



AMS Safety Analysis

Using AMS in Safety Instrumented System Applications

Project:
AMS Safety Analysis

For:
Emerson Process Management
Fisher-Rosemount Systems, Inc.
12001 Technology Drive
Eden Prairie, MN.

Contract No.: Q03/03-09
Report No.: R03/03-09 R001
Version V1, Revision R1.0, May 23, 2003

Management summary

Emerson Process Management's AMS system can be effectively used to meet many of the requirements of IEC 61511 in safety instrumented system applications. In such an application the AMS system is considered "non-interfering" and is not part of the safety function.

AMS can be effective in SIS installation and commissioning, SIS maintenance, SIS modification and the design requirements associated with those phases of the safety lifecycle. Features of AMS including individual login security, automatic audit trail and SNAP-ON diagnostics will allow the user to meet specific safety lifecycle requirements. The system as reviewed was created with a HART multiplexer.

For SIS installation and commissioning, AMS allows the user to verify proper setup and operation of field instruments. AMS increases effectiveness of operation and maintenance (mechanical integrity) programs. Remote diagnostic capabilities allow periodic proof tests to be performed thereby extending the time period between off-line proof tests. During SIS modification, AMS can be used to compare new configurations with previous configuration. This is done to confirm that only changes per the update plan were made and that they were made correctly.

Compared to current practices, AMS usage should be less error prone and clearly traceable.

Two important things must be done to insure system safety with AMS. The AMS system must be setup with individual password security for those authorized to perform SIS maintenance and modification activities. Procedures must be established to insure proper usage of the 275 handheld communicator. In addition during design verification, the failure rates of the HART multiplexer must be accounted for in the probabilistic analysis of each SIF.

Table of Contents

Management summary.....	ii
1 Purpose and Scope.....	2
2 Project management	2
2.1 exida.com	2
2.2 Roles of the parties involved	2
2.3 Standards used	2
2.4 Reference documents	2
2.4.1 Documentation provided by the customer	2
2.4.2 Industry References	3
3 System Description.....	4
4 AMS Usage per IEC 61511 requirements.....	5
4.1 SIS Design and Engineering	5
4.2 Installation and Commissioning	6
4.3 SIS Operation and Maintenance	7
4.4 Modification	8
5 AMS Restrictions	8
6 Terms and Definitions.....	9
7 Status of the document.....	9
7.1 Releases	9
7.2 Future enhancements of the document.....	9
8 Appendix A: Human Factors Safety Analysis – Parameter Changes	10

1 Purpose and Scope

The purpose of this report is to explain the optimal usage of the Emerson Asset Management Solutions (AMS) package in safety instrumented system (SIS) applications in order help fulfill requirements of ANSI/ISA S84.01-1996 and IEC 61511 (ANSI/ISA 84.01-2003).

2 Project management

2.1 exida.com

exida.com is one of the world's leading knowledge companies specializing in automation system safety and availability. Founded by several of world's top reliability and safety experts, *exida.com* has over one hundred cumulative years of experience in automation safety. *exida.com* is a partnership with offices around the world. *exida.com* offers training, coaching, project oriented consulting services, Internet based safety engineering tools, detail product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida.com* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Emerson Process Management (FRS)
exida.com

Developer of the AMS software
Project leader and assessor of the AMS software per the requirements of IEC 61511

2.3 Standards used

The services delivered by *exida.com* were performed based on the following standards.

N1 IEC 61511:2003 Part 1 Functional Safety – Safety instrumented systems for the process industry sector.

2.4 Reference documents

2.4.1 Documentation provided by the customer

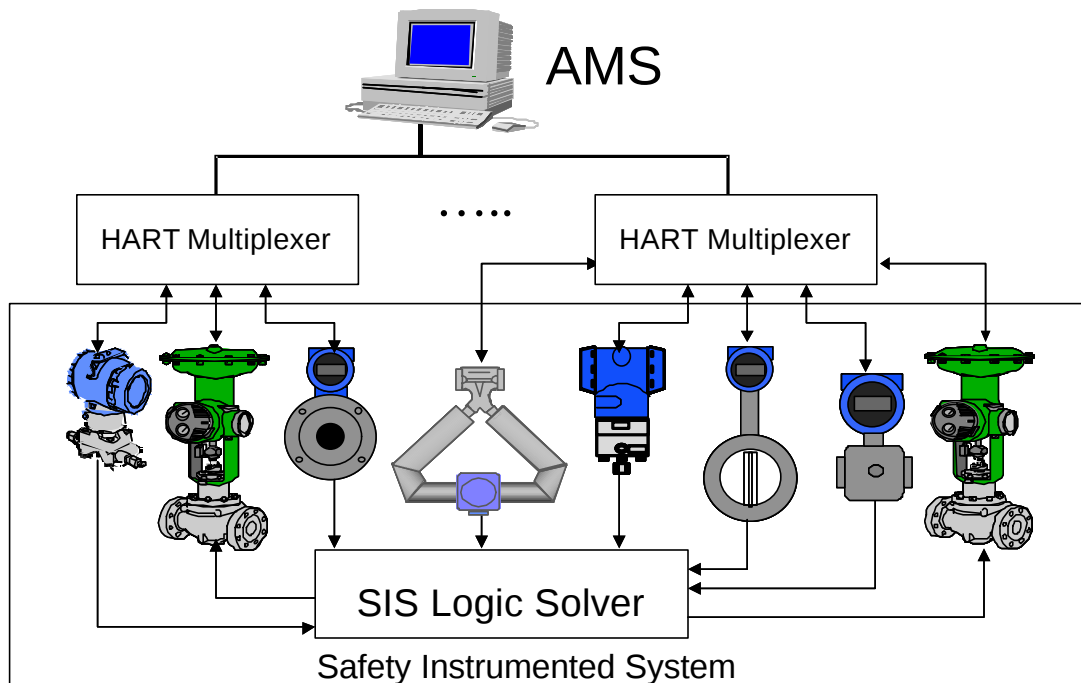
D1	AMS Version 6	Asset Management Solutions software and manuals
D2	AMS Brochure	D350697X012, 2-2000.
D3	Product Data Sheet	ValveLink SNAP-ON Application, January 2003
D4	Product Data Sheet	Audit Trail, January 2003

2.4.2 Industry References

- | | | |
|----|-------------------------------|---|
| R1 | 1 st Edition, 2003 | Safety Equipment Reliability Handbook, exida, ISBN # 0-9727234-0-4, Page 105, ELCON MULTIPLEXER 2700 |
| R2 | 1 st Edition, 2003 | Safety Equipment Reliability Handbook, exida, ISBN # 0-9727234-0-4, Page 106, Endress+Hauser Fieldgate FXA520 |
| R3 | FMEDA Report | Exida, FMEDA including SFF determination and PFD calculation, P+F 02/4-11, July 2002, Version 1, Revision 1.2 |

3 System Description

The system under review in this report is shown in Figure 1.



The system consists of a computer running AMS software, HART multiplexer(s), and connections to the field instruments that are part of a safety instrumented system.

Note that the HART multiplexer wiring will vary depending on manufacturer. A typical HART termination panel uses a resistor to extract a HART signal that is routed to the multiplexer. The transmitter signal does not pass through the multiplexer and therefore the multiplexer is not considered part of the safety instrumented system.

4 AMS Usage per IEC 61511 requirements

IEC 61511, Part 1, contains requirements for the entire lifecycle of a safety instrumented system. AMS software can be used to meet requirements in key areas of the lifecycle:

Section 11, SIS Design and Engineering

Section 14 Installation and Commissioning

Section 16 SIS Operation and Maintenance

Section 17 Modification

4.1 SIS Design and Engineering

In section 11.6.4, IEC 61511 states that:

“Smart sensors shall be write protected to prevent inadvertent modification from a remote location, unless appropriate safety review allows the use of read/write. The review should take into account human factors such as failure to follow procedures.”

AMS provides capabilities to reduce human systematic errors. These include:

- Individual user login with password
- Automatic audit trail
- Storage of field device configurations with automatic comparison

When these are used within a company quality system, systems can be designed without using jumpers in transmitters. This would require that security be established within the AMS system. The security would allow only those trained in company management of change procedures to make parameter changes to instruments used in safety instrumented systems. Periodic on-line test and inspection procedures should also include use of AMS to check that expected SIS parameters as stored in AMS are still current. AMS audit tracking should be used to track down any unauthorized changes (inadvertent changes through a 275 HART Communicator for example) discovered during the periodic inspection. See Appendix A for a human factors review.

In section 11.7.2.1, IEC 61511 states that:

“The design of PE SIS maintenance/engineering interface shall ensure that any failure of this interface shall not adversely affect the ability of the SIS to bring the process to a safe state. This may require disconnecting of maintenance/engineering interfaces, such as programming panels, during normal SIS operation.”

It is possible that a HART multiplexer can fail in such a way as to adversely impact the ability of a SIS to bring the process to a safe state. However, the HART multiplexer will have minimal impact. Several manufacturers have had their equipment analyzed by component level FMEDA and provide worst case dangerous failure rates that must be used in the probabilistic SIL verification. **When this is done, if the safety instrumented function meets the probabilistic integrity requirements, the HART MULTIPLEXER may be connected at all times.** This is important if the AMS system is to be used to fulfill other requirements of the IEC 61511 standard.

In section 11.7.2.2, IEC 61511 states that:

"The maintenance/engineering interface shall provide the following functions with access security protection..."

AMS requires that each person using the system login with a password.

In section 11.7.2.4, IEC 61511 states that:

"Enabling and disabling the read-write access shall be done only by a configuration or programming process using the maintenance/engineering Interface with appropriate documentation and security measures."

In addition to the individual security with password, AMS provides an automatic audit trail that documents all activities including any occasion to enable/disable read-write access.

In section 11.8.1, IEC 61511 states that:

"The design shall allow for testing of the SIS either end to end or in parts. Where the interval between scheduled process downtime is greater than the proof test interval, then on-line testing facilities are required."

On-line self-test facilities now available in smart instruments can be remotely activated using AMS with SNAP-ON diagnostics. This can provide for partial on-line testing of a SIF extending the time period between off-line tests. AMS will automatically create a record of the test and has provisions to allow entry of additional comments by test personnel.

In section 11.8.4, IEC 61511 states that:

"Forcing of inputs and outputs without taking the SIS out of service shall not be allowed unless supplemented by procedures and access security. Any such forcing shall be annunciated or alarmed, as appropriate."

AMS provides individual login security and automatically creates a record of the event with its audit trail feature. Audit trail records date, time user and "as found/as left" information. This level of automatic recording has been shown to be an effective mechanism for enforcement of management of procedures.

AMS Alert Monitor provides annunciation of any device left in loop check.

4.2 Installation and Commissioning

In section 14.2.3, IEC 61511 states that:

"The safety instrumented system shall be commissioned in accordance with planning in preparation for the final system validation. Commissioning activities shall include, but not be limited to, confirmation of the following:

earthing (grounding) has been properly connected;

energy sources have been properly connected and are operational;

transportation stops and packing materials have been removed;

no physical damage present;

all instruments have been properly calibrated;

all field devices are operational; ..."

AMS allows the user to verify that instruments are properly calibrated and operation. With AMS a user can take full advantage of diagnostic capabilities and calibration capabilities of smart field devices to verify that all settable parameters are correct. AMS can be used to verify device calibrations.

In section 14.2.4, IEC 61511 states that:

"Appropriate records of the commissioning of the SIS shall be produced, stating the test results and whether the objectives and criteria identified during the design phase have been met. If there is a failure, the reasons for the failure shall be recorded."

AMS produces records of activities through the audit trail feature. Audit trail records date, time user and "as found/as left" information.

4.3 SIS Operation and Maintenance

In section 16.2.1, IEC 61511 states that:

"Operation and maintenance planning for the safety instrumented system shall be carried out. It shall provide the following:

routine and abnormal operation activities;

proof testing, preventive and breakdown maintenance activities;

the procedures, measures and techniques to be used for operation and maintenance;

verification of adherence to operations and maintenance procedures;

when these activities shall take place;

the persons, departments and organizations responsible for these activities."

AMS can be used to as an essential part of periodic inspection and test process. Procedures can be created within the AMS software and used with a scheduler to remind personnel when tests must be performed. Responsible persons can be documented within the system.

In section 16.2.2, IEC 61511 states that:

"The user shall maintain records that certify that proof tests and inspections were completed as required. These records shall include the following information as a minimum:

- a) *description of the tests and inspections performed;*
- b) *dates of the tests and inspections;*
- c) *name of the person(s) who performed the tests and inspections;*

d) *serial number or other unique identifier of the system tested (e.g., loop number, tag number, equipment number, and SIF number);*

e) *results of the tests and inspection (e.g., “as-found” and “as-left” conditions).”*

The AMS audit trail feature can be used to provide records that proof tests and inspections were completed as required. Most of the required information is automatically stored in the AMS database. The SIF identification number can be manually entered using the Manual Audit Trail entry. Results of the tests and inspection are also automatically recorded or may be entered manually.

4.4 Modification

In section 17.2.5, IEC 61511 states that:

“Appropriate information shall be maintained for all changes to the SIS. The information shall include:

a description of the modification or change;

the reason for the change;

identified hazards which may be affected;

an analysis of the impact of the modification activity on the SIS;

all approvals required for the changes;

tests used to verify the change was properly implemented and the SIS performs as required;

appropriate configuration history;

tests used to verify the change has not adversely impacted parts of the SIS which were not modified.”

An AMS system is often the tool used to make changes to smart field instruments. It automatically records details including date, time user and “as found/as left” information. The Manual Audit Trail entry can be used to enter specific impact analysis information for a specific device or at the plant database level. All authorization and change approval information can also be entered through Manual Audit Trail if not automatically established by AMS security.

5 AMS Restrictions

To meet requirements of IEC 61511, the AMS software must be setup per the following:

“The AMS System must be specified, installed and configured in a documented and structured manner following recognized Quality standards.”

“HART devices in SIS systems should be logged with the Hart Communication Foundation and used according to Technology guides and the DDL specifications in the EDDL International Standard (IEC 61804-2).”

Security – the administrator duty must be assigned to an individual with proper training in SIS importance. This individual must establish user identities and passwords for all those authorized to perform maintenance and testing on the SIS. Security may be assigned only to those with proper training in SIS management of change. Company procedures must be established for the use of AMS in SIS applications. In particular the procedure must prevent the use of a 275 handheld communicator from being used to change any safety critical parameters.

Training –Those responsible for execution of SIS procedures must be trained in those procedures, proper operation of AMS and general requirements of SIS operation and maintenance.

6 Terms and Definitions

AMS Asset Management Solution (Emerson Product Name)

DDL Device Description Language

FMEDA Failure Modes Effects and Diagnostic Analysis

FSM Functional Safety Management

IEC International Electrotechnical Commission

SIF Safety Instrumented Function

SIL Safety Integrity Level

SIS Safety Instrumented System

7 Status of the document

7.1 Releases

Version: V1

Revision: R1.0

Version History: V0, R0.1: Initial document
V1, R1.0: Added comments from reviewers

Authors: William Goble, Bill Mostia

Review: V0, R0.1: reviewed by client, Bill Mostia

Release status: released

7.2 Future enhancements of the document

None anticipated.

8 Appendix A: Human Factors Safety Analysis – Parameter Changes

IEC 61508, Part 2, Table A.18 requires the following measures to reduce systematic errors in the operations and maintenance phase of the safety lifecycle:

1. Modification Protection (HR – Highly Recommended): This requirement specifically refers to inadvertent or unauthorized hardware modifications. AMS can be used to check for hardware modifications to the system due to removal of equipment. This is detected whenever any devices in the AMS directory no longer respond to AMS commands. This tool helps provide modification protection.

IEC 61508, Part 3, Table A.8 contains six techniques and measures to be used during software “modification.” The only relevance to devices connected to AMS is when safety critical parameters are changed.

1. Technique 5. Software configuration management: If properly set up and maintained, AMS requires a password in order to change engineering ranges. An examination of parameters in a pressure transmitter (3051S) indicates that this is the only parameter that may prevent the safety function from properly performing. In addition, AMS Audit Trail automatically logs all changes with date and time, person performing the change and as found/as left information. Change controls with audit capability are well-accepted features of a good software configuration management system.
2. Technique 6. Data recording and analysis: AMS Audit Trail helps fulfill this technique as well providing automatic recording of date, time, person making change and as-found/as-left information. In addition, AMS provides the capability of checking parameters in HART devices and comparing the parameters in the device against those stored in AMS. This monitoring could detect any unauthorized parameter change done by a handheld communicator or corrupted communication message.

General Human Factors Checklist:

Human errors have been shown to be associated with various conditions of a task. These include accessibility to tools, clarity of instructions, usability of tools, task overload and work schedules. A general checklist was reviewed for relevant items to insure that AMS can be used to reduce human error when changing safety critical parameters in connected devices.

Accessibility	AMS should be installed in a location where the system is readily accessible by those who need to use it. Fortunately AMS may be installed in engineering facilities due to the computer communications.
Clarity	AMS provides a clear human interface via Windows based dialog boxes.
Usability	AMS provides menu driven options and a clear user interface.
Training	Training is available on AMS usage. Company procedures should authorize only only personnel who have been properly trained on AMS usage and the safety instrumented systems.
Accountability	Audit Trail automatically records date, time, person and as-found/as-left information. This enforces accountability.
Work Overload	It is expected that an AMS system be established in an environment where sufficient time is allocated to perform safety critical work. No system can protect against this condition.
Deliberate Tampering	Audit Trail automatically records date, time, person and as-found/as-left information. This can help discourage deliberate tampering.
Environment	AMS can be installed in a proper engineering workplace where distractions are not as likely.
Displays/Control not visible	All AMS displays and controls are similar to standard personal computer operations and readily visible.