Safety manual for Smart ESD Device 700 Series for Safety Instrumented Systems

SAFETY PRECAUTIONS

Safety precautions are for ensuring safe and correct use of this product, and for preventing injury to the operator and other people or damage to property. The marking and its meaning of the safety precautions are as follows. You must observe these safety precautions and read the contents of this safety manual.

⚠ **WARNING**
Warnings are indicated when mishandling this product might result in death or serious injury to the user.

1. Purpose

This safety manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the smart ESD device 700 series for safety instrumented systems (700 SIS). The following document must be thoroughly reviewed and implemented as part of the safety lifecycle. This information is necessary for meeting the IEC 61508 or IEC 61511 functional safety standards.

⚠**WARNING**

- **This instruction manual supplement is not intended to be used as a stand-alone document. It must be used in conjunction with the following manual:**
  Smart ESD Device 700 series for Safety Instrumented Systems User's Manual (CM2-AVP772-2001)

2. Device Description

The 700 SIS is a current-pneumatic smart ESD (Emergency Shut Down) device. It receives a DC current or voltage signal from a logic solver and controls a pneumatic valve. In addition to this basic function, the 700 SIS has communication capabilities, an automatic configuration program, and self-diagnostics functions. Optional analog output or discrete output can be used for diagnostic annunciation.

Model No.	Pilot relay type	Input signal	Diagnostic Annunciation
AVP770	Single-Acting/ Double-Acting (Configurable)	4–20 mA 4 mA to trip, de-energize to trip	DO*1
AVP771			AO*2
AVP772			N/A
AVP780		0–20 mA 0 mA to trip, de-energize to trip	DO*1
AVP781			AO*2
AVP782			N/A
AVP790		0–24 VDC 0 V to trip, de-energize to trip	DO*1
AVP791			AO*2
AVP792			N/A

*1. DO: Discrete Output
*2. AO: Analog Output

3. Terms, Abbreviations, and Acronyms

DD	Device Description, an electronic data file that describes specific features and functions of a device to be used by host applications.
DTM	Device driver that provides a unified structure for accessing device parameters, configuring and operating the devices, and diagnosing problems.
700 SIS	Smart ESD device, product model designation for Safety Instrumented System applications
FMEDA	Failure Mode Effect and Diagnostic Analysis
HART	Highway Addressable Remote Transducer, open protocol for digital communication superimposed over a direct current. HART is a registered trademark of the Field-Comm Group.
HFT	Hardware Fault Tolerance
Low Demand Mode	Mode of operation of a safety instrumented function where the demand interval is greater than twice the proof test interval.
LUI	Local User Interface of the 700 SIS
PFDavg	Average Probability of Failure on Demand
PVST	Partial Valve Stroke Test, used for the same meaning as Partial Stroke Test (PST)
Safety	Freedom from unacceptable risk of harm.
Safety Function	Function of a device or combination of devices intended to be used within a Safety Instrumented System to reduce the probability of a specific hazardous event to an acceptable level.
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
Type A Element	"NonComplex" element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2.

4. Related Literature

- Smart ESD Device 700 series for Safety Instrumented Systems User's Manual (CM2-AVP772-2001)
- IEC 61508: 2010 Functional safety of electrical/electronic/programmable electronic safety-related systems
- ANSI/ISA 84.00.01-2004 (IEC 61511 Mod.) Functional Safety – Safety Instrumented Systems for the Process Industry Sector
- Exida FMEDA Report for Azbil AVP700 SIS-Report No. AZB 12-03-041 R001

Contact us to acquire the User's Manual and the FMEDA report.

5. General Requirements

⚠WARNING

- **To ensure safe and proper functioning of equipment, users of this document must carefully read all instructions, warnings, and cautions in this safety manual and the User's Manual.**

● Refer to the User's Manual (CM2-AVP772-2001) for mounting and configuration.

● Personnel performing maintenance and testing on the 700 SIS shall have knowledge about a valve, a positioner, and SIS. Otherwise, they shall receive adequate training and education.

6. Safety Instrumented System Design

6-1. Safety Function

The application of the 700 SIS is limited for SIS to low demand mode. Table 1 describes the normal and safe states of the 700 SIS. The 700 SIS may be operated with one of the following control signals:

● **0–24 VDC**: Normal operation is with a 24 VDC signal applied to the 700 SIS. A shutdown command is issued by interrupting the loop or changing the voltage signal to 0.5 VDC or less.

● **0–20 mA**: Normal operation is with a 20 mA current loop signal applied to the 700 SIS. A shutdown command is issued by interrupting the loop or changing the current signal to 0.5 mA or less.

● **4–20 mA**: Normal operation is with a 20 mA current loop signal applied to the 700 SIS. A shutdown command is issued by changing the current signal to 4 mA (nominal).

Table 1. Normal and Safe States

Pilot relay type	Input Voltage or Current	Normal State	Safe State
Single-Acting	0 VDC, 0mA, or 4 mA	-	P1 < 5% of Supply
	24 VDC or 20 mA	P1 ≥ 95% of Supply	-
Double-Acting	0 VDC, 0mA, or 4 mA	-	P2–P1 ≥ 95% of Supply
	24 VDC or 20 mA	P1–P2 ≥ 95% of Supply	-

P1: Pressure output 1 of the 700 SIS
P2: Pressure output 2 of the 700 SIS

6-2. SIL Capability

● Systematic Integrity
SIL 3 Capable— the 700 SIS has met manufacturer design process requirements of IEC 61508 Safety Integrity Level 3.

● Random Integrity
The 700 SIS is classified as a Type A device according to IEC 61508. The complete final element subsystem will need to be evaluated to determine the SFF. If the SFF of the subsystem is >90%, and the PFDavg < 10-3, the design can meet SIL 3 @ HFT=0.

6-3. Failure Rates

Refer to the FMEDA report (Report No. AZB 12-03-041 R001) for all failure rates. The failure rate data is only valid for the useful lifetime of the 700 SIS. The failure rates will increase after this time period. Reliability calculations based on the data listed in the FMEDA report for mission times beyond the useful lifetime may yield results that are too optimistic, i.e. the calculated Safety Integrity Level will not be achieved. In order to claim diagnostic coverage for Partial Valve Stroke Testing, it is automatically performed at a rate at least ten times faster than the Proof Test frequency. Consult the FMEDA report for a detailed list of the assumptions used in the analysis.

6-4. Application Limits

● Safety Instrumented Function design verification must be done for the entire collection of equipment used in the Safety Instrumented Function including the 700 SIS. The SIS must fulfill the requirements according to the Safety Integrity Level, especially the limitation of average Probability of Failure on Demand (PFDavg)

● The system's response time is dependent on the entire final element subsystem. The user must verify the system response time is less than the process safety time for each final element.

● The 700 SIS fault reaction time is determined by the partial valve stroke test interval plus the mean time to repair.

● The valve actuation means must be of a type that automatically moves the valve to the safe state when the 700 SIS achieves the safe state. Valve stroke time under these conditions may also need to be considered as part of the SIS design.

● The supply air pressure must not exceed 700 kPa. Conditions of supply air in the User's Manual (CM2-AVP772-2001) must be followed.

● The SIS positioner mode must be set to "ON-OFF" to perform a partial valve stroke test. (PVST cannot be performed in "Positioning" mode.)

6-5. Environmental Limits

● Operating ambient temperature: -40 to +80°C [Note]

● Humidity: 5% to 100%RH

Note: It varies according to the explosion-proof type.
Refer to the User's Manual for details.

6-6. Application of the AO/DO for Diagnostic Annunciation

When using the Failure Rates "with PVST", the system must be capable of monitoring the 700 SIS for alarm conditions.

□ Check that the smart ESD device is a model with analog output or discrete output. (If the model has no output, the Failure Rates "with PVST" are not applicable.)

The worst-case diagnostics detection time is determined by the PVST interval that is configured by the user.
Notification of the result of diagnostics is output within 30 seconds of detecting a failure.

⚠WARNING

- **HART communication can be used for informational purposes but is not safety-certified for diagnostic annunciation.**

7. Installation and Commissioning

☐ Verify that the 700 SIS is suitable for use in this Safety Instrumented Function.

☐ Verify that nameplate markings are suitable for the hazardous location (if required).

☐ Verify appropriate connections to the logic solver are made by referring to the instruction and safety manual of the logic solver.

☐ Verify that SIS Positioner Mode is selected appropriately.

☐ Verify that Password Protection is enabled.

☐ If applying "with PVST" failure rates, verify that the SIS Positioner Mode is "ON-OFF", the scheduled PST is enabled, and the PST Interval is configured appropriately.

☐ The safety function of the 700 SIS within the final control element subsystem along with the overall SIS safety function must be tested after installation to ensure that it meets safety demand and applicable process safety time requirements.

☐ The system's response time must be less than the process safety time. The 700 SIS will start to release the pressure within 3 seconds.

8. Operation

If "In use by an Operator" status is active when a PST is scheduled, the scheduled PST will not start at the scheduled time and will be postponed until the next scheduled time. "In use by an Operator" means that one operator (LUI or HART host) is exclusively allowed to configure or calibrate the 700 SIS. This is done by "Allow operator action" method for HART host or by holding down the left button of the LUI.

If applying "with PVST" failure rates, do not change the state of the 700 SIS to "In use by an Operator". When it is necessary to do so, check the PST Next Execute Time.

Password Protection must be enabled during operation.
When it is enabled, the correct password is required to change the state of the 700 SIS to "In use by an Operator". This prevents accidental interference with the scheduled PST.

9. Periodic Inspection and Repair

Periodic testing, consisting of proof tests is an effective way to reduce the PFDavg of the 700 SIS instrument as well as the valve and actuator it is connected to.
Results of periodic inspections and tests should be recorded and reviewed periodically.

9-1. Test Procedure for the 700 SIS

Proof tests are full-stroke tests that are manually initiated. As part of the test, the capability of the SIF to achieve the defined safe state must be verified. The proof test interval must be established for the SIF based on the failure rates of all the elements within the function and the risk reduction requirements. This determination is a critical part of the design of the SIS. A proof test will detect most of dangerous undetected failures not detected by the 700 SIS automatic diagnostics. A proof test includes the following steps:

☐ If applying "with PVST" failure rates, set the scheduled PST to Disabled to avoid personal injury.

☐ Read the 700 SIS alarm information using a HART communicating device such as Valstaff software or a DD- or DTM- based host. Any active alarm messages must be investigated and resolved.

☐ Bypass the final control element or take appropriate action to avoid a false trip.

☐ If used, bypass the diagnostic annunciation (analog output or discrete output from the 700 SIS) or take appropriate action to avoid a false trip.

☐ Check for excessive air supply consumption.

☐ Set the input to the 700 SIS to the trip value (0, 4 mA, or 0 V).

☐ Verify that the 700 SIS and attached valve fully move to the defined safe state within the required safety time through an instrument independent means (visual or other).

☐ Restore the input to the 700 SIS to the normal value.

☐ Observe that the 700 SIS and attached valve return to its normal state through an instrument-independent means (visual or other).

☐ Inspect for any leaks, visible damage or contamination.

☐ Inspect the unit for any loose screws or other incorrect mechanical condition.

☐ If applying "with PVST" failure rates, set the scheduled PST to Enabled.

☐ Record the test results and any failures in your company's SIF inspection database.

☐ Remove the bypass and restore normal operation.

9-2. Maintenance

Refer to Smart ESD Device 700 Series for Safety Instrumented Systems User's Manual (CM2-AVP772-2001).

9-3. Repair and replacement

Repair consists of taking corrective action (according to the troubleshooting and repair procedures given in the User's Manual).
If the 700 SIS breaks down, it must be repaired by exchanging the main part.

Please, read ‘Terms and Conditions’ from following URL before the order and use.

http://www.azbil.com/products/bi/order.html

Specifications are subject to change without notice.

Azbil Corporation
Advanced Automation Company

1-12-2 Kawana, Fujisawa
Kanagawa 251-8522 Japan
URL: http://www.azbil.com/

1st edition: Dec. 2015