D800027X022
December 2008

DeltaV™ Safety Instrumented System

Safety Manual

DeltaV™

EMERSON™
Process Management

EMERSON™
Process Management

Printed in UK

The contents of this publication are presented for informational purposes only, and while every effort has been made to ensure their accuracy, they are not to be construed as warranties or guarantees, expressed or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the design or specification of such products at any time without notice.

Contents

1 DeltaV SIS Safety Manual

This document contains important information on how DeltaV SIS is to be used in a safety instrumented system to place and/or maintain the equipment under control in an appropriate state when expected to do so. The guidelines in this document must be followed when using DeltaV SIS in a safety-critical application.

To determine whether this document is the most recent revision applicable to a particular revision of the SLS1508, compare the part number shown on the cover of this document to the part numbers shown at the following website:

http://www.EasyDeltaV.com/SISSafetyManual/

1.1 Certification

The information in this document applies to the following hardware and software components of DeltaV SIS.

Safety Rated	SLS1508 hardware module revision 4.xx SLS1508 firmware revision 1.xx.xx.xx cr SLS1508 firmware revision 2.xx.xx.xx cr Secure Write workstation software DvSwSever.exe DvSwCommandMsgV1.dll DvSwServerHelper.dll ValidateExemem.dll
Safety Relevant	SISNet Repeater hardware module SISNet Repeater firmware SLS1508 simplex termination block SLS1508 redundant termination block DeltaV MD Controller hardware DeltaV MD Controller firmware DeltaV Explorer DeltaV Control Studio in SIS module context
Interference-Free	All other DeltaV hardware, firmware, and software components not listed above

TÜV has certified the SLS1508 hardware and firmware as suitable for use in applications with a maximum Safety Integrity Level of 3 (SIL3) according to IEC 61508. The SIL3 certification applies to both simplex and redundant SLS1508s. Redundancy increases availability, but does not increase safety. Both simplex and redundant SLS1508s provide the hardware fault tolerance and safe failure fraction to meet SIL3 architectural requirements. In order for your application to satisfy a SIL3 requirement, the probability of dangerous failure for the given safety instrumented function must be in the SIL3 range.

The SLS1508 is certified for use in both the low demand and high demand mode of operation as defined by IEC 61508.

Refer to "Product Specifications (Appendix A)" for failure rate and other data to help you verify that your safety requirements are being met and for additional considerations for using the SLS1508 in high demand mode.

1.2 Management of Functional Safety

DeltaV SIS is intended to be used in accordance with a defined safety lifecycle such as that described in IEC 61511. Emerson Process Management recommends the following additional functional safety management requirements.

Competence of Persons - Engineering

All persons involved in the initial implementation or modification of the application software should have appropriate training. Opportunities for training include reading this manual, reading DeltaV Books Online, and attending a training class taught by Emerson Process Management-certified personnel. Formal training is available through Emerson Process Management Educational Services. For information, visit

http://www.emersonprocess.com/education/contacts_centers.asp

Competence of Persons - Installation and Hardware Maintenance

All persons involved in installation and hardware maintenance activities should have appropriate training. Opportunities for training include reading this manual, reading *Installing Your DeltaV Safety Instrumented System Hardware*, reading DeltaV Books Online, and attending a training class taught by Emerson Process Management-certified personnel. Formal training is available through Emerson Process Management Educational Services.

Competence of Persons - General

All persons involved in any aspect of DeltaV SIS use, including engineers, operators, supervisors, maintenance personnel, and system administrators, should have training in the importance of safety instrumented systems. All persons should have specific training in the procedures for which they are responsible. DeltaV system administrators must ensure that all individuals having security keys for DeltaV SIS activities are trained and competent.

For technical support contact information and for reporting product issues, visit:

http://www.emersonprocess.com/systems/support/ratecard.htm

Refer to “Fault Detection, System Response, and Repair Procedures” in Appendix D for more information on reporting product issues.

1.3 Restrictions

The practices required in the use of DeltaV SIS are summarized below. Each topic is discussed in greater detail in “Required Practices (Appendix B).”

- You must complete a full functional test of the SLS1508 configuration before the SLS1508 is allowed to provide the protection function in a running process.

  After a subsequent download and prior to the SLS1508 continuing to provide its protection function unsupervised, you must assess what has changed in the SLS1508 since the last functional test by examining the CRC values in DeltaV Diagnostics Explorer. Any SIS module or I/O channel that indicates a change must be revalidated, that is, a functional test must be completed.

  You are allowed to download an SLS1508 while it is providing the protection function in a running process, under the following conditions:

  1. The equipment under control of the SLS1508 must be supervised during the download and until completion of the functional test (or until it is determined that a functional test is not required).
  2. The shortest process safety time associated with the SLS1508 must be long enough for operators to monitor and react, and thus manually provide the protection function during the download and functional test.

- The SLS1508 is designed for a deenergized to trip operation such that the tripped state for the process is achieved when SLS1508 output channels are deenergized. The SLS1508 can be used in fire and gas and other normally deenergized applications provided special installation and configuration guidelines are followed. Refer to “Required Practices (Appendix B)” for more information.
- The use of HART Two-state Output channels on the SLS1508 is intended for certain final elements. You should physically connect a channel of this type to only a Fisher Controls DVC6000 digital valve controller with ESD tier (firmware revision 6 or later) or to a digital valve controller certified by Emerson Process Management as being equivalent. Appendix B has more information on using digital valve controllers with the SLS1508. For the current list of digital valve

controllers certified for use with HART Two-state Output channels on the SLS1508, visit:

http://www.EasyDeltaV.com/SISSafetyManual/

- The Non-Secure Parameter Reference is a user-defined parameter type available in SIS modules for non-safety-critical use. If a parameter of this type contributes to a safety-critical control action, special consideration is required in SIS module logic to validate the parameter value. The application programmer must not allow the safety function to be compromised based on the value of a Non-Secure Parameter Reference. Refer to “Required Practices (Appendix B)” for more information.

1.4 Engineering Practices

Other than the Non-Secure Parameter Reference, all configuration elements available in SIS modules may be used without special consideration in a safety-critical application, up to and including SIL3. This includes the Calculation-Logic function block expression language, which is a limited variability language.

Other than using the Non-Secure Parameter Reference, the SIS module environment prevents you from doing anything that is not allowed. For example, the SIS module prevents direct access to HART digital variables. However, you are permitted to access HART digital variables on SLS1508 channels using a Non-Secure Parameter Reference. HART diagnostic data can be brought into an SIS module by choosing options in the HART_ERRORS parameter on SLS1508 HART channels. You can select which HART error conditions in the device cause Bad status to be integrated with the analog value on the channel.

The configurer of SIS module logic has influence over the SLS1508's response to certain faults detected in the SLS1508 and field instruments. The SLS1508 automatically responds to faults common to all I/O channels, such as a malfunction of a processor or a memory failure, by deenergizing all output channels. This leaves output devices under control of the partner when using redundant SLS1508s. For faults specific to one I/O channel or one field device, the SLS1508 integrates Bad status with the value on the channel.

The SIS module must be configured to respond to Bad status as required by the application. Such configuration is straightforward. The SLS1508 propagates the status of I/O channels and function block input and output parameters in a predetermined way. Configuring the system response to Bad status is a matter of choosing status options, fault state options, and certain time duration values as the application requires. Note that a fault on an output channel does not prevent deenergization in the case of a demand to trip on that channel. There is an automatic, secondary means of deenergization when needed.

Refer to “Engineering Practices (Appendix C)” for more information on configuring the system response to detected faults and additional topics. For detail on fault detection and how the SLS1508 and DeltaV SIS responds to those faults refer to “Operations and Maintenance Practices (Appendix D)”. The DeltaV SIS book in DeltaV Books Online has detailed information on the features of the function blocks available in SIS modules.

1.5 Operations and Maintenance Practices

DeltaV SIS has a built-in bypass facility for managing maintenance overrides. A bypass allows a maintenance activity such as calibration, proof testing, or repair of a transmitter or other sensor to take place without a concern for a spurious trip. Bypasses in SIS module logic in the SLS1508 can be set and cleared from DeltaV workstations using a secure write operation, which is part of the TÜV Type Approval. No special consideration is required for communications between DeltaV workstations and the SLS1508. Refer to “Operations and Maintenance Practices (Appendix D)” for additional information on the DeltaV SIS bypass facility.

The DeltaV SIS secure write server is used for runtime changes to parameters in the SLS1508 made from DeltaV workstations, including maintenance bypasses, operator resets, and all other parameters that are allowed to be changed at runtime. DeltaV SIS prevents runtime parameter changes in the SLS1508 from succeeding if the secure write server has not been utilized. DeltaV Operate contains a secure data entry expert to configure interfaces for writing parameter values at runtime using the secure write server. The secure write capability is integrated with DeltaV Operate dynamos and faceplates for the advanced SIS function blocks and in DeltaV Control Studio Online/Debug for SIS modules.

A secure write is a two-step procedure. A person initiates the write from a DeltaV workstation by entering data or clicking on a display element. Then a confirmation dialog displays the data to be written. When the person has confirmed the entered value, a packet with the original and confirmed data is sent to the SLS1508. The write succeeds if the SLS1508 validates the original, confirmed information as being the same and if the destination is correct.

Note *It is not necessary to do a functional test after a secure write. You can be certain that the parameter value in the SLS1508 is the value confirmed.*

The secure write operation is in addition to DeltaV security. The user who is logged in at the DeltaV workstation must have the software key to the lock associated with the writable parameter and parameter field. The SIS module's plant area must be assigned to the workstation.

You must conduct a periodic proof test of each SLS1508 to reveal potential dangerous faults not detected by continuous runtime diagnostics in the SLS1508. The necessary frequency of the proof test is a function of the required probability of dangerous failure for the safety instrumented function(s) associated with the SLS1508. The proof test is conducted by forcing the SLS1508 to go through reset and power-up testing. This is initiated by using a context menu command from DeltaV Diagnostics Explorer and has no adverse impact on a running process when redundant SLS1508s are used.

An automatic proof test is optional for redundant SLS1508s based on a configured proof test interval. There are no known dangerous undetected faults present immediately following successful power-up testing. Therefore a 99.9% proof test coverage factor is conservative and can be justified.

Refer to "Operations and Maintenance Practices (Appendix D)" for more information on proof testing. Appendix D also contains additional topics on recommended operations and maintenance practices for DeltaV SIS.

2 Product Specifications (Appendix A)

2.1 Failure Rate Data for SIL Verification

In order to verify that a safety instrumented function (SIF) meets the required safety integrity level (SIL) you must determine the probability of the SIF failing dangerously. The tables in this section contain failure rate data for estimating the probability of the logic solver subsystem of the SIF failing dangerously. Third party tools are available for estimating the probability of failure associated with the SLS1508. For more information, refer to:

http://www.EasyDeltaV.com/SISSafetyManual/

Low Demand Mode of Operation

In the low demand mode of operation the proof test frequency is at least twice the expected demand rate. Stated another way, the periodic proof test occurs at regular intervals at least twice during the expected time between demands.

SIL verification for the low demand mode uses the average probability of failure on demand (PFDavg) for the SIF. You can use the failure rate data in Tables 2-1 and 2-2 to estimate the PFDavg for the SLS1508 subsystem of the SIF.

Table 2-1 is a worksheet to estimate the total dangerous undetected (DU) failure rate of the SLS1508 subsystem of the SIF. The DU failure rate is a function of the number of SLS1508s involved in the SIF. It is not a function of the number of I/O channels in the SIF. There is no assignable DU failure rate for the I/O circuitry of the SLS1508.

Table 2-2 estimates the total dangerous detected (DD) failure rate of the SLS1508 subsystem of the SIF. The SLS1508 reacts to dangerous detected (DD) failures by deenergizing outputs. The exception is the presence of potentially dangerous failures detected on input channels, where the configurer of SIS module logic determines the SLS1508's response. Input channel circuitry in the SLS1508 has a DD failure rate whose impact on PFDavg must be considered.

Table 2-1 Instructions

- Enter the number of SLS1508s that drive output channels in this SIF. Typically there is one SLS1508, either simplex or redundant, used to drive the output channel or channels.
- If there are input channels in this SIF wired to a different SLS1508 than the one driving the outputs, enter the number of additional SLS1508s whether simplex or redundant.
- Multiply the number of SLS1508s by the DU failure rate (failures per hour) and enter the result. Sum the results to get the total DU failure rate.

Table 2-1 Worksheet for Approximating the SLS1508 DU Failure Rate for a SIF

Number of simplex SLS1508s driving output channels in this SIF.		X	6.0E-9 (6 FITs)	=	
Number of redundant SLS1508s driving output channels in this SIF.		X	1.2E-8 (12 FITs)	=	
Number of SLS1508s other than those driving output channels in this SIF.		X	6.0E-9 (6 FITs)	=	
Total DU failure rate (failures per hour)					

Table 2-2 Instructions

Enter the number of input channels in this SIF. Then multiply the number of channels by the DD failure rate (failures per hour) and enter the result. Sum the results to get the total DD failure rate.

Table 2-2 Worksheet for Approximating the SLS1508 DU Failure Rate for a SIF

Number of Analog Input + HART Analog Input channels in this SIF.		X	2.6E-8 (26 FITs)	=	
Number of Discrete Input channels in this SIF.		X	1.6E-8 (16 FITs)	=	
Total DD failure rate (failures per hour)					

You can approximate the PFDavg of the logic solver subsystem using the total failure rates in Tables 2-1 and 2-2, a common proof test period for the SLS1508s in the SIF, and your maximum allowed repair time.

$$\text{PFDavg (LS)} = \lambda_{DU} * T / 2 + \lambda_{DD} * RT$$

where:

λ_{DU} = Total DU failure rate from Table 2-1

T = Proof test period in hours

λ_{DD} = Total DD failure rate from Table 2-2

RT = Allowed repair time in hours

Determine the PFDavg for the SIF by summing the PFDavg for the logic solver subsystem with the PFDavg for the sensor and final element subsystems.

High Demand Mode of Operation

In the high demand mode the periodic proof test does not occur at least twice during the expected demand interval, but the demand interval is sufficiently longer than the fault detection and reaction time. SIL verification for the high demand mode uses the probability of dangerous failure per hour (PFH).

There are several additional considerations when operating in the high demand mode. Generally it is easy to avoid operating in high demand mode by reducing the proof test interval on the SLS1508. But if there is a practical constraint in the proof testing frequency of another subsystem of the SIF that causes the SIF to operate in the high demand mode, the additional considerations of high demand mode apply to the SLS1508 too.

Consider the following before operating in high demand mode.

- The expected demand interval must be at least an order of magnitude longer than the maximum time required for the SLS1508 to detect a dangerous failure and deenergize outputs. This requirement precludes operating in the continuous demand mode as defined by IEC 61508. Refer to “Response Time Data” in this appendix and “Maximum Fault Detection Time” in Appendix D for more information.
- The allowed repair time for failures detected on input channels must be restricted by SIS module configuration so that the SLS1508 deenergizes applicable outputs if the repair cannot be completed in time. There are two factors for determining the maximum time allowed for a repair.

1. The expected demand interval must still be an order of magnitude longer than the sum of the allowed repair time and maximum fault detection/ reaction time.

2. The process safety time must still be longer than the sum of the allowed repair time and the maximum response time for all subsystems of the SIF.

Refer to "Configuring the SLS1508 Response to Detected Faults" in Appendix C for more information.

If you allow no repair time for DD failures on input channels, the PFH for the SLS1508 subsystem of the SIF is the total DU failure rate from Table 2-1.

$$\text{PFH (LS)} = \lambda_{DU}$$

If you allow time to repair DD failures on input channels, the PFH for the SLS1508 subsystem uses the failure rates from both tables, the allowed repair time, and the expected demand interval.

$$\text{PFH (LS)} = \lambda_{DU} + \lambda_{DD} * \text{RT} / \text{DI}$$

where:

λ_{DU} =	Total DU failure rate from Table 2-1
λ_{DD} =	Total DD failure rate from Table 2-2
RT =	Allowed repair time in hours
DI =	Expected demand interval in hours

Determine the PFH for the SIF by summing the PFH for the logic solver subsystem with the PFH for the sensor and final element subsystems.

2.2 Common Cause Failures

The common cause factor, Beta, is the fraction of failures that can impact both SLS1508s of a redundant pair. Both SLS1508s of a redundant pair must succeed in deenergizing outputs when a demand to trip occurs. A dangerous undetected failure results in a system failure for the pair whether the dangerous undetected failure occurs in one or both SLS1508s. Therefore, with respect to dangerous undetected failures, Beta can be assumed to be 0 for approximate probability of failure calculations.

2.3 Failure Rate Data for Availability

The mean time to failure spurious (MTTFS) is a measure of the time between failures that result in a process shutdown. It takes into account safe failures that can cause outputs to deenergize and the dangerous detected failures that cause the SLS1508 to deenergize its outputs.

MTTFS	
Simplex SLS1508	33 years
Redundant SLS1508	>3000 years

Not all safe failures in the SLS1508 result in a process shutdown. A safe failure on an analog input channel will not necessarily cause a trip (if it is part of a 2oo3 voting arrangement, for example), whereas a detected dangerous failure of a CPU will always result in a reset of the SLS1508 and a process shutdown on a simplex SLS1508.

MTTFS for a SIF is a function of the number and type of channels and the number of SLS1508s involved. You can estimate MTTFS for a SIF by dividing the number of years by the number of SLS1508s involved in the SIF.

2.4 Response Time Data

The response time for a SIF must be less than the process safety time. The SIF has a response time associated with the sensor, logic solver, and final element subsystems. The sum of the response times must be less than the process safety time. The response time of the logic solver subsystem is the time between any change on a SIF input channel that should result in a trip and the time that the output channel or channels change to the tripped state. The time is measured from screw terminal to screw terminal.

The response time is impacted by the configured scan rate of the SLS1508 containing SIS module logic for the SIF and by whether there is a fault present in the SLS1508. There is some variability due to the alignment of the change at the input screw terminal and I/O scanning in the SLS1508. Table 2-3 shows the maximum response times.

Table 2-3 Maximum SLS1508 Response Time with No Faults Present

SLS1508 Scan Rate (milliseconds)	Maximum Response Time with no Faults Present (milliseconds)
50	175
100	275
150	375
200	475

Although the probability of an undetected fault being present at the time of a demand is extremely low, you should assume a fault may be present when allocating the response time for the logic solver subsystem. At the time of demand a fault such as a stuck On output channel delays the trip by the amount of time it takes the SLS1508 to determine that the channel did not go Off and to initiate a reset to remove power. The maximum fault detection/reaction time for any scan rate is 400 milliseconds. Therefore you should allocate 575 milliseconds for the logic solver subsystem response time for an SLS1508 whose scan rate is 50 milliseconds.

Note the following concerning response times for the logic solver subsystem.

1. The response time does not increase if an input channel of the SIF is on an SLS1508 other than the SLS1508 that is driving outputs.
2. If there are multiple SIS modules involved in the SIF with communication using secure parameters, the maximum response time increases by the scan rate of the SLS1508 containing the secure parameter (not the secure parameter reference). For example, two SIS modules at a 50-millisecond scan rate increases the maximum response time from 175 to 225 milliseconds.
3. If SIS module logic includes delays such as the trip delay time in voter function blocks, the response time increases by the length of those delays.

2.5 Limits

2.5.1 Product Life

The lifetime limit of the SLS1508 is 20 years based on the worst case component wear-out.

2.5.2 Environmental Conditions

Refer to *Installing Your DeltaV Safety Instrumented System Hardware* for limits on environmental conditions.

2.5.3 Application Limits

Application limits are imposed by the DeltaV Engineering Tools applications. Special consideration is not required to prevent limits from being exceeded. Refer to “System Capacities” in the Configuration book of DeltaV Books Online for the SIS application limits.

3 Required Practices (Appendix B)

This section contains additional information on required practices as they relate to restrictions in the use of DeltaV SIS.

3.1 Installation and Site Acceptance Testing

Installation of a DeltaV SIS system must conform to guidelines in *Installing Your DeltaV Safety Instrumented System Hardware.*

Your site acceptance procedures should include functional testing of the application programs running in SLS1508s. Section 3.2 contains requirements related to downloading and testing the SLS1508.

3.2 Managing Changes in the DeltaV SIS Runtime System

You can make a change to the DeltaV SIS runtime system by doing either of the following:

- Downloading the application program from the ProfessionalPLUS configuration database to an SLS1508
- Changing a parameter value in the SLS1508 using a secure write operation from DeltaV Operate or Control Studio Online/Debug

An SLS1508 download differs from a runtime parameter change from a management of change perspective. You are required to perform a functional test after a download. Parameter values can be changed in the SLS1508 only through a secure write operation, which is self-validating.

3.2.1 Downloading the SLS1508

DeltaV SIS provides a convenient way to determine what changes have been made to the runtime system as a result of an SLS1508 download, and thus, what subset of the logic in the SLS1508 must be revalidated, that is, functionally tested, after the download.

Downloading of an SLS1508 is always a user-initiated event. After the initial download, a subsequent download is generally not necessary unless you have made changes to the configuration database applicable to the SLS1508. An SLS1508 also needs a subsequent download if it loses power for more than 10 days or it has been removed from the carrier. Loss of power for less than 10 days results in an initializing reload of the application program from within the SLS1508 when power is restored to it.

3.2.1.1 Functional Testing After the Initial Download

Warning You must complete a full functional test of the SLS1508 configuration before the SLS1508 is allowed to provide the protection function in a running process.

After an initial download of an SLS1508 you must ensure that all the output channels respond appropriately as you manipulate the value of input channels on that SLS1508 (and other SLS1508s, if applicable). This initial test must be a screw terminal to screw terminal test, preferably from sensor to final element.

The functional test in the SLS1508 is required even if the SLS1508 logic has already been tested using Control Studio Online/Debug while the SLS1508 configuration is assigned to the ProfessionalPLUS workstation.

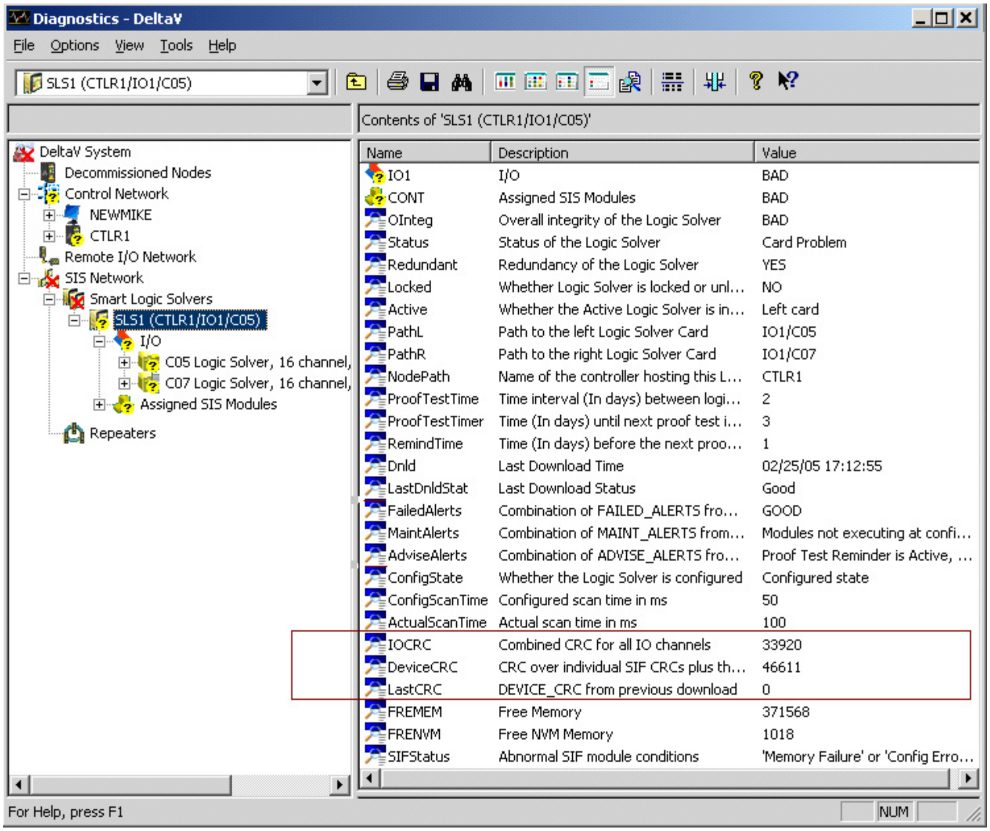
3.2.1.2 Recording CRC Values

The SLS1508 calculates a number of Cyclic Redundancy Check (CRC) values as it processes a download script. The CRC values are visible in Diagnostics Explorer and are useful for verifying whether subsequent downloads produce logic in the SLS1508 identical to what had been running. A different CRC value for a given SIS module or I/O channel after a download indicates that there is some difference in what is now running in the SLS1508. The CRC value calculated by the SLS1508 accurately reflects what is running in the SLS1508 when the download script is applied. Diagnostics Explorer shows the CRC values calculated by the SLS1508, which include:

- An overall CRC for the device (DeviceCRC)
- A CRC for each SIS module (CRC)
- A combined CRC for all the I/O channels (IOCRC)
- A CRC for each individual I/O channel (CH_CRC)
- The overall device CRC from the previous download (LastCRC)

Note *Whenever you perform a functional test of the logic in an SLS1508, document the applicable CRC values along with the test results as part of your safety lifecycle management procedures.*

Figure 3-1 is an example of the Diagnostics Explorer showing the diagnostic parameters of the SLS container with the CRC values highlighted.



Name	Description	Value
IO1	I/O	BAD
CONT	Assigned SIS Modules	BAD
OInteg	Overall integrity of the Logic Solver	BAD
Status	Status of the Logic Solver	Card Problem
Redundant	Redundancy of the Logic Solver	YES
Locked	Whether Logic Solver is locked or unl...	NO
Active	Whether the Active Logic Solver is in...	Left card
PathL	Path to the left Logic Solver Card	IO1/C05
PathR	Path to the right Logic Solver Card	IO1/C07
NodePath	Name of the controller hosting this L...	CTLR1
ProofTestTime	Time interval (In days) between logi...	2
ProofTestTimer	Time (In days) until next proof test i...	3
RemindTime	Time (In days) before the next proo...	1
Dnld	Last Download Time	02/25/05 17:12:55
LastDnldStat	Last Download Status	Good
FailedAlerts	Combination of FAILED_ALERTS fro...	GOOD
MaintAlerts	Combination of MAINT_ALERTS from...	Modules not executing at confi...
AdviseAlerts	Combination of ADVISE_ALERTS fro...	Proof Test Reminder is Active, ...
ConfigState	Whether the Logic Solver is configured	Configured state
ConfigScanTime	Configured scan time in ms	50
ActualScanTime	Actual scan time in ms	100
IOCRC	Combined CRC for all IO channels	33920
DeviceCRC	CRC over individual SIF CRCs plus th...	46611
LastCRC	DEVICE_CRC from previous download	0
FREMEM	Free Memory	371568
FRENVM	Free NVM Memory	1018
SIFStatus	Abnormal SIF module conditions	'Memory Failure' or 'Config Erro...

Figure 3-1 Diagnostics Explorer Showing SLS CRC Values

3.2.2 Subsequent Downloads

After the initial download, an SLS1508 requires a subsequent download when there have been configuration changes made to it and the time is appropriate to apply the changes. When an SLS1508 is downloaded, it receives a complete download script, not a partial script of the changes that have been made. The SLS1508 processes the script and replaces the entire running configuration after copying certain parameter information where possible, so that non-disruptive online changes occur (see “Downloading to a Running Process” in this section).

Warning After a subsequent download and prior to the SLS1508 continuing to provide its protection function, you must assess what has changed in the SLS1508 since the last functional test by examining the CRC values in Diagnostics Explorer. Any SIS module or I/O channel that indicates a change must be revalidated.

If the overall CRC value for the SLS1508 matches the value from the previous download, you can be certain the identical configuration is running in the SLS1508 after the download. However, the overall CRC must have the same value as your documented, last-tested overall CRC or some functional testing is required. Compare the overall CRC with your documented last-tested value. If they differ, check for differences between the current CRC value for each of the four potential SIS modules and your documented last-tested value for each SIS module. Also check for differences between the combined I/O CRC value and your documented, last-tested combined I/O CRC value.

Caution Whenever you download an SLS1508, compare the newly calculated overall CRC value with your documented last-tested value even if you do not anticipate a difference.

Any SIS module whose CRC value differs from the last-tested value must have a functional test done before it can provide its protection function in a running process. Unless the download is being done online, that is, while the process is running, your standard test procedure for that SIS module should be followed. For modifications to the standard test procedure following an online download, see “Functional Testing After Download to a Running Process” in this section.

If the combined I/O CRC value differs from your documented last-tested value, examine each of the 16 individual channel CRC values to see which differ from the documented last-tested value. Any difference implies a change in a configurable I/O channel parameter value. For channels whose CRC value has changed, perform tests according to Table 3-1 based on the channel type.

Table 3-1 When to Test Channel Parameters when the CRC Value Changes After a Download

Channel type	Configurable parameter	When to test…
Analog Input	NAMUR_ENA	Test if configured as True.
	OVERRANGE_PCT UNDERRANGE_PCT	Test channel if referenced by an Analog Input function block (in this or another SLS1508) with the "Bad if Limited" bit set in STATUS_OPTS.
HART Analog Input	NAMUR_ENA OVERRANGE_PCT UNDERRANGE_PCT	Same as Analog Input channel.
	HART_ERRORS DISPARITY_DETECT	Not required; HART communication is not safety-critical.
Discrete Input	LINEFAULT_DETECT	Test if configured as True.
Discrete Output	LINEFAULT_DETECT	Test if configured as True.
HART Two-state Output	DISPARITY_DETECT DV_SLOTn_CODE DV_SLOT_CONFIG	Not required; HART communication is not safety-critical.

3.2.2.1 Downloading to a Running Process

The need to make configuration changes to an SLS1508 after it is protecting a running process should be infrequent, and the need to download those changes prior to the next scheduled outage should be even less frequent.

Warning You are allowed to download an SLS1508 while it is providing the protection function in a running process, with the following restrictions:

1. The equipment under control of the SLS1508 must be supervised during the download and until completion of the functional test (or until it is determined that a functional test is not required).

2. The shortest process safety time associated with the SLS1508 must be long enough to allow time for operators to monitor and react, and thus manually provide the protection function during the download and functional test.

Some changes require a download to the SLS1508 to take effect. Other changes can be made using a secure write operation so that functional testing can be avoided. There are certain changes that require an SLS1508 download, but do not result in a change to the overall CRC value in the SLS1508 after the download completes. Table 3-2 lists various changes that can be made, what is required to apply the change to the runtime system, and the impact to the SLS1508 overall CRC value.

Table 3-2 How to Apply SLS1508 Configuration Changes to the Runtime System

Change Made to the Configuration Database	How to Apply the Change to the Runtime System and the Resulting Impact to the SLS1508
• Add/delete a function block. • Add/delete a user-defined parameter or change its definition. • Add/delete a wire. • Change a configurable but not runtime-writable SIS module parameter value. • Change a configurable I/O channel parameter value. • Change an SLS1508 scan rate or global publishing property.	Requires an SLS1508 download to take effect. Changes the SLS1508 CRC value.
• Change an SLS1508 property other than scan rate or global publishing. • Change an SIS module property. • Change a HART device property.	Requires an SLS1508 download to take effect, but *does not* change the SLS1508 CRC value.
• Change a runtime-writable SIS module parameter value.	Can be changed by a secure write or a download; if changed by a download, changes the SLS1508 CRC value, but not if changed by a secure write. Changes the SLS1508 CRC value on the next download if changed using a secure write, then uploaded.
• Change a configurable field of an alarm parameter (ENAB, PRI, INV, SUPTMO). • Change the value of a function block parameter with a STRING data type.	Can be changed using a write or a download; *does not* change the SLS1508 CRC value in either case.
• Change a parameter filter flag or category.	Requires neither a download nor a secure write to take effect. Applies only to the configuration system.

Any successful download performed on an SLS1508 replaces the application program running in the SLS1508. If the desired change can be applied using a secure write to an SIS module parameter instead of doing a download, it is preferable to make the change using the secure write in order to avoid having to do a functional test while the process is running.

Keep in mind that after uploading the parameter change to the configuration database, a subsequent download results in a change to the overall SLS1508 CRC value. There is no requirement to do a subsequent download as a result of a runtime parameter change. However, if the runtime change is uploaded, the next time a download is done a functional test is required even if there were no other changes made to the configuration database.

3.2.2.2 Functional Testing After Download to a Running Process

You may modify your standard test procedure when the process is running to reduce the likelihood of the test causing a process disruption. You can use Control Studio Debug and the Force Value function to isolate sections of logic. The logic within an SIS module can be tested in this way by observing parameter values without manipulating the I/O at the screw terminals. However, at some point during the test you must validate that I/O function blocks are properly linked with the screw terminals and that secure parameter references are properly linked with their referenced secure parameters. Suggested test procedures are described in Table 3-3.

Table 3-3 Suggested Test Procedures After Download to a Running Process

Item	Test Procedure for "Properly Linked"
Discrete Input channel	1. If value of OUT_D of DI function block is 1, do a "force value" on the destination of wire from OUT_D. 2. Disconnect physical wire on input channel. Confirm value of OUT_D goes to 0. 3. Restore. **Note 1:** For energize to trip applications or when the "Invert Input" IO option is used, it may be necessary to manipulate the input channel to confirm the link. **Note 2:** Repeat for all DI function blocks in all SIS modules in this SLS1508, whether the physical channel is on this or another SLS1508.
Analog Input channel HART Analog Input channel	1. Measure the current at the input screw terminals. 2. Calculate the expected value on OUT of the AI function block using the value of L_TYPE and OUT_SCALE. 3. Confirm that the expected value matches the value of OUT. **Note 1:** Repeat for all AI function blocks in all SIS modules in this SLS1508, whether the physical channel is on this or another SLS1508. **Note 2:** If the value on OUT is the same for multiple AI blocks, it is necessary to manipulate one or more input channels to confirm the links.
Secure Parameter Reference	1. Do a "force value" on the destination of wire from the parameter. 2. Using Control Studio Debug for the source SIS module, do a "force value" on the referenced secure parameter. 3. Change the value on the secure parameter and confirm that the value changes in the destination module. 4. Restore.
Discrete Output channel HART Two-state Output channel	1. Open the process bypass valve for the final element. 2. Cause the value on CAS_IN_D of the DO/DVC function block to change state by manipulating the logic using "force value" or other means. 3. Visually verify that the final element changes state (or measure the voltage/current at the screw terminal). 4. Restore. **Note:** If there is no process bypass capability, it is acceptable to temporarily block the actuation of the final element. In either case you must be able to provide the protection function manually.

3.3 Using the SLS1508 in Fire & Gas and Normally Deenergized Applications

Warning You are permitted to use the SLS1508 in fire and gas and other normally deenergized (energize-to-actuate) applications by adhering to the following conditions.

1. Redundant SLS1508s must be used whenever output channels are being driven.

2. A separate, monitored power source is required for each SLS1508 card in redundant pairs driving output channels.

3. 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. The use of Two-state HART Output channels is not allowed in energize-to-actuate applications.

4. The configuration guidelines in this section must be followed.

5. Fire and gas applications must comply with local fire codes by following standards such as EN54 in Europe and NFPA72 in the United States.

The DTA-Inverting relay module is installed near the SLS1508 and is wired to both the Discrete Output channel and supplemental Discrete Input channel. The Diode module is installed near the final element and is wired to the DTA-Inverting relay module and final element. The DTA-Inverting relay module adds 30 milliseconds to the response time of the SIF. Refer to *Installing Your DeltaV Safety Instrumented System Hardware* for installation details.

A DTA-Inverting relay and Diode module pair provides the following functions.

- Inverts the output of the SLS1508 Discrete Output channel. When the Discrete Output channel is Off, the final element receives 24V power. When the Discrete Output channel is On, the final element does not receive 24V power.
- Delivers an output of up to 5 Amps continuous to the final element when the Discrete Output channel is Off.
- Provides feedback using the supplemental Discrete Input channel indicating whether the field wiring is connected to the 24V inputs of the DTA-Inverting relay module. When the Discrete Output channel is On and 24V power is not being supplied to the final element by the DTA-Inverting relay module, the feedback to the supplemental input channel indicates On (and vice versa).
- Provides line fault monitoring from the SLS1508 to the Diode module using the supplemental Discrete Input channel. When the Discrete Output channel is On and 24V power is not being supplied by the DTA-Inverting relay module, the field circuit has continuity through the Discrete Input channel for monitoring for both open and short circuits. When 24V power is being applied by the DTA-Inverting relay module, there is no line fault monitoring.

Table 3-4 provides a summary of the DTA-Inverting relay finctions.

Table 3-4 Summary of the DTA-Inverting Relay Function

Process State	SLS DO Channel	Relay Output	SLS DI Channel	Line Fault Detection?
Normal	On	Off	On	Yes
Tripped	Off	On	Off	No

The following configuration guidelines must be followed in normally deenergized applications.

- Discrete Input channels used for feedback from DTA-Inverting relay modules must have line fault detection enabled (LINEFAULT_DETECT = True).
- If the normal operating value on a Discrete Input channel used in the application is Off, the channel must have line fault detection enabled. This requires that end

of line resistors be installed according to *Installing Your DeltaV Safety Instrumented System Hardware*.

- Discrete Output channels should have line fault detection enabled.
- SIS module logic must use the same deenergize to trip approach used in normally energized applications.
  - For example, inputs to a Discrete Voter or CEM function block should be 1 for a normal operating condition and 0 for a process trip condition. If the normal operating value on a Discrete Input channel is Off, the Invert option should be selected in the IO_OPTS parameter of the Discrete Input function block.
  - The input to a Discrete Output function block should be 1 for a normal operating condition and 0 to drive the process to the tripped state or to mitigate the consequences of a hazard. The DTA-Inverting relay module inverts the output to the final element.
- SIS module logic should provide feedback for the state of the final element. This can come from the final element itself using a limit switch or auxiliary contacts. The feedback can also come from the supplemental Discrete Input channel from the DTA-Inverting relay module, which indicates whether power was routed to the Diode module. A suggested approach for using the feedback in the SIS module is to wire the OUT_D of the Discrete Input function block to RDBK_IN_D of the Discrete Output function block. Be sure to deselect the "Enable detection based on PV_D value" option in FSTATE_OPTS in the Discrete Output block for this application.

3.4 Using HART Two-State Output Channels and Digital Valve Controllers

Warning The use of HART Two-state Output channels on the SLS1508 is intended for certain final elements. You should physically connect a channel of this type to only a Fisher Controls DVC6000 digital valve controller with ESD tier (firmware revision 6 or later) or a digital valve controller certified by Emerson Process Management as being equivalent.

A HART Two-state Output channel is manipulated by SIS module logic through the use of a Digital Valve Controller (LSDVC) function block. The SLS1508 applies 20 milliamps on the channel when the block's OUT_D parameter is 1. The value of the OFF_CURRENT parameter in the DVC block determines the current applied when the value of OUT_D is 0. Options for OFF_CURRENT include "0 milliamps" and "4 milliamps." Table 3-5 summarizes the characteristics of the OFF_CURRENT options.

Table 3-5 Characteristics of the OFF_CURRENT Options

0 milliamps	4 milliamps
• Power is removed entirely from the digital valve controller when SIS module logic drives the channel Off. The digital valve controller places the final element in the tripped state.	• The digital valve controller places the final element in the tripped state when SIS module logic drives the channel Off. • HART communication with the digital valve controller continues while the final element is in the tripped state.

Note *If you choose "4 milliamps" as the off-current option for a HART Two-state Output channel, consider installing the digital valve controller (DVC6000ESD or equivalent) and valve/actuator in a four-wire arrangement.*

A four-wire arrangement uses two output channels on the SLS1508. A HART Two-state Output channel is connected to the DVC6000ESD. A Discrete Output channel is connected to a 24V solenoid valve installed in the pneumatic line between the DVC6000ESD and the valve actuator. Visit the following website:

http://www.EasyDeltaV.com/SISSafetyManual/

for a link to additional information on installing and using the Fisher Controls DVC6000ESD.

3.5 Using Non-Secure Parameter References in SIS Modules

The Non-Secure Parameter Reference is a user-defined parameter type available on the Special Items palette when an SIS module has been opened with Control Studio. This parameter type is used to read a parameter located in a different module, either an SIS or non-SIS module. Runtime communication involves the I/O bus between the DeltaV controller and the SLS1508, which is not safety rated. Reading a parameter in another SIS module using a non-secure reference uses I/O bus communication even if the SIS module is in the same SLS1508. It is preferable to use a Secure Parameter and Secure Parameter Reference to communicate between SIS modules because they use the safety-rated Peer bus and the update rate is at the SLS scan rate (the non-secure update rate is 1 second). However, secure parameter communication is done using the Boolean data type. For data types other than Boolean, a Non-Secure Parameter Reference can be more convenient if the use is not safety-critical.

3.5.1 Non-Safety-Critical Use

A Non-Secure Parameter Reference can be used without special consideration when the value does not contribute to a safety-critical control action.

Examples of non-safety-critical use include:

- Reading a HART digital variable from a control module for feedback only. By means of an external reference parameter a control module is able to access HART digital variables from HART devices connected to SLS1508 channels. The actual valve position feedback from a digital valve controller, for example, can be read into an SIS module using a Non-Secure Parameter Reference, then compared to a limit and wired to the RDBK_IN_D input of a DVC function block.
- Reading the commanded state for a motor or discrete valve from a control module, then applying a safety interlock and driving an output channel of the SLS1508. This use is not considered safety-critical because the safety interlock always overrides the value of the commanded state.

3.5.2 Safety-Critical Use

If a Non-Secure Parameter Reference contributes to a safety-critical control action, special consideration is required in SIS module logic to validate the parameter value. The configurer must not allow the safety function to be compromised based on the value of a Non-Secure Parameter Reference.

An example of safety-critical use is a batch safety application that reads the active phase or recipe in order to apply the appropriate trip limit(s) for the current state of the process. It is important to validate the value read into the SIS module by some independent means. An example of independent confirmation of the current process state is inferring the state by using process inputs from channels of this or other SLS1508s, or using operator input from a secure write operation to confirm the state. If the value of the Non-Secure Parameter Reference cannot be validated by an independent method, the most conservative trip limit values should be applied.

A Non-Secure Parameter Reference has a value and a status. Normally the status is that of the referenced parameter. If there is a communication issue between the DeltaV controller and the SLS1508, the status of the Non-Secure Parameter Reference becomes BadNoComm. If the source parameter has Bad status or the SLS1508 is not able to read its value, the Non-Secure Parameter Reference has Bad status. Therefore, SIS module logic should take appropriate action when the status is Bad if the use is safety-critical. Refer to "Using Bad Status in the SIS Module" in Appendix C for more information.

The Limit function block can be used downstream from a Non-Secure Parameter Reference to limit its value within a valid range. The block has an option parameter (LIMIT_OPT) that determines the output value when the input is outside the valid range. Choices include clamping the value at the limit, using the last value prior to limit violation, and using a configurable default value.

4 Engineering Practices (Appendix C)

4.1 Requiring a Reset Before Outputs Can Become Energized

The configurer of SIS module logic determines which conditions allow deenergized output channels of the SLS1508 to become energized. It is generally desirable to require an operator reset before the equipment under control is allowed to go from a shutdown or tripped state to the normal operating state. But in some cases the output channels should be allowed to change from deenergized to energized based on input channel values without operator intervention, for example, as soon as an interlock condition clears. DeltaV SIS function blocks provide an easy way to configure SIS module logic to either require or not require an operator reset before applicable output channels can become energized.

There are certain situations where a powered SLS1508 keeps output channels deenergized independent of SIS module logic. When the SLS1508 is going through power-up testing following a reset or restart, has detected a persistent fatal error, or is in an unconfigured state, output channels remain deenergized. Otherwise, SIS module logic determines the output channel state.

The recommended technique for requiring an operator reset is to use the Cause Effect Matrix (LSCEM) function block. It has a REQUIRE_RESETn parameter for each extensible EFFECTn output of the block. Each Effect output is wired to one or more output function blocks, which are bound to output channels. When REQUIRE_RESETn is True (the default value), the EFFECTn output cannot transition from 0 to 1 unless STATEn is “Ready to Reset” and RESETn has been changed to True, typically by a secure write from DeltaV Operate. When REQUIRE_RESETn is False, EFFECTn can transition from 0 to 1 when associated Cause inputs have become inactive and other permissives are satisfied, without a reset.

The “require reset” option is also available in the two output function blocks, but it should be used there only if there is no CEM block in upstream SIS module logic.

4.2 Configuring the SLS1508 Response to Detected Faults

4.2.1 Faults Detected on Input Channels

Faults detected by the SLS1508 on input channels can originate in field devices, field wiring, or in the SLS1508 input circuitry. The SLS1508 responds to faults detected on input channels by integrating Bad status with the channel value and annunciating the fault. Refer to “Operations and Maintenance Practices (Appendix D)” for more information on how faults are annunciated. The SLS1508 does not automatically deenergize output channels when faults are detected on input channels. SIS module logic must be configured to take action based on the requirements of the application. For example, you may want to prevent a trip from occurring in the presence of a fault on an input channel, or cause a trip immediately when a fault is detected, or initially prevent a trip yet cause a trip some time later if the fault persists. SIS function blocks contain parameters to facilitate the configuration of these options.

4.2.1.1 Getting Bad Status into the SIS Module

You have some control over how Bad status on input channels can get into SIS modules. Certain input channel parameters and function block parameters impact the detection of faults on input channels and whether Bad status becomes available to SIS module logic.

4.2.1.1.1 Analog Input Channels

An analog input channel always has Bad status when the measured current is outside the sensor failure limits, 0.78 mA (-20.12%) and 22.66 mA (116.6%). The limits can be exceeded due to faults in the transmitter, field wiring, or the SLS1508. You can cause the channel to have Bad status when the current reaches a value inside the sensor failure limits.

Changing the NAMUR_ENA channel parameter to True enables NAMUR limit detection, which results in Bad status being applied when the current is greater than 21.0 mA (106.25%) or less than 3.6 mA (-2.5%) for four consecutive seconds.

When the channel value exceeds the channel’s configured OVERRANGE_PCT or UNDERRANGE_PCT value, high-limited or low-limited status is applied to the channel. The STATUS_OPTS parameter in the Analog Input (LSAI) function block has a “Bad if Limited” option. When the AI block’s referenced input channel has high or low limited status, the block applies Bad status to its PV and OUT parameters if the option is selected.

The HART Analog Input channel's HART_ERRORS parameter allows you to select which HART diagnostic conditions detected in the HART transmitter or by the SLS1508 cause Bad status to be integrated with the analog value on the channel (the FIELD_VAL_PCT channel parameter). The default value of HART_ERRORS ignores all HART diagnostic errors, meaning the presence of an error condition does not cause Bad status on the channel. If you deselect "Ignore Field Device Malfunction," for example, the channel has Bad status if the transmitter reports a device malfunction, allowing this HART diagnostic to be integrated with your SIS module logic. "What's This" help on HART_ERRORS explains the various diagnostic conditions available.

4.2.1.1.2 Discrete Input Channels

Faults detected in discrete input circuitry by the SLS1508 result in Bad status on the channel. The SLS1508 detects open and short circuits in field wiring if line fault detection has been enabled on the channel using the LINEFAULT_DETECT parameter. When line fault detection is enabled, you must use a NAMUR sensor or install end of line resistors in series and parallel according to *Installing Your DeltaV Safety Instrumented System Hardware.* An open or short detected through line fault detection results in Bad status on the channel.

Line fault detection is required when the field switch is normally open, that is, when the channel is On to indicate a demand.

Line fault detection is recommended when the field switch is normally closed, that is, when the channel is Off to indicate a demand. If an open circuit occurs in the field wiring, it is a safe failure whether or not line fault detection has been enabled. But a short in the field can be a dangerous failure and be undetected, unless line fault detection is enabled, in which case the channel has Bad status.

4.2.1.2 Using Bad Status in the SIS Module

Two function blocks are available in SIS modules to manipulate output channels: the Discrete Output (LSDO) block and the Digital Valve Controller (LSDVC) block. Each has a CAS_IN_D input parameter whose value is the commanded state for the output channel, which is wired from upstream logic in the SIS module. When the status of CAS_IN_D changes to Bad, the block starts a timer whose value is stored in the FSTATE_TIMER parameter. If and when the timer reaches the configured FSTATE_TIME value, the block enters the fault state if the "Enable detection based on CAS_IN_D status" option is selected in FSTATE_OPTS. The block drives the output channel Off when it is in the fault state.

SIS function blocks have a predetermined way of propagating the status of input parameters to output parameters. Faults detected on input channels cause Bad status to reach output function blocks in SIS modules depending on the configuration of other function blocks in the SIS module. The configured value of FSTATE_TIME in output blocks determines how long status can be Bad before the output block initiates a trip. The default value is 300 seconds, which gives enough time for operators to bypass a Bad input and take corrective action before a trip is initiated. Use an appropriate value for FSTATE_TIME in each output function block. Some SIFs can tolerate a high number corresponding to your allowed repair time, while other SIFs may require a low number of just a few seconds.

Figure 4-1 illustrates the use of common SIS function blocks to create shutdown logic in an SIS module. The status on the output parameter of the input function blocks, LSAI and LSDI, is the status of the referenced input channel. The Analog Voter (LSAVTR) and Discrete Voter (LSDVTR) blocks propagate Bad status on input parameters selectively. For example, if a single input of a 1oo2 or 2oo3 voter block has Bad status, OUT_D continues to have Good status because there are enough good inputs for a real process demand to cause a trip. However, if a single input of a 1oo1 or 2oo2 voter block has Bad status, its OUT_D has Bad status. If a Cause input of a Cause Effect Matrix (LSCEM) block has Bad status, all Effect outputs associated with that input have Bad status.

AVTR, DVTR, and CEM function blocks have a configurable STATUS_OPT parameter, which impacts how the blocks determine the *value* of their output parameter(s) based on the status of their inputs. These blocks determine the *status* of their output parameter(s) by a fixed status propagation algorithm unique to the block and independent of the STATUS_OPT parameter. This assures that if Bad status is capable of preventing a process demand from causing a trip, Bad status propagates to the output function block(s). Refer to the function block documentation in the DeltaV SIS book in DeltaV Books Online for more detail on the impact of the STATUS_OPT parameter in these blocks.

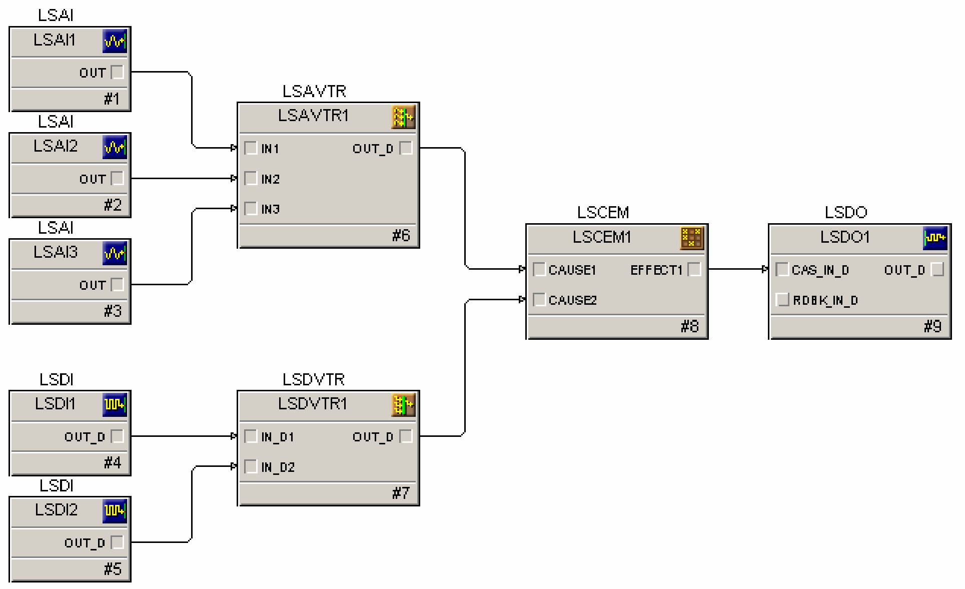


Figure 4-1 Example Use of SIS Function Blocks for a Shutdown Function

4.2.2 Faults Detected on Output Channels

Faults detected by the SLS1508 on output channels can originate in field devices, field wiring, or the SLS1508 output circuitry. As with input channels, the SLS1508 responds to faults on output channels by integrating Bad status with the channel value and annunciating the fault.

A fault on an output channel does not prevent the output from being deenergized should there be a demand to trip on that channel. Suppose a Discrete Output channel is stuck On due to a fault in the output circuitry. When SIS module logic detects a process demand to trip and the DO block drives the channel Off, power remains On as a result of the fault. However, the SLS1508 reads back the output as still being On and initiates a reset, which opens the master power switch and deenergizes all output channels on the SLS1508. When the LINEFAULT_DETECT parameter on Discrete Output channels is True (the default value), the SLS1508 detects and annunciates stuck On conditions by means of periodic pulse testing. In this way a failed unit can be replaced before a demand occurs, thereby avoiding a trip on all output channels. LINEFAULT_DETECT should remain configured as True unless the final element cannot tolerate the 1 millisecond Off pulse during each 50 millisecond period.

If the SLS1508 detects an open or short in field wiring or the output circuitry, it integrates a special status with the channel value called Bad SensorFailure LowLimited. Output function blocks detect this status on the referenced output channel and optionally drive the output channel Off. If the “Enable detection based on output channel status” option is set in the block’s FSTATE_OPTS parameter, the block enters the fault state and drives the channel Off immediately upon detection. The FSTATE_TIME value is not used in this case.

An open or short in field wiring implies the final element is in the deenergized state. Therefore the default value for the “Enable detection based on output channel status” option drives the channel Off when an open or short is detected. In order to keep the channel Off after it is driven Off, an operator reset must be required somewhere. The reset can be on the final element itself, in the output function block, or in the upstream CEM function block.

Figure 4-2 shows a recommended configuration technique.

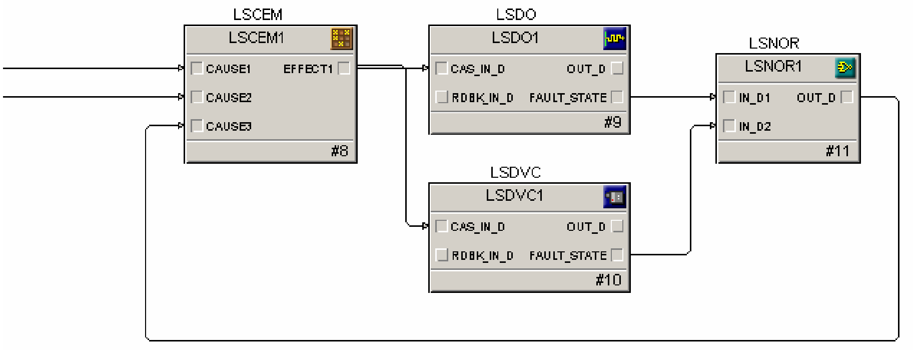


Figure 4-2 Example Use of a CEM Block for Latching Off an Output Fault

The CAUSE3 input of the CEM block has a value of 1 when neither output function block is in the fault state. FAULT_STATE is normally an internal parameter, but in this example it is exposed as an output parameter on the DO and DVC blocks and wired to a NOR block. If either output block detects an open or short on its referenced channel, a trip occurs on EFFECT1 of the CEM block and both output blocks drive their outputs Off (because CAS_IN_D becomes 0). The block that detected the open or short had already driven its output Off. The outputs remain Off until an operator reset is done on the Effect by changing RESET1 of the CEM block to True. The fault state condition clears when a Discrete Output channel is driven Off because the diagnostic no longer detects the condition. The same is true for a HART Two-state Output channel when OFF_CURRENT is “0 milliamps.”

This technique applies to the case where a coordinated trip of multiple final elements is required when any of the final elements involved in an interlock becomes deenergized due to an open or short. If you want to drive Off only the output with the open or short, use a separate CEM Effect output for each output block and wire FAULT_STATE into a separate Cause input.

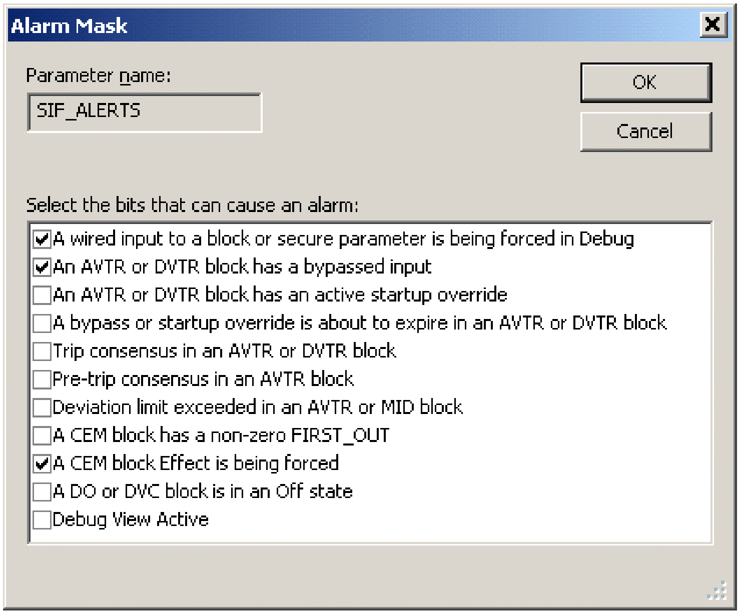
In some applications it may not be desirable to drive an output Off when an open or short is detected. For example, you may want the final element to become energized without operator intervention whenever an intermittent short clears. In this case de-select the “Enable detection based on output status” option in FSTATE_OPTS of the output block.

4.3 Using an SIS Module Template to Meet Operator Notification Requirements

DeltaV SIS allows you to create a new SIS module starting from an existing SIS module or SIS module template in addition to creating a new, empty SIS module. When creating SIS module logic, it is preferable to start with an SIS module template rather than an empty SIS module. DeltaV SIS provides one SIS module template named SIS_DEFAULT having an empty diagram view and two alarm parameters. Start from this template or one of your own so you do not have to manually create standard alarms in each SIS module.

The SIS_DEFAULT module template contains two alarms, BYPASS_ALM and IO_ALM. BYPASS_ALM references bits in the SIF_ALERTS parameter found in all SIS modules. IO_ALM references bits in the SIF_ERRORS parameter common to all SIS modules. SIF_ERRORS and SIF_ALERTS are bitstring parameters whose bits hold conditions detected in function blocks in the SIS module. When the alarm references a parameter whose parameter type is Option Bitstring, you select which bits cause the alarm to be active.

BYPASS_ALM references conditions in SIF_ALERTS shown by the selected check boxes in the dialog in Figure 4-3.



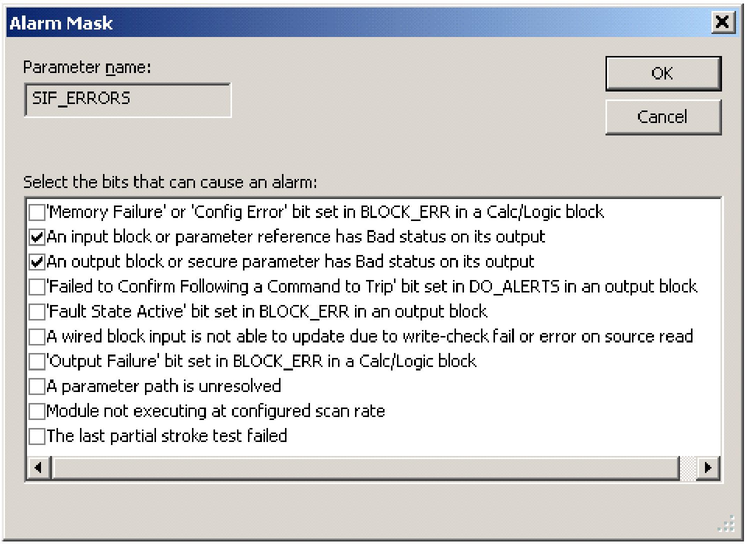
Parameter name: SIF_ALERTS

Select the bits that can cause an alarm:

- ☑ A wired input to a block or secure parameter is being forced in Debug
- ☑ An AVTR or DVTR block has a bypassed input
- □ An AVTR or DVTR block has an active startup override
- □ A bypass or startup override is about to expire in an AVTR or DVTR block
- □ Trip consensus in an AVTR or DVTR block
- □ Pre-trip consensus in an AVTR block
- □ Deviation limit exceeded in an AVTR or MID block
- □ A CEM block has a non-zero FIRST_OUT
- ☑ A CEM block Effect is being forced
- □ A DO or DVC block is in an Off state
- □ Debug View Active

Figure 4-3 SIF_ALERTS Mask for BYPASS_ALM

IO_ALM references conditions in SIF_ERRORS shown by the selected check boxes in the dialog in Figure 4-4.



Parameter name: SIF_ERRORS

Select the bits that can cause an alarm:

- □ 'Memory Failure' or 'Config Error' bit set in BLOCK_ERR in a Calc/Logic block
- ☑ An input block or parameter reference has Bad status on its output
- ☑ An output block or secure parameter has Bad status on its output
- □ 'Failed to Confirm Following a Command to Trip' bit set in DO_ALERTS in an output block
- □ 'Fault State Active' bit set in BLOCK_ERR in an output block
- □ A wired block input is not able to update due to write-check fail or error on source read
- □ 'Output Failure' bit set in BLOCK_ERR in a Calc/Logic block
- □ A parameter path is unresolved
- □ Module not executing at configured scan rate
- □ The last partial stroke test failed

Figure 4-4 SIF_ERRORS Mask for IO_ALM

Whichever SIS module template you use to create a new SIS module, make sure it contains the standard alarm parameters needed to meet your operator notification requirements. The alarms can reference SIF_ERRORS and SIF_ALERTS at the SIS module level or specific parameters in function blocks within the SIS module. SIF_ERRORS and SIF_ALERTS are recommended for standard alarms because they are not dependent on having particular function blocks on the diagram. It is a matter of preference whether to have more standard alarms that reference fewer conditions or fewer standard alarms that reference more conditions. You could choose to have an alarm parameter called ERROR_ALM, which references all bits in SIF_ERRORS. When ERROR_ALM becomes active, the operator can see which conditions are active on the generic faceplate for SIS modules in DeltaV Operate.

4.4 Choosing the SLS1508 Scan Rate

The default scan rate for SIS module execution in the SLS1508 is 50 milliseconds. You can change the scan rate to 100, 150, or 200 milliseconds from the SLS properties dialog in DeltaV Explorer. Increasing the SLS scan rate value impacts the execution rate of SIS modules. But diagnostic cycle times in the SLS1508 remain constant, with the exception of the main processor comparison diagnostic, which is a function of SIS module scan rate.

The recommended scan rate to use whenever possible is 50 milliseconds. This scan rate minimizes the input to output response time. The only reason to change the scan rate beyond the default 50 milliseconds is if the SLS1508 is not able to execute the SIS module or modules at the configured scan rate.

At download time the SLS1508 estimates the total execution time of the SIS modules. If the configured scan rate is not long enough for the estimated execution time, the SLS1508 sets the actual scan rate to the next higher value and sets a maintenance alert (a referenced condition in the standard SLS alarm MAINT_ALM), which indicates "Modules not executing at configured scan rate." This alert creates an audible alarm in DeltaV Operate. DeltaV Diagnostics Explorer shows this condition in the parameter MAINT_ALERTS at the SLS level. Diagnostics Explorer also shows the configured and actual scan rates in the CFG_SCAN_TIME and ACT_SCAN_TIME parameters at the SLS level.

When the configured and actual scan rates do not match, the SIS modules are still executing and providing the protection function. The response time is longer than had been expected based on the configured scan rate, and a persistent diagnostic error is present. For this reason you should change the configured scan rate and re-download the SLS1508 if a mismatch is indicated after a download.

If the total estimated SIS module execution time exceeds 200 milliseconds, the SLS1508 does not apply the downloaded script and the download fails.

4.5 Configuration Considerations for Online Downloads and Restarts

4.5.1 Online Downloads

If you anticipate a need to make online changes to SIS module logic, that is, to download SLS1508s that are protecting a running process, you should ensure the download does not disrupt the process. The SLS1508 copies certain state information and operating data from running SIS modules into newly downloaded SIS modules so that the download is nondisruptive. The parameters whose values are copied from the running module are said to have the "preserved on download" characteristic and are shown as such in parameter tables for SIS function blocks in the DeltaV SIS book in DeltaV Books Online.

When you create top-level parameters in SIS modules or SIS composite blocks, you select on the properties dialog whether or not the parameter is to be preserved on a download. If there is a chance you will make online downloads, you should test the behavior following a download by simulating normal operating conditions. If you discover an issue, the first step is to see if a top-level parameter needs to be preserved on download. If the issue persists, consider the use of the SYSSTAT function in a Calc/Logic function block expression. The SYSSTAT function detects the first time the SIS module runs after a download (or restart or switchover) so that conditional logic can execute on that scan.

4.5.2 Restarts After Power Failures

A restart occurs after power is restored to an SLS1508 that had a running configuration prior to losing power for less than 10 days. During a restart the SLS1508 reapplies the last downloaded configuration and restores parameters that had been saved to non-volatile memory. At the time power is lost, outputs of the SLS1508 are deenergized, which should result in the same output state as after the original download. After a restart the goal is to retain the same process state that occurred as a result of the power failure, yet to restore the parameter values that were saved to non-volatile memory, which are more current than the last downloaded values.

The SLS1508 saves certain parameter values to non-volatile memory when the value changes at runtime. These parameters have the "restored on restart" characteristic. Applicable SIS function block parameters are shown as having this characteristic in parameter tables for SIS function blocks in DeltaV Books Online. Top-level parameters created in SIS modules and SIS composite blocks have this characteristic by default, but from the properties dialog you can change them to have the "preserved on download" characteristic instead.

If there is an opportunity for an SLS1508 to lose power due to the power source not being redundant or not having an uninterruptible power supply, you should test the behavior following a restart. If you discover an issue, the first step is to see if a top-level parameter needs to be changed to "restored on restart." If the issue persists, consider the use of the SYSSTAT function in a Calc/Logic function block expression. The SYSSTAT function detects the first time the SIS module runs after a restart (or download or switchover) so that conditional logic can execute on that scan.

Most runtime-writable parameters are eligible to be restored on restart if they have changed since the last download, either by a secure write operation from a workstation, or by SIS module logic itself. The exception is wired input parameters of SIS function blocks. Parameter values transferred on wired links are not saved to non-volatile memory. However, assignments made by Calc/Logic block expressions are saved to non-volatile memory.

Parameter values stored in non-volatile memory are cleared on a download. Be sure to upload parameter values written by secure writes from workstations prior to downloading.

4.6 System Administration

4.6.1 Database Backups

It is valuable to always have a current backup of the configuration database in case you need to replace your ProfessionalPLUS workstation for any reason. An automatic daily export is recommended beginning with the engineering phase and continuing through the entire lifecycle. Use the Daily Export feature of DeltaV Database Administrator to configure automatic database exports.

4.6.2 Configuration Changes After Startup

After the process is running it is useful to have an offline DeltaV system available in case you need to make and test configuration changes to SIS modules. If you make changes to SIS modules in the configuration database of your production system, you should be prepared for a potential need to download them at any time, for example, if a simplex SLS1508 needs to be replaced. It is better to import tested changes into the production system just before you plan to download them.

4.6.3 Uploading Parameter Changes

When you change parameter values at runtime using a secure write from DeltaV Operate or Control Studio Online/Debug, the change is recorded in the workstation so that you can upload the change to the configuration database later. Uploading the change to the database keeps the database value in sync with the runtime value. However, if there is a need to download the SLS1508, the new CRC value is different from the existing value and a functional test is required. One SLS1508 of a redundant pair can be replaced without a download. If you are using simplex SLS1508s, you may want to forgo uploading parameter changes so that a download does not require a functional test. Instead, check to see if there are any pending uploads prior to downloading. If so, record the changes, do the download, then manually repeat the secure write operations.

5 Operations and Maintenance Practices (Appendix D)

5.1 Bypasses and Other Overrides

DeltaV SIS has built-in capability for creating applications that follow guidelines set forth in the IEC 61511 standard and TÜV's Maintenance Override white paper related to maintenance bypasses. DeltaV SIS does not constrain you to using its built-in bypass capability. You are free to create custom logic and interfaces for this purpose.

The following subsections describe the built-in bypass capability in DeltaV SIS.

5.1.1 Override Types

Maintenance Bypass

During a maintenance activity such as calibration, proof testing, or repair of a transmitter, a maintenance bypass temporarily prevents the process value on the input channel from contributing to a potential trip. The Analog Voter and Discrete Voter function blocks provide the built-in maintenance bypass capability. When an individual input is bypassed for maintenance, its vote to trip is not considered in voting logic. A maintenance bypass is set and cleared by an operator or maintenance technician using a secure write operation from a workstation or a physical key switch, but could be cleared by the voter block itself upon a configurable timeout.

Startup Bypass

While a process is starting up, a startup bypass temporarily overrides a process value to allow time for it to reach a value that does not initiate a trip. The Analog Voter and Discrete Voter function blocks provide the built-in startup bypass capability. The block output maintains the normal operating value while the startup bypass is active. A startup bypass is initiated by an operator using a secure write operation or by the voter block detecting a process startup condition. The startup bypass is cleared after a configurable time period or optionally when the voter block detects a process condition.

Parameter Force

This override uses Control Studio Debug mode to force a wired input parameter on a function block diagram to have a value other than the source value. The use of parameter forces is intended for functional testing, not when the SIF is providing its protection function unsupervised.

CEM Effect Force

This override forces an Effect output on a CEM function block to the normal or tripped value, thereby forcing the output channel value. The CEM Effect force is intended for testing or to manipulate final elements while the process is not running. It should not be used as a maintenance bypass; individual inputs should be bypassed for maintenance purposes.

5.1.2 Configuration of Bypasses

The configurer of SIS module logic uses the BYPASS_OPTS parameter in the voter function blocks to determine which maintenance and startup bypass options apply for the block usage. Refer to the Analog Voter and Discrete Voter function blocks topics in the DeltaV SIS book in DeltaV Books Online for details on the various bypass options.

The configurer must provide a means to annunciate to the operator when a maintenance bypass or force condition is active. The built-in capability is provided through the SIS_DEFAULT module template, which has an alarm parameter, BYPASS_ALM, referencing bits in the SIF_ALERTS bitstring parameter found in all SIS modules. The referenced bits roll up the state of override conditions in the SIS module and in the voter and CEM function blocks in the module. BYPASS_ALM is active when a maintenance bypass is active in any voter block in the module, an Effect is being forced in any CEM block, or a wired input is being forced using Control Studio Debug. Startup bypasses are not annunciated by default, but can be configured to do so using a check box.

The ability to set and clear maintenance bypasses in voter function blocks at runtime can be configured using dynamos for the voter function blocks in DeltaV Operate configure mode. For more information, refer to the topics on SIS function block dynamos and faceplates in the DeltaV SIS/Operator Graphics section of DeltaV Books Online.

5.1.3 Operation of Bypasses

A Maintenance bypass is typically used in either of two situations.

1. There is a planned maintenance activity on a transmitter or other sensor. A single input is bypassed to prevent that input from causing a spurious trip during the activity.

2. A failure occurs in a transmitter, the field wiring, or the input circuitry of the SLS1508 during normal operation. A maintenance bypass is used to prevent Bad status from causing a trip in the output function block (if the failure itself did not already cause a trip).

The bypass is set from a process display in DeltaV Operate, for example, by clicking on an input check box of the voter function block dynamo and then confirming the selection. A set bypass is cleared using the same procedure. While the bypass is set, BYPASS_ALM remains active and the toolbar button for the SIS Alarm List is visible in the DeltaV Operate toolbar, meaning there is at least one active, unacknowledged, or suppressed SIS alarm in the list. A click on the toolbar button opens the SIS Alarm List display. Operators should be aware of all alarms visible on this display. The handoff at shift change should include a review of the SIS Alarm List. You can create other alarms related to bypasses by referencing alarm conditions determined in the voter blocks. These alarms include a reminder that the expiration of a bypass is imminent and whether a bypassed input is voting to trip.

The history of bypass activity is available in the Event Chronicle of DeltaV Process History View. No special configuration is required. The setting and clearing of bypasses and bypass permits are recorded whether they are done using secure writes from workstations or physical switches. An event record is also created whenever the block removes a bypass due to a timeout.

The following example scenario illustrates a case where a maintenance bypass is used following a failure.

The Failure

A HART transmitter fails, resulting in a Field Device Malfunction HART error and a down-scale output value as configured in the device.

How the Logic Responds

Bad status enters the SIS module logic in the SLS1508 because the HART_ERRORS parameter on the input channel was configured to not ignore the Field Device Malfunction error. The Analog Voter block in the SIS module has a “Greater Than” detection type and a 1oo1 voting arrangement. Bad status propagates through the voter block, but the down-scale value does not cause a trip value on the output of the block. Bad status continues to propagate through the CEM block and causes the fault state timer to start in the Discrete Output block, but no trip occurs on the output.

How the Operator Responds

The Bad status has caused IO_ALM in the SIS module to become active and appear on the alarm banner in DeltaV Operate. The operator clicks the module button in the alarm banner, which changes the main display to the interlock display created for the SIF and pops up the SIS module faceplate. The operator assesses the impact of the failure by looking at the interlock display, which was created with function block dynamos. It is clear that a trip has not occurred, but the operator sees on the DO block dynamo that the fault state timer value is incrementing and sees the time value at which the output block initiates a trip. The operator clicks the bypass check box for the transmitter and confirms the "set bypass." The fault state timer stops incrementing and retains its value. The operator initiates the repair activity for the transmitter, knowing that manual supervision of the SIF is necessary while the bypass is active because the SLS1508 is not able to respond to a demand if one occurs. Manual supervision implies that a local measurement is available for the process value and the operator can be notified if a demand occurs and has a means to manually initiate a trip.

There are several variations to this scenario to consider.

1. Suppose the voting arrangement is 1oo2. In this case the Bad status does not propagate. Manual supervision is not necessary. The SIF is still able to respond to a demand based on the other transmitter. The operator bypasses the Bad input so a trip does not occur when the transmitter is replaced.

2. Suppose the voting is 2oo3. In this case the operator merely follows up on repair for the transmitter. No maintenance bypass is needed. The other two transmitters are providing the protection and there is no concern that a trip might occur when the transmitter is replaced.

3. Suppose the transmitter failure results in an up-scale output value. With a 1oo1 or 1oo2 voting arrangement, a false trip occurrs. A 2oo3 voting arrangement has the same result as a down-scale output value. But 2oo2 voting starts the fault state timer in the output block because there are not enough good inputs to ensure a proper response to a potential demand.

Whenever Bad status enters an SIS module and a determination is made that a repair is required, the repair should be completed within the allowed repair time for the SIF to prevent the PFDavg or PFH from exceeding the SIL verification value.

5.2 Fault Detection, System Response, and Repair Procedures

The SLS1508 executes extensive self-testing on a continuous basis to detect potential faults. This section presents an overview of fault detection, how the SLS1508 and DeltaV SIS respond to a detected fault, and what you should do if a fault occurs. Although the presence of a fault is expected to be uncommon, it is important to have a fundamental understanding of the topic.

Faults detected by SLS1508 diagnostics are generally related to hardware failures in the SLS1508, but can also be associated with field devices and field wiring, or other conditions not related to hardware. Some faults have the potential to prevent the appropriate response to a process demand, some do not. The SLS1508's response and the recommended action depend on the type of fault detected.

The terms fault and error are used interchangeably. Not all diagnostic conditions detected and annunciated by the SLS1508 are faults or errors. Some merely cause an advisory alert such as a reminder that a proof test of the SLS1508 is due soon.

DeltaV SIS responds to faults detected in the SLS1508 in one of three ways:

1. The SLS1508 responds to a detected fault by initiating a shutdown; a DeltaV SIS alarm occurs.

   The SLS1508 has detected a fatal error, which results in a reset and deenergization of all output channels on this SLS1508 card. Reasons for a fatal error include, among others, a processor has failed and does not arm the hardware watchdog, a processor has detected that a critical task did not complete in a timely fashion, or the main processors have calculated different output values. An alarm occurs following a fatal error, but the particular alarm depends on whether the SLS is simplex or redundant.

2. A DeltaV SIS alarm occurs when the SLS1508 detects a fault; the SLS1508 continues providing its protection function.

   The SLS has detected a non-fatal condition. An alarm occurs because the condition requires an operator action such as initiating maintenance or taking steps to clear the condition. When a non-fatal condition is active, the SLS1508 is still able to respond to a process demand. In some cases a demand results in a reset of the SLS1508 if an error condition is already present, for example, an output channel is stuck On.

3. DeltaV SIS logs an event record when the SLS1508 detects a fault; the SLS1508 continues providing its protection function.

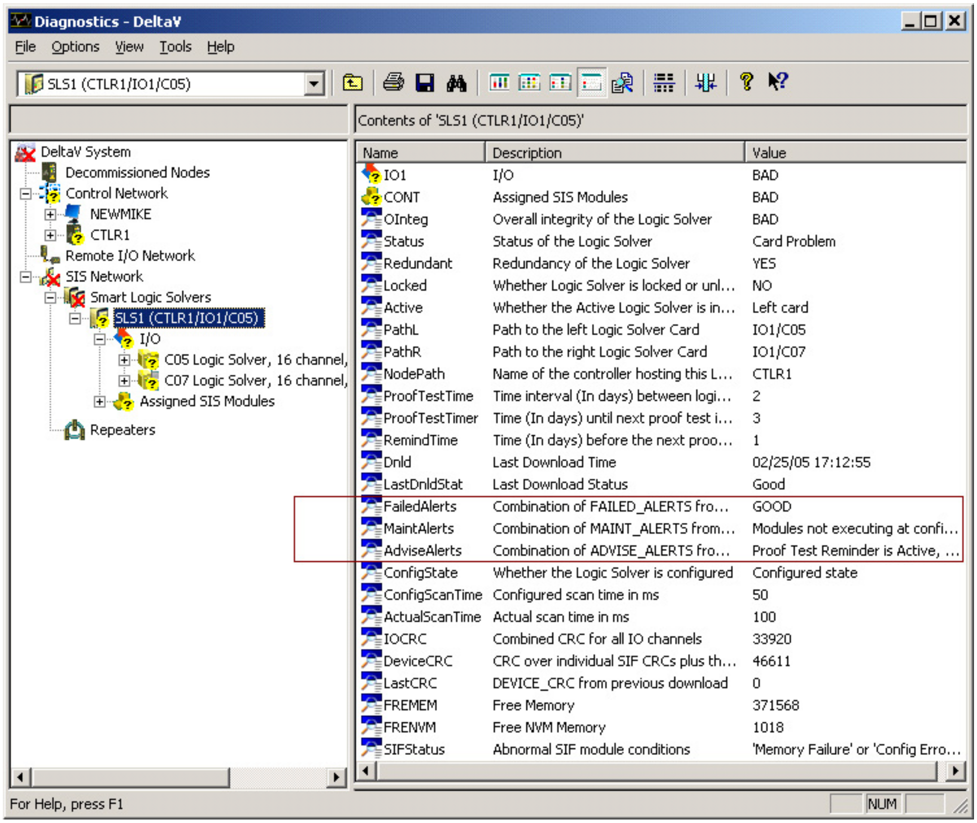
The SLS has detected a non-fatal condition, but no alarm occurs because immediate action is not required. An event record is added to Event Chronicle, which may be of interest in a future investigation. DeltaV SIS creates event records for all annunciated conditions in addition to these event-only conditions.

5.2.1 How DeltaV SIS Annunciates Faults

DeltaV SIS provides standard alarms to annunciate, in DeltaV Operate, faults detected by the SLS1508. No special configuration is required. At runtime the alarms are part of a container with the SLS name. When an SLS alarm appears on the alarm banner in DeltaV Operate and is clicked by the operator, the SLS faceplate opens. The faceplate shows the active alarm(s): FAILED_ALM, MAINT_ALM, ADVISE_ALM, or COMM_ALM. It also shows the text for the active condition or "Multiple conditions" if more than one alert condition is active for the particular alarm.

A button on the faceplate toolbar opens Diagnostics Explorer in the context of the SLS. The SLS container has a number of diagnostic parameters accessible at runtime by the SLS path. There is also a container for the SLS1508 card, accessible at runtime by the controller path using the leftmost slot number of the card, for example, CTLR1/IO1/C05/*param_name*.

A redundant SLS has diagnostic parameters for each SLS card and for the SLS itself. Figure 5-1 is an example of Diagnostics Explorer showing the diagnostic parameters for the highlighted SLS. There is an "alerts" bitstring parameter associated with the Failed, Maint, and Advise alarms. The alarm is active if any bit is set in the corresponding alerts parameter. The Comm alarm is active if the DeltaV controller cannot communicate with the SLS1508 (or both cards, if redundant).

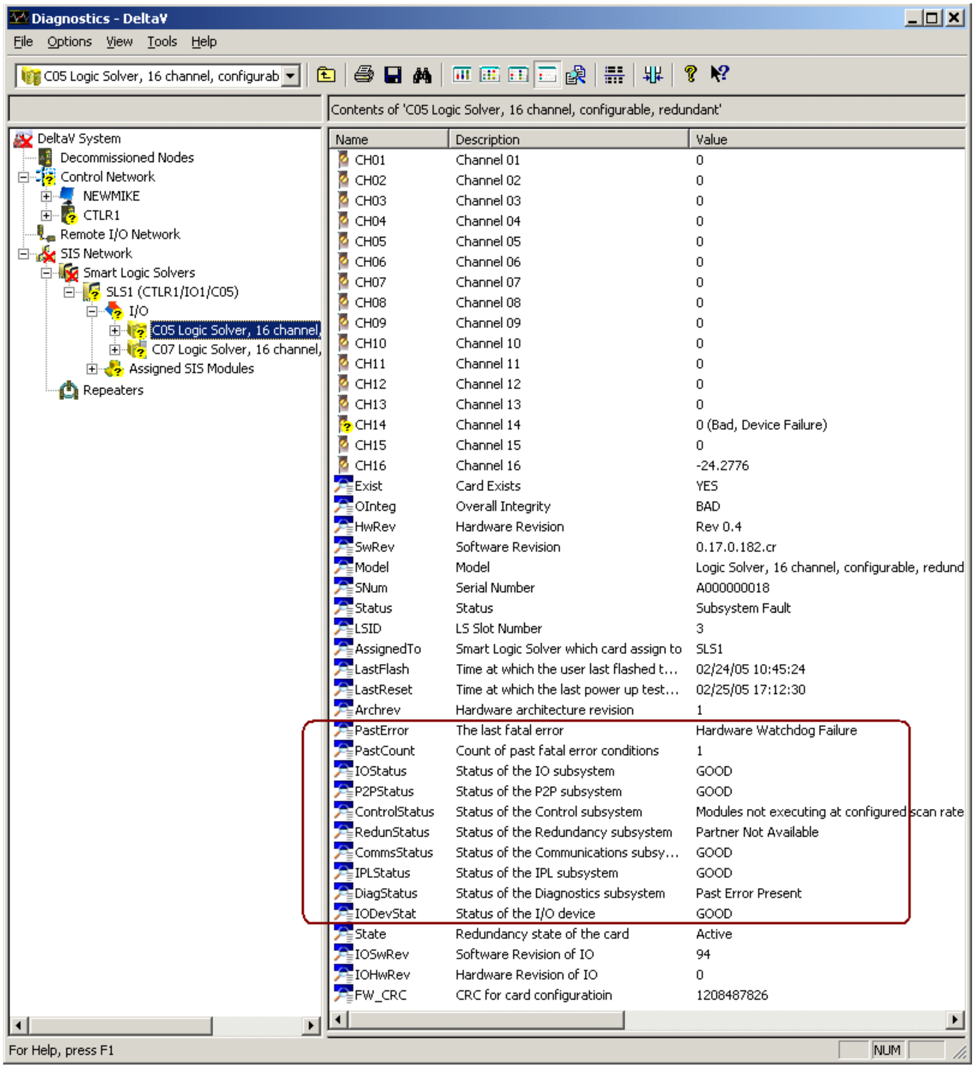

Diagnostics - DeltaV
File Options View Tools Help
SLS1 (CTLR1/IO1/C05)
Contents of 'SLS1 (CTLR1/IO1/C05)'
For Help, press F1
NUM

- DeltaV System
  - Decommissioned Nodes
  - Control Network
    - NEWMIKE
    - CTLR1
  - Remote I/O Network
  - SIS Network
    - Smart Logic Solvers
      - SLS1 (CTLR1/IO1/C05)
        - I/O
          - C05 Logic Solver, 16 channel,
          - C07 Logic Solver, 16 channel,
        - Assigned SIS Modules
    - Repeaters

Name	Description	Value
IO1	I/O	BAD
CONT	Assigned SIS Modules	BAD
OInteg	Overall integrity of the Logic Solver	BAD
Status	Status of the Logic Solver	Card Problem
Redundant	Redundancy of the Logic Solver	YES
Locked	Whether Logic Solver is locked or unl...	NO
Active	Whether the Active Logic Solver is in...	Left card
PathL	Path to the left Logic Solver Card	IO1/C05
PathR	Path to the right Logic Solver Card	IO1/C07
NodePath	Name of the controller hosting this L...	CTLR1
ProofTestTime	Time interval (In days) between logi...	2
ProofTestTimer	Time (In days) until next proof test i...	3
RemindTime	Time (In days) before the next proo...	1
Dnld	Last Download Time	02/25/05 17:12:55
LastDnldStat	Last Download Status	Good
FailedAlerts	Combination of FAILED_ALERTS fro...	GOOD
MaintAlerts	Combination of MAINT_ALERTS from...	Modules not executing at confi...
AdviseAlerts	Combination of ADVISE_ALERTS fro...	Proof Test Reminder is Active, ...
ConfigState	Whether the Logic Solver is configured	Configured state
ConfigScanTime	Configured scan time in ms	50
ActualScanTime	Actual scan time in ms	100
IOCRC	Combined CRC for all IO channels	33920
DeviceCRC	CRC over individual SIF CRCs plus th...	46611
LastCRC	DEVICE_CRC from previous download	0
FREMEM	Free Memory	371568
FRENVM	Free NVM Memory	1018
SIFStatus	Abnormal SIF module conditions	'Memory Failure' or 'Config Erro...

Figure 5-1 Diagnostics Explorer Showing Contents of the SLS Container

Figure 5-2 is an example of the Diagnostics Explorer showing the diagnostic parameters of the left SLS card of a redundant pair. The right SLS card has the same parameters. There is a bitstring parameter for the status of each subsystem. The bits in these subsystem status parameters map into bits of the alerts parameters in the SLS container. A simplex SLS has direct mapping, but a redundant SLS combines the subsystem status conditions into the alerts parameters. If the subsystem status condition is active in either SLS1508 card, the mapped alert condition is active.


Diagnostics - DeltaV
File Options View Tools Help
C05 Logic Solver, 16 channel, configurab
For Help, press F1
NUM

- DeltaV System
  - Decommissioned Nodes
  - Control Network
    - NEWMIKE
    - CTLR1
  - Remote I/O Network
  - SIS Network
    - Smart Logic Solvers
      - SLS1 (CTLR1/IO1/C05)
        - I/O
          - C05 Logic Solver, 16 channel,
          - C07 Logic Solver, 16 channel,
        - Assigned SIS Modules
    - Repeaters

Contents of 'C05 Logic Solver, 16 channel, configurable, redundant'

Name	Description	Value
CH01	Channel 01	0
CH02	Channel 02	0
CH03	Channel 03	0
CH04	Channel 04	0
CH05	Channel 05	0
CH06	Channel 06	0
CH07	Channel 07	0
CH08	Channel 08	0
CH09	Channel 09	0
CH10	Channel 10	0
CH11	Channel 11	0
CH12	Channel 12	0
CH13	Channel 13	0
CH14	Channel 14	0 (Bad, Device Failure)
CH15	Channel 15	0
CH16	Channel 16	-24.2776
Exist	Card Exists	YES
OInteg	Overall Integrity	BAD
HwRev	Hardware Revision	Rev 0.4
SwRev	Software Revision	0.17.0.182.cr
Model	Model	Logic Solver, 16 channel, configurable, redund
SNum	Serial Number	A000000018
Status	Status	Subsystem Fault
LSID	LS Slot Number	3
AssignedTo	Smart Logic Solver which card assign to	SLS1
LastFlash	Time at which the user last flashed t…	02/24/05 10:45:24
LastReset	Time at which the last power up test…	02/25/05 17:12:30
Archrev	Hardware architecture revision	1
PastError	The last fatal error	Hardware Watchdog Failure
PastCount	Count of past fatal error conditions	1
IOStatus	Status of the IO subsystem	GOOD
P2PStatus	Status of the P2P subsystem	GOOD
ControlStatus	Status of the Control subsystem	Modules not executing at configured scan rate
RedunStatus	Status of the Redundancy subsystem	Partner Not Available
CommsStatus	Status of the Communications subsy…	GOOD
IPLStatus	Status of the IPL subsystem	GOOD
DiagStatus	Status of the Diagnostics subsystem	Past Error Present
IODevStat	Status of the I/O device	GOOD
State	Redundancy state of the card	Active
IOSwRev	Software Revision of IO	94
IOHwRev	Hardware Revision of IO	0
FW_CRC	CRC for card configuratioin	1208487826

Figure 5-2 Diagnostics Explorer Showing Contents of the SLS Card Container

Refer to the “SLS Diagnostic Parameters” topic in the DeltaV SIS book of DeltaV Books Online for details on the subsystem status and alert bitstring parameters.

The topic describes:

- The text and meaning of each condition
- How subsystem status bits map into alert bits
- What action to take when an alert condition becomes active
- Which conditions annunciate and impact device integrity
- Which conditions are event-only and do not impact device integrity

You can change the priority of the Failed, Maint, Advise, and Comm alarms. Because certain error conditions can exist momentarily, avoid alarm priorities that are auto-acknowledging.

5.2.2 Evaluating and Responding to Annunciated Faults

When a fault or other annunciated condition occurs, there are multiple sources of information to be evaluated prior to taking action. The evidence left by the condition is a function of the type of fault and whether the SLS is simplex or redundant.

The first step in the evaluation is determining whether the condition is fatal or non-fatal.

- A *fatal* error in a *simplex* SLS generally results in a process shutdown because output channels of the SLS card are deenergized. An active Comm alarm occurs immediately.
- A *non-fatal* error in a *simplex* SLS does not impact the process. There is no Comm alarm, but there is a Maint or Advise alarm depending on the condition.
- A *fatal* error in one card of a *redundant* SLS does not impact the process because the other SLS card continues to drive outputs. An active Maint alarm occurs immediately because the partner card with the fatal error is not available.
- A *non-fatal* error in a *redundant* SLS results in an active Maint or Advise alarm. The evidence differs from a fatal error in that the partner card has not gone through reset, so it continues to be available to the card without the error condition.

The next step is determining whether the error condition is still present. Typically detected faults are persistent, that is, they are caused by a hardware failure and require that the SLS card be replaced. But some conditions are momentary, clearing after being active briefly. In this case an inactive, unacknowledged alarm is present. Diagnostic parameters do not indicate the cause of the alarm because the condition is no longer active. Event Chronicle must be used to determine which condition caused the alarm when the alarm is no longer active.

5.2.3 Evaluating Fatal Errors

Fatal errors result in a reset of the affected SLS card. The evidence of a fatal error changes based on the time since the fatal error occurred. Immediately after a fatal error the SLS card resets and begins its power-up testing, which completes in about two minutes. During this time the SLS card is not reporting diagnostic information to the DeltaV controller. A redundant partner of this SLS card indicates that its partner is not available while it is power-up testing. If the fatal error is momentary, the “partner not available” condition clears when power-up testing is complete. But if the fatal error is persistent, the “partner not available” condition remains.

The SLS card stores the reason for a fatal error in a diagnostic parameter called PAST_ERROR (PastError in Diagnostics Explorer). The value of PastError is updated when the SLS card finishes power-up testing following a fatal error. Persistent fatal errors are expected to cause the same condition to be detected when the SLS card begins running its continuous diagnostic tests. The outcome is another reset. When an SLS1508 detects the same fatal error on two back-to-back resets, it enters a reduced startup state where SIS modules do not execute and outputs cannot be powered On. The SLS card’s Status is “Not Operational” and DiagStatus is “Persistent Fatal Error After Powerup.”

A simplex SLS copies its card parameter PastError into its SLS parameter FailedAlerts when the fatal error persists after power-up tests complete. Immediately after the fatal error is detected a Comm error occurs, which becomes inactive when power-up tests complete. At this time the Failed alarm becomes active.

A redundant SLS behaves differently. PastError is not copied from the Standby card into FailedAlerts of the SLS because the Active card continues to operate. The SLS has not failed; only the Standby has failed. Note that the Standby card may have been the Active card at the time the error occurred. A redundant SLS has a Maint alarm due to the Standby partner not being available. The Maint alarm occurs immediately after the fatal error.

Note *Persistent fatal errors generally require a hardware repair. The hardware must be returned to Emerson for repair. Before returning the hardware, perform a manual reset of the affected SLS card using Diagnostics Explorer. If the error continues to be present after power-up tests complete, which is expected, please contact the Global Service Center (GSC) for technical support prior to contacting Customer Service for a Material Return Tracking (MRT) number. The GSC will help determine the necessary action and forward the call to Customer Service if needed. For contact information, visit:*

http://www.emersonprocess.com/systems/support/ratecard.htm

The PastError parameter retains the reason for the most recent fatal error. PastError clears (returns to Good) the next time a reset occurs that is not due to an error condition, for example, a manual reset is done.

Table 5-1 summarizes the evidence and action required when the various classes of errors occur in simplex and redundant SLSs. The table shows the state of alarm and diagnostic parameters approximately five minutes after the error is detected.

Table 5-1 Summary of the Evidence of SLS1508 Errors and the Action Required

Error Type	Simplex SLS		Redundant SLS	
	Evidence	Action	Evidence	Action
Non-Fatal, Momentary	Inact-Unack alarm (MAINT or ADVISE)	Check Event Chronicle records to determine error condition. Record error occurrence; report to Emerson if there is a repeat occurrence.	Inact-Unack alarm (MAINT or ADVISE)	Check Event Chronicle records to determine error condition and affected card. Record error occurrence; report to Emerson if there is a repeat occurrence.
Non-Fatal, Persistent	Act-Unack alarm (MAINT or ADVISE)	Check _ALERTS parameter associated with alarm to determine error condition. Report error to Emerson.	Act-Unack alarm (MAINT or ADVISE)	Check _ALERTS parameter associated with alarm to determine error condition. Check _STATUS parameters on both cards to determine affected card. Report error to Emerson.
Fatal, Momentary	Inact-Unack COMM_ALM	Restart the process at the appropriate time. Check PAST_ERROR on card to determine error condition. Report error to Emerson.	Inact-Unack MAINT_ALM	Check PAST_ERROR on Standby card to determine error condition. Report error to Emerson.
Fatal, Persistent	Act-Unack FAILED_ALM Act-Unack MAINT_ALM, MAINT_ALERTS includes '”Card Not Fully Operational.” STATUS (card) is “Not Operational.” DIAG_STATUS on card includes “Persistent Fatal Error After Powerup.”	Check FAILED_ALERTS on SLS or PAST_ERROR on card to determine error condition. Do a manual reset of card, replace card if necessary. Report error to Emerson.	Act-Unack MAINT_ALM, MAINT_ALERTS includes “Partner Not Available” and “Card Not Fully Operational.” STATUS (Standby card) is “Not Operational.” DIAG_STATUS on Standby card includes “Persistent Fatal Error After Powerup.”	Check PAST_ERROR on Standby card to determine error condition. Do a manual reset of Standby card; replace card if necessary. Report error to Emerson.

Explanation of Terms in Table 5-1

Non-Fatal – The error is not safety-critical and results in a notification action only.

Fatal – The error causes a reset of the SLS card to deenergize outputs on that card. For a simplex SLS, final elements in the field are commanded to the tripped state. For a redundant SLS, the affected card resets, which results in the partner being the Active card, but final elements in the field are not affected.

Momentary – The error condition is active briefly, then clears.

Persistent – The error condition remains active indefinitely.

Inact-Unack – The alarm condition is inactive, but the alarm has not been acknowledged.

Act-Unack – The alarm has not been acknowledged and the alarm condition is still active.

Report the error to Emerson – Most, but not all, errors should be reported to Emerson. Some conditions are not errors but advisory alerts and can be cleared by an action such as a configuration change or upload/download. Refer to the "SLS Diagnostic Parameters" topic in the DeltaV SIS book of DeltaV Books Online prior to reporting a diagnostic condition. Momentary, non-fatal conditions should be reported only when the same condition has occurred multiple times.

Please report actual errors by contacting technical support at:

http://www.emersonprocess.com/systems/support/ratecard.htm

5.2.4 Maximum Fault Detection Time

The cycle time for continuous diagnostics varies. Some faults are detected within one millisecond of occurrence. Some are detected at a 50-millisecond diagnostic cycle time, which is independent of the configured SLS scan rate for SIS modules; others require the condition to be present for multiple 50-millisecond cycle times.

The maximum fault detection time for a fatal error is eight diagnostic scan cycles or 400 milliseconds. This means the input to output response time of the SIF can increase no more than 400 milliseconds due to the presence of a fault.

Fault detection time using main processor comparison diagnostics is a function of the configured SLS scan rate for SIS modules. At the slowest scan rate of 200 milliseconds, detection time is still within 400 milliseconds.

The longest diagnostic cycle times in the SLS1508 are related to memory testing. A failed memory test results in a fatal error within one hour of the memory error occurrence. However, if a process demand occurs after a memory failure but before detection of the memory failure, another diagnostic, such as the task checkpoint monitor or main processor comparison test, indirectly detects the memory error within the 400 milliseconds.

5.2.5 Fault Detection in SISNet Repeaters

Unlike the SLS, SISNet Repeaters do not have a runtime container with alarms to annunciate faults. Instead, repeaters use the DeltaV node status facility to annunciate faults. If a DeltaV node such as a controller has Bad overall integrity (OINTEG), the node has an active node status alarm in DeltaV Operate. Included in the roll-up of a controller's OINTEG is an integrity parameter for its SIS subsystem called SINTEG. SINTEG is Bad if any SLS card or any repeater associated with the controller has a Bad OINTEG.

5.3 Proof Testing the SLS1508

SLS1508s must be proof tested periodically to ensure there are no dangerous faults present that are not being detected by continuous runtime diagnostics. A manual proof test for an SLS1508 is initiated from a DeltaV workstation and causes the SLS1508 card to go through reset and power-up testing. Proof testing of SLS1508 cards can also be done automatically.

Immediately following successful power-up testing there are no known dangerous faults present. Choose the proof test interval for an SLS1508 based on the associated SIF requiring the shortest proof test period to achieve the required probability of dangerous failure for its logic solver subsystem.

The SLS1508 proof test timer automatically counts the number of days since the last reset occurred. The SLS properties dialog in DeltaV Explorer has a Proof Testing tab for entering the required proof testing interval and a reminder time value.

The SLS1508 provides an alert when the number of days since the last reset exceeds the configured time. A reminder alert occurs a configured number of days before the "exceeds" alert to assist maintenance personnel in the planning of manual tests.

There is an event record for the setting and clearing of proof test alerts. The proof test timer for a redundant SLS1508 indicates the number of days since the last reset of the Active card, which always occurs earlier than the last reset of the Standby card.

5.3.1 Automatic Tests

Automatic proof testing is available for redundant SLS1508s only. The Proof Testing tab of the SLS properties dialog has an “Enable automatic proof test to run at reminder time” check box. When checked, the SLS1508 performs the proof test when the number of days since the last reset reaches the configured time. The test begins five minutes after the SLS1508 sets the reminder alert. In this case the reminder alert informs the operator that a test will occur soon so that the Partner Not Available alerts can be ignored after the test begins. At the time of automatic proof test:

- The Active card starts the test by initiating a switchover to the Standby card. If the Standby card is not available, the Active card tries again in five minutes.
- After switchover the Standby card becomes Active and the new Standby card goes through reset and begins power-up testing. There is no adverse impact to the running process. An event record confirms successful power-up testing.
- The new Active card still has a proof test due, so it waits for its partner to become available then initiates a switchover. When the partner has become the Active card, the new Standby card goes through reset and power-up testing. An event record confirms successful power-up testing of the SLS card.

5.3.2 Manual Tests

The following procedure should be used for manual proof testing of the SLS1508.

Simplex SLS1508

1. Initiating a manual reset on a simplex SLS1508 results in all outputs being deenergized. If you must proof test a simplex SLS online, you need to temporarily bypass or block final elements and provide manual supervision.

2. The SLS must be Unlocked to initiate a manual reset. Select the SLS1508 under SIS Network in Diagnostics Explorer. If the value of the Locked parameter is Yes in the contents pane, right-click on the SLS1508 and select Unlock. Click Confirm on the secure write confirmation dialog.

3. Right-click on the SLS1508 and select “Force Reset on Active.” Clicking Confirm on the confirmation dialog results in all outputs being deenergized.

4. The SLS1508 goes through power-up testing and returns to the configured state. The proof test timer resets to 0. There are two event records, one for the user reset command and one from the SLS1508 confirming that power-up tests completed successfully.

Redundant SLS1508

The procedure for a redundant SLS1508 allows the proof test to be done online without adversely affecting the running process.

1. The SLS must be Unlocked to initiate a manual reset. Select the SLS1508 under SIS Network in Diagnostics Explorer. If the value of the Locked parameter is Yes in the contents pane, right-click on the SLS1508 and select Unlock. Click Confirm on the secure write confirmation dialog.

2. Right-click on the SLS1508 and select “Force Reset on Standby.” Click Confirm on the confirmation dialog.

3. Wait several minutes for the Standby card to complete power-up tests and become configured by the Active card. The Partner Not Available maintenance alert goes inactive when the Standby card is fully configured.

4. Right-click on the SLS1508 and select “Switchover.” Click Confirm on the confirmation dialog.

5. The previously reset Standby card becomes the new Active card and the new Standby card goes through power-up tests and is configured by the new Active card. The proof test timer is 0. There are four event records, two for the user reset and switchover commands and two for the SLS cards, confirming that power-up tests completed successfully.

5.4 Upgrading Firmware

Future releases of DeltaV software will potentially include updated firmware for the SLS1508 and SISNet Repeater. It may not be necessary to upgrade the firmware in SIS hardware components when the remainder of the DeltaV system is upgraded to a new release. But if a new SIS firmware revision has desired features or fixes a specific issue, you can upgrade to the new revision by installing files from a DeltaV workstation to flash memory in the SLS1508 or SISNet Repeater.

The DeltaV Controller Upgrade Utility is used to upgrade the firmware in an SLS1508 or SISNet Repeater. After a DeltaV workstation has been upgraded with a new release or a service pack has been installed, the firmware upgrade files are located in the default DeltaV\ctl folder. Launch the Controller Upgrade Utility from the Windows Start button using the DeltaV Installation menu. Click the Help button for instructions.

5.5 Making Online Scaling Changes in HART Transmitters

A special procedure is recommended if you need to make an online change to the upper or lower range value in a HART transmitter connected to a channel of the SLS1508. The SLS1508 does not automatically synchronize the scaling between the HART device and the associated AI function block in the SIS module. Scaling must be configured independently.

In the SIS module, scaling is set using the EU100 and EU0 fields of the OUT_SCALE parameter in the AI function block. To change the scaling in the HART device you must use AMS or a HART Communicator. Downloading the SLS1508 or changing OUT_SCALE in the AI block at runtime does not affect scaling in the HART device. Similarly, changing the upper or lower range value in the HART device does not cause a change to EU100 or EU0 of OUT_SCALE in the AI block.

If an online scaling change is made in the HART device, there is a step change in the OUT parameter of the associated AI block, and the value is incorrect until an equivalent manual change is made to the OUT_SCALE parameter of the AI block. When making online scaling changes, a standard procedure should be followed to prevent spurious trips and to ensure that matching scaling is achieved. The recommended procedure is as follows.

1. Bypass the AVTR function block input wired from the OUT parameter of the AI block assigned to the HART device's channel using the AVTR dynamo on the process display in DeltaV Operate. If the TRIP_STATUS parameter of the AVTR block becomes "Trip Inhibited" as a result of the bypass, manually monitor the SIF while the input is bypassed.

2. Make the scaling change in the HART transmitter using AMS.

3. Use Control Studio Online to make the equivalent change to the OUT_SCALE parameter of the associated AI function block.

4. Check to see that the OUT parameter of the AI block has the expected online engineering units value.

5. Remove the bypass.

6. Upload the change in the OUT_SCALE parameter to the configuration database.