature (during normal operation)	43° C (109 °F) ± 2 °C
Humidity	
Operating	10% to 95% RH, non-condensing
Storage and Transport	10% to 95% RH, non-condensing
Vibration	
Functional Stress	5Hz to 9Hz
Continuous	1.7mm amplitude
Occasional	3.5mm amplitude

Table 16 - Environmental Specification

Attribute	Value
Withstand	10Hz to 150Hz
Acceleration	0.1g in 3 axes
Endurance	10Hz to 150Hz
Acceleration	0.5g in 3 axes
Shock	15g peak, 11ms duration, ½ sine
Altitude	
Operating	0 to 2000m (0 to 6,600 ft.)
Storage and Transport	0 to 3000m (0 to 10,000 ft.) This equipment must not be transported in unpressurized aircraft flown above 10,000 ft.
Electromagnetic Interference	Tested to the following standards: IEC 61326-1:2015, Class A; IEC 61326-3-1:2017, EN 54-4: 1997, A1; IEC 61131-2:2017; EN 62061:2005.
Hazardous Location Capability	Suitable for Class I Div 2 and Zone 2.

IMPORTANT This equipment is not certified for use in a Zone 1 location

This equipment is not certified for use in a Zone 0 hazardous environment.

NOTE **Casing**: Standard AADvance modules also have a plastic casing and are rated IP20: Protected against solid objects over 12mm (1/2in.) for example "fingers". There is no specific protection against liquids.

Electromagnetic Immunity and Emissions

The AADvance system has been designed and tested to withstand normal levels of conducted and radiated electromagnetic interference and electrostatic discharge. Electrical noise conditions may vary greatly, depending on the equipment installation, wiring, other installed equipment, and its proximity to the AADvance equipment.

A detailed analysis of the installation electrical and magnetic conditions is rare. It is therefore necessary to ensure that the system as a whole complies with the client's requirements or appropriate standards IEC 61000-6-2:2016 and IEC 61000-6-4:2018; within Europe, the CE mark requirements form a legal minimum.

For systems for applications outside Europe it is recommended that at least the same measures be applied, and confirmation sought from the client or end user that electromagnetic interference (EMI) levels are within those shown in the table.

Table 17 - Immunity to Electromagnetic Emissions

Standard	Conditions	Notes
Radiated Emissions		
CISPR 11:2015+A1:2016+A2:2019	Class A N/A	Not applicable Access to controller must be restricted to appropriately trained maintenance personnel operating in accordance with and relevant ESD mitigating procedures.
Radiated Field Immunity		
IEC 61000-4-3 Ed. 3.2:2010	10V rms/m (unmodulated) 80MHz-2GHz: 80% 1 kHz AM 1Hz Pulse Modulation 50:50 duty cycle. 1V rms/m (unmodulated) 2 GHz, 2.7 GHz 80% 1 kHz AM	The equipment additionally complies with fail-safe performance criteria at increased levels of 20V/m over the range 80MHz to 1GHz and 3V rms/m (unmodulated) over the range 2GHz to 6GHz.
Fast Transient/Burst Immunity		
IEC 61000-4-4:2012	DC Power:2kV I/O and Signalling Ports: 1kV	The equipment additionally complies with fail-safe performance criteria at increased levels of 2 kV between I/O or signalling ports and ground and at increased levels of 3 kV between DC power port and ground.
Surge Immunity		
IEC 61000-4-5:2014+A1:2017	DC Power 1kV/2kV line-line/lineground I/O Port: 1kV line-ground only	The equipment additionally complies with fail-safe performance criteria at increased levels of 2 kV between I/O or signalling ports and ground.
Conducted RF Immunity		
IEC 61000-4-6 Ed. 4.0:2013	10V rms (unmodulated) 150kHz — 100MHz 80% 1kHz AM, 1Hz PM 50:50 duty.	The equipment additionally complies with fail-safe performance criteria at increased levels of 20V rms.
Power Frequency Magnetic Field immunity voltage Dips, Short interruptions and Voltage Variations Immunity		
IEC 61000-4-8:2009	30A rms/m, 50Hz and 60Hz	Not Applicable
Immunity to Conducted Common Mode		
Disturbance, 0 to 150 kHz IEC 61000-4-16:2015	DC & I/O Ports: 1 to 10V rms increasing at 20dB/decade from 1,5KHz to 15kHz: 10V rms from 15kHz to 150k Hz 100V rms for 1s at 16.6Hz, 50Hz and 60Hz 10V rms continuous at 150Hz and 180Hz	None
Voltage Dips, Short Interruptions and Voltage Variations for DC Input Power Ports		
IEC 61000-4-29:2000	40% for 10ms 0% for 20ms	The performance criteria for these tests is fail-safe

Table 18 - Immunity to Electrostatic Discharge

Standard	Conditions	Notes
IEC 61000-4-2:2000	Air discharge ± 8 kV Contact discharge ± 6 kV	None

If the anticipated EMI exceeds these levels, additional protection measures such as a suitably screened and earthed enclosure shall be applied.

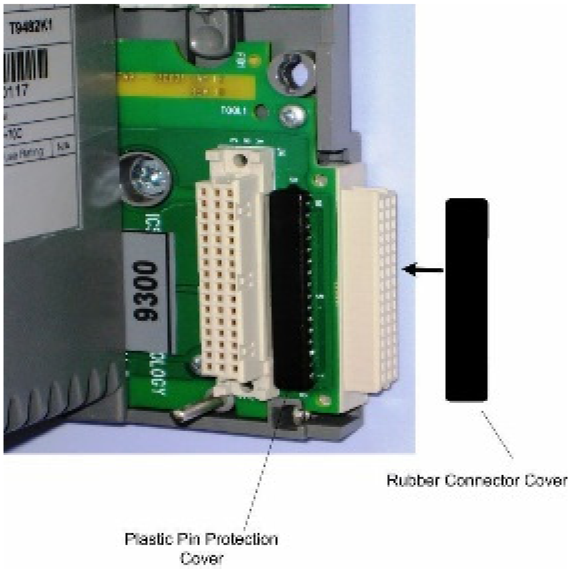
Marine Certification

AADvance has been tested and found to comply with the EMC requirements of BS EN 60945:2002. EMC compliance within a marine environment is dependent on and can only be assured by the use of:

- shielded Ethernet cables
- adequate bonding of the system chassis to a suitable ground reference

Fit EMC Static Protection Covers

For EMC static protection you should fit the black plastic protection covers (supplied with the base units) over any exposed 48 pin DIN connectors on the T9300 I/O Base unit.



Using Shielded Cabling for Ethernet and Serial Ports

When using cable lengths that exceed 3m for Ethernet and Serial communication you must use shielded cable to remain within the emission and immunity standards. Also ensure that the shields are grounded to the controller chassis.

IMPORTANT The system is resistant to radio interference due to its bus structure. However, sensible use of site radios is advised; do not use radios inside or near an open panel.

AADvance System Power Requirements

The AADvance controller is designed to operate from two independent 24V dc power supplies with a common return path, that is, the 24V return shall be common between the power feeds.

The controller must be supplied with system power from a power source that complies with SELV and PELV standards. SELV (safety extra-low voltage) is a voltage which does not exceed 30 Vrms, 42.4 Vpeak and 60 Vdc between conductors, or between each conductor and earth in a circuit which is isolated from the line voltage by a safety transformer. PELV (protected extra-low voltage) is an extra low voltage circuit with a protective partition from other circuits which has a protective earth connection.

To meet SELV and PELV requirements the power source must have a safety transformer with a protective partition between the primary and secondary windings so that the windings are galvanic and electrically isolated.

The power supplies and power distribution, if incorrectly designed, present a potential common cause failure. It is therefore necessary to:

Establish the power philosophy, specific earthing philosophy, power requirements, and the separation requirements where items of equipment are separately supplied, for example system internal supplies and field loop supplies.

Ensure that the chosen PSUs are compatible with the power feeds provided. Alternatively, measures should be implemented to ensure that the power feeds remain within the specifications of the PSUs.

Define the power distribution requirements, together with the protective philosophy for each distribution, for example current limited at source or protective devices. Where protective devices are used, it is important to establish that sufficient current be available to ensure their protective action and that the protective device can break the maximum prospective fault current.

Ensure that the power supplies are sufficient for the system load and for any foreseeable load requirements and load transients.

Ensure that the power supplies have a minimum output hold-up time of 10ms.

Ensure that the power distribution cabling is sized to accommodate the maximum prospective fault currents and tolerable voltage losses. This is specifically important where floating supplies are employed and other power sources may result in high prospective fault currents in the event of multiple earth fault conditions.

⚠ **ATTENTION:** The power supplies used shall conform to the electrical requirements and tests defined in IEC 61131 Part 2, EN 61010-1 and EN 60950 and shall be of appropriate capacity for the system.

NOTE It is highly recommended that the negative side of the field supply be connected to earth (ground). This will avoid possible fail danger conditions that can be caused by some earth fault monitors used with floating power supplies.

System Security

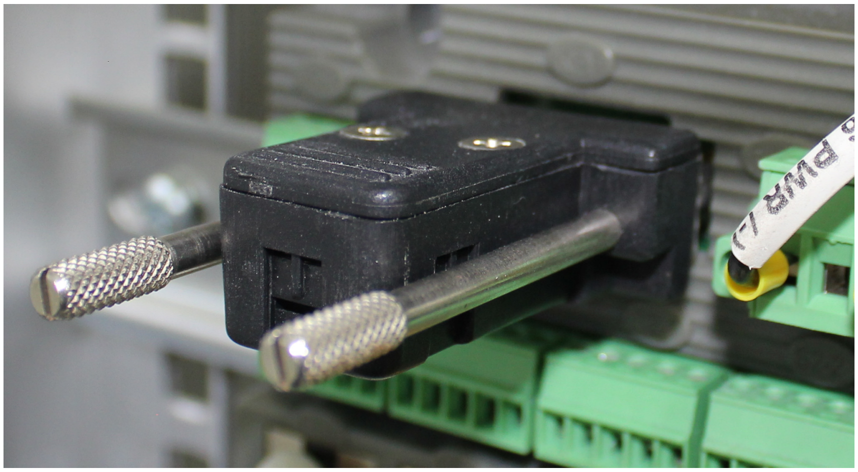
An AADvance system, with its computers and DCS interfaces, whether using Ethernet networks or Serial links is likely part of a larger corporate network which may expose the system to accidental or malicious infection, attack or less obvious security vulnerabilities. If appropriate (or defined in the SRS), a security risk assessment should be carried out and the appropriate level of risk mitigation applied.

There are some simple steps that can be taken to help prevent such issues:

- Consider network and computer security, for example:
  - The AADvance system should not be on a network with open unsecured access to the Internet.
  - The Firewall must be active on the computer, helping prevent access to the relevant Ethernet ports on each communication interface. Anti-virus software must be installed and be kept up-to-date.

NOTE Firewalls have been known to affect the operation of the AADvance Discover tool.

  - The computer must be password-protected. If using a laptop, keep the laptop locked when not in use.
  - If the software uses a hardware license USB dongle, keep the USB dongle secure. The software will not run without the USB dongle.
  - The application should be password-protected.
  - Removable media, such as USB storage devices and CDs, should be virus checked before use within the system.
  - The **program enable key** must be inserted into the processor base unit to let you change the application or I/O configuration. Make sure the key is removed when the changes are finished.



Notes:

Checklists

This chapter contains a number of example checklists. These are provided as an aid for qualified engineers. In general each checklist item should result in "yes", where this is not the case a justification should be produced.

Pre-Engineering Checklists

The checklists provided within this section are applicable to the requirements. It should be recognized that the requirements will undergo refinement, particularly, in the early stages of a project. The information provided initially may be 'outline'; in this case these checklists should be used to help identify where omission has occurred or where further refinement is necessary.

Scope Definition Checklist

Description	Yes/No
Has a summary description of the intended application been provided?	
Is the intended installation environment defined? If so: does this include both normal and possible abnormal conditions? does this include geographical distribution requirements?	
Does the installation position the modules in the upright position to verify that non-forced air cooling is effective?	
Does the installation environment meet the environmental specification for the controller?	
Has a list of all the third-party equipment interfaces been provided and are definitions of both the protocol and the data to be interchanged established?	
Are all of the plant interfaces defined, including the signal qualities and characteristics?	
Have any special or abnormal conditions that exceed the normal equipment capabilities been highlighted to enable special measure to be implemented?	
Is the presented information adequate to support the necessary level of understanding of the plant/EUC and its environment?	
Has a risk analysis been completed to determine the Safety Integrity Levels that need to be handled by the system?	

Functional Requirements Checklist

Description	Yes/No
Is the definition of each of the required functions complete?	
Are the interfaces, signals, and data associated with each function clearly identified?	
Where a 'tag referencing' scheme is used for these signals, has a summary description of the naming convention been provided to facilitate an understanding of the role of the signal?	
Have the performance requirements for each function, or collective functions, been defined?	

Description	Yes/No
Have the operating modes of the EUC, process or plant been clearly defined?	
Have the functions required to operate in each plant operating-mode been identified?	
Have the transitions between each plant operating-mode been defined? Have the functions necessary to affect these transitions been established?	

Safety Requirements Checklist

Description	Yes/No
Have all of the functional requirements been allocated a required safety requirements class?	
Has the safety-related timing for each safety-related function, including process safety time (PST) and fault tolerance period, been established?	
Have the safety requirements been approved?	
Are there clear definitions of the external interfaces involved in each of the safety-related functions? (These may already be defined in the functional requirements).	
Is there now sufficient information to understand how the plant should be controlled safely in each of its intended operating modes?	
Are the AADvance® System Build Manual installation instructions available for installing and commissioning the system?	
Does the application program shut down the SIL 3 safety instrumented functions if a faulty module has not been replaced within the MTTR assumed for the system in the PFD calculations?	
Have the application programs been set up to monitor the "discrepancy alarms" and alert the operators when a discrepancy alarm occurs?	
Do the energize to action configurations conform to the restrictions (defined in this safety manual) that should be applied when using these configurations?	
Have the Controller System Security Measures been set up and observed?	
Have the Communication Port security measures been set up and observed?	

Engineering Checklists

I/O Architecture Checklist

Description	Yes/No
Has the PST been specified?	
What is the PST?	
Has the fault detection time for the system been specified?	
What is the fault detection time?	
Is the safety-accuracy adequate for the application?	
Where the fault detection time is greater than the PST, does the safety-related I/O configuration provide a fail-safe configuration? **Note:** If not, the system topology shall be discussed with the client to ensure that the system implementation is safe.	
If the probabilities of failure on demand for each function have been specified, has they been met?	
Do the selected architectures provide solutions where there is no single power source or distribution point of failure that could lead the system to fail to function safely when required?	
Have sensor fault conditions been taken into account?	
For each of the I/O signal types, do the I/O modules provide the correct characteristics and behaviour for the intended sensor or actuator (including minimum and maximum load requirements)? **Note:** If not, have additional interfacing elements been included to ensure that the effective signal is compatible with the selected module type?	
Has the allocation of signals to I/O modules and channels considered each of the signals' function?	
Do safety related inputs and outputs use only those configurations identified as safety related?	

Description	Yes/No
Are there any safety-related, normally de-energized outputs? If so have redundant power sources, power failure warning and line monitoring been provided?	
Have actuator fault conditions been taken into account?	
Has an actuator testing schedule been created for regular actuator maintenance?	
Have field power supplies conforming to EN 61010-1 or EN 60950 been used?	
Have variables been set up to report the safety accuracy value for each channel?	
Have variables been set up to report "safe-values" when a channels' safety accuracy value fails because it is reported to be outside its accuracy figure?	
Has a maximum duration for a single channel operation of an I/O module been specified in accordance with the application requirements?	
Has the Shutdown option for each SIL 2 or SIL 3 Output Channel been set to OFF?	
If HART Pass-Through is used, have the safety precautions been observed and implemented?	

Language Selection Checklist

Description	Yes/No
Are any functions not in the previously tested libraries required? If so has provision been made to adequately test these functions?	

Override Requirements Checklist

Description	Yes/No
Are the effects of overriding fully understood, particularly where the override action will affect independent parts of an application?	
Has a method of enabling, or more importantly removing, the overrides for the system as whole, or individual sub-systems, been provided?	
Have programming or procedural measures been defined to ensure that no more than a single override may be applied to a given safety-related process unit?	
Have indication of the presence of override conditions and recording their application and removal been defined?	
Is there an alternative method of removing an override?	
Are there programming or procedural measures to limit the period of override?	

Input/Output Module Configuration Checklist

Description	Yes/No
For each of the I/O signal types, do the I/O module settings provide the correct characteristics and behavior for the intended sensor or actuator?	
Have the thresholds been verified with both increasing and decreasing field signal levels and with margins to allow for the measurement accuracy?	
Do threshold states remain unique under all operating tolerances?	
For all configurations, have tests been defined and executed to 100% test the required operation?	
Have Dual Output modules been configured for Energize to trip SIL 3 applications?	
Has guidance been followed to ensure that SIL 3 signals are shut down outside the time limit imposed by the MTTR assumed for the PFD calculations?	
Has the "Hold Last State" been set up for the Digital Output channels and if so has the affect on the safety functions been taken into account?	

Description	Yes/No
Has input or output forcing been used on any channels and has the affect on the safety function been fully taken into account so that it does not jeopardize functional safety?	
Has a method of manually removing a forced condition (e.g. manually operated switches) been set up to remove the forced condition on safety related inputs?	
Has the AADvance® Workbench software or AADvance®-Trusted® SIS Workstation software system configuration backup copy been tested?	

Processor and Application Checklist

Description	Yes/No
If bindings communications is used, are the timeouts set to a response time within the required PST?	
Have you dual/triple processor been configured for SIL 3 and high demand applications?	
Have you recommended shut down actions for single module configuration outside of the MTTR assumed for the PFD calculations?	
Has security protection been used to prevent unauthorized access to the application programs?	
Have full branch and data tests been carried out on IL (AADvance Workbench version 1.4 only) and ST program flow functions?	
Have safety related control programs been implemented within separate programs from non-safety related control elements?	
Is the data flow programmed so that it goes from Safety functions to non-safety functions?	
Are the processor modules loaded with the latest firmware versions?	
Are all processors using the same firmware versions?	
Do the application programs ensure that all safety related elements are in their safe state during start up?	
Have alternate protection measure been considered for safety related functions should you need to do an on-line change?	
Ensured that HART data is not used as the primary process measurement in a safety related function SIF?	
The HART Pass-Through function has been disabled if the device configuration status is not monitored and alarmed to help prevent unauthorized or accidental changes to the field device configuration.	

Testing Checklist

Description	Yes/No
Have all of the functions and function blocks used been fully tested?	
Was CVT enabled when you compiled your application? Has SFC not been used?	
Has the application been fully tested?	
Are the scan and response times in accordance with the PST requirements (< ½ PST)?	
Have the climatic conditions been verified to be suitable?	
Have Test Plans and Test Specifications been developed for the system?	
Has the system been fully tested to the Test Plans and Test Specifications?	

History of Changes

This appendix contains the new or updated information for each revision of this publication. These lists include substantive updates only and are not intended to reflect all changes. Translated versions are not always available for each revision.

ICSTT-RM446Q-EN-P, October 2021

Change
Updated for AADvance® system release 1.41 TÜV Rheinland certification.
Updated AADvance system release and software information in AADvance Release section.
Added Black Channel I/O bus in AADvance Features section.
Changed ANSI ISA 84.00.01:2004 (IEC 61511-2 Mod) to ANSI/ISA 61511-1:2018 in Reference Documents table.
Updated Attention table in Compiler Verification Tool Safety Requirement section.

ICSTT-RM446P-EN-P, February 2021

Change
Updated for AADvance® system release 1.40 TÜV Rheinland certification.
Updated publication template.
Changed *workstation* to *computer.*
Added AADvance®-Trusted® SIS Workstation software information where applicable.
Changed *Workbench* to *software* where applicable.
Changed *Workbench* to *AADvance Workbench software* where applicable.
Added reference to AADvance-Trusted SIS Workstation Software User Guide, publication ICSTT-UM002.
Changed *programs (POUs)* to *program organization units (POUs).*
Applied latest publication template.
Updated AADvance system release and software information in AADvance Release section.
Updated number of modules required for Processor for SIL 2, High Demand, DTT in Table summarizing module configuration for SIL compliance.
Updated security steps in System Security section.
Updated AADvance Communication Ports table in AADvance Communication Ports section.
Added EN 298:2012 information in Non-Hazardous Installation Requirements section.
Changed *BindRespTimeout* to *Bind Response Timeout* and *BindReqTimeout* to *Bind Request Timeout* in Configuring Variable Bindings section.
Added reference to publications that provide information on peer-to-peer configurations for AADvance® Workbench software version 2.1 and AADvance-Trusted SIS Workstation software in Safety Related Peer-to-Peer Configurations section.
Added NFPA 87 Requirements section.
Updated suggested range of values in Digital Input Field Loop Circuits section.
Added alternative option for manually entering Recovery Mode in Recovery Mode section.
Updated analog input module values in Input Module Safety Accuracy section.

ICSTT-RM446P-EN-P, February 2021

Change
Changed *Commanded Values and Scaling Factor* to *Commanded Values and Scaling Factor (Command State)* in Analogue Output Module Safety Functions section.
Changed AADvance Workbench Configuration section to AADvance Application Security and updated section content in AADvance Application Security section.
Updated to indicate that IL and SFC languages are supported only by AADvance Workbench software version 1.4 in Language Selection section.
Updated information on new or previously untested function in Testing of New or Previously Untested Functions section.
Changed limit from 250 individual programs within a single project to 65,536 program organization units (POUs) in a project in Individual Safety Related Functions section.
Updated section content in Compiler Verification Tool Safety Requirement section.
Updated multiple entries in Glossary section.

ICSTT-RM4460-EN-P, July 2019

Change
Updated for Release 1.34 IEC 61508 Edition 2.0 certification

ICSTT-RM446N-EN-P, April 2018

Change
Update for AADvance Release R1.40

Issue 13, March 2016

Change
Added support for EN 298 and NFPA 87

Issue 12, April 2015

Change
Revised with comments received from TÜV

Issue 11, March 2015

Change
Finalised for AADvance Release 1.34

Issue 11B, March 2015

Change
Updates to spelling and other typographical errors following internal review

Issue 11A, March 2015

Change
Update to R1.34 first draft

Issue 10_C, July 2013

Change
Update after peer review

Issue 10_B, June 2013

Change
Draft issue for release 1.3 incorporating changes following TUV review comments. Also added specifications for electrostatic discharge.

Issue 10_A, August 2012

Change
Updated for additional information about the Analogue Output Module

Issue 10, July 2012

Change
Updates for Release 1.3 and 1.3.1

Issue 09[1], March 2011

Change
Updates for release R1.2

[1] Previously Issue 1.2

Issue 08, November 2010

Change
Update for SIL 2 and SIL configurations change, MTTR change, UL requirements, Check lists change, peer review comments.

Issue 07, February 2010

Change
Update for TUV review additional comments.

Issue 06, January 2010

Change
Update for TUV review and comments

Issue 05, October 2009

Change
TUV approval release

Issue 04, September 2009

Change
Release 1.1 for TUV approval

Issue 03, August 2009

Change
QA review updates

Issue 02, April 2009

Change
Reformat to match associated product user manuals

Issue 01, January 2009

Change
First Issue

The following terms and abbreviations are used throughout this manual. For definitions of terms not listed here, refer to the Allen-Bradley Industrial Automation Glossary, publication AG-7.1.

A

accuracy The degree of conformity of a measure to a standard or a true value. See also 'resolution'.

achievable safe state A safe state that is achievable.

> **NOTE** Sometimes, a safe state cannot be achieved. An example is a non-recoverable fault such as a voting element with a shorted switch and no means to bypass the effect of the short.

actuator A device which cause an electrical, mechanical or pneumatic action to occur when required within a plant component. Examples are valves and pumps.

AITA Analogue input termination assembly.

alarms and events (AE) An OPC data type that provides time stamped alarm and event notifications.

allotted process safety time The portion of the total process safety time allotted to a sub function of that process.

application software Software specific to the user application, typically using logic sequences, limits and expressions to read inputs, make decisions and control outputs to suit the requirements of the system for functional safety.

architecture Organizational structure of a computing system which describes the functional relationship between board level, device level and system level components.

asynchronous A data communications term describing a serial transmission protocol. A start signal is sent before each byte or character and a stop signal is sent after each byte or character. An example is ASCII over RS-232-C. See also 'RS-232-C, RS-422, RS-485'.

availability The probability that a system will be able to carry out its designated function when required for use — normally expressed as a percentage.

B

backplane clip A sprung, plastic device to hold together two adjacent AADvance® base units. Part number 9904. Used in pairs.

base unit One of two designs which form the supporting parts of an AADvance controller. See 'I/O base unit' and 'processor base unit'.

bindings Bindings describe a "relationship" between variables in different AADvance controllers. Once a variable is "bound" to another variable, a unique and strong relationship is created between the two variables and the SIL 3 Certified SNCP protocol is used to verify that the consuming variable is updated with the data from the producing variable.

black channel A communication path whose layer (i.e. cabling, connections, media converters, routers/switches and associated firmware/software, etc.) has no requirement to maintain the integrity of safety critical data transferred over it. Measures to detect and compensate for any errors introduced into the black channel must be implemented by the safety critical sender and receiver (by software and/or hardware means) to make sure the data retains its integrity.

blanking cover A plastic moulding to hide an unused slot in an AADvance base unit.

boolean A type of variable that can accept only the values 'true' and 'false'.

BPCS Basic process control system. A system which responds to input signals and generates output signals causing a process and associated equipment to operate in a desired manner, but which does not perform any safety instrumented functions with a claimed safety integrity level of 1 or higher.

Refer to IEC 61511 or to ANSI/ISA—84.00.01—2004 Part 1 (IEC 61511-1 Mod) for a formal definition.

Equivalent to the Process Control System (PCS) defined by IEC 61508.

breakdown voltage The maximum voltage (AC or DC) that can be continuously applied between isolated circuits without a breakdown occurring.

BS EN 54 A standard for fire detection and fire alarm systems.

BS EN 60204 A standard for the electrical equipment of machines, which promotes the safety of persons and property, consistency of control response and ease of maintenance.

bus A group of conductors which carry related data. Typically allocated to address, data and control functions in a microprocessor-based system.

bus arbitration A mechanism for deciding which device has control of a bus.

C

CIP Common Industrial Protocol. A communications protocol, formally known as 'CIP over Ethernet/IP™', created by Rockwell Automation for the Logix controller family, and which is also supported by the AADvance controller. AADvance controllers use the protocol to exchange data with Logix controllers. The data exchange uses a consumer/producer model.

clearance The shortest distance in air between two conductive parts.

coding peg A polarization key, fitted to the 9100 processor base unit and to each termination assembly, which verifies that only a module of the correct type may be fitted in a particular slot. Part number 9903.

coil In IEC 61131-3, a graphical component of a Ladder Diagram program, which represents the assignment of an output variable. In MODBUS language, a discrete output value.

Compiler Verification Tool (CVT) An automatic software utility that validates the output of the application compilation process.

configuration A grouping of all the application software and settings for a particular AADvance controller. The grouping must have a 'target', but for an AADvance controller it can have only one 'resource'.

consumer The consuming controller requests the tag from the producing controller.

contact A graphical component of a Ladder Diagram program, which represents the status of an input variable.

continuous mode Where the Safety Instrumented Function in the Safety System is continually maintaining the process in a safe state.

controller A logic solver; the combination of application execution engine and I/O hardware.

controller system Contains one or more controllers, power sources, communications networks, and computers.

coverage The percentage of faults that will be detected by automated diagnostics. See also 'SFF'.

creepage distance The shortest distance along the surface of an insulating material between two conductive parts.

cross reference Information calculated by the AADvance® Workbench software or AADvance®-Trusted® SIS Workstation software relating to the dictionary of variables and where those variables are used in a project.

D

data access (DA) An OPC data type that provides real-time data from AADvance controllers to OPC clients.

de-energize to action A safety instrumented function circuit where the devices are energized under normal operation. Removal of power de-activates the field devices.

dictionary The set of internal input and output variables and defined words used in a program.

discrepancy A condition that exists if one or more of the elements disagree.

DITA Digital input termination assembly.

DOTA Digital output termination assembly.

E

element A set of input conditioning, application processing and output conditioning.

energize to action A safety instrumented function circuit where the outputs and devices are de-energized under normal operation. Application of power activates the field device.

EUC Equipment Under Control. The machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.

expansion cable assembly A flexible interconnection carrying bus signals and power supplies between AADvance base units, available in a variety of lengths. Used in conjunction with a cable socket assembly (at the left hand side of a base unit) and a cable plug assembly (at the right hand side of a base unit).

F

fail operational state A state in which the fault has been masked. See 'fault tolerant'.

fail safe The capability to go to a pre-determined safe state in the event of a specific malfunction.

fault reset button The momentary action push switch located on the front panel of the 9110 processor module.

fault tolerance Built-in capability of a system to provide continued correct execution of its assigned function in the presence of a limited number of hardware and software faults.

fault tolerant The capability to accept the effect of a single arbitrary fault and continue correct operation.

fault warning receiving station A centre from which the necessary corrective measures can be initiated.

fault warning routing equipment Intermediate equipment which routes a fault warning signal from the control and indicating equipment to a fault warning receiving station.

field device Item of equipment connected to the field side of the I/O terminals. Such equipment includes field wiring, sensors, final control elements and those operator interface devices hard-wired to I/O terminals.

fire alarm device A component of a fire alarm system, not incorporated in the control and indicating equipment which is used to give a warning of fire — for example a sounder or visual indicator.

fire alarm receiving station A centre from which the necessary fire protection or fire fighting measures can be initiated at any time.

fire alarm routing equipment Intermediate equipment which routes an alarm signal from control and indicating equipment to a fire alarm receiving station.

function block diagram An IEC 61131 language that describes a function between input variables and output variables. Input and output variables are connected to blocks by connection lines. See 'limited variability language'.

functional safety The ability of a system to carry out the actions necessary to achieve or to maintain a safe state for the process and its associated equipment.

G

group A collection of two or three input modules (or two output modules), arranged together to provide enhanced availability for their respective input or output channels.

H

hand-held equipment Equipment which is intended to be held in one hand while being operated with the other hand.

HART HART (Highway Addressable Remote Transducer) is an open protocol for process control instrumentation. It combines digital signals with analogue signals to provide field device control and status information. The HART protocol also provides diagnostic data. (For more details of HART devices refer to the HART Application Guide, created by the HART Communication Foundation, and their detailed HART specifications. You can download documents from www.hartcomm.org.)

high demand mode Where the Safety Instrumented Function in the Safety System only performs its designed function on a demand, and the frequency of demands is greater than one per year.

hot swap See live insertion.

I

I/O base unit A backplane assembly which holds up to three I/O modules and their associated termination assembly or assemblies in an AADvance controller. Part number 9300. See 'I/O module' and 'termination assembly'.

I/O module A collation of interfaces for field sensors (inputs) or final elements (outputs), arranged in a self-contained and standardized physical form factor.

IEC 61000 A series of international standards giving test and measurement techniques for electromagnetic compatibility.

IEC 61131 An international standard defining programming languages, electrical parameters and environmental conditions for programmable logic controllers. Part 3, which is entitled 'Programming Languages', defines several limited variability languages.

IEC 61508 An international standard for functional safety, encompassing electrical, electronic and programmable electronic systems; hardware and software aspects.

IEC 61511 An international standard for functional safety and safety instrumented systems (SIS) for the process industry, encompassing electrical, electronic and programmable electronic systems, hardware and software aspects.

indicator A device which can change its state to give information.

input (variable) A value passed from an I/O module to the processor module.

instruction list An IEC 61131 language, similar to the simple textual language of PLCs. See 'limited variability language'.

integer A variable type defined by the IEC 61131 standard.

IXL IXL stands for ISaGRAF® eXchange Layer. This is the communication protocol between ISaGRAF-based components.

K

key connector The receptacle on the AADvance controller for the program enable key. A 9-way 'D' type socket, located on the 9100 processor base unit.

L

ladder diagram An IEC 61131 language composed of contact symbols representing logical equations and simple actions. The main function is to control outputs based on input conditions. See 'limited variability language'.

LAN Local area network. A computer network covering a small physical area, characterised by a limited geographic range and lack of a need for leased telecommunication lines.

live insertion The removal and then reinsertion of an electronic module into a system while the system remains powered. The assumption is that removal of the module and reinsertion will cause no electrical harm to the system. Also referred to as 'hot swap'.

low demand mode Where the Safety Instrumented Function only performs its designed function on demand, and the frequency of demands is no greater than one per year.

M

manual call point A component of a fire detection and fire alarm system which is used for the manual initiation of an alarm.

mission time The time that the SIF (Safety Instrumented Function) is designed to be operational.

MODBUS An industry standard communications protocol developed by Modicon. Used to communicate with external devices such as distributed control systems or operator interfaces.

MODBUS object Represents the configuration settings for a MODBUS Master or for its associated slave links in the AADvance Workbench software or AADvance-Trusted SIS Workstation software. The settings include communication settings and messages.

module locking screw The AADvance latch mechanism seen on the front panel of each module and operated by a broad, flat-blade screwdriver. Uses a cam action to lock to the processor base unit or I/O base unit.

N

NFPA 85 The Boiler and Combustion Systems Hazards Code. Applies to certain boilers, stokers, fuel systems, and steam generators. The purpose of this code is to contribute to operating safety and to help prevent uncontrolled fires, explosions and implosions.

NFPA 86 A standard for Ovens and Furnaces. Provides the requirements for the prevention of fire and explosion hazards in associated with heat processing of materials in ovens, furnaces and related equipment.

NFPA 87 The code for recommended practice for fluid heaters. This code provides safety guidance in order to minimize fire and explosion hazards in Type F, Type G and Type H fluid heating systems including the control system and related equipment.

O

on-line The state of a controller that is executing the application software.

OPC A series of standards specifications which support open connectivity in industrial automation.

output (variable) A value passed from the processor module to an I/O module.

P

peer to peer A Peer to Peer network consists of one or more Ethernet networks connecting together a series of AADvance and/or Trusted controllers to enable application data to be passed between them.

pinging In MODBUS communications, sending the diagnostic Query Data command over a link and by receiving a reply ensuring that the link is healthy and the controller is able to communicate with the master. No process data is transferred or modified. In the case of slave devices that will not support pinging then the Standby command will default to Inactive state, but no error will be returned.

portable equipment Enclosed equipment that is moved while in operation or which can easily be moved from one place to another while connected to the supply. Examples are programming and debugging tools and test equipment.

process safety time (PST) For equipment under control this represents the period of time a dangerous condition can exist without the protection of a safety instrumented system before a hazardous event occurs.

processor base unit A backplane assembly which holds all of the processor modules in an AADvance controller. Part number 9100. See also 'processor module'.

processor module The application execution engine of the AADvance controller, housed in a self-contained and standardized physical form factor.

producer A controller producing a tag to one or more consumers, at the request of the consumers.

program enable key A security device that protects the application from unauthorized access and change, in the form factor of a 9-way 'D' type plug. Part number 9906. Supplied with the processor base unit. See also 'key connector'.

project A collection of configurations and the definition of the linking between them. See 'configuration'.

proof test A periodic test performed to detect dangerous hidden faults in a safety instrumented system (SIS) so that, if necessary, a repair can restore the system to an 'as new' condition or as close as practical to this condition.

Proof tests are designed to reveal both Systematic and Random failures, Proof tests may be required depending on how the technology has been implemented.

AADvance product data is given for a Useful Life of 20 years. For a Mission Time of up to 20 Years, proof testing is not required. For Mission Times greater than 20 years, any products that are still in service once that time is reached should be replaced.

protocol A set of rules that is used by devices (such as AADvance controllers, serial devices and engineering computers) to communicate with each other. The rules encompass electrical parameters, data representation, signalling, authentication, and error detection. Examples include MODBUS, TCP and IP.

PST Process Safety Time. The process safety time for the equipment under control (denoted PSTEUC) is the period a dangerous condition can exist before a hazardous event occurs without a safety system as a protection.

R

real A class of analogue variable stored in a floating, single-precision 32-bit format.

redundancy The use of two or more devices, each carrying out the same function, to improve reliability or availability.

resolution The smallest interval measurable by an instrument; the level of detail which may be represented. For example, 12 bits can distinguish between 4096 values.

RS-232-C, RS-422, RS-485 Standard interfaces introduced by the Electronic Industries Alliance covering the electrical connection between data communication equipment. RS-232-C is the most commonly used interface; RS-422 and RS-485 allow for higher transmission rates over increased distances.

RTC Real-time clock.

RTU Remote terminal unit. The MODBUS protocol supported by the AADvance controller for MODBUS communications over serial links, with the ability to multi-drop to multiple slave devices.

S

safe state A state which enables the execution of a process demand. Usually entered after the detection of a fault condition; it makes sure the effect of the fault is to enable rather than disable a process demand.

safety accuracy The accuracy of a signal within which the signal is guaranteed to be free of dangerous faults. If the signal drifts outside of this range, it is declared faulty.

safety-critical state A faulted state which helps prevent the execution of a process demand.

Safety Requirements Specification (SRS) Specification containing the functional requirements for the SIFs and their associated safety integrity levels (IEC61511).

sensor A device or combination of devices that measure a process condition. Examples are transmitters, transducers, process switches and position switches.

sequential function chart An IEC 61131 language that divides the process cycle into a number of well-defined steps separated by transitions. See 'limited variability language'.

SFF Safe Failure Fraction. Given by (the sum of the rate of safe failures plus the rate of detected dangerous failures) divided by (the sum of the rate of safe failures plus the rate of detected and undetected dangerous failures).

SIF Safety Instrumented Function. A form of process control that performs specified functions to achieve or maintain a safe state of a process when unacceptable or dangerous process conditions are detected.

SIL Safety Integrity Level. One of four possible discrete levels, defined in IEC 61508 and IEC 61511, for specifying the safety integrity requirements of the safety functions to be allocated to a safety-related system. SIL4 has the highest level of safety integrity; SIL1 has the lowest.

The whole of an installation (of which the AADvance system forms a part) must meet these requirements in order to achieve an overall SIL rating.

SNCP SNCP (Safety Network Control Protocol) is the Safety Protocol that allows elements of an AADvance System to exchange data. SNCP is a SIL 3 certified protocol which provides a safety layer for the Ethernet network making it a "Black Channel".

SNTP Simple Network Time Protocol. Used for synchronizing the clocks of computer systems over packet-switched, variable latency data networks.

structured text A high level IEC 61131-3 language with syntax similar to Pascal. Used mainly to implement complex procedures that cannot be expressed easily with graphical languages.

synchronous A data communications term describing a serial transmission protocol. A pre-arranged number of bits is expected to be sent across a line per second. To synchronise the sending and receiving machines, a clocking signal is sent by the transmitting computer. There are no start or stop bits.

T

TA See 'termination assembly'.

target An attribute of a 'configuration' which describes characteristics of the AADvance controller on which the configuration will run. Includes characteristics such as the memory model and the sizes of variable types for the controller.

TCP Transmission control protocol. One of the core protocols of the Internet Protocol suite. It provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer. Common applications include the World Wide Web, e-mail and file transfer and, for an AADvance controller, MODBUS communications over Ethernet.

termination assembly A printed circuit board which connects field wiring to an input or output module. The circuit includes fuses for field circuits. The board carries screw terminals to connect field wiring to the controller, and the whole assembly clips onto the 9300 I/O base unit.

TMR Triple modular redundant. A fault tolerant arrangement in which three systems carry out a process and their result is processed by a voting system to produce a single output.

U

U Rack unit. A unit of measure used to describe the height of equipment intended for mounting in a standard rack. Equivalent to 44.45mm (1-¾ inches).

V

validation In quality assurance, confirmation that the product does what the user requires.

verification In quality assurance, confirmation that the product conforms to the specifications.

voting system A redundant system (m out of n) which requires at least m of the n channels to be in agreement before the system can take action.

W

withstand voltage The maximum voltage level that can be applied between circuits or components without causing a breakdown.

Notes:

Rockwell Automation Support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, and product notification updates.	rok.auto/support
Knowledgebase	Access Knowledgebase articles.	rok.auto/knowledgebase
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
Literature Library	Find installation instructions, manuals, brochures, and technical data publications.	rok.auto/literature
Product Compatibility and Download Center (PCDC)	Download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes.	rok.auto/pcdc

Documentation Feedback

Your comments help us serve your documentation needs better. If you have any suggestions on how to improve our content, complete the form at rok.auto/docfeedback.

Waste Electrical and Electronic Equipment (WEEE)

At the end of life, this equipment should be collected separately from any unsorted municipal waste.

Rockwell Automation maintains current product environmental information on its website at rok.auto/pec.

Rockwell Otomasyon Ticaret A.Ş. Kar Plaza İş Merkezi E Blok Kat:6 34752, İçerenkÖy, İstanbul, Tel: +90 (216) 5698400 EEE YÖnetmeliğine Uygundur

Connect with us.

rockwellautomation.com — expanding **human possibility**™

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication ICSTT-RM446Q-EN-P - October 2021
Supersedes Publication ICSTT-RM446P-EN-P - Februrary 2021