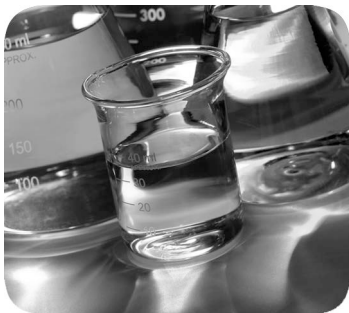


# AADvance Eurocard Controller

Catalog Numbers T9120 T9531 T9501 T9842 T9551 T9581



---

## 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 and other considerations.



**WARNING:** Identifies information about practices or circumstances 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.



**CAUTION:** Identifies information about practices or circumstances that can cause property damage or economic loss.

---

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

---

**NOTE** Provides key information about the product or service.

---

**TIP** Tips give helpful information about using or setting up the equipment.

---

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).

---



### Issue Record

This manual contains new and updated information as indicated in the following table.

Issue	Date	Comments
01	Jan 2013	First Issue
02	Jan 2015	Updates after Exida review and additional security information added.
C	May 2018	Incorporation of Exida updates reformatting of tables and hypertext references
D	Dec 2023	Updates for the AADvance Eurocard 1.41 system release

### Summary of changes in this Document Issue

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

Changes described in the table are denoted in the document with black bars in the left margin, unless the change occurs throughout the publication.

Topic	Page
Changed <i>workstation</i> to <i>computer</i> , where applicable.	Throughout
Changed <i>workbench</i> to <i>software</i> , where applicable.	Throughout
Changed <i>controller</i> to <i>Eurocard controller</i> , where applicable, for clarity.	Throughout
Changed <i>Workbench</i> to <i>AADvance® Workbench software</i> or <i>AADvance®-Trusted® SIS Workstation software</i> , where applicable, to provide clarity.	Throughout
Updated release number AADvance Eurocard 1.32 to AADvance Eurocard 1.41.	Throughout
Updated references from <i>Doc No. ICSTT-RM457 AADvance Eurocard PFH and PFD<sub>avg</sub> Data.</i> to <i>Doc No. ICSTT-RM449 AADvance Controller and AADvance Eurocard Controller PFH and PFD<sub>avg</sub> Data.</i>	Throughout
Removed references to hazardous environments as the Eurocard Controller is not certified for them.	Throughout
Added how to locate product notices and product safety advisories.	9
Updated the URL for the Product Compatibility and Download Center.	10
Updated software listed in the AADvance Release section.	10
Updated the Verification of the Safety Manual section.	17
Updated the Controller Subsea Certification section with current standards.	17
Updated Vocabulary and Conventions introductory paragraph for clarity.	17
Updated the AADvance Eurocard Controller – Overview section: increased the initial number of processor modules for Eurocard configuration from one to two.	18
Provided clarifications regarding module wiring harnesses and backplanes.	18
Updated 9441 Eurocard Digital Output Module description with <i>commoned</i> .	19
Changed <i>transport protocol</i> to <i>communication protocol</i> in the Communication Interfaces section.	20

Topic	Page
Changed <i>Fault tolerant topologies</i> to <i>Fail safe or fault tolerant topologies</i> in the Eurocard Controller Features section.	21
Added <i>Black Channel I/O bus information</i> in the Eurocard Controller Features section.	22
Added IEC 61508 certification to the list of key features in the Eurocard Controller Features section.	22
Added that the AADvance Eurocard system also supports OPC when using a Standalone OPC Server.	22
Updated the description of Process Safety Time, added the purpose, and updated appropriate use information.	22
Updated the Fault Tolerance in Eurocard Controllers section with SIL 2 and SIL3 safety system processor requirements.	22
Updated <i>1001D</i> to <i>1001</i> in the Internal Diagnostics and Fault Reporting section.	23
Added how to clear latched diagnostic faults in the Internal Diagnostics and Fault Reporting section.	23, 23
Updated Threat Analysis section: changed <i>system threat analysis</i> to <i>security risk assessment</i> , and <i>high risk threats mitigated</i> to <i>all identified risks mitigated</i> .	25
Updated <i>secure network communications protocol</i> to <i>Rockwell Safety Network Control Protocol (SNCP)</i> and added <i>Black Channel</i> for clarity.	25
Updated Availability column in the AADvance Communication Ports table.	25
Updated the Reference Documents table.	26
Updated the IEC standard from IEC 60664-1 to IEC 61010-1, and added surrounding air temperature ratings to the System Installation Environment section.	31
Added surrounding air temperature ratings to the Pollution Degree Definition section.	32
Renamed the Preserving Functional Safety section to Maintaining Functional Safety.	34
Updated Eurocard SIL 2 Fault Tolerant and High Demand architectures. Simplex processor configurations can no longer be used for safety applications and have been removed from SIL-rated supported architectures.	Throughout Chapter 3 (37)
Updated all wiring diagrams.	Throughout Chapter 4 (45)
Changed <i>BindRespTimeout</i> to <i>Bind Response Timeout</i> .	57
Changed <i>BindReqTimeout</i> to <i>Bind Request Timeout</i> .	57
Updated the table titled Certified Peer-to-Peer Configurations in the Peer-to-Peer section. Peer-to-Peer configurations approved for use in safety-related functions have been modified to require that more data block types utilize duplicate data blocks compared for equivalence within the receiving application.	60
Removed Industrial Functional Safety Standards section (including NFPA 72, NFPA 86 Requirements, EN 50156, BS EN 54 Requirements, and EN 54 section 7.12 Dependencies on More Than One Alarm Signal) from Chapter 6.	n/a
Moved some HART Passthrough information to a new section titled Precautions for HART in a Safety System.	66
Updated processor recovery guidance in the Eurocard Processor Recovery Mode section.	67
Updated the Eurocard I/O Module Safety Related Parameters.	68
Updated Attention statement regarding Input and Output Forcing.	69
Clarified that the analogue output module cannot be used for safety-related purposes in the Output Module Safety Functions section.	72
Changed <i>IEC61511 (ANSI ISA-84.00.01)</i> to <i>IEC61511</i> in the introductory Application Program Development Attention statement.	73
Updated application security guidance in the AADvance Application Security section.	73

Topic	Page
Updated the list of Safety Languages to note those that are only relevant to AADvance Workbench version 1.4.0	74
Added a new section titled Sequential Function Chart.	75
Updated the number of supported program organization units (POUs) in a project from 250 to 65,536.	76
Updated compiler verification requirements in the Compiler Verification Tool Safety Requirement section.	77
Updated the Environmental Specification table entries for Vibration, Altitude, Electromagnetic Interference, and Sub Sea Qualification.	81, 82, 82, 82
Updated SELV (safety extra-low voltage) description.	82
Updated standards in the Eurocard System Power Requirements Attention statement.	83
Added items to the Safety Requirements Checklist.	86
Added that one Safety System Checklist item is only applicable to AADvance Workbench version 1.40.	87
Updated a Safety System Checklist item with new standards references.	87
Changed the name of the <i>Workbench Safety Implementation Checklist</i> to <i>Application Checklist</i> .	88
Added items to the Associated AADvance Publications table.	91
Added glossary term Input (variable).	98
Added glossary term Mission time.	99
Added glossary term Output (variable).	99
Added glossary term Safety Requirements Specification (SRS).	101





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:

<http://www.rockwellautomation.com/global/support/overview.page>

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 Tech Connect Account or free Rockwell Automation Member Account. Account holders can subscribe to important product updates, including Product Safety Advisories and Product Notices.

To locate product notices and product safety advisories, go to the above web-page and search the Knowledgebase for *product notice Eurocard* or *product safety advisory Eurocard*.

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

<https://compatibility.rockwellautomation.com/Pages/home.aspx#/scenarios>

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 Eurocard system release 1.41 and these software:

- AADvance® Workbench software version 1.40
- AADvance Workbench software version 2.1
- AADvance®-Trusted® SIS Workstation software version 1.02.04

---

**NOTE** AADvance Eurocard 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 Eurocard 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](http://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

<http://rockwellautomation.custhelp.com>

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 please click on the following link:

[https://rockwellautomation.custhelp.com/app/answers/detail/a\\_id/898272](https://rockwellautomation.custhelp.com/app/answers/detail/a_id/898272)

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 Eurocard controllers for a Safety Instrument Function. It sets out standards (which are mandatory) and makes recommendations to make sure that installations fulfill 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 fulfilled 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.

---

**NOTE** The AADvance Eurocard controller is a logic solver. It uses processor modules and I/O modules. An AADvance system is formed by one or more controllers, their power sources, communications networks and computers.

---

## 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:

<http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page>



**Chapter 1**

**Introduction to the AADvance Eurocard Controller**

Verification of the Safety Manual ..... 17  
 Controller Subsea Certification ..... 17  
 Terminology..... 17  
     Vocabulary and Conventions ..... 17  
 AADvance Eurocard Controller - Overview ..... 18  
 Eurocard Controller System Components..... 18  
     Certified Module Revision List ..... 21  
     Software ..... 21  
     AADvanceDiscover..... 21  
 Eurocard Controller Features ..... 21  
     Eurocard Process Safety Time ..... 22  
     Fault Tolerance in Eurocard Controllers ..... 22  
     Internal Diagnostics and Fault Reporting..... 23  
     Calculations of Probability of Failure upon Demand..... 24  
 Eurocard Failure Rates..... 24  
     Eurocard System Security ..... 24  
     Communication Port Security..... 25  
     Eurocard Related Documents..... 26

**Chapter 2**

**Functional Safety Management**

The Safety Management System ..... 27  
 The Safety Life-cycle..... 27  
     Scope Definition ..... 28  
     Hazard and Risk Analysis ..... 28  
     System Functional and Safety Requirements ..... 29  
     System Engineering..... 29  
     Application Programming..... 30  
     System Production ..... 31  
     System Installation Environment ..... 31  
     System Commissioning ..... 32  
     Safety System Validation ..... 32  
     System Integration..... 33  
     Competency ..... 33  
     Operation and Maintenance Plan..... 34  
     Maintaining Functional Safety..... 34  
     Functional Safety Assessment..... 34  
 Safety Integrity Design..... 35

**Chapter 3**

**Eurocard Controller System Architectures**

Creating Eurocard Architectures ..... 37  
     Eurocard SIL 2 Fail-safe Architecture ..... 38  
     Eurocard SIL 2 Fault Tolerant Input Architecture..... 39

Eurocard SIL 2 Output Architecture ..... 40  
 Eurocard SIL 2 Fault Tolerant and High Demand Architecture 41  
 Eurocard SIL 3 Architectures ..... 42  
 SIL 3 Fault Tolerant I/O Architectures ..... 42  
 Eurocard SIL 3 Fail-safe I/O, Fault Tolerant Processor ..... 43

**Chapter 4**

**Field Configurations**

Eurocard Analogue Input Module Field Loops ..... 45  
 Eurocard Digital Input field Loops ..... 49  
 Eurocard Analogue Output Module Field Loops ..... 51  
 Eurocard Digital Output Field Loops ..... 53

**Chapter 5**

**Safety Networks**

Bindings and the SNCP Network ..... 55  
     Configuring SNCP Safety Network ..... 56  
     Configuring Variable Bindings ..... 57  
 Peer-to-Peer ..... 58

**Chapter 6**

**Eurocard Functional Safety System Implementation**

Eurocard I/O Modules in Safety Applications ..... 61  
 Energize to Action Configurations ..... 63  
 Controller Process Safety Time (PST) ..... 63  
 Sensor Configurations ..... 64  
 Actuator Configurations ..... 64  
 Eurocard HART ..... 65  
 Eurocard Processor Safety Functions ..... 66  
 Processor Functional Safety Configuration ..... 67  
     Eurocard Processor Module Reaction to Faults ..... 67  
     Eurocard Processor Recovery Mode ..... 67  
 I/O Module Safety Functions ..... 68  
     Eurocard I/O Module Safety Related Parameters ..... 68  
     I/O Module Process Safety Time (PST) ..... 68  
     Input and Output Forcing ..... 69  
     Maintenance Overrides ..... 69  
 Input Module Safety Functions ..... 70  
     Reactions to Faults in the Input Modules ..... 71  
     Input Data Safety Accuracy ..... 71  
 Output Module Safety Functions ..... 72  
     Digital Output Module Safety Functions ..... 72  
     Eurocard Analogue Output Module ..... 73  
 Application Program Development ..... 73  
     AADvance Application Security ..... 73  
     Language Selection ..... 74  
     Testing of New or Previously Untested Functions ..... 75

Compiler Verification Tool Safety Requirement ..... 77  
 Communications Interaction..... 78  
 Program Testing..... 79  
 On-line Modification..... 80  
 Eurocard Module Physical Installation ..... 80  
 Environmental Requirements ..... 81  
 Environmental Specification AADvance Eurocard Controller .... 81  
 Eurocard Electromagnetic Capability ..... 82  
 Eurocard Shielded Cable for Ethernet and Serial Ports..... 82  
 Eurocard System Power Requirements ..... 82

**Chapter 7**

**Checklists**

Pre-Engineering Checklists..... 85  
 Scope Definition Checklist..... 85  
 Functional Requirements Checklist ..... 86  
 Safety Requirements Checklist..... 86  
 Processor Checklist ..... 86  
 Safety System Checklist ..... 87  
 Application Checklist..... 88  
 Safety Networks Checklist ..... 88  
 I/O Checklist ..... 89  
 Override Requirements Checklist..... 90  
 Testing Checklist..... 90

**Chapter 8**

**Additional Resources**

Associated AADvance Eurocard Publications..... 91

**Glossary .....93**





## Introduction to the AADvance Eurocard Controller

This chapter introduces the Safety Manual for an AADvance Eurocard controller.

### Verification of the Safety Manual

The AADvance Eurocard system and the user Safety Manual are certified by an independent certification body to meet the requirements of IEC 61508 SIL 3. This Safety Manual was reviewed as part of the assessment.

### Controller Subsea Certification

Subsea Qualification: The Eurocard Modules have been tested to the Q1 requirement specified in Section 9.2.3.2 of API 17F, Edition 4 (Errata 1 & 2).

### Terminology

The terms certification and certified are used in this Manual, this refers to the functional safety certification of the system to IEC 61508 SIL 3 and other related standards.

### 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 Eurocard system to IEC 61508 SIL 3 and other relevant standards.

This Manual contains rules and recommendations:

- **Rules** are mandatory and must be followed if the resulting safety system is to be a SIL3 compliant application. These are identified by the term '**must**' in the Safety instructions.
- **Recommendations** are not mandatory, but if they are not followed, extra safety precautions must be taken in order to certify the system. Recommendations are identified by the term '**it is highly recommended**'.

## AADvance Eurocard Controller - Overview

The AADvance Eurocard system is specifically designed for functional safety and critical control applications, it supplies a flexible, scalable and distributed solution for these applications. The system can be used for safety implemented functions and process control applications that are non-safety but critical to a business.

The controller is a logic solver that has processor modules, I/O modules and field termination assemblies, a system can be configured specifically to a user's process control requirements. It runs project applications developed and deployed from the AADvance® Workbench software or AADvance®-Trusted® SIS Workstation software.

A system is assembled from one or more controllers, a combination of I/O modules, power sources, communications networks and user computers. It can operate as an independently functioning system or as a distributed node of a larger system.

A Eurocard configuration starts with two processor modules and I/O modules, and can be expanded to a maximum of three processor modules and 18 I/O modules. The modules are standard Eurocard PCBs that are coated for protection. This design allows a user to choose a different container as an alternative to a standard rack installation. It enables a controller to be used in diverse and more unusual operational environments.

AADvance Eurocard modules are designed to allow the use of custom wiring harnesses or a custom-designed backplane. The wiring loom design will be based on the system configuration of processors and I/O modules that make up the controller. Details about building a wiring loom and connecting the modules using it are given in the topic "Wiring Loom Requirements".

## Eurocard Controller System Components

An AADvance Eurocard controller can be assembled from the following modules and assemblies:

- A 9120 Eurocard Processor Module is built from a Eurocard Processor CPU PCB and a Eurocard Processor Interface PCB: The Processor performs all the processing functions and application logic solving, internal and external communications with the redundant I/O control network and external networks, I/O scanning, and it initiates the built-in diagnostic testing processes.
- 9531 Eurocard Analogue Input Module, 8 Ch. Isolated: Analogue input modules are simplex modules. Redundancy is created by the wiring harness connecting two input modules together and to the dual analogue input termination assembly.
- 9501 Eurocard Digital Input Module, 24 V dc, 8 Ch. Isolated: Digital input modules are simplex modules. Redundancy is created by the wiring harness connecting two input modules together with the same field connections to each module.

- 9842 Euro Analogue Input Termination Assembly (TA), 8 Ch. Simplex: The TA supplies the field connections for the analogue input signals and interfaces with the 9531 Eurocard Analogue Input Module through a high reliability hypertac connector. Also supplies a higher load termination resistance and is useful for underwater applications.
- 9551 Eurocard Digital Output Module, 8Ch, Isolated, commoned: This supplies signals applicable for directly interfacing to the output field devices. A simplex output module is always two output switches in series, fault tolerance occurs when two modules operate in parallel. These modules supply the voltage and current for each channel, the values given when configured in a redundant configuration are the sum (or combined) value for the two modules operating in parallel.
- 9581 Eurocard Analogue Output Module: This supplies signals for directly interfacing to the analogue field devices. Analog Output modules are simplex, but have a fail safe disconnect switch.

---

**NOTE** Eurocard Analogue Output modules are designed and developed using the same methods as all other Eurocard modules, but at this time they cannot be used in a redundant group arrangement and are not approved for use in a safety related application. They can be considered as non-interfering when used as part of a safety system.

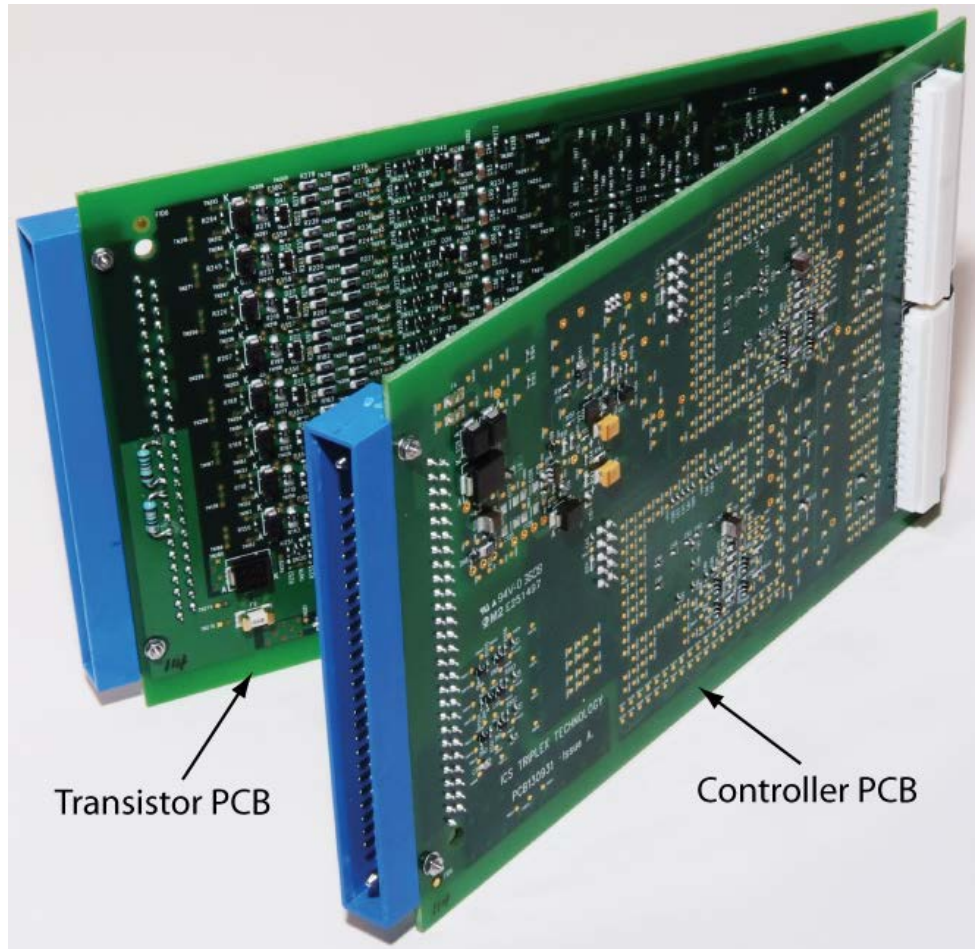
---

All Eurocard modules have comprehensive built-in diagnostics, in the event a fault, a redundant configuration with diagnostics maximizes system availability.

### Typical Eurocard Module Hardware

The following illustration shows the typical Eurocard module variant:

**Figure 1 - Eurocard Module (Digital Output)**



### Communications Interfaces

The configuration, programming, and maintenance interface to this controller is through the 10/100 Base T Ethernet ports located on the processor modules.

The Ethernet and serial ports can be configured to use a number of different communication protocols in simplex and redundant configurations for connection to other AADvance Eurocard controllers or third party equipment. Communications between the processors and I/O modules uses a proprietary communications protocol over a custom wired harness.

A safety network control protocol (SNCP), developed by Rockwell Automation for the AADvance system, permits distributed control and safety using new or existing network infrastructure while making sure the data is secure and has integrity. 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 distributed system can be administered from one or more computers placed at convenient locations.

## Certified Module Revision List

Latest list of hardware and firmware configurations, as approved by the certifying body, is available in the Literature Library as Eurocard AADvance Controller - Safety certificate. The document number is [ICSTT-CT007](#). A list of compatible module configurations is available in the Release Notes on the Product Compatibility and Download Center (PCDC).

## Software

### AADvance® Workbench software or AADvance®-Trusted® SIS Workstation software

The application development software is known as the AADvance Workbench software or AADvance-Trusted SIS Workstation and is used to configure and program your system. It is compliant with IEC 61131-3 and is a complete software environment for a controller. It supplies the tools to create local and distributed control applications using the five languages of IEC 61131-3. Refer to the AADvance Configuration Guide (Doc. [ICSTT-RM405](#)) for information about configuring your system.

### AADvanceDiscover

The AADvanceDiscover utility uses a Discovery and Configuration Protocol (proprietary to Rockwell Automation) to find and identify AADvance devices connected to the control network, and to configure the controller identifiers, and network IP addresses of those devices. Refer to the AADvance Configuration Guide (Doc. [ICSTT-RM405](#)) for information about using the AADvance Discover utility.

## Eurocard Controller Features

An AADvance Eurocard system controls complex and frequently critical processes in real time executing programs that accept external sensor signals, find a solution for logic equations, do calculations for continuous process control and generating control signals.

The AADvance Eurocard system key features are as follows:

- Fail safe or fault tolerant topologies — 1oo1, 1oo2D and 2oo3.
- Flexible construction using modules to assemble a bespoke system.
- Operates independently as a functional system or as part of a larger distributed network.
- Can be used for a fault tolerant safety related system.

- The Black Channel I/O bus facilitates the interconnection of mixed architectures consisting of both AADvance and AADvance Eurocard Technologies.
- Scalable I/O module expansion without system interruption.
- Provides a secure SIL 3 rated 'Black Channel' external communication network over Ethernet.
- IEC 61508 certified
- Supports industry standard protocols such as HART.
- Supports OPC when using an OPC Portal or Standalone OPC Server.

## Eurocard Process Safety Time

The generally accepted understanding of process safety time is the period 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 Eurocard Controllers

For safety applications you must define how the control system will react when there are faults. As faults multiply, this becomes the system's state of degraded operation or fault tolerance level.

AADvance Eurocard Systems can be configured as either fail safe, fault tolerant or as a combined fail safe/fault tolerant architecture. Dual or triple processors are required for a SIL 2 or SIL 3 safety system.

Fail Safe architectures are where single AADvance Eurocard system modules are used. For this architecture, when a fault is identified in a module, the faulty module (or part of a module) will go to its safe state (e.g. off, or de-energized).

Fault tolerant architectures are where redundant modules are configured. When a fault occurs in a module, although the faulty module (or part of a module) will go to its safe state, the redundant partner module will continue its usual operation and the data processing is not interrupted.

Combined architectures are where combinations of single and redundant modules are used where applicable for the safety functions being put in place.

## Internal Diagnostics and Fault Reporting

Internal diagnostics are necessary for fault tolerance. The AADvance Eurocard controller has sophisticated internal diagnostic systems to identify faults that occur during operation and raise applicable alarm and status indications. The diagnostic systems run automatically and test for system faults related to the controller (processor and I/O modules), and field faults related to field I/O circuits.

The internal diagnostics detect and report safe and dangerous failures. A dual module arrangement, for example, diagnostics can address dangerous failures and help redress the balance between failure to react and spurious responses. Thus a dual system could be 1oo2D reverting to 1oo1 on the first identified fault and reverting to fail-safe when the two modules have a fault.

The comprehensive internal diagnostics that find and show covert and overt failures and report a serious problem immediately, but filter unimportant safe failures to prevent spurious alarms. The diagnostic systems monitor these less important items regularly and do not report them as a problem unless there have been many occurrences of a possible fault. These diagnostics will tell users that there are faults so that users can repair the system in the MTTR (used for the PFD calculations) and maintain the system's fault tolerance and integrity level.

To clear latched diagnostic faults after the initiating cause is resolved, use the remote fault reset feature.

---

**NOTE** The remote fault reset feature clears any latched fault condition. If the initiating cause is not resolved, faults will be re-annunciated, but this may be seconds-to-hours after the reset, depending on the fault type or fault class.

---



**WARNING:** Safety wiring principles must be employed for field loops if it is necessary for the user to guard against short circuit faults between I/O channels. The AADvance Eurocard controller internal diagnostics do not identify external short circuits between channels.

---

**NOTE** Refer to the AADvance Configuration Guide Doc No: [ICSTT-RM405](#) for the SIS Workstation Online help for instructions on how to configure the 'Remote Reset' feature.

---

## Calculations of Probability of Failure upon Demand

For information regarding the calculation, also for PFD/PFH numbers allocated for the AADvance system refer to the PFD calculation document (Doc No: [ICSTT-RM449](#) AADvance Controller and AADvance Eurocard Controller PFH and PFD<sub>avg</sub> Data) listed in the approved version list.

## Eurocard Failure Rates

For the purposes of Failure Rate calculation, AADvance products have a useful lifetime of 20 years. Refer to [ICSTT-RM449](#) for AADvance Controller and AADvance Eurocard Controller PFH and PFD<sub>avg</sub> Data.

## Eurocard System Security

AADvance serial networks are closed and local and have limited protocol functionality, so they are immune to any external attack apart from local deliberate sabotage. The AADvance Eurocard system, however, with its computers and DCS interfaces, uses Ethernet networks which are frequently part of a larger corporate network and can expose the system to accidental or malicious infection or attack.

The following general security steps should be used to ensure 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, preventing 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 AADvanceDiscovery utility so it may be necessary to temporary disable the Firewall when using this tool.

---

- The computer must be password protected.
- If the computer is a laptop, it must be kept locked when not in use.
- If the computer uses a hardware license USB dongle it must be kept secure, without it the computer will not run.
- The AADvance Workbench software or AADvance-Trusted SIS Workstation software must be password protected. This can be done when the software is installed.



The application must be password protected if a program enable key is not used on the system.

### Threat Analysis

A security risk assessment must be performed and all identified risks must be appropriately mitigated before the system is commissioned.

## Communication Port Security

The Rockwell Safety Network Control Protocol (SNCP), used by the AADvance system, permits distributed control and safety using new or existing network infrastructure as a 'Black Channel' 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; rather, the complete distributed system can be administered from one or more computers placed at convenient locations.

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 1 - AADvance Communication Ports**

Protocol	Port Number	Availability	Purpose
TCP	502	When configured	MODBUS Slave
TCP	1132	Always available	ISaGraf, application downloads, debug, SoE etc.
TCP	10001- 10006	When configured (and the application is stopped)	Transparent Comms Interface (Serial Tunnelling)
TCP	44818	Always available	CIP Produce & Consume
UDP	123	When configured	(S)NTP
UDP	1123,1124	Always available	IXL 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 or controller	Trusted peer-to-peer
UDP	44818	Always available	CIP Producer & Consume



**WARNING:** Unused open ports that are not configured should be blocked, this can be done at the firewall settings. Refer to the AADvance Workbench Configuration Guide or SIS Workstation Online help for the instructions about blocking these ports.

## Eurocard Related Documents

The following documents are related to the safety requirements applicable to the AADvance Eurocard controller and its applications.

**Table 2 - Reference Documents**

Document	Title
IEC 61508:2010 Part 1-7	Functional safety of electrical/electronic programmable safety-related systems
EN 61131-2:2017	Programmable controllers – Part 2: Equipment requirements and test
IEC 61326-3-1	Electrical equipment for measurement, control and laboratory use - EMC

---

**IMPORTANT** Users must consider any National, Regional and Industrial standards when building and operating a system.

---

# 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. Frequently, the Safety Management and Quality systems will be integrated in a single set of procedures. The integrator must have an accredited quality management system.

The Safety Management System must include:

- A statement of the policy and strategy for achieving and maintaining functional safety.
- A safety planning procedure, which will cause 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, as well as change control. The change control procedures must include records of modification requests, the impact analysis of proposed modifications and the approval of modifications. The baseline for change control must be specified clearly.
- Configuration items must 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 making sure that persons are competent to do activities and fulfill their responsibilities.

## The Safety Life-cycle

The safety life-cycle is specified by the IEC 61508 standard. It is designed to structure a system's development into specified 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 adjustment
- Decommissioning

The definition of each life-cycle stage must include its inputs, outputs and verification activities. It is not necessary to have different stages in the lifecycle addressing each of these elements independently; but it is important that all of these stages are covered during the lifecycle. Specific items that must be considered for each of these life-cycle elements are specified 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 give a clear definition of its interfaces with the process and with all third party equipment. This stage must also show the derived requirements resulting from the intended installation environment, such as environmental conditions and power sources.

In most cases, the client will supply this information. The system integrator must review this information and get a full understanding of the intended application, the bounds of the system to be supplied and its intended operating conditions.

## Hazard and Risk Analysis

The hazard and risk analysis has three objectives:

- The first objective is to identify the hazards and hazardous events of the controlled system for all reasonably foreseeable circumstances, such as fault conditions and misuse.
- Secondly, the event sequences that can cause a hazardous event must be specified.
- Lastly, the risks related to the hazardous event must be specified.

This risk analysis will supply 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 must be allocated to specified 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 must be clearly identified. Where non-standard field devices, communications interfaces or communications protocols are necessary, it is especially important that detailed requirements for these interfaces are established and documented at this stage.

The client must give the functional requirements, where this information is not supplied the requirements must be specified by the System Integrator and they must agree them with the client. Although, it is also necessary to collate these requirements into a document, together with any clarification of the requirements. It is recommended that logic diagrams be used to show 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 find their safety relevance. Where necessary, other safety requirements must be identified and documented to make sure 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 necessary safety integrity level and safety-related timing requirements must be specified for each safety-related function. For each function the required safety failure mode must be determined. The client must supply this information or it must be specified and agreed with the client as part of this phase. The System Integrator must make sure 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 different stages, the first defining the overall system architecture, and the second detailing the engineering of the different architectural blocks.

The architectural definition must show 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 must be specified at this stage.

The detailed engineering design will refine the architectural elements and culminate in specialized information for system build. The design will 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 must make sure that procedural methods are devised and applied to identify them.

The system design must include facilities to permit field maintenance tasks to be done.

Each installation will be designed to make sure that the control equipment is operated in environments that are within its design tolerances. Therefore, the operating environment will supply the proper control of temperature, humidity, vibration and shock and sufficient shielding and earthing to decrease the exposure to sources of electromagnetic interference and electrostatic discharge.

## Application Programming

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

An overall application program software architecture must be specified at the application programming stage. This architecture will identify the software blocks and their functions.

The application programming will address methods for addressing system specific testing, diagnostics and fault reporting.

It is highly recommended that simulation testing be performed on each software block. The simulation testing must be used to show that each block does its intended tasks and does not fulfill unintended functions.

It is also highly recommended that software integration testing is done in the simulation environment before commencing hardware-software integration. The software integration testing must show that all software blocks interact correctly to do their intended tasks and do not perform unintended functions.

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

- **Architectural definition.** The application program will be divided into self-contained 'blocks' to simplify the implementation and testing. Safety and non-safety functions must be kept apart as far as possible at this stage.
- **Detailed design and coding.** The detailed design and coding stage will add detail to the design and implement each of the blocks identified by the architectural definition.
- **Testing.** The testing stage will make sure that the operation of the application is satisfactory; it is recommended that the application blocks first be tested individually and then integrated and tested together. All of this testing must be initially done within the simulation environment.
- **Fault handling strategy.** This stage defines the fault handling strategy.

The resultant application software will be integrated with the system hardware and full integration testing performed on the system.

## System Production

The system production stage implements the detailed system design. The production techniques, tools and equipment, together with those used for production testing of the system, must be applicable for the specified safety requirements class.

## System Installation Environment

An AADvance Eurocard system can be installed in a non-hazardous environment. The installation environment can be a source of common cause failure so it is necessary that the installation assessment not only covers the environmental specification for the AADvance Eurocard system but also includes the following:

- the prevailing climatic conditions.
- type of area, e.g; is it a 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.

In a non-hazardous environment a system does not have to be installed in an enclosure; however, the area where it is installed must not be more than a Pollution Degree 2 environment in accordance with IEC 61010-1.

The surrounding air temperature ratings are:

- For the 9120 Processor module = 70 °C
- For all other I/O modules and termination assemblies = 70°C

## 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.

The surrounding air temperature ratings are:

- For the 9120 Processor module = 70 °C
- For all other I/O modules and termination assemblies = 70 °C

### 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 the enclosure and making a decision about the installation environment.

### Physical Installation

The installation process is a potential source of common cause failure, therefore it must be in line with the following:



**WARNING:** You must use the installation guidelines given in the AADvance Eurocard Controller System Build Manual [ICSTT-RM455](#) and installation and any commissioning procedures that comply with applicable international or local codes and standards.

---

### System Commissioning

The commissioning stage is to prove the system installation and make sure that there is correct 'end-to-end' functionality, together with the connection between the controller and the requisite sensors and final elements. It is likely that groups of functions are commissioned in stages rather than all of the system, for example accommodation area functions before production functions. It is important that the commissioning sequence is specified and the measures to be taken to make sure operation is safe during such periods of partial commissioning. These measures must be system specialized and must be defined clearly before starting any commissioning. It is also important to define that any temporary measures implemented for test purposes, or to permit partial commissioning, are removed before all of the system goes live.

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

### Safety System Validation

Safety system validation will test the integrated system to make sure that it is compliant with the safety requirements specification at the intended safety requirements class. The validation activities must include those necessary to



show that the system implements the safety actions during normal start-up and shutdown and under abnormal fault modes.

The validation will make sure that each functional safety requirement has been put in place 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 will also look at the possible external common cause failures (power sources and environmental conditions) and make sure that the system will supply fail-safe operation when these conditions surpass its design capabilities.

## System Integration

The system integration stage will integrate the application programs with the controller. Where multiple systems are used to satisfy 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 satisfy the requirements of the intended safety requirements class, the system integration will make sure that there is full compliance of the software and hardware with the functional safety requirements.

## Competency

The achievement of Functional Safety requires that safety functions are put in place and maintained during the Safety Life-cycle by persons that are competent in Functional Safety systems.

The following competence factors must be addressed when assessing and justifying the competency level of persons to do their duties:

- Engineering experience applicable to the application area
- Engineering experience applicable to the technology
- Functional safety engineering experience applicable 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 involvement and whether it is related to the duties that are to be undertaken and the technology being used.

---

**IMPORTANT** If the correct level of competence does not exist, training and procedures must be developed to attain the necessary levels of competence.

---

## Operation and Maintenance Plan

An Operation and Maintenance Plan helps to make sure that functional safety can be maintained after 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 give guidance and use procedures to make sure that the persons or organizations accountable for operation and maintenance can keep the system operating to the specified safety levels.

- The Operating and Maintenance Plan must include the following items:
- Clear definitions of power up and power down sequences. These definitions must make sure that the sequences never cause resulting periods when the system cannot operate safely when a hazard is present.
- The procedures for re calibrating sensors and actuators. The recommended calibration periods must be included.
- The procedures for frequently testing the system at regular intervals, together with definitions of the maximum intervals between testing.
- Definitions of the overrides to be applied to be able to do maintenance to the sensors and actuators.
- The procedures for maintaining system security.

## Maintaining Functional Safety

Design changes will inevitably occur during the system life-cycle; to make sure that the system safety is preserved, such changes must be carefully managed. Procedures defining the measures for updating the plant or system must be specified and documented. These procedures are the responsibility of the end user, but the system integrator must supply sufficient guidance so that the procedures keep the required level of functional safety during and after the changes.

## Functional Safety Assessment

The functional safety assessment will make sure that the functional safety performance of the system is effective. The assessment, in this context, is limited to the safety-related system and must make sure that the system is designed, constructed and installed in accordance with the specified safety requirements.

The assessment will look at each required safety function and its related safety properties. The effects of faults and errors in the system and application programs, failures external to the system and procedural deficiencies in these safety functions are to be looked at.

The assessment is to be completed by an audit team that must include independent assessors from outside of the project. At least one functional

safety assessment must be done before the start-up of the system and the introduction of any possible hazards.

## **Safety Integrity Design**

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

All modules have built in redundancy and have been designed to be resistant to multiple faults.



## Eurocard Controller System Architectures

This chapter explains the different system architectures that can be configured for an AADvance Eurocard controller. A controller can be configured to manage the following safety related system requirements:

- non-safety applications
- low demand or high demand fault tolerant applications
- SIL 2 low demand and high demand applications
- SIL 3 safety related system application

---

### IMPORTANT ANALOGUE OUTPUT MODULES

The Eurocard Analogue Output Module has not been verified or certified for use in a Safety System. It cannot be used as part of a safety path and it cannot be used in a dual redundant configuration. It will not, however, interfere with the other modules used in a Safety System.

---

### Supported Modules and Configurations

Module type	AADvance Eurocard Variant	Supported Configurations
Processor	T9120	Dual or TMR
Digital Input 8 Channel Isolated	T9501	Simplex or Dual
Analogue Input 8 Channel Isolated	T9531	Simplex or Dual
Digital Output 8 Channel	T9551	Simplex or Dual
Analogue Output 2 Channel	T9581	Simplex Two Isolated Channels Non-interfering

## Creating Eurocard Architectures

To create a controller architecture for different applications you install the modules in the required hardware arrangement and then configure the same arrangement using the AADvance® Workbench software or AADvance®-Trusted® SIS Workstation software. The processor module will make sure that the internal software configuration matches the hardware arrangement.

The modules can be arranged to supply two fundamental architectures based on dual and triple processor configurations. To these can be added I/O modules in redundant and/or fault tolerant configurations based on the following arrangements:

- Input modules in simplex, dual redundant formations
- Output modules in simplex and dual arrangements (not Analogue Output modules)

A system can use different I/O architectures in one controller; for example, you can configure simplex and dual input modules with dual processor modules. The construction of the controller enables you to create numerous other arrangements that can be tailored for a specified application.

The wiring loom hypertac connectors have polarization keying set to match the polarization on the Eurocard PCB connectors. Each Eurocard PCB connector has polarizing positions printed on the PCB side of the connector; one polarizing pip will align with a number and the other with a letter.

**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, publication [ICSTT-RM405](#), or the AADvance-Trusted SIS Workstation Software User Guide, publication [ICSTT-UM002](#), for information about these procedures.

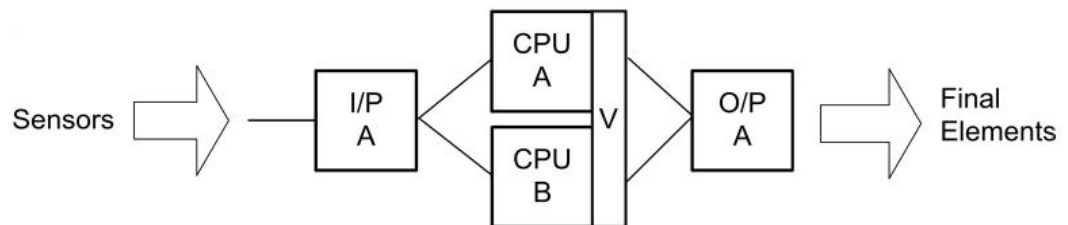
**Eurocard SIL 2 Fail-safe Architecture**

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.

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

**Figure 2 - Non-Safety and SIL 2 Fail-safe Architecture**



**Table 3 - Modules for SIL 2 Fail-Safe Architecture**

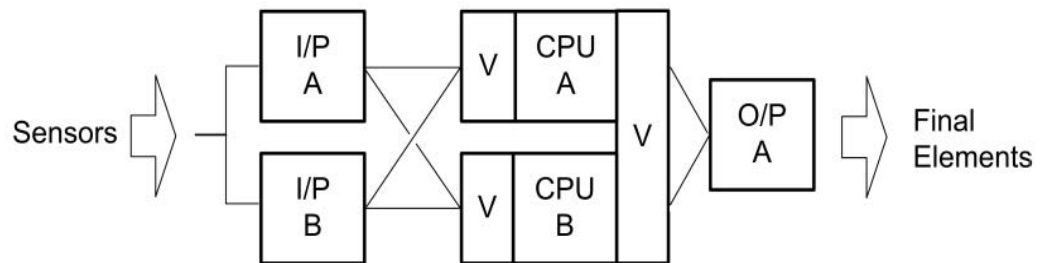
Module type	Position
T9501 Digital Input Module, 24V dc, 8 Channel or T9531 Analogue Input Module, 8 Channel + T9842 Analogue Input TA, 8 Channel, Simplex	I/P A
2 x T9120 Processor Module	CPU A and CPU B
T9551 Digital Output Module, 24V dc, 8 Channel, isolated	O/P A

### Eurocard SIL 2 Fault Tolerant Input Architecture

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.

**Figure 3 - SIL 2 Fault Tolerant Input Architecture**

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 processors. The output module operates in 1oo1D under no fault conditions and will fail-safe on the first identified fault.

---

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

---

**Table 4 - Modules for SIL 2 Architecture**

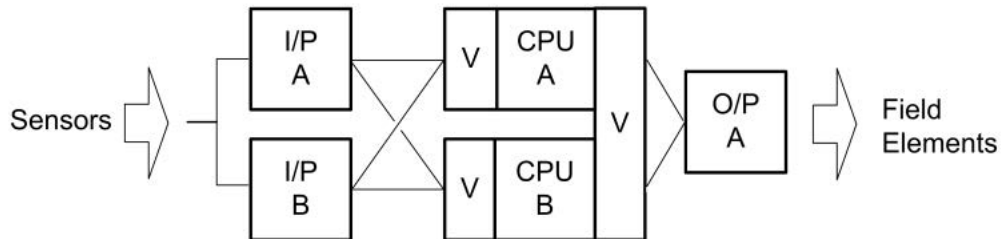
Module Type	Position
2 x T9501 Digital Input Module, 24V dc, 8 Channel or 2 x T9531 Analogue Input Module, 8 Channel, Isolated, + 2 x T9842 Analogue Input TA, 8 channel, simplex	I/P A and I/P B
2 x T9120 Processor Module	CPU A and CPU B
T9551 Digital Output Module, 24V dc, 8 Channel	O/P A

### Eurocard SIL 2 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.

**Figure 4 - SIL 2 Output Architecture (Redundant Input Modules Shown)**



The following conditions apply:

**Table 5 - Modules for SIL 2 Fault Tolerant Output Architecture (Redundant Input Modules Used)**

Module Type	Position
2 x T9501 Digital Input Module, 24V dc, 8 Channel. or 2 x T9531 Analogue Input Module, 8 Channel + 2 x T9842 Analogue Input TA, 8 Channel, Simplex	I/P A and I/P B
2 x T9120 Processor Module	CPU A and CPU B
1x T9551 Digital Output Module, 24V dc, 8 Channel	O/P A



## Eurocard SIL 2 Fault Tolerant 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.

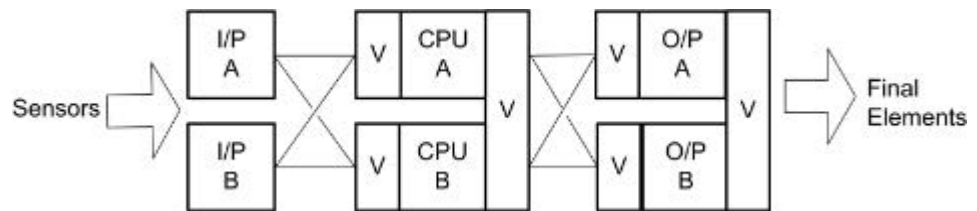
A triple input module arrangement can also be configured if it is required to increase the fault tolerance of the input. When a triple input module arrangement is configured the input modules operate in a 2oo3D under no fault conditions, degrade to 1oo2D on detection of the first fault in any module, 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 SIL 2 fault tolerant applications you must use a minimum of a dual processor configuration. Dual output modules are necessary for energize to action applications.

**Figure 5 - SIL 2 Fault Tolerant Input Architecture**



**WARNING:** For Continuous Mode applications the measures specified in this section for SIL 2 fault tolerant applications must be applied.

**Table 6 - Modules for SIL 2 Fault Tolerant High Demand Architecture**

Module Type	Position
2 × T9501 Digital Input Module, 24V dc, 8 Channel or 2 × T9531 Analogue Input Module, 8 channel + T9842 Analogue Input TA, 8 channel, simplex	I/P A and I/P B
2 x T9120 Processor	CPU A and CPU B
2 × T9551 Digital Output Module, 24V dc, 8 Channel	O/P A and O/P B

### Eurocard SIL 3 Architectures

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

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

Faulted input modules in a SIL 3 arrangement can 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 identified fault, the system must be restored to at least 1oo2D by replacing the faulty processor module within the MTTR assumed in the PFD calculations or 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.

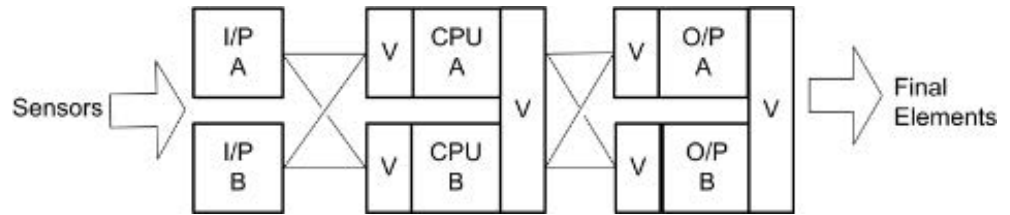
### SIL 3 Fault Tolerant I/O Architectures

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 identification of the first fault in one of the two modules and fail-safe when there are faults on the two modules.

Similarly the input modules operate in 1oo2D under non faulted conditions and 1oo1D on the identification of the first fault in one of the two modules and will fail-safe when there are faults on the two modules.

The processor must be repaired within the MTTR assumed in the PFD calculations or SIL 3 safety instrumented functions must be shutdown.

**Figure 6 - SIL 3 Fault Tolerant I/O Architecture**



### Digital Output Modules

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

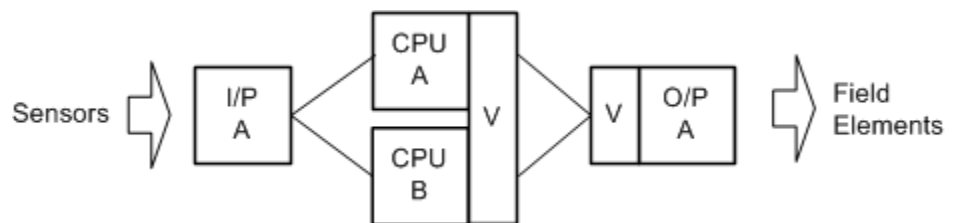
**Table 7 - Modules for SIL 3 Fault Tolerant Architectures**

Module Type	Position
2 × T9501 Digital Input Module, 24V dc, 8 Channel or 2 × T9531 Analogue Input Module, 8 Channel + 2 × T9842 Analogue Input TA, 8 channel, simplex	I/P A and I/P B
2 × T9120 Processor Module	CPU A and CPU B
1 × T9551 Digital Output Module, 24V dc, 8 Channel for de-energize to action. or 2 × T9551 Digital Output Module, 24V dc, 8 Channel for energize to action.	O/P A and O/P B

### Eurocard SIL 3 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 degrade to 1oo1D on detection of the first fault in one of the two modules. When there are faults on the two modules the configuration will fail-safe.

**Figure 7 - SIL 3 Fail-safe I/O with Fault Tolerant Processor Architecture**



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.

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

Module Type	Position
T9501 Digital Input Module, 24V dc, 8 Channel or T9531 Analogue Input Module, 8 channel + T9842 Analogue Input TA, 8 Channel, Simplex	I/P A
2 x T9120 Processor Module	CPU A and CPU B
1 x T9551 Digital Output Module, 24V dc, 8 Channel	O/P A

## Field Configurations

The following are recommended field loop circuits for the I/O modules.



**ATTENTION:** Use cable monitoring and circuit integrity cable as applicable for the application, because inter-channel short circuits cannot be identified by an AADvance Eurocard controller.

---

**NOTE** You must make sure that there is no crossover between channels.

---

### Eurocard Analogue Input Module Field Loops

For analogue input field loops use 22 AWG multi core cabling and connect to the termination assembly connector. For a SELV system power environment The 24 Vdc input voltage must be fused and the recommended fuse rating is 50 mA.

#### 2- Wire Analogue Input Field Loop Circuit

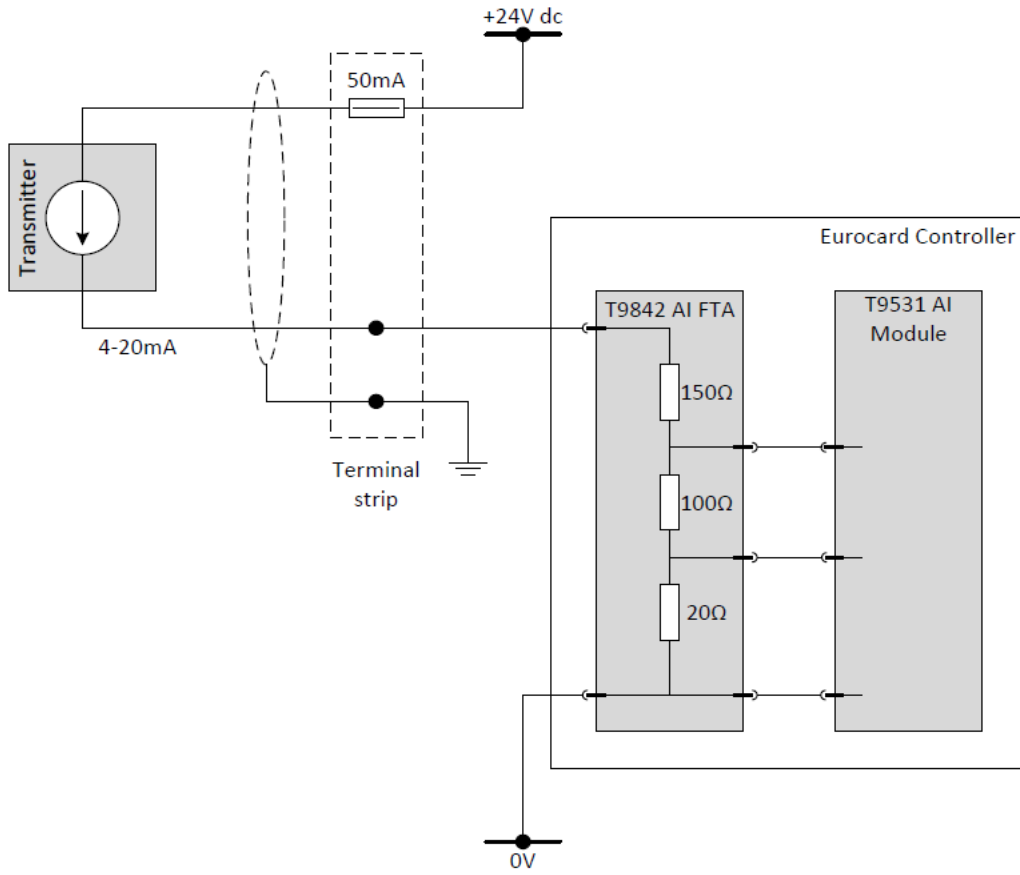
This field loop connection method is used for 2-wire field devices.

---

**IMPORTANT** The 150  $\Omega$  \* resistor is rated to tolerate sustained operation and limits the maximum current through the circuit when the transmitter loop is short circuited.

---

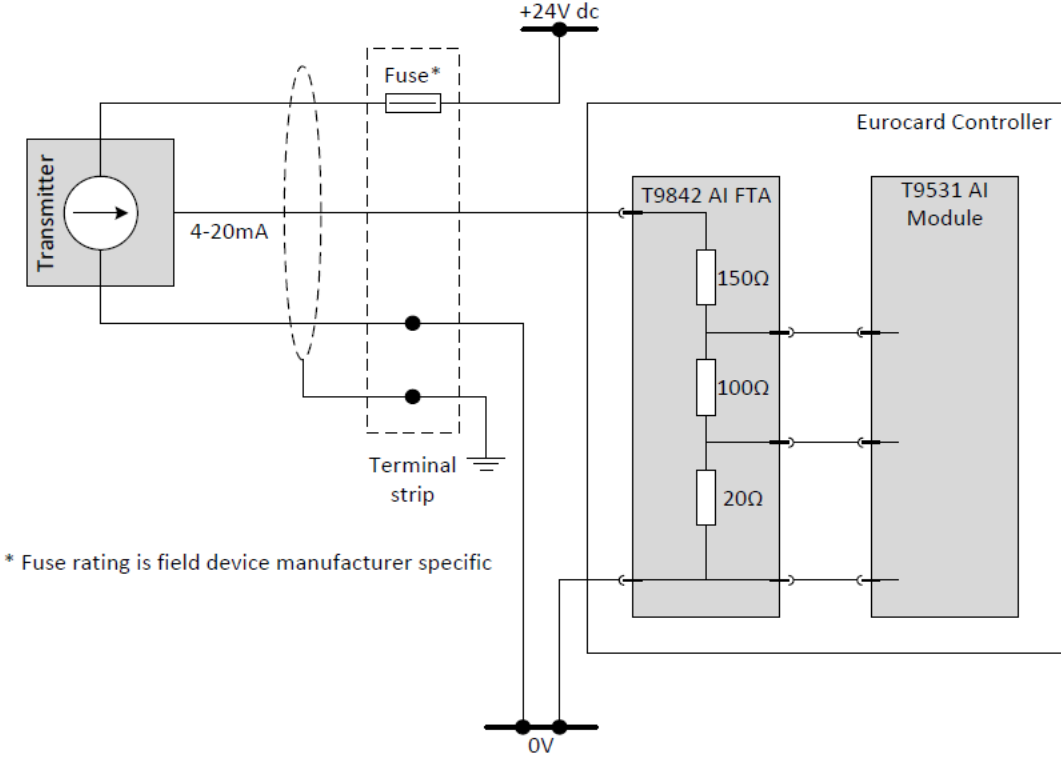
Figure 8 - Analogue Input 2-Wire Field Element Wiring



### 3-Wire Analogue Input Field Circuit

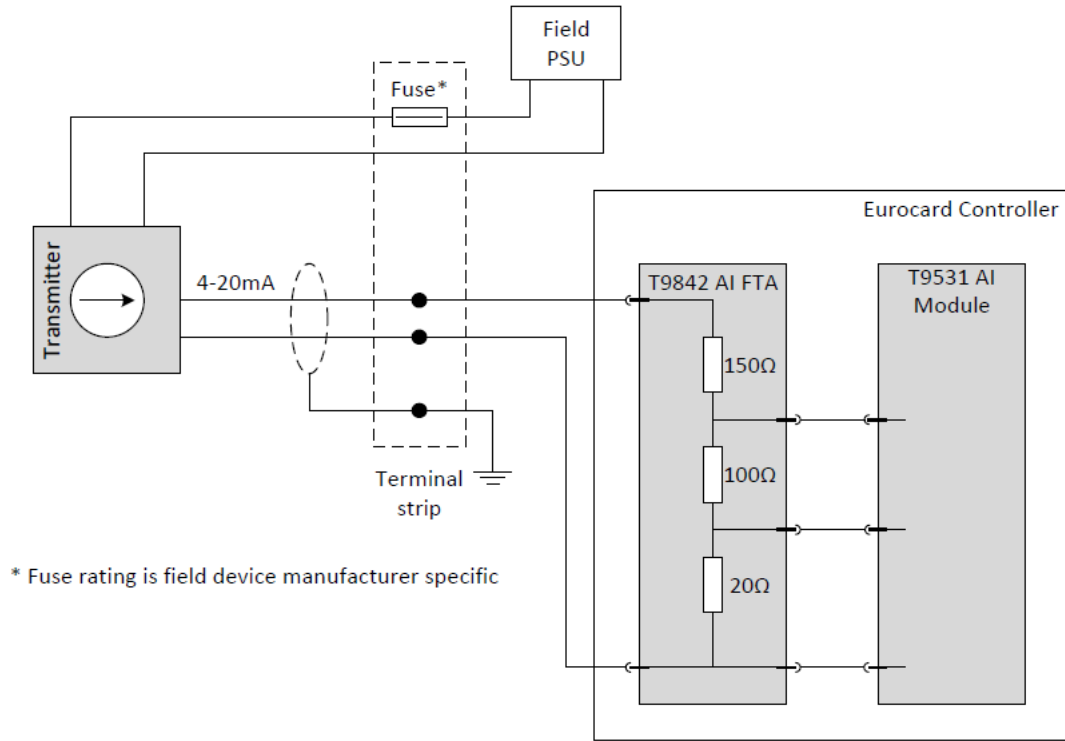
This field loop connection method is used for 3-wire analogue field devices.

Figure 9 - Analogue Input 3-wire Field Element Wiring



### 4-Wire Analogue Input Field Loop Circuit

This field loop circuit is method is used for 4-wire analogue field devices.

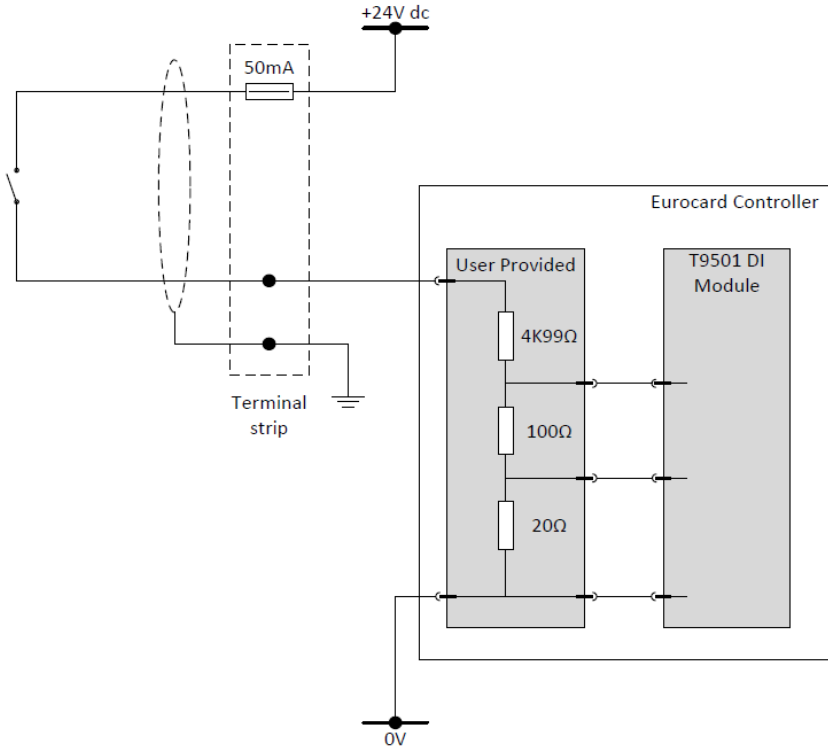




# Eurocard Digital Input field Loops

You can set up the field loops for digital input with or without line monitoring.

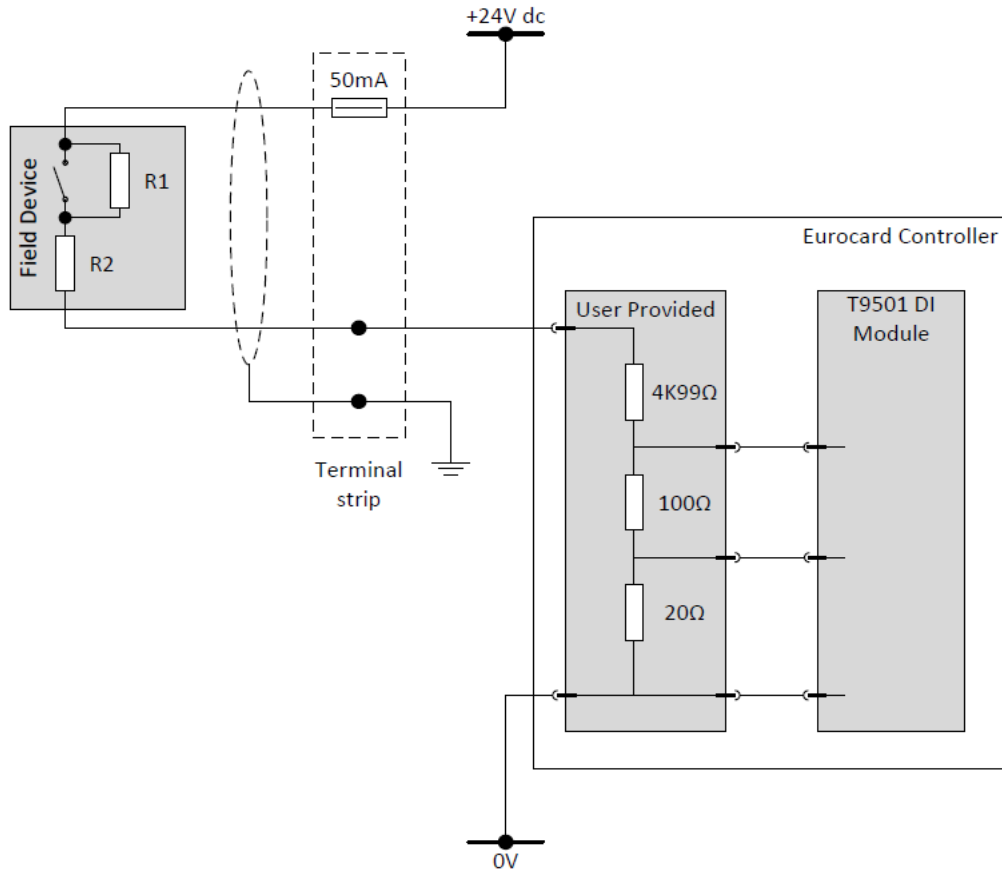
## Standard Field Loop



User-Provided Termination Resistor Specification		
Resistance	Tolerance	Power
4K99Ω	5%	1W
100Ω	0.1%	1W
20Ω	0.1%	1W

### Line Monitoring Field Loop for ESD

Figure 10 - Line Monitoring for ESD



The recommended values for R1 and R2 are as follows:

- R1 = 15 KΩ 1 %, 1 W (maximum power dissipated is 47 mW at 26.4 V)
- R2 = 3K9Ω 1%, 1 W (maximum power dissipated is 182 mW at 26.4 V)

Recommended threshold values for ESD line monitoring:

Threshold ID	Value mV
Maximum Allowed	= 32000
<b>SHORT CIRCUIT</b>	
Threshold 8	= 19000
Threshold 7	= 18500
<b>ON (nominal 16 V)</b>	
Threshold 6	= 11000
Threshold 5	= 10500
<b>INDETERMINATE</b>	
Threshold 4	= 6500
Threshold 3	= 6000
<b>OFF (nominal 8 V)</b>	

Threshold ID	Value mV
Threshold 2	= 3500
Threshold 1	= 3000
	<b>OPEN CIRCUIT</b>

#### Assumptions

- Loop supply voltage =  $24V \pm 10\%$
- Maximum field cable line resistance:  $< 100 \Omega$  this means  $50\Omega + 50 \Omega$  for the two cables.
- Minimum isolation between the field loop connectors is  $0.75 M\Omega$ .
- These values will let the input find more accurately different voltage levels that represent OPEN CIRCUIT - OFF - ON - SHORT CIRCUIT and will also identify Over Voltage and input which is not ON or OFF. The values make sure that a line fault will be declared before it becomes possible for a false declaration of ON and OFF states because of a combination of resistor value drift and loop voltage variation.

## Eurocard Analogue Output Module Field Loops

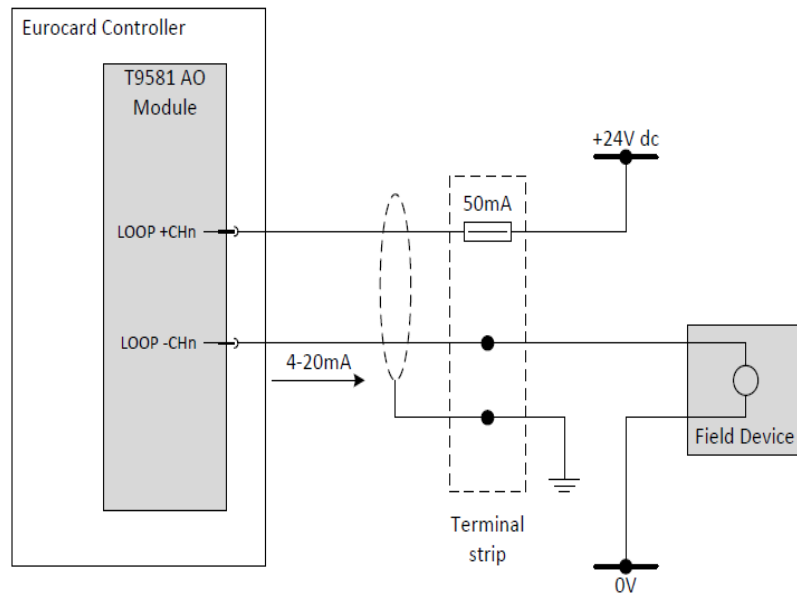
The analogue output module is a current regulator and the current to flow is into the loop plus terminal and out of the loop minus terminal. Connect the field wiring to the hypertac connectors using 22 AWG multi core cabling.

There are two recommended field loop circuits for analogue output modules as follows:

#### System Power Field Loop Circuit

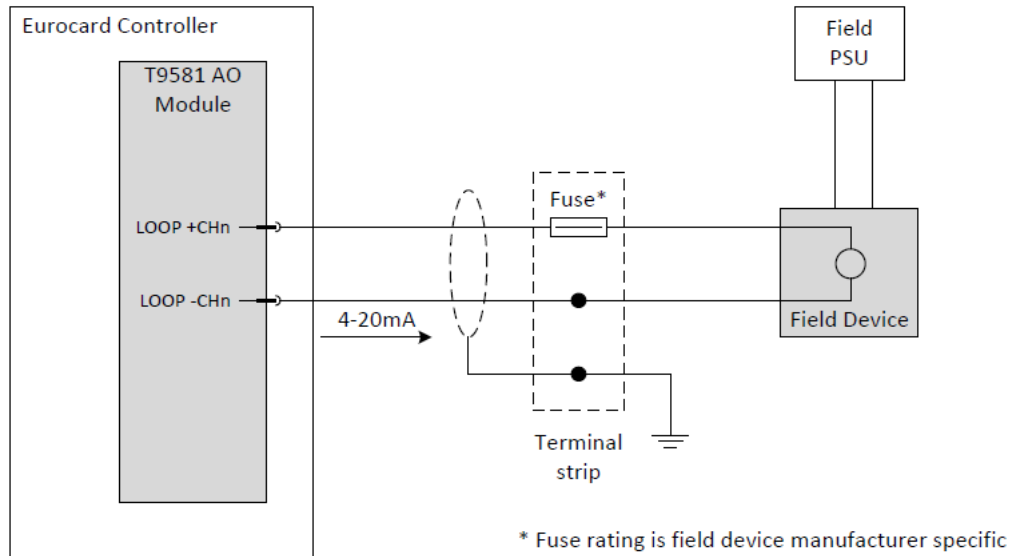
This circuit is applicable for field devices powered by the system. The channel will pass a requested current between 0mA and 24 mA. The field device can be connected as shown or alternatively between the + 24 Vdc supply and the loop plus terminal.

Figure 11 - Analogue Output Field Circuit with System Power



## Field Power Circuit

This circuit is applicable for field devices that are powered locally and expect a current-controlled signal loop.

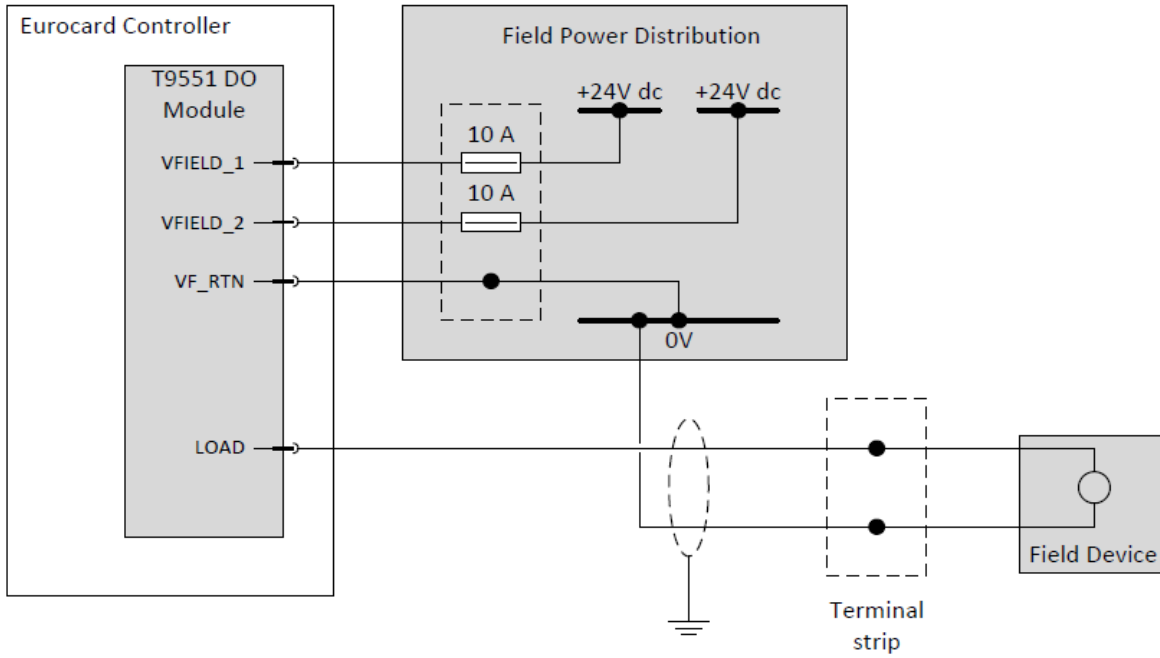


## Eurocard Digital Output Field Loops

It is recommended that digital output field supplies are routed through 10 A fuses before they are connected to the module. On an AADvance Eurocard controller, these fuses must be attached externally to the module. Connect the field wiring to the hypertac connectors using 22 AWG multi core cabling.

- The field power must be supplied with an isolating source.
- The minimum current required for line monitoring is 10 mA per module, 20 mA for a dual pair.

Figure 12 - Digital Output Field Loops



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

## Safety Networks

AADvance Eurocard supplies two safety network functions that will permit the sending and receiving of data across a SIL 3 rated safety communication across the Ethernet communications link:

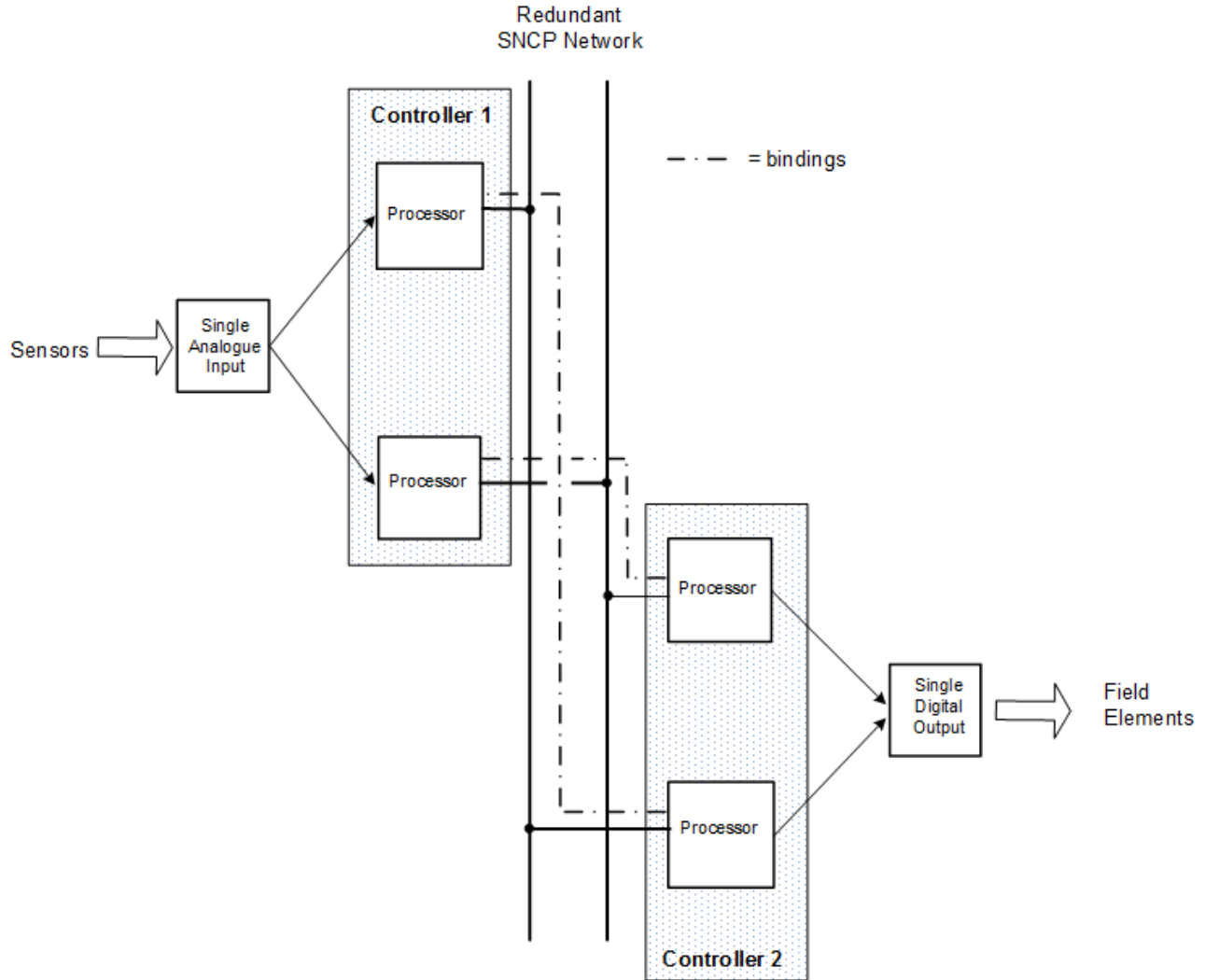
- Safety Network Protocol (SNCP)
- Peer-to-Peer

### **Bindings and the SNCP Network**

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 all of the sending and receiving of data. It schedules the sending and receiving of data, sending the diagnostic data, managing the safety response if faults occur and managing the communications redundancy. A SNCP network is illustrated in the diagram.

First there must be a physical connection between the two controllers. 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 change 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 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, therefore, careful consideration must be given to the network topology during the applications specification and design phase.

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



### Configuring SNCP Safety Network

The SNCP protocol can be configured in the AADvance Eurocard controller to supply a safety network; refer to the AADvance Controller Configuration Guide (Doc No. [ICSTT-RM405](#)) for full configuration procedures and the



AADvance-Trusted SIS Workstation Software User Guide (Doc No. [ICSTT-UM002](#)).



**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, related SIF outputs must be configured to shutdown on loss of communications.
- For energize to trip configurations, link failures must be repaired within the MTTR.

**NOTE** Additional measures must be implemented to make sure that the process stays within its safe operating parameters during the repair time; these other measures must be specified in the local Operating and Maintenance procedures written for maintaining the SIF for the specified 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 specified timeout is discarded and the system continues using its last state value. Once disconnected the consumer attempts to find 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 response containing new 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. If a producer fails to receive a binding data request from a consumer within this timeout value, the link to the consumer system is closed. If the consumer system is still functional it will timeout the link from its end.

An UpdateTimeout value can also be configured. This timeout is used in 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 find its binding connections.



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

Two function blocks are supplied that make sure the overall status of the bindings communication subsystem is available to the application:

- KvbConsNetStatus: indicates consumer status for a specified bindings link (identified by the Producers Resource Number and IP Address)
- KvbProdNetStatus: indicates producer status for a specified bindings link (Identified by the Consumers Resource Number and its IP Address).

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 found in the Producing Resource.

## Peer-to-Peer

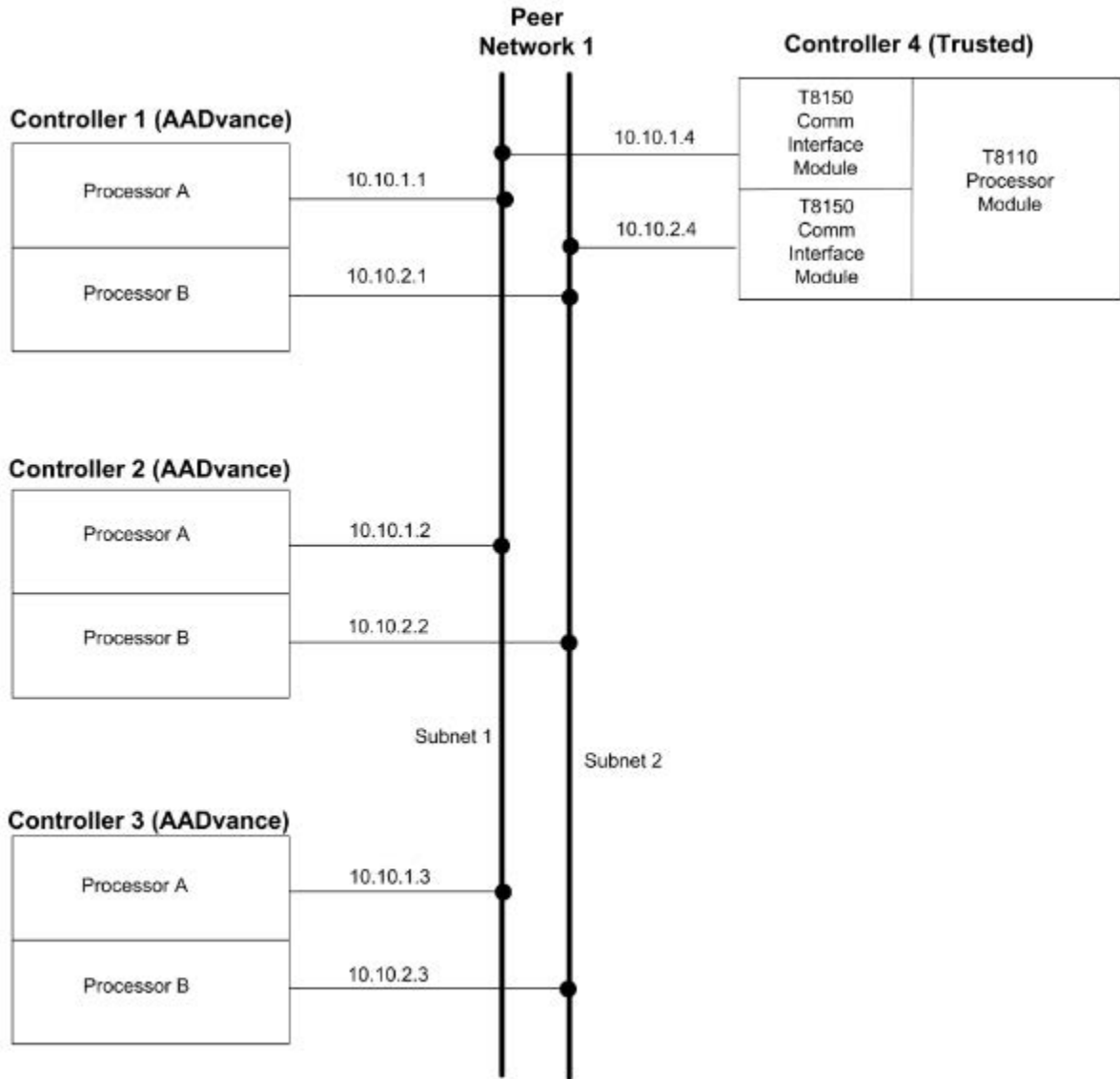
AADvance Eurocard supplies the capability for a SIL 3 certified Peer-to-Peer data connections, permitting safety data to be transferred between AADvance Eurocard and Trusted Controllers. The Trusted Peer-to-Peer network protocol lets you share safety data between AADvance Eurocard systems or AADvance Eurocard and Trusted TM systems across an Ethernet network. Data can be transferred between individual systems or from one to many systems at the same time using multicast network connections. Peer-to-Peer communication is configured by specifying a peer network controller and I/O devices in the application program.

AADvance Eurocard 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 different networks (from general purpose, for security and integrity). Any of the AADvance Eurocard or Trusted ports can be used for Peer-to-Peer data connections see Example shown below.

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 returns this acknowledgment to the master. The master repeats this with

the next and all slaves in turn. Finally the master transmits it's 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:

**Table 9 - Certified Peer-to-Peer Configurations**

AADvance Data Block	Trusted Equivalent	Certified Configuration	Conditions
DI 16 channels DO 16 channels	Dxpdi16 Dxpdo16	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.
AI 16 channels AO 16 channels DI 128 channels DO 128 channels AI 128 channels AO 128 channels	Dxpai16 Dxpao16 Dxpdi128 Dxpdo128 Dxpai128 Dxpao128	Certified for use over a single communication network or multiple networks	Certified as safety-related and can be used for safety-critical communication up to SIL 3 applications provided two separate AI & AO 16 channel, DI & DO 128 channel, or AI & AO 128 channel data block pairs are defined and used for safety values. The safety values from the duplicated data blocks must be compared, with equivalency verified, within the receiving application.

---

## Eurocard Functional Safety System Implementation

This chapter gives the implementation guidelines for a safety implemented system.

### Eurocard I/O Modules in Safety Applications

The AADvance Eurocard system supports single module configurations, where it is permitted to stop the system or allow the signals relating to that module to change to their default fail-safe state. It also supports fault tolerant I/O configurations where it is required to make sure that system operation continues if a fault occurs. All configurations can be used for safety-related applications; the selection of a configuration is based on the end-user's fault tolerance requirements.

**ATTENTION: ANALOGUE OUTPUT MODULES**

The Eurocard Analogue Output Module has not been verified or certified for use in a SIF. It cannot be used as part of a safety path in a SIF and it cannot be used in a dual redundant configuration. It will not, however, interfere with the safety path or other modules used in a SIF.

---

The input modules can be configured as a simplex or dual arrangement. Digital output modules can be configured as a simplex or dual arrangement. All input I/O modules include line-monitoring facilities; it is recommended that these line monitoring facilities be enabled for safety-related I/O.



**CAUTION:** For normally de-energized field circuits input I/O line monitoring facilities must be enabled.

---

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

---

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. This will make sure that the system remains on-line even if a demand during the execution of the tests occurs. I/O channel discrepancy and deviation monitoring enhances the verification and fault identification of module or field failures.

The processor reports any identified I/O fault to the AADvance® Workbench software or AADvance®-Trusted® SIS Workstation software application and gives an alarm signal for a central alarm indicator. In all cases, even when there is a fault during this time, the system will continue to respond when configured in a fault tolerant arrangement (dual group arrangement).



**ATTENTION:** When a channel cannot report a value within a safety accuracy specification of 1% of the full scale measurement 'safe' values are reported by the variables. Thus, an I/O channel fault condition results in a fail-safe state.

The maximum length of time 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.

The application program must be designed to shut down energize to action SIL 3 safety instrumented functions if a faulty output module has not been replaced within the MTTR.

---

When a module is operating in dual mode and a state or value discrepancy occurs and, 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 digital and analogue input module configurations.



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

---

## Energize to Action Configurations

In cases where one or more outputs are used in an energize to action configuration, all the requirements given below must be followed for all safety related outputs.



**ATTENTION:** Certain applications can require energize to action for inputs and/or outputs. Energize to action configurations must only be used if the following restrictions apply:

- At least two independent power sources are used. These power sources will supply emergency power for a safe process shutdown or a time span required by the application.
- Each power source must be supplied with power integrity monitoring with safety critical input read back into the system controller or implicit power monitoring supplied by the I/O modules. Any power failure will cause an alarm.
- Unless supplied implicitly in the I/O modules, all safety critical inputs and outputs will be fitted with external line and load integrity monitoring and safety critical read back of the line-status signals. Any line or load failure will cause an alarm.
- For SIL 3 energize to trip applications a minimum of dual output modules must be used.

## Controller Process Safety Time (PST)

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

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

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

where PST<sub>euc</sub> is the process safety time for the equipment under control. As an example, think about a system function using one sensor and one actuator given the following parameters:

- PST<sub>euc</sub>: 10,000 ms
- Sensor delay: 250 ms
- Time for actuator (an ESD valve) to fully operate: 1,750 ms

So, in this example, the setting of PST for the controller will be less than or exactly 3,000 ms.

## Sensor Configurations

The following applies to the use of sensors in a Safety Application:



**ATTENTION:** In safety critical input applications using a single sensor, it is important that the sensor failure modes are 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 Eurocard system, or by manual intervention testing.

---

The function of a signal must be thought about when allocating the module and channel in the system. In many cases, redundant sensor and actuator configurations can be used, or differing sensor and actuator types supply different identification and control possibilities. Plant facilities frequently have related signals such as start, and stop signals. In these cases it is important to make sure that failures beyond the system's fault-tolerant capability do not cause it to be unable to respond safely or accidental operation. In some cases, it will be necessary for channels to be allocated on the same module, to make sure that a module failure results in the related signals failing-safe.

Sensor configurations must be thought about. In most cases it will be necessary to divide the signals across modules. Where non-redundant configurations are employed, it is especially important to make sure that the fail-safe action is generated in case of failures in the system.

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

## Actuator Configurations

The following applies to actuator use in a Safety Application:



**ATTENTION:** 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, by dynamic process conditions that are verified in the AADvance system, or by manual intervention testing.
- The function of a signal must be thought about when allocating the module and channel in the system. In many cases, redundant actuator configurations can be used, or differing actuator types can supply different control and mitigation possibilities. Plant facilities frequently have related signals; in these cases it is important to make sure that failures beyond the system's fault-tolerant capability do not cause it to be unable to respond to safety demands or accidental operate.



- In some cases, it will be necessary for the channels to be allocated on the same module, to make sure that a module failure cause the related signals to fail-safe. Although, it will be necessary to share the signals across modules. Where non-redundant configurations are employed, it is especially important to make sure that the fail-safe action is generated in case of failures in the system.
- Field loop power must be thought about in the allocation of signals to output channels and modules. For normally energized configurations, field loop power failure will cause the fail-safe reaction. As with the allocation of signals to modules, there can be related functions where loss of field power must be thought of in the same manner as the signal allocation. Where signals are powered from different power groups, it is important that this separation is maintained when allocating the signals to modules, i.e. that accidental coupling between power groups, and particularly return paths, are not generated.

## Eurocard HART

The AADvance Eurocard 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 Analogue Input/Output modules use HART commands #03 to collect data from the field device as specified 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 supply the following information:

- current in milli-amps
- process measurement in engineering units
- errors on HART communication seen by device
- status of the field device
- time in milli-seconds 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 identify 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 4-20 mA Analogue signal itself, HART data can take a maximum of 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 Passthrough

AADvance Eurocard also supports the ability to pass HART data between an external Asset Management System (AMS) and Field Devices. This is strictly a "Passthrough" mechanism using a dedicated AADvance HART DTM. This "Passthrough" capability can be enabled or disabled under application control.

## Eurocard Processor Safety Functions

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

- solving application logic
- Communication functions - Inter Processor Link (IPL), Bindings (SNCP) and Peer-to-Peer
- communication with I/O modules such as receiving input values, sending commanded output values, coordinating and starting diagnostics
- enforcement of system PST
- fault indications and degradation of the processor module
- enforcement of input PST
- diagnostics, fault indications and degradation of I/O modules
- Recovery mode operation

## Firmware Updates

The processor modules must have identical firmware versions, their firmware can be updated when in the Recovery Mode using the ControlFlash software. The procedures for using ControlFlash are contained in the AADvance Controller Configuration Guide (Doc No. [ICSTT-RM405](#)). The AADvance-

Trusted SIS Workstation Software User Guide (Doc No. [ICSTT-UM002](#)) is also available.



**WARNING:** You should not attempt to upgrade the processor firmware on a running system. ControlFlash will not warn you that a system is running and you will lose control of the application when the system reboots.

## Processor Functional Safety Configuration

The processor module supports a set of I/O configuration options; for example and checks that the I/O hardware configuration including the module locations and the actual module type in a slot.

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 AADvance Configuration Guide [ICSTT-RM405](#).

### Eurocard Processor Module Reaction to Faults

The processor module reports faults by AADvance® Workbench software or AADvance®-Trusted® SIS Workstation software application variables or/and a set of LEDs. They report the following information:

- Module presence
- Module health and status
- Channel health and status
- IPL status

**NOTE** The fault reports are also stored a processor diagnostic record that can only be accessed and retrieved for analysis by Rockwell support.

### Eurocard Processor 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 enabling the remote fault/reset join feature immediately after the module has booted up. If your system stops it can be because it has entered Recovery Mode.

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 the application stops the Modules go into the states specified in this manual as the reaction to faults for each module type. When in Recovery Mode the I/O communications are disabled and the Application code is not running.

---

## I/O Module Safety Functions

This section describes the I/O safety parameters.

### Eurocard 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 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 use, 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 input module is set to a fail-safe state and returns safe values to the controller.

#### Digital output module PST

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

## Input and Output Forcing

The AADvance® Workbench software or AADvance®-Trusted® SIS Workstation software has functions for forcing of individual inputs and outputs. Software uses the term 'locking' to show what forcing means.



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

Forcing for AADvance Eurocard systems is enabled by default 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 must be implemented using the application program. The Force LED on the front of the Processor Module indicates when one or more I/O points are forced. The application program can find out how many points are currently forced; it is highly recommended that this information be used to control another status display and/or for logging purposes.

If the forcing facility is used when the system is in-service, a safety-related input connected to an operator accessible switch must be implemented to remove the force condition.

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

## Maintenance Overrides

Maintenance Overrides set inputs or outputs to a specified 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 do a periodic test, calibration or repair of a module, sensor or actuator.

To correctly put in place a maintenance override scheme within the AADvance Eurocard system, the override or 'bypass' logic must be programmed within the Application Program, with a different set of safety-related input points or variables enabling the bypass logic.



**ATTENTION:** To let maintenance overrides occur safely, TÜV has documented a set of principles that must be followed. These principles are published in the document "Maintenance Override" by TÜV Süddeutschland / TÜV Product Service GmbH and TÜV Rheinland.

There are two basic methods to check safety-related peripherals connected to the AADvance Eurocard 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 can be integrated with the operator display, or maintenance can be covered by other strategies. In such installations, the guidance given in section is to be followed. A checklist for the application of overrides is given in the Checklists chapter.

## Input Module Safety Functions

An I/O 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 change the field current into a voltage. Input values are updated by the software at least once for each application cycle.

I/O modules in a redundant group can be replaced or installed on-line without affecting the controller operation when at least one is fitted and is fully operational. However, each module must be installed one at a time and permitted to educate before the next module is installed.

The input module will operate in a SIL 2 or SIL 3 configuration for energize to action and de-energize to trip applications. The module has 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

### On-line Updates

The I/O configuration in the software can be changed through an online update. The procedure to enable the on-line update feature is contained in the AADvance Configuration Guide [ICSTT-RM405](#). The following safety precautions should be followed.



**ATTENTION:** On-line updates should be carried out with caution. It is recommended that an on-line change is not performed unless it is absolutely necessary as it could reduce the safety integrity of the system while the update is in progress. Also if the on-line changes to the I/O configuration are incorrect it can stop the application. Before doing an on-line update alternative safety measures should be set up and be present until the update is finished and the system restored to full operation.

---

## Reactions to Faults in the Input Modules

When an input channel is not able to report a voltage within a safety accuracy specification of 1 % of the full scale measurement range, then the module returns safe values to the processor. Signals also 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 LED status information, store fault codes in the fault log and can also report faults by the software application variables. The following status information is given:

- Module presence
- Module health and status
- Channel health and status
- Field faults
- Application variables give an echo of the module LED status indicators for each module of the software

## Input Data Safety Accuracy

The input modules report the channel state and the line fault state by comparing the input of the two individual reported values are within the safety accuracy limit.

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

- Digital Input Module = 4 %
- Analogue Input Module = 1 %

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

- Digital Input Module = 8 %
- Analogue Input Module = 2 %

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)
- line fault TRUE
- Discrepancy TRUE
- Channel Fault TRUE
- Count value 0



**ATTENTION:** In safety critical applications, the discrepancy alarms will be monitored by the application program and used to generate an alarm to make the plant operations personnel aware of the problem.

## Output Module Safety Functions

The digital output module has user-configurable safety features. The analogue output module cannot be used for safety-related purposes.

### 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 has 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 (together with 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 PFD & PFH data has been calculated on the basis that the shutdown state is configured to the OFF state. Therefore the OFF state will be used for SIL 2 and SIL 3 applications.
- When a module fails then all the channels are set to the de-energized state.



### 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

### Eurocard Analogue Output Module

The Eurocard analogue output module cannot be used for a safety related path. It can be used in a safety related system and regarded as a non-interfering module to the safety path.

## Application Program Development

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



**ATTENTION:** Development of application software consisting of programs (POUs), User Defined Functions and user Defined Function Blocks must follow the requirements specified in IEC 61511 for LVL languages and the requirements specified in IEC 61508 for FVL languages. However, these requirements can be waived if the programs (POUs) used have previously been tested and validated to be in line with IEC 61511/IEC 61508 and validation evidence is supplied as part of the Project Test Documentation.

The stages specified in the following sub-sections must also 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:** Applicable security protection must be implemented to 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 Knowledge base articles.

---

## Language Selection

The AADvance® Workbench software or AADvance®-Trusted® SIS Workstation software offers many programming tools to develop algorithms to fulfill 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 in the table.

### Safety Languages

- Function Block (FB)
- Instruction List (IL) (AADvance Workbench version 1.40 only)
- Structured Text (ST)
- Ladder Diagrams (LD)
- Sequential Function Chart (SFC) (AADvance Workbench version 1.40 only)

### Safety Related Languages

The AADvance Eurocard controller supports a comprehensive set of certified functions. The certified functions set includes the most commonly used function.

These tested functions can be used freely in the development of an application. Further functions can be used if testing is complete commensurate with the level used for the commonly used function.



**ATTENTION:** IL (AADvance Workbench version 1.40 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 is 100% testable, such functions could be:

- Burner flame supervision together with temperature and air/gas pressure monitoring
- Burner gas-to-air ratio control/supervision
- Parts or all 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 for which testing is necessary. However, a single safety function must not be divided into different blocks; such a division is likely to cause the introduction of errors during maintenance activities.

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

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



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

---

The new or previously untested function can be:

- a generic function block, which forms part of the software, but has not previously been subject to the level of testing specified herein, or
- a project-specific function block, which is written to satisfy the needs of a particular property within an application program and can include 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 property must be exploited to permit the allocation of individual safety related functions to different programs. Where such programs contain independent logic paths, these must be investigated to find out if they are different safety functions. Where they are different, it is recommended that these be allocated to their own program, if they conform to the recommendation to minimizing the coupling between programs.

Cases must be looked at to permit 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 not necessary to apply the same degree of rigorous development and testing to all functions in 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 include status indication, data reporting and sequence of events. It is important to make sure that these elements are not safety related. For example, some safety cases rely on human intervention and thus the correct operation of status indication.



**ATTENTION:** The safety related elements must be put in place in different programs to those of non-safety related elements. Where information passes between these elements, it must be arranged that the direction of flow is from safety related to non-safety related only.

---

### Defensive Measures

In defining the Application the programmer must think about the possible 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 must be checked where possible. Similarly, values received from input interfaces must be checked where possible. In many cases, it will also be possible to monitor permutations of data, inputs and plant operating modes to look at the plausibility of the information and program measures to make sure that responses are safe in case of implausible conditions.



**ATTENTION:** Safety related functions must be latched when in their tripped condition to 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 must be written to make sure that safety related functions are in their safe state during system startup.

### **Minimize Logic Depth**

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

Where there is nested logic, it will be possible to find out the correct operation of all intermediate logic connections.

The use of memory (latch) components in the safety function will be minimized. Similarly, the permutation of conditions that cause their activation will 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:** CVT must be enabled for all safety related systems. 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 Knowledgebase Document 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 Knowledge base 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 Knowledge base articles.

## Communications Interaction

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



**ATTENTION:** Data received from external equipment that controls safety-related functions or affects their operation must be handled with caution.

The application program will handle received data that it is limited to interactions which:

- Initiates safety operations, i.e. initiates shutdown sequences
- Resets signals, with the reset action only possible when the initiating conditions have been removed
- Initiate timed start-up override signals which are removed automatically either on expiration of the start period or when the related signal has stabilized in the normal operating condition
- Adjust control parameters within specified 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 must be thought about and measures taken to make sure that the system will respond safely in the event of erroneous data. Alternatively, measures can be implemented in the application to make sure that the data is valid and has integrity.

## Program Testing

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

The scenarios must include possible plant conditions, sequences of plant conditions and system conditions together with 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, must be exercised.

Where the logic includes memory or timing elements, additional tests will be specified to exercise all the possible sequences of input permutations to start their operation.



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

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

- All inputs are exercised through their full allowable range
  - All outputs are exercised through their all of the program's 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, together with 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 looked at.
- 

## Cross Reference Checking

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

## On-line Modification

It is highly recommended that on-line changes are not done unless it is necessary as it could decrease the safety integrity of the system while doing the changes. Where changes have to be carried out on-line alternative safety measure must be put in place for the duration of the change.

Certain modifications can be performed without directly affecting the system's safety function, for example the physical installation of more modules in a redundant group. Although these modifications will not change the system's operation until the system configuration and application program have been adjusted, caution must be exercised to make sure that the adjustments do not change other safety related functions.

The procedures to enable the on-line update and do an on-line update are found in the AADvance Configuration Guide: Doc No. [ICSTT-RM405](#).

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

---

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

---



**ATTENTION:** Changes that change the system's ability to respond safely, or can cause other plant disruption should not be done on-line unless alternative protection measures can be used for the duration of such changes.

---

## Eurocard Module Physical Installation

The installation environment is a possible source of common cause failure, so it is important that the compatibility of the equipment with the environment is known. The environment includes the prevailing climatic, hazardous area, power sources, earthing and EMC conditions. When elements of the system are installed in differing locations it is important to know the environment conditions for each location.

For custom rack mounting arrangements environmental tests must be done to make sure that the specified operating conditions (see Environmental Specification) are not exceeded. Calculate the total module supply power and field loop power consumption before designing the enclosure and deciding upon the installation environment, because these values will show the heat dissipation of the controller. Module supply power and field loop power



consumption values are given in the Eurocard System Build Manual Doc. No [ICSTT-RM455](#).



**CAUTION: HEAT DISSIPATION AND ENCLOSURE POSITION**

System and field power consumption by modules and termination assemblies is dissipated as heat. You must think about the impact of this heat dissipation on the design and positioning of your enclosure. Modules operating at the extremes of the temperature band for a continuous period can have decreased reliability.



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



**CAUTION: 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 Requirements

## Environmental Specification AADvance Eurocard Controller

The following environmental specification applies to all AADvance Eurocard controller modules.

**Table 10 - Environmental Specification**

Attribute	Value
Temperature	
Operating	-25 °C to 70 °C (-13 °F to 158 °F) all Modules.
Storage and Transport	-40 °C to 70 °C (-40 °F to 158 °F) all Modules.
Humidity	
Operating	10 % to 95 % RH, non-condensing
Storage and Transport	10 % to 95 % RH, non-condensing
Vibration	
IEC 60068-2-64 (Test Fh, Operating)	20 to 80 Hz, increasing @ +3 dB/Octave, 80 to 350 Hz @ 0.04 g <sup>2</sup> /Hz, 350 to 2000 Hz @ -3 dB/Octave. 6 g rms overall. 10 minutes single axis delivered as one continuous test

Attribute	Value
Altitude	
Operating	2000 m or less (6562 ft or less)
Storage and Transport	0 to 3000 m (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 61326-3-1:2017; IEC 61131-2:2017
Sub Sea Qualification	API-17 F:2017 Standard for Subsea Production and Processing Control Systems

## Eurocard Electromagnetic Capability



### CAUTION: EMC SURGE PROTECTION

Additional suitable protection is required to ensure the continued operation of the AADvance Eurocard System when exposed to surge events which may, for example, occur from remote lightening strikes.

## Eurocard Shielded Cable for Ethernet and Serial Ports

When using cables longer than 3 m for Ethernet and Serial communication you must use shielded cable to stay within the emission and immunity standards. Also make sure that the shields are grounded to the controller chassis.

**IMPORTANT** The system is resistant to radio interference as long as the guidelines are followed when assembling the wiring harness. These guidelines are included in the Eurocard System Build Manual Doc. No [ICSTT-RM455](#).

## Eurocard System Power Requirements

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

The controller should 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 is no larger than 30 V ac r.m.s., 42 V peak or 60 V dc 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 satisfy 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, have a possible common cause failure, so it is 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.
- Make sure that the chosen PSUs are compatible with the power feeds supplied. Alternatively, measures must be put in place to make sure that the power feeds stay 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 find out that sufficient current will be available to make sure that their protective action and the protective device can break the maximum prospective fault current.
- Make sure that the power supplies are sufficient for the system load and for any foreseeable load requirements and load transients.
- Make sure that the power supplies have a minimum output hold-up time of 10 ms.
- Make sure that the power distribution cabling is sized to allow the maximum prospective fault currents and tolerable voltage losses. This is specifically important where floating supplies are employed and other power sources can cause high prospective fault currents if multiple earth faults occur.



**ATTENTION:** The power supplies used must satisfy the electrical requirements defined in IEC 61010-2-201 in addition to the electrical requirements and tests for EL1 defined in EN62368-1 (formerly referred to as SELV) and must be of applicable capacity for the system.

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



## Checklists

This chapter contains a number of example checklists. These are to be used by competent engineers. In general each checklist item must have a "yes" response, where the answer is "no" there must be a reason for this.

### Pre-Engineering Checklists

The checklists supplied in this section are applicable to the requirements. It must be recognized that the requirements will undergo refinement, particularly, in the early stages of a project. The information supplied initially can be 'outline'; these checklists can be used to identify where omission has occurred or where more refinement is necessary.

#### Scope Definition Checklist

Description	Yes/No
Has a summary description of the intended application been supplied?	
Is the intended installation environment specified?	
Does the installation environment satisfy the environmental specification for the controller?	
Has a list of all the third-party equipment interfaces been supplied and are definitions of the protocol and the data to be interchanged established?	
Are all of the plant interfaces specified, together with the signal qualities and characteristics?	
Have any special or unusual conditions that go above the normal equipment capabilities been highlighted to permit special measures to be put in place?	
Is the presented information sufficient to support the necessary level of understanding of the plant/EUC and its environment?	
Has a risk analysis been completed to find out 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 related to each function clearly identified?	
Where a 'tag referencing' scheme is used for these signals, has a summary description of the naming convention been supplied to increase your understanding of the role of the signal?	
Have the performance requirements for each function, or collective functions, been specified?	
Have the operating modes of the EUC, process or plant been clearly specified?	
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 effect 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, together with process safety time (PST) and fault tolerance period, been found?	
Have the safety requirements been approved?	
Are there full definitions of the external interfaces involved in each of the safety related functions? (These could already be specified in the functional requirements).	
Is there now sufficient information to understand how the plant will 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 energize to action configurations conform to the restrictions (specified in this safety manual) that must 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?	

### Processor Checklist

Description	Yes/No
Has the processor PST been specified?	
What is the PST?	
Have you dual/triple processor been configured for SIL 3 and high demand and continuous mode applications?	
Are the processor modules loaded with the most recent firmware versions?	
Are all processors using the same firmware versions?	
Have alternative protection measures been thought about for safety related functions if you have to do an on-line change?	

## Safety System Checklist

Description	Yes/No
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 access that has not been authorized to the application programs?	
Have full branch and data tests been carried out on IL (AADvance Workbench version 1.40 only) and ST program flow functions?	
Have safety related control programs been put in place in different programs from non-safety related control elements?	
Is the data flow programmed so that it goes from Safety functions to non-safety functions?	
Do the application programs make sure that all safety related elements are in their safe state during start up?	
Have alternative protection measures been thought about for safety related functions if you have to do an on-line change?	
Have the installation guidelines given in the AADvance System Build Manual and installation and any commissioning procedures that comply with applicable international or local codes and standards been followed.	
On-line changes: Changes that change the system's ability to respond safely, or can cause other plant disruption cannot be done on-line unless alternative protection measures can be used for the duration of such adjustments. Have alternate measures been implemented.	
Do the power supplies used satisfy the electrical requirements defined in IEC 61010-2-201 in addition to the electrical requirements and tests for EL1 defined in EN 62368-1 (formerly referred to as SELV) and are they of applicable capacity for the system.	
Has System Configuration Back-up and restore been tested ?	

### Application Checklist

Description	Yes/No
Has security protection been used to prevent access that has not been authorized to the application programs. Refer to the Knowledge base article <a href="#">KB609247</a> for additional information about the correct use of security passwords within the software.	
Have full branch and data tests been carried out on IL and ST program flow functions?	
Do the application programs make sure that all safety related elements are in their safe state during start up?	
Have safety related control programs been put in place in different programs from non-safety related control elements?	
Is the data flow programmed so that it goes from Safety functions to non-safety functions?	
Do the application programs make sure that all safety related elements are in their safe state during start up?	
Have alternative protection measures been thought about for safety related functions if you have to do an on-line change?	
Are any functions not in the previously tested libraries required? If so has it been made possible to sufficiently test these functions?	
Does the Development of application software consisting of programs (POUs), user defined functions and user defined Function Blocks follow the requirements specified in IEC 61511 for LVL languages and the requirements specified in IEC 61508 for FVL languages.	
Where IL and ST include program flow control functions, have full branch and data coverage tests been performed on these sections of program.	
Have application programmer generated function blocks used for safety-related applications been subjected to exhaustive testing, commensurate with that used for the commonly used functions.	
Have the safety related elements been put in different programs to those of non-safety related elements. Where information passes between these elements, it must be arranged that the direction of flow is from safety related to non-safety related only.	
Are safety related functions latched when in their tripped condition to prevent intermittent field faults from removing the trip condition.	
Has CVT been enabled for safety related applications	
Have safety related functions been tested.	

### Safety Networks Checklist

Description	Yes/No
If bindings communications is used, are the timeouts set to a response time within the required PST?	
For SNCP bindings to be used in a Simplex Network configuration, SIL 3 are the following conditions met: <ul style="list-style-type: none"> <li>For de-energize to trip configurations, related SIF outputs must be configured to shut down on loss of communications.</li> <li>For energize to trip configurations, link failures must be repaired within the MTTR.</li> </ul>	
For SNCP network additional measures must be thought about and carried out to make sure that the process stays within its safe operating parameters during the repair time; these other measures must be specified in the local Operating and Maintenance procedures written for maintaining the SIF for the specified plant or process.	
Have unused ports been protected by firewall settings ?	



## I/O Checklist

Description	Yes/No
Has the I/O module 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 sufficient for the application?	
Where the fault detection time is larger than the PST, does the safety-related I/O configuration supply a fail-safe configuration? If not, the system topology will be discussed with the client to make sure that the system implementation is safe.	
HART: If HART is used have these guidelines been implemented: <ul style="list-style-type: none"> <li>Do not use HART variables as the primary initiator for a Safety Instrumented Function. The HART protocol does not satisfy the applicable integrity levels for Safety Instrumented Functions.</li> <li>Make sure that HART is disabled for field devices that do not have a locked configuration. This will prevent the use of HART to change a device configuration.</li> <li>Make sure that the custom data for the device (this is the data given in response to HART command #03) is used in accordance with the device manufacturers published recommendations.</li> </ul>	
HART Passthrough: Have the following precautionary guidelines been implemented: <ul style="list-style-type: none"> <li>Make sure that HART Passthrough is enabled only under control of the application.</li> <li>Make sure that HART Passthrough is enabled only when necessary.</li> </ul> Configure the application to start an alarm if HART Passthrough is enabled on any safety-critical channel of any module.	
Do the selected architectures supply solutions where there is no single power source or distribution point of failure that could cause the system to fail to function safely when required?	
Has cable monitoring and circuit integrity cable been used for the application, because inter-channel short circuits cannot be identified by an AADvance Eurocard controller.	
For energize to action configurations have the following been implemented: <ul style="list-style-type: none"> <li>At least two independent power sources must be used. These power sources will supply emergency power for a safe process shutdown or a time span required by the application.</li> <li>Each power source must be supplied with power integrity monitoring with safety critical input read back into the system controller or implicit power monitoring supplied by the I/O modules. Any power failure will cause an alarm.</li> <li>Unless supplied implicitly in the I/O modules, all safety critical inputs and outputs will be fitted with external line and load integrity monitoring and safety critical read back of the line-status signals. Any line or load failure will cause an alarm.</li> <li>For SIL 3 energize to trip applications a minimum of dual output modules must be used.</li> </ul>	
Have sensor configurations and fault conditions been taken into account?	
For each of the I/O signal types, do the I/O modules have the correct characteristics and behavior for the intended sensor or actuator (including minimum and maximum load requirements)? If not, have other interfacing elements been included to make sure 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?	
Are there any safety-related, normally de-energized outputs? If so have redundant power sources, power failure warning and line monitoring been supplied?	
Have safety wiring principles must been employed for field loops to guard against short circuit faults between I/O channels. The AADvance Eurocard controller internal diagnostics do not identify external short circuits between channels.	
Digital Output Channels: For inductive loads, have back EMF protection diodes been fitted at the load.	
Output Modules: Has careful thought been given to the effect on the process of using the 'hold last state' setting. The PFD & PFH data has been calculated on the basis that the shutdown state is configured to the OFF state. Thus the OFF state must be used for SIL2 and SIL3.	

Description	Yes/No
Digital Output: Invalid calibration: In Energize to Action configurations- the digital output module will not be able to come out of the Shutdown mode until the module has been re-calibrated (module calibration checking procedures and intervals are given in the AADvance Troubleshooting and Maintenance Manual Doc No: <a href="#">ICSTT-RM406</a> )	
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 below the 1 % 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?	

### Override Requirements Checklist

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

### 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 the application been fully tested?	
Are the scan and response times in accordance with the PST requirements (< ½ PST) been checked?	
Have the climatic conditions been verified to be applicable?	
Have Test Plans and Test Specifications been developed for the system?	
Has the system been fully tested to the Test Plans and Test Specifications?	

## Additional Resources

### Associated AADvance Eurocard Publications

For more information about the AADvance Eurocard system refer to the associated Rockwell Automation technical manuals shown in table below.

Resource	Document Number
Safety Manual	<a href="#">ICSTT-RM456</a>
System Build Manual	<a href="#">ICSTT-RM455</a>
Configuration Guide	<a href="#">ICSTT - RM405</a>
OPC Portal Server User Manual	<a href="#">ICSTT - RM407</a>
PFH and PFD <sub>avg</sub> Data Manual	<a href="#">UCSTT-RM449</a>
Solutions Handbook	<a href="#">ICSTT - RM447</a>
Troubleshooting and Maintenance Manual	<a href="#">ICSTT - RM406</a>
AADvance Controller Configuration Guide Workbench 2.x	<a href="#">ICSTT - RM458</a>
AADvance-Trusted SIS Workstation Software User Guide	<a href="#">ICSTT-UM002</a>
Industrial Automation Wiring and Grounding Guidelines	<a href="#">1770-4.1</a>
Product Certifications website	<a href="https://rok.auto/certifications">https://rok.auto/certifications</a>

Publication	Purpose and Scope
Safety Manual	This technical manual defines how to safely apply AADvance Eurocard 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.
Solutions Handbook	This technical manual describes the features, performance and functionality of the AADvance Eurocard Controller and systems. It gives guidance on how to design a system to satisfy your application requirements.
System Build Manual	This technical manual describes how to assemble a system, switch on and validate the operation of your system.
Configuration Guide	This software technical manual defines how to configure an AADvance Eurocard controller using the AADvance® Workbench software or AADvance®-Trusted® SIS Workstation software to satisfy your system operation and application requirements.
Troubleshooting and Maintenance Manual	This technical manual describes how to maintain, troubleshoot and repair an AADvance Eurocard controller.
OPC Portal Server User Manual	This manual describes how to install, configure and use the OPC Server for an AADvance Eurocard controller.
PFH and PFDavg Data	This document contains the PFH and PFD <sub>avg</sub> Data for the AADvance Eurocard controller. It includes examples on how to calculate the final figures for different controller configurations.

## Glossary of Terms

### 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

- bindings** Bindings describe a "relationship" between variables in different AADvance Eurocard controllers. Once a variable is "bound" to another variable, a unique and strong relationships is created between the two variables and the SIL 3 Certified SNCP protocol is used to ensure 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.
- 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.
- 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 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 Eurocard controller. AADvance Eurocard 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.

**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)** The Compiler Verification Tool (CVT) is an automatic software utility that validates the output of the application compilation process. This process, in conjunction with the validated execution code produced by the AADvance® Workbench software or AADvance®-Trusted® SIS Workstation software, ensures a high degree of confidence that there are no errors introduced by the AADvance®-Trusted® SIS Workstation software, the AADvance Eurocard, or the compiler during the compilation of the application.

**configuration** A grouping of all the application software and settings for a particular AADvance Eurocard controller. The grouping must have a 'target', but for an AADvance Eurocard 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** One or more controllers, their 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 Eurocard 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.

## 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 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](http://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 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.

## 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** A representation of the configuration settings for a MODBUS Master or for its associated slave links, within the AADvance® Workbench software or AADvance®-Trusted® SIS Workstation software. The settings include communication settings and messages.

## 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 Eurocard 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 module** The application execution engine of the AADvance Eurocard 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.
- project** A collection of configurations and the definition of the linking between them. See 'configuration'.
- proof test** A test performed at a predetermined frequency which functionally tests all of the components that comprise a Safety Instrumented Function, designed specifically to reveal any undetected failures that may exist so that they can be repaired to ensure that the Safety Instrumented Function continues to meet its designed performance criteria over the entire safety life cycle.
- protocol** A set of rules that is used by devices (such as AADvance Eurocard 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 Eurocard 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 prevents 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 Eurocard 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 Eurocard 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".

**SNTTP** 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 Eurocard 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 Eurocard 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.

**TÜV certification** Independent third party certification against a defined range of international standards including IEC 61508.

## 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<sup>-3/4</sup> 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.







# Rockwell Automation Support

Use these resources to access support information.

<b>Technical Support Center</b>	Find help with how-to videos, FAQs, chat, user forums, Knowledgebase, and product notification updates.	<a href="http://rok.auto/support">rok.auto/support</a>
<b>Local Technical Support Phone Numbers</b>	Locate the telephone number for your country.	<a href="http://rok.auto/phonesupport">rok.auto/phonesupport</a>
<b>Technical Documentation Center</b>	Quickly access and download technical specifications, installation instructions, and user manuals.	<a href="http://rok.auto/techdocs">rok.auto/techdocs</a>
<b>Literature Library</b>	Find installation instructions, manuals, brochures, and technical data publications.	<a href="http://rok.auto/literature">rok.auto/literature</a>
<b>Product Compatibility and Download Center (PCDC)</b>	Download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes.	<a href="http://rok.auto/pcdc">rok.auto/pcdc</a>

## 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](http://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 compliance information on its website at [rok.auto/pec](http://rok.auto/pec).

Allen-Bradley, expanding human possibility, and Rockwell Automation are trademarks of Rockwell Automation, Inc.

EtherNet/IP is a trademark of ODVA, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

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](http://rockwellautomation.com) — expanding **human possibility**<sup>®</sup>

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) 2663 0600, Fax: (32) 2 663 0640

ASIA PACIFIC: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608, FAX: (65) 6510 6699

UNITED KINGDOM: Rockwell Automation Ltd., Pitfield, Kiln Farm, Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908) 838-800, Fax: (44)(1908) 261-917

Publication ICSTT-RM456D-EN-P - February 2024

Supersedes Publication ICSTT-RM456C-EN-P - August 2021

Copyright © 2024 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.