Certification Report of the DeltaV SIS

Revision No.:	1.2
Date:	2005-08-16
Report Number:	701-023/2003T
Product:	DeltaV SIS
Customer:	Emerson Process Management 12301 Research Blvd Austin, TX. 78759 USA
Order Number:	20685997
Inspection Authority:	RWTÜV Systems GmbH Safety Approval Service – SAS Hübnerstr. 3 86150 Augsburg Germany
Accredited Laboratory:	RWTÜV Systems GmbH Member of TÜV NORD Group Safety Related Services - SRS Postfach 10 32 61 45032 Essen Germany
Responsible:	Author: (Josef Neumann) Reviewer: (Gerhard M. Rieger)

This document is only valid in it's entirety and separation of any part is not allowed.

Content **Page**

1 Subject of certification 3
2 Basis of certification 4
3 Standards 5
4 Definitions 6
5 Overview of the system configuration 7
5.1 Distributed Control System 8
5.2 Embedded SLS System 8
6 System Level and Communication Links 9
6.1 User Interface 10
6.2 ACN (Area Control Network) 10
6.3 DeltaV Controller and I/O 10
6.4 (SLS) Logic Solver 10
6.5 SISnet Repeater 13
7 Detail SLS Design 14
7.1 Main Processor 1 14
7.2 I/O Processor 16
7.3 WDT (Watchdog Timer) 16
7.4 Field Power Control 16
7.5 Power Conversion 17
7.6 I/O Circuits and (Field) Termination Block 17
8 Hardware and software identification 17
9 Documentation 18
10 Assessment activities and results 19
10.1 Development Process 19
10.2 System Architecture 21
10.3 Proven In Use 22
10.4 Hardware Design and FMEDA 23
10.5 Software Design and Implementation 26
10.6 Verification and Validation 27
10.7 Fire detection and fire alarm systems 28
10.8 Safety Manual 29
11 Summary 29

1 Subject of certification

This report compiles the results of the assessment of the DeltaV SIS of Emerson Process Management. The services of RWTÜV Systems GmbH (thereafter known as RWTÜV) were ordered by Emerson Process Management to certify the DeltaV SIS because of its use in safety-relevant applications by the process industry (e.g. oil & gas and chemical industry) with the goal of achieving a successful approval of the DeltaV SIS in the framework of the certification of safety-components.

The DeltaV SIS is to be certified in accordance with IEC 61508 for single use in Safety Integrity Level 3 (SIL 3) applications and for low demand and high demand mode of operation.

The DeltaV SIS is based upon the existing DeltaV which already has a documented history for the proven in use consideration under IEC 61508, the industry standard for safety electronic systems.

2 Basis of certification

An effective assessment in order to meet all the requirements for a complete certification requires the following testing segments to be successfully completed:

- Development process
- Safety system structure and Safety Requirements
- Hardware design
- Software design and implementation
- Proven in use documentation
- Safety verification steps and the validation tests
- Test specification and test results

Including the following principal functional safety considerations:

- Hardware failure-behaviour
- Software failure-avoidance
- Probabilistic and Common Cause consideration
- Safety Manual

3 Standards

Because of the application area of the DeltaV SIS, the following standards are relevant:

List of standards	
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems SIL 3 capability, Type B, Low and High Demand
IEC 61508-1:1998	Part 1: General Requirements
IEC 61508-2:2000	Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
IEC 61508-3:1998	Part 3: Software requirements
EN54-2: 1997	Fire detection and fire alarm systems Part 2: Control and indicating equipment

4 Definitions

E/E/PE	Electrical/electronic/programmable electronic
E/E/PES	Electrical/electronic/programmable electronic system
FIT	Failure In Time ($1*10^{-9}$ failures per hour)
FSM	Functional Safety Management
FMEDA	Failure modes, effects, and diagnostic analysis
HART	Highway Addressable Remote Transducer
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof-check frequency
IOP	I/O Processor
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency
OS	Operating system
P2P	Peer to peer
PFD	Probability of Failure on Demand
PFD_{AVG}	Average Probability of Failure on Demand
SCI	Serial Communications Interface
SCC	Serial Communications Controller
SF	Safety Function
SFF	Safety Failure Fraction
SIF	Safety Instrumented Function
SIS	Safety Instrumented System; Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
SIL	Safety Integrity Level.
SLS	Smart Logic Solver
SRS	Safety Requirements Specification
λ_{du}	Dangerous Undetected (DU) Failure Rate [1/h]
Type A component	“Non-Complex” component (using discrete elements); for details see 7.4.3.1.3 of IEC 61508-2
Type B component	“Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2

5 Overview of the system configuration

The DeltaV SIS system is a “Safety Rated Logic Solver with I/O” that is embedded within a Basic Process Control System (DeltaV Control and I/O System). This Logic Solver is also called SLS (Smart Logic Solver) or SLS1508 which refers to the certified SLS. At the module or unit level, the DeltaV SIS architecture is designed to achieve SIL3 capability for non-redundant configurations through extensive internal diagnostics and two channel circuitry within one SIS unit. The DeltaV SIS Safety PES can also be used in a redundant configuration to increase availability.

SLS´s publish their I/O data and configured control outputs to otherSLS’s via a P2P (Peer to Peer) Bus.

As a User Option, there may also be a an SISnet Repeater used to provide P2P Bus connectivity to SLS’s located in separate DeltaV Controllers.

The SLS interfaces to an independent set of safety related sensors and actuators, which are supplied by other vendors.

The SLS Control and I/O System use modular I/O to interface with process equipment (also supplied by other vendors).

The SLS Control and I/O System is capable of “shadowing” the safety logic functions to provide visibility, event logging, and alarms to Users via the DeltaV User Interface based on Windows XP (or later). Information from the SLS is sent to the DeltaV Controller to allow visibility via the normal control system tools.

Process Engineers, Operators and Maintenance Technicians have the ability to view information and status related to the SLS. Maintenance Technicians will also have access to status information provided by LEDs on the SLS and MPG.

Safety Engineers are allowed to create, and make changes to the safety logic. User software keys enable these functions.

5.1 Distributed Control System

The standard DeltaV is a state of the art DCS (Distributed Control System) using third party and internally developed hardware and software platforms. Users create a configuration using a set of Engineering Tools, and store that configuration in a single database. The configuration is then downloaded to individual User Interface, Control, and I/O Devices. Several features for alarm handling and event logging are built into the system.

The DeltaV SIS is the certified safety system for safety relevant applications.

The Safety Manual for DeltaV SIS will require the user to functionally test his configuration prior to allowing the plant to operate under control of the SLS.

The Operator Interface uses Microsoft Windows XP (or later) to provide services to the individual users. These include security and password-protected access to certain functions. Standard PCs and networking components are used.

The Operator Interface will contain an applet to enforce a two-stage write mechanism for any safety related parameters. This will be a stand-alone applet that is rated as Safety Critical. This applet is also referred to as the “Secure Write Mechanism”.

The Control and I/O Subsystem uses custom designed embedded processors and field circuits. The controller is used by the SLS subsystem as a communications path for configuration, operational view, and diagnostic status.

The I/O subsystem contains modules to process individual I/O channels for the Control System, and bus Interfaces.

5.2 Embedded SLS System

The new family within the DeltaV product line is designed to meet the requirements of IEC61508 to a SIL3 level as a Safety Instrumented System. This will function as an independent subsystem of the Control and I/O portion of the DeltaV DCS.

The DeltaV I/O subsystem contains physical mounting and addressing for 64 I/O cards. The SLS is doublewide I/O card, and consumes two I/O slots. There can be from 0 to 32 SLS’s located within each DeltaV Controller.

The SLS subsystem will contain one or more SLS’s residing within the I/O subsystem on the DeltaV Controller. These have the capability to share their local I/O to support

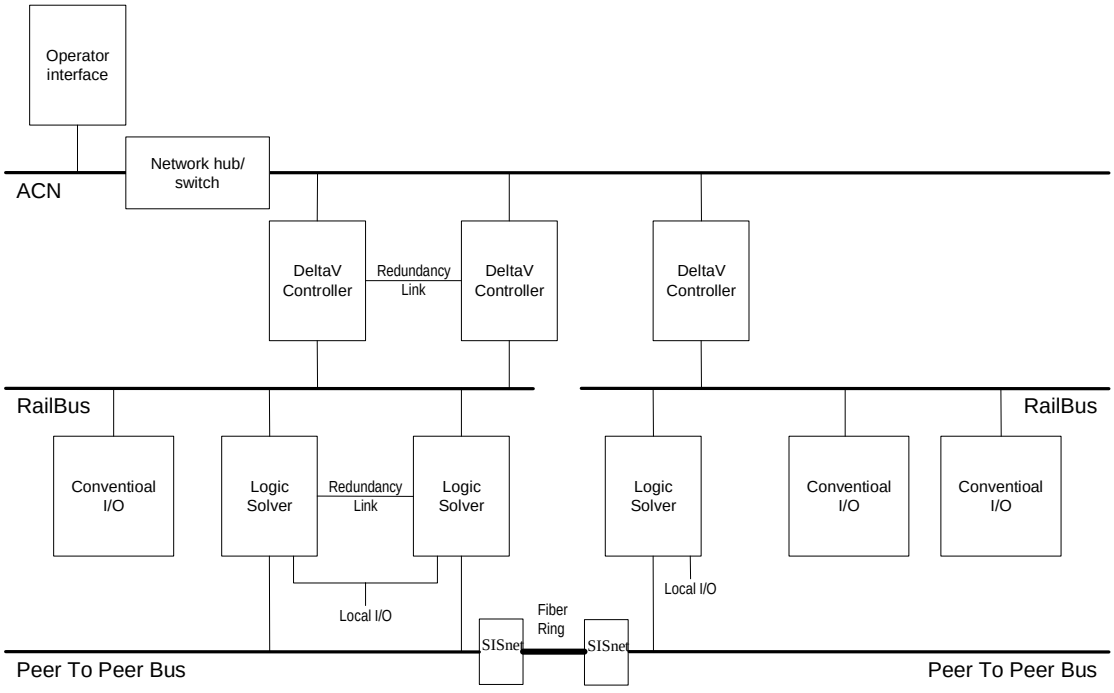
larger and/or distributed safety strategies.

SLS's under different DeltaV Controllers can communicate selected outputs (Secure Parameters) of their calculations to other SLS's to use as safety critical inputs for their own calculations. These data items are published and propagated via a fiber optic ring architecture using an SISnet Repeater. The SISnet Repeater will support communications from SLS's within 0 to 32 DeltaV Controllers.

The MPG will distribute messages that were created by Safety Critical Software within the SLS and maintain the encapsulation of those messages. The MPG will be rated as non-interfering.

6 System Level and Communication Links

Picture 1 shows a physical view of the system. It provides an overview of the overall system and the communication links:



Picture 1: Block diagram of the system

6.1 User Interface

The user interface is used to download programs and parameters. Configuration tools are used for the Control and Safety logic. New function blocks, are available to the user for implementing safety logic. There is a “Secure Write Mechanism” to allow the user to confirm changes in parameters associated with the user safety function.

6.2 ACN (Area Control Network)

Messages associated with the configuration will be extended to provide appropriate measures for Safety Communications. The used products are off the shelf Hubs and Switches.

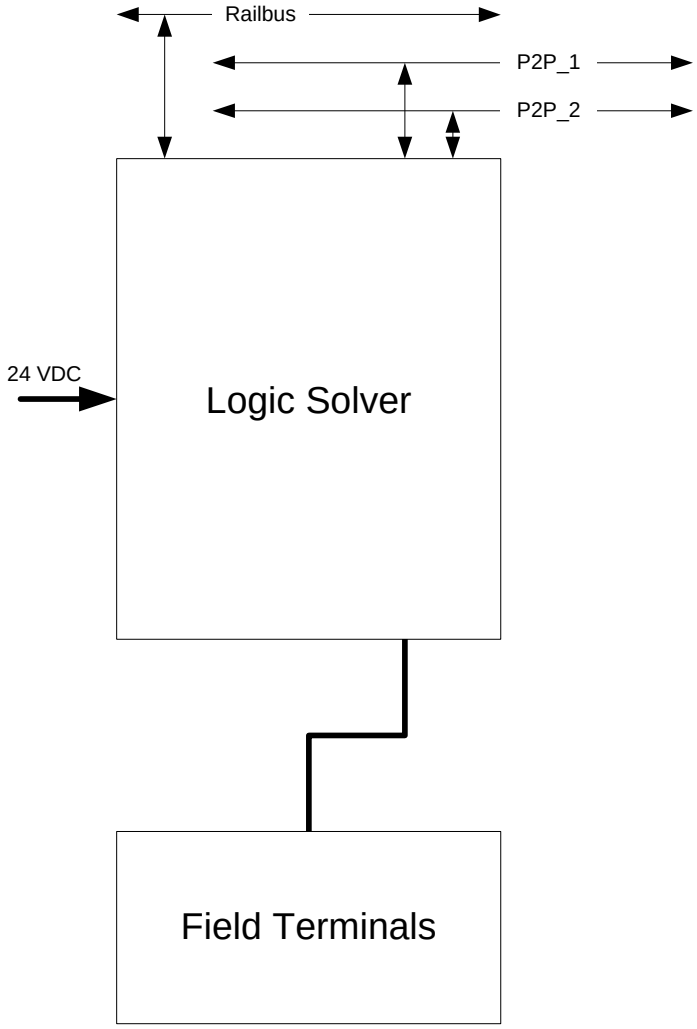
6.3 DeltaV Controller and I/O

A new version of the 2-Wide Controller Carrier (backplane) was created to remove DeltaV Controller connections to the P2P Bus, and to provide termination for one end of the P2P Bus. A revised extender cable carrier provides termination for the other end of the bus.

The firmware of the DeltaV Controller includes support of the Railbus communications to the SLS, and shadowing for new function blocks used in the SLS. Diagnostic information is transmitted from the SLS and SISnet Repeater on a periodic basis.

6.4 (SLS) Logic Solver

The SLS is a self contained SIL3 Controller and I/O combination that will be located within the DeltaV Controller’s I/O Subsystem. The SLS is powered independently, and performs its configured safety function independently from the DeltaV Controller and I/O subsystems.



Picture 2: Block diagram of the single system

The DeltaV I/O subsystem hardware is used to mount the SLS, and communications with the DeltaV Controller are used to configure the safety function. Further, the DeltaV Controller is used to receive data and diagnostics status from the SLS. All communications with the DeltaV Controller are provided via the Railbus, which is also used for all conventional I/O attached to the DeltaV Controller.

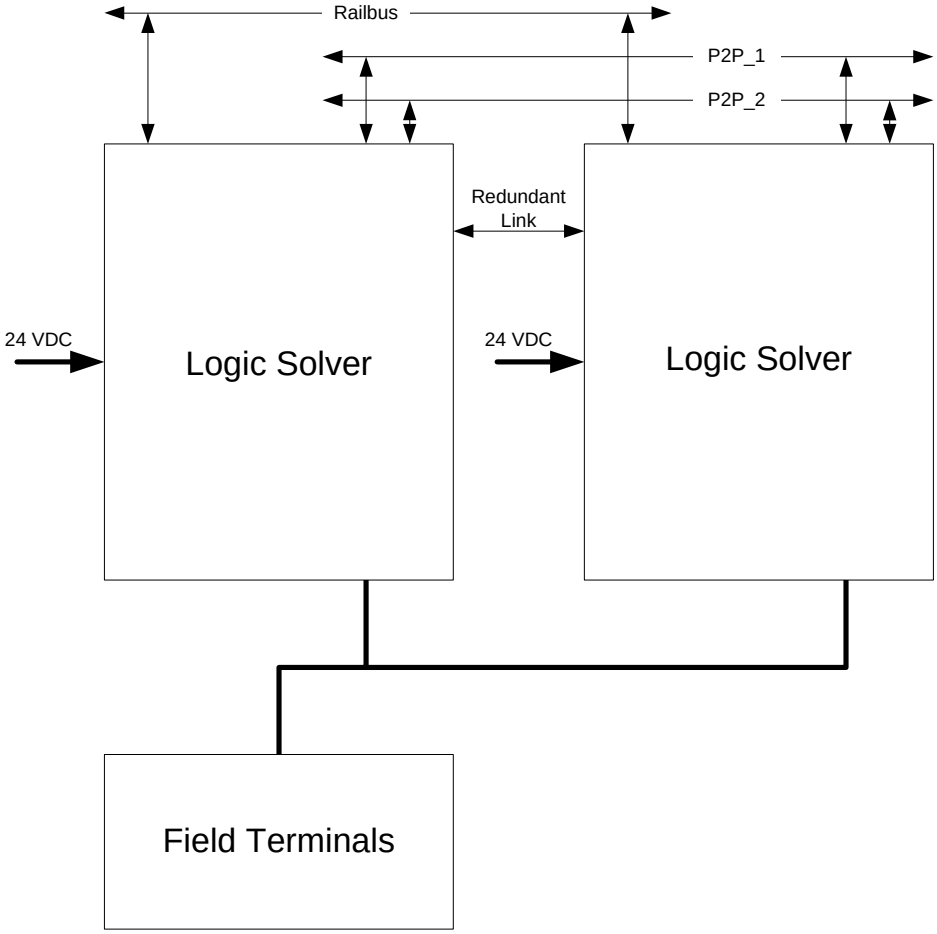
The SLS is powered separately from the DeltaV Controller, so that loss of power to the DeltaV Controller will not affect the operation of the SLS.

The SLS uses a termination block to make the connections to safety field sensors and actuators. The SLS supports 16 individual channels that can be configured to be either: Discrete Input (Dry Contact or 12 VDC Namur sensors), Discrete Output (24VDC High Side Switch), Analog Input (4-20 mA) or 2-State DVC (20 mA). The AIN and DVC channels can be enabled to support HART communications. This is known as Flexible I/O.

The SLS package is a new size, which is a doublewide I/O card format. This is required to support multiple processors and 16 channels of Flexible I/O. Because the card is double wide, it will take up the address space for two I/O cards. The first address will show up in the system as an SLS, the second address will show up as an empty slot in the I/O Subsystem.

The SLS has the capability to publish its I/O values so that larger strategies may be created by using inputs from multiple SLS units. Further, the SLS can publish Secure Parameters that are the (Boolean) outputs of its local calculations. These can be used to extend the strategy, or to provide early warning of a decision to shut down in one area of the plant prior to the process trip in a different area. These messages are transferred over a redundant Peer to Peer (P2P) bus.

The SLS may be installed in a redundant fashion to improve availability and reduce “nuisance trips”. The redundant SLS’s share a term block to require only one field connection per I/O channel and communicate the status between them via a “redundancy link”. This redundancy link is a point to point communications path between a pair of SLS’s when they are connected to a Redundant Termination Block.



Picture 3: Block diagram of the redundant system

6.5 SISnet Repeater

The SISnet Repeater is a device that is used to extend the P2P bus beyond the Logic Solvers connected to one DeltaV Controller. All of the P2P messages are published to all SLS's on a given DeltaV Controller. When Secure Parameter values need to be shared outside of this scope, a redundant SISnet Repeater must be installed.

The SISnet Repeater takes P2P messages that are configured by the user as "global", and broadcasts them to a fiber optic "ring". Each SISnet Repeater forwards global data from its local SLS, and forwards all data from the previous SISnet Repeater in the ring. (Once a message has gone the whole way around the ring, it is not forwarded.) All messages distributed around the ring are re-broadcast to the SLS's on the controller backplane that the SISnet Repeater is located in.

7 Detail SLS Design

The overall design is described in the following sections. Some of the functionality is partitioned between different circuit boards.

As shown, this design involves two Microprocessors. These are used to improve the diagnostic coverage of the calculation portion of the SLS. There are multiple communication bus interfaces.

Both processors run the Logic Engine Task, and the results are compared.

Both processors have a Diagnostic Task which monitors the status and execution of the other tasks running on that processor. If all are running correctly, the Watchdog Timer is armed.

7.1 Main Processor 1

There are two “main” or Logic processors in an SLS. Each has a dedicated interface to a SDRAM block, a Battery Backed SRAM and Real Time Clock chip.

Four LEDs are located on the front of each module. A green LED (labelled “POWER”) is illuminated to indicate the module is powered. A red LED (labelled “ERROR”) will be illuminated as a result of certain error conditions as specified in the Software Functional Specification. Two yellow LEDS will provide operational status as specified in the Software Functional Specification.

The SLS will store its configuration in Flash memory to allow a re-start after a power outage. A commission circuit is used to make sure that an SLS moved from one location to another does not restart automatically. The commission circuit holds its status up to 24 hours as long as the Card is not removed from the Term Block.

Railbus (Controller to SLS Interface)

Railbus is the serial interface between the Controllers and I/O Subsystem. It is used to configure and initialize the SLS, but after the safety function is up and running, does not impact the safety function and been certified as interference free. The SLS will use this interface to report status and diagnostic information the DeltaV Controller and User Interface.

Peer to Peer Bus

The SLS can communicate with other SLS's via a Peer-to-Peer bus. This is a Time Slice protocol which allows each SLS to communicate (publish) its I/O data and configured "reference" parameters that are the result of calculations.

This bus is implemented in a half duplex mode, which allows one SLS to talk during its time slice. The bus uses a RS-485 physical layer on signals on the DeltaV I/O Backplane. These lines are not used by any other DeltaV products.

There are two independent busses, to provide improved availability. Messages on the bus are protected by a CRC that is maintained back to both Main Processors.

Redundancy Link

The redundancy link is a full duplex point-to-point communication port between a Logic Solver and its redundant partner (if present). The signal is routed thru the Term Block that is shared by the two logic solvers. The microprocessors on each SLS use the same data for the calculations, so this bus is used to exchange configuration and status information.

During the configuration process for the standby, the configuration, any parameter (tuning) changes, and any working data for the blocks (i.e. timer values) are transferred on this link. During run-time operations, status and heartbeat are exchanged to verify a proper execution.

I/O Processor Link

A port is used to provide the interface between the microprocessors and the IOP (I/O Processor). This is used to provide configuration to the I/O Channels and provide I/O Data and status back to the microprocessors. Data transfer between the processors is protected via a CRC and must occur during expected timing windows.

The MP2 and IOP circuitry are optically isolated to allow the MP1/2 Circuitry to be grounded (referenced) to Railbus, and the I/O Circuitry to be grounded (referenced) to I/O Field Power.

7.2 I/O Processor

The I/O Processor is a stand-alone microcontroller that includes onboard memory. The IOP contains a windowed watchdog timer that will reset the processor if not armed. The IOP is powered up in Reset, and held there until released by the MP2 processor. The IOP has the capability to read the output of the Field Power Control. This is used to test the Watchdog Timer's control of the Field Power.

Most of the functionality of the IOP is dedicated to reading input values, writing outputs, and reading diagnostic values, which include output read-backs for all of the channel types.

7.3 WDT (Watchdog Timer)

Each of the MP processors arms an independent windowed Watchdog Timer. If either WDT is armed early or late, the power is removed from the field circuit. Next a high level interrupt is provided to the processor which timed out, to allow that processor to save state and failure information. Finally after a delay, all three processors on the SLS are placed in RESET.

7.4 Field Power Control

This section enables the power that is used to power field circuits. The WDT section provides an overall enable for the power, and the IOP has independent power control for Discrete Output, and all other Circuits. The IOP has the ability to read if Field Power is present before and after it's control switches.

7.5 Power Conversion

There are three different types of power conversion on the design. 24 VDC input power is converted by an isolated DC/DC to provide power for the microprocessors and associated circuitry. The output of this DC/DC is referenced (grounded) to the Railbus ground.

24 VDC is also converted into a logic supply for the IOP and I/O Circuitry. This DC/DC is not isolated, because it is referenced (grounded) to the return for the Input Power.

Power used for the AI/DI/AO field circuits is boosted up to 29 VDC by a DC/DC converter. The WDT and the Field Power Control section control this converter, so it can be shut down by either the WDT or the IOP.

7.6 I/O Circuits and (Field) Termination Block

The SLS provides 16 channels of flexible I/O. Each I/O Channel can be configured by the user as a Discrete Output, Discrete Input, Analog Input, or Analog Output. Both analog channel types support HART communications.

The AOUT and DOUT circuitry are diode isolated to allow a redundant pair to dual drive the outputs. Both circuits have a readback to detect if the DOUT is energized, or if current is flowing in the AOUT circuit. The AIN uses a “range resistor” pair on the term block. When redundant units are used, both read the voltage from the same resistor. However since the AOUT circuit sources the current, a second comparison value is available on each card.

8 Hardware and software identification

The following revisions are considered for the certification:

SLS1508 Software:

Firmware revision 1.xx.xx.xx cr

SLS1508 Hardware:

Hardware revision: 4.x

9 Documentation

[M1] DeltaV SIS System Description, exida, 2004-04-11

[M2] DeltaV SIS Safety Requirements Specification, 2005-05-20

[M3] Delta V SIS Software Architecture Description, 2005-06-02

[M4] SIS Proven-in-Use Operating System Hours, exida, 2005

[M5] DeltaV SIS Work Package Plan, 2005-05-23

[M6] DeltaV Project Management Plan, 2005-05-23

[M7] SW Hazop with Module Testing (with TÜV Tests), 2005-07-06

[M8] Hardware Schematics, 2005-03-25

[M9] System Level FMEDA, exida, 2005-11-07

[M10] Software Criticality Analysis, 2003-11-04

[M11] SIS Integration Testing Test Procedure Overview, 2005-03-23

[M12] DeltaV SLS Fault Injection Test Report (with TÜV Tests), V1, 2005-05-16

[M13] Safety Manual, 2005

[M14] EN 54-1 Requirements Review, exida, 2005-03-10

[M15] Failure Modes, Effects and Diagnostic Analysis, exida, V1.4, 2005-08-16

[M16] Markov Model Analysis, exida, V1.1, 2004-09-24

[M17] DeltaV SIS Validation System Test Plan, 2005-06-01

[M18] SIS Integration Testing, Test Procedure Results, 2005-03-26

Documents of RWTÜV:

[M19] Concept Report, V1.0, 2003-07-25

[M20] Protocol of the FSM Audit, V1.0, 2003-25-07

[M21] Fault Injection Test Report for the hardware of DeltaV SIS, V1.0, 2005-06-07

[M22] Fault Injection Test Report for the software of DeltaV SIS, V1.0, 2005-06-07

[M23] Protocol of the Architecture Assessment, V1.0, 2003-07-25

[M24] Checklist IEC 61508, 2005-06-08

[M25] Protocol of the assessment of the DeltaV SIS, V1.0, 2005-06-06

10 Assessment activities and results

10.1 Development Process

General aspects and scope:

The assessment of the development process has been performed within the certification of the DeltaV SIS. In the certification process a safety management audit has been performed to cover the relevant requirements of the IEC 61508, in respect of the fulfilment of the requirements to the safety quality procedures.
The scope of the Functional Safety Management Audit covers the specified Safety Lifecycle Phases of the IEC61508. The scope is as follows:

For design, developing, manufacturing and integration of microprocessor based safety systems.

For the Functional Safety Management Audit according to IEC 61508 it was essential that the functional safety management and the software development process are designed for the SIL 3. The FSM procedures are used to reduce the systematic failure rate.

Structuring of the development process:

The document DeltaV SIS Project Management Plan [M6] describes the Emerson Process Management development processes and procedures. The functional management system is based on the existing ISO9000:2000 quality system. The aim of the assessment was to show that the defined procedures are not only defined but also used and lived in the project.

The Functional Safety Management Audit covered the following areas:

- Overall safety planning (regarding quality)
- Company FSM procedure
- Feedback control and improvement of safety processes
- Validation test planning
- Change and Configuration management
- Hardware design and development method
- Software design and development method
- Requirement specifications
- Safety Manual

An important part of the audit was to discuss safety aspects of the project with the participants and to ask for the relevant documents and the access to the relevant information. Also the specific knowledge about safety processes and internal review activities were reviewed. Actual documentation was partly reviewed and the statements of the participants were compared with the relevant parts of the documents.

Result:

The audits, interviews and document reviews performed at July 25, 2003 have shown that the Functional Safety Management System defined in the listed documents complies with the applicable sections of the IEC 61508.

No major findings were detected in the audit.

If changes to the Safety Management Systems are performed than RWTÜV must be informed.

10.2 System Architecture

The system documents have been reviewed to verify compliance of the system architecture with the standard listed in clause 3 "Standards".

Based on the set of requirements RWTÜV Safety Approval Service –SAS has evaluated whether the implemented fault detection and fault control measures which are defined for the DeltaV SIS were sufficient to meet the requirements. The system architecture was evaluated in regards to completeness and correctness against the Safety Requirements Specification and the System FMEDA. The system architecture has to be designed for a Type B subsystem according the IEC 61508-2.

The FMEDA verified the defined safe state of the DeltaV SIS in the event of possible malfunctions. Probable deviation from the specified function of the unit was also considered to be a malfunction.

Result:

The review from RWTÜV has shown that the system architecture of the DeltaV SIS is consistent against the Safety Requirements Specification. The specifications in the documentation are consistent and complete and clearly presented. The system concept with the chosen architecture design and the selected measures of fault detection and fault control is able to fulfil the Safety Integrity Level 3 with a Safe Failure Fraction of >99%.

10.3 Proven In Use

For the operating system of the DeltaV SIS the proven-in-use consideration was used to show compliance with the standard. For the DeltaV SIS this information was obtained by the testing group. An excessive testing was provided by Emerson Process Management for up to 186 of SLS and 109 SIS Net Repeaters in operation.
In the considered time period an overall summary of 1.284.267 operating hours have been accumulated. In this time period there have been no significant revisions or changes to the software.

Operation Hours = 1.284.267 hrs for the operating system

In the calculation of the operation hours it is assumed that the units are controlled online on a 24 hours basis and failure modes are reported to the operators.

Result:

The documented operating hours for the operating system are sufficient for the use at SIL 3 applications depending on the calculation of the PDF and SFF.

10.4 Hardware Design and FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration.

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is an extension of the FMEA. It combines standard FMEA techniques with additional analysis to identify online diagnostic techniques and the failure modes relevant to safety system design. It is a technique recommended to generate failure rates for each important category (see “failure category in table 1) in the safety model.

The DeltaV SIS is classified as a Type B device according to IEC61508, having a worst-case hardware fault tolerance of 0.

The following tables show the failure rates resulted from the DeltaV SIS FMEDA [M15] when using the system in a simplex configuration. Table 1 lists the failure rates for the common part of the DeltaV SIS. This data is independent of the number of I/O channels.

Table 1: Failure rates DeltaV SIS Simplex Safety PES – Common Part

Failure category	Failure rate (FIT)
Fail Safe Detected	1056
Fail Safe Undetected	15
Fail Dangerous Detected	1308
Fail Dangerous Undetected	6
Annunciation Detected	1052
Annunciation Undetected	203
No Effect	737

Table 2 lists the failure rates for the various I/O channel configuration. This data reflects a single configured I/O channel.

Table 2: Failure rates DeltaV SIS Simplex Safety PES - per Channel

Failure category	**Failure rate (FIT)**			
	AI channel	DI channel	AO channel	DO channel
Fail Safe Detected	32	13	32	21
Fail Safe Undetected	0	30	0	0
Fail Dangerous Detected	26	16	26	12
Fail Dangerous Undetected	0.008	0	0.008	0
Annunciation Detected	8	8	8	5
Annunciation Undetected	14	11	14	4
No Effect	43	47	43	15

Table 3 lists the failure rates for DeltaV SIS according to IEC 61508.

Table 3: Failure rates according to IEC 61508

Failure Categories	λ_{sd} (FIT)	λ_{su} (FIT)	λ_{dd} (FIT)	λ_{du} (FIT)
Common	2112	955	1308	6
AI Channel	40	57	26	0.008
DI Channel	21	89	16	0
AO Channel	40	57	26	0.008
DO Channel	26	19	12	0

These failure rates are valid for the useful lifetime of the product which is > 20 years.

The user of the DeltaV SIS can utilize these failure rates in a probabilistic model of a safety instrument function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL).

Safe Failure Fraction

According to IEC 61508, the Safe Failure Fraction (SFF) of the DeltaV SIS must be calculated. The SFF is the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault. As both the Fail High and Fail Low failure categories are assumed to be detected by the logic solver (regardless of the fact if their effect is safe or dangerous), the Safe Failure Fraction can be calculated independently of the DeltaV SIS application. Note that according to IEC61508 definitions the no effect failures need to be considered in the Safe Failure Fraction calculation as safe failures. The Safe Failure Fractions that result for the DeltaV SIS are listed in the following table:

Table 4: Safe Failure Fraction of the DeltaV SIS

DeltaV SIS Safety PLC	***SFF***
DeltaV SIS Safety PLC – Simplex configuration	> 99%
DeltaV SIS Safety PLC – Redundant configuration	> 99%

The architectural constraint type for the DeltaV SIS is Type B. The SFF and required SIL determine the level of hardware fault tolerance that is required per requirements of IEC 61508. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

The expected lifetime of the DeltaV SIS is > 20 years. The reliability data listed the FMEDA report is only valid for this period. The failure rates of the DeltaV SIS may increase sometime after this period.

Result:

With these results from the calculation it can be shown, that the DeltaV SIS is able to fulfil SIL 3 capability for the hardware design in a single configuration and redundant configuration.

10.5 Software Design and Implementation

The software of the DeltaV SIS is described in the Software Architecture Description. Reviews from RWTÜV have been performed to the overall design documentation and the detailed description and the Software Critically Analysis. The system software is based on two controllers with comparison capabilities. On each controller specific test routines are running to detect hardware faults. The basis of the software architecture is performed by the operating system. Through intensive testing over a longer period (see proven-in-use report for the operating system) the absence of systematic failures could be shown sufficiently. The communication modules were also tested extensively by the module and validation testing. All interfaces have been covered and analysed.

The internal comparison features, test routines and detection of corrupted RAM areas, reach a sufficient safe failure fraction > 99%.

Result:

The software design and Implementation is compliant to IEC 61508 part 3 for the required SIL.

10.6 Verification and Validation

The test specification defined in the Validation Test Specification and Plan from the manufacturer has been reviewed. The list of validation tests are referenced to the Requirement Specification. The review has shown that the requirements are covered by the validation plan.

After the execution of the validation tests by the manufacturer, the test results have been reviewed by RWTÜV. The test results are also referenced to the Design Specification.

Additional sample testing of the DeltaV SIS have been defined by RWTÜV and a separate list of test items has been generated. The defined tests have been executed at the manufacturer by RWTÜV. The definition and results are documented in the RWTÜV Fault Injection Test Reports.

Result:

The review of the Validation Test Specification, the Validation Test Report from the manufacturer and the performing of the sample tests by RWTÜV have shown, that the defined tests are consistent to the Design Specification and the tested results can be compared to the tests of the manufacturer. The test definitions are sufficient to prove compliance with the standard.

10.7 Fire detection and fire alarm systems

To use the DeltaV SIS in fire and gas systems according EN54-2 in energized to actuate applications there are some extensions to consider:

- Redundant SLS1508s must be used whenever output channels are being driven
- A separate power source is required for each SLS1508 card in redundant pairs driving output channels.
- Each Discrete Output channel on the SLS1508 must interface with the final element using an Auxiliary Relay DTA-Inverting module and an Auxiliary Relay Diode module.
- A supplemental Discrete Input channel is required for each output for feedback and line fault monitoring.

These basic features of the control system have been reviewed with the DeltaV SIS documentation and the details of the extension relay module and diode module have been discussed with the manufacturer using the drawings of the modules. A complete checklist was reviewed with the manufacturer to show compliance with the requirements.

Result:

The review of the documentation and the relevant chapters in the safety manual shows that the DeltaV SIS together with the hardware extension modules is suitable for the use in installations of fire detection and fire alarm applications according EN54-2. Furthermore the requirements of the EN54-2 regarding the application conditions must be taken into account.

10.8 Safety Manual

The safety manual has been reviewed to fulfil the requirements of the considered standards. Specifically the section about Proof Testing has been checked according the defined measures to be followed up by the end user to be compliant with the considered standards according failure detection which are not covered by the diagnostic of the DeltaV SIS.

Result:

The review has shown that the safety manual meets the requirement of the considered standards. Detailed descriptions are included for the end user to install, operate and maintain the DeltaV SIS in the required safety level.

11 Summary

The assessment of the DeltaV SIS has shown that the system design, the safety functional management and the system structure are compliant with the IEC 61508, SIL 3 and with the specific extension boards it is suitable for fire detection and fire alarm systems if the specific conditions for the application are considered. The defined development process of the software for modifications together with the proven in use consideration is in accordance with SIL 3 requirements.

The validation and testing activities have shown the compliances between the realised DeltaV SIS implementation and the safety requirements specification.

The actual version of the Safety Manual [M13] must be considered for the use in safety relevant applications.