MOORE INDUSTRIES WORLDWIDE

Safety Instrumented Systems: The “Logic” of Single Loop Logic Solvers

April 2009

The industrial process industry is experiencing a dynamic growth in Functional Process Safety applications.

Much of this growth has been driven by increased awareness of destruction of property, injuries and loss of life associated with tragic events that are widely publicized in the worldwide media. Companies, of course, have a moral and legal obligation to limit risk posed by their operations. In addition to their social responsibilities, the costs of litigation measuring in the billions of dollars has caught the eye of risk management executives worldwide.

As a result, management recognizes the financial rewards of utilizing a properly designed process system that optimizes reliability and safety.

That’s why companies are now actively taking steps to comply with various national and worldwide safety standards such as ANSI/ISA 84 and IEC 61508/61511. To accomplish this, safety practitioners look to a “new generation” of equipment specifically designed and approved for use in Safety Instrumented Systems that utilize Electrical and/or Electronic and/or Programmable (E/E/PE) technologies.

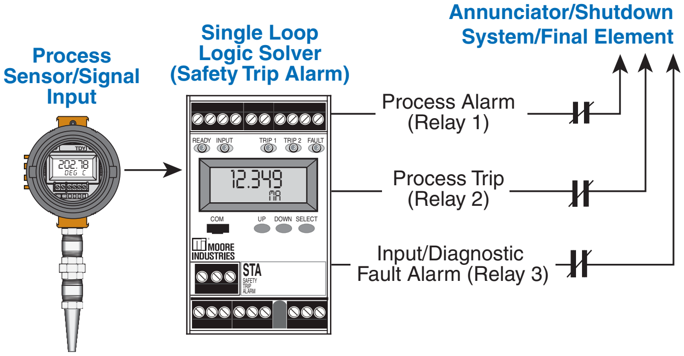
Safety Instrumented Systems

A Safety Instrumented System (SIS) is defined as an instrumented system used to implement one or more Safety Instrumented Functions (SIF). A SIS is composed of any combination of sensors, logic solvers and final control elements for the purpose of taking a process to a safe state when predetermined conditions are violated (Figure 1).

A SIF is a function to be implemented by a SIS that is intended to achieve or maintain a safe state for the process with respect to a specific hazardous event.

A simple, yet highly reliable, safety trip alarm performs as a Single Loop Logic Solver in Safety Instrumented Systems (SIS).

Figure 1. *In addition to logic solvers, a typical Safety Instrumented System (SIS) is composed of any number or combination of sensors and final control elements.*


Process Sensor/Signal Input
Single Loop Logic Solver (Safety Trip Alarm)
Annunciator/Shutdown System/Final Element
Process Alarm (Relay 1)
Process Trip (Relay 2)
Input/Diagnostic Fault Alarm (Relay 3)
202.78
DEG C
12.349
mA
READY
INPUT
TRIP 1
TRIP 2
FAULT
COM
UP
DOWN
SELECT
MOORE INDUSTRIES
STA

Examples of SIF applications include:

- Shutdown in a Hazardous Chemical Process Plant
- Open a Valve to Relieve Excess Pressure
- On/Off Control to Prevent Tank Overflow
- Shutdown Fuel Supply to a Furnace
- Add Coolant to Arrest Exothermic Runaway
- Automatic Shutdown When Operator Not Present
- Close a Feed Valve to Prevent Tank Overflow
- Initiate Release of a Fire Suppressant
- Initiate an Evacuation Alarm

IEC 61508 Provides Guidelines

To help companies implement a SIS, the International Electrotechnical Commission (IEC) developed IEC 61508, the standard for “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems”.

The main objective of IEC 61508 is to provide a design standard for Safety Instrumented Systems to reduce risk to a tolerable level by following the overall hardware and software safety life cycle procedures, and by maintaining the associated stringent documentation.

IEC 61508 has become the benchmark used mainly by safety equipment suppliers to show that their equipment is suitable for use in Safety Integrity Level (SIL) rated systems.

Learn More About IEC 61508 and Functional Safety on the IEC Web Site at:

http://www.iec.ch/zone/fsafety/fsafety_entry.htm

Explanations • Definitions • FAQ

For legacy products, suppliers are performing an Failure Modes, Effects and Diagnostic Analysis (FMEDA) hardware only assessment which provides failure data for SIS designers and may also provide proven-in-use data. This does not include any assessment of the product development process which contributes to systematic faults in the product design.

New products that are fully compliant with IEC 61508 address systematic faults by a full assessment of fault avoidance and fault control measures during hardware and software development.

Safety Integrity Level (SIL)

To determine a SIL, the safety practitioner team RISK/PROCESS HAZARD ANALYSIS (PHA) procedure identifies all process hazards, estimate their risks and decide if that risk is tolerable. Once a SIL has been assigned to a process, the safety practitioner has to verify that the individual components (sensors, logic solvers, final elements, etc.) that are working together to implement the individual Safety Instrumented Functions (SIF) comply with the constraints of the required SIL.

For any device used in a SIS, the team must pay close attention to each device's Safety Failure Fraction (SFF) and Probability of Failure on Demand (PFDavg). See Tables 1 and 2 for additional information. For each device in the SIF, both of these numbers have to be compared to the rules outlined in the safety standards to ensure that they are sufficient for use in the required SIL of the SIS. If these devices are classified as Type B, such as micro-processor based devices, the development process including software must also be assessed and approved for the required SIL level. While the standards do allow proven-in-use data as proof of a device's reliability, such information is usually very hard to verify and document. For this reason many end users prefer fully assessed devices by third party organizations.

Table 2. *To be considered for a specific SIL level application, a Type B "Complex" device (such as a microprocessor-based logic solver), must achieve a defined SFF rating. The higher SFF permits higher SIL suitability, plus specifies redundancy levels at each level.*

Safety Failure Fraction (SFF)	Hardware Fault Tolerance (HFT) for Type B Device		
	0	1	2
< 60%	Not Allowed	SIL 1	SIL 2
≥ 60%	SIL 1	SIL 2	SIL 3
≥ 90%	SIL 2	SIL 3	
≥ 99%	Special requirements apply (see IEC 61508)		

Safety Failure Fraction (SFF): The ratio of the average rate of safe failures plus dangerous detected failures of the subsystem to the total average failure of the subsystem.
Type B Device: A "Complex" device using contollers or programmable logic per IEC 61508.
Hardware Fault Tolerance (HFT): A level of required device redundancy. For example, a HFT of 1 means that there are at least 2 devices in the system and a dangerous failure of 1 device does not prevent the safety function from performing.

It is always the responsibility of the end user to perform or verify the calculations for the entire safety loop. Since a SIF relies on more than one device, it is imperative that all devices in the loop work together to meet the required SIL levels. The device's SFF and the PFDavg values used for these calculations can be found in a FMEDA report.

Table 1. *The SIL is a measure of the amount of risk reduction provided by a Safety Instrumented Function, with SIL 4 having the highest level of safety integrity, and SIL 1 the lowest. Table 1 describes safety in three columns—all mathematically related (e.g., RRF = 1/PFD).*

Safety Integrity Level (SIL)	Safety Availability	Probability of Failure on Demand Avg (PFD_{avg})	Risk Reduction Factor (RRF)
SIL 4	>99.99%	0.0001 to 0.00001	10,000 to 100,000
SIL 3	99.90% to 99.99%	0.001 to 0.0001	1,000 to 10,000
SIL 2	99.00% to 99.90%	0.01 to 0.001	100 to 1000
SIL 1	90.00% to 99.00%	0.1 to 0.01	10 to 100

Safety Availability: The availability of a SIS to perform the task for which it was designed as presented in percentage (%) in order of magnitude steps from 90% to 99% for SIL 1 up through 99.99% to 99.999% for SIL 4.

Probability of Failure on Demand Average (PFD_{avg}): Likelihood that a SIS component will not be able to perform its safety action when called upon to do so. A SIL is based on a PFD average of the safety function.

Risk Reduction Factor (RRF): Defined as $1/PFD_{avg}$, the number of times that risk is reduced as a result of the application of a safeguard (typically a more convenient expression for describing SIF effectiveness than SIL or availability).

FMEDA Reports

IEC 61508 requires a quantitative, as well as qualitative, assessment of risk. A Failure Modes, Effects and Diagnostic Analysis (FMEDA) provides a systematic way to assess the effects of all probable and known failure modes, including on-line monitoring and error checking, of a SIS component. It is a detailed circuit and performance evaluation that estimates failure rates, failure modes and diagnostic capability of a device. This data is provided to be used by a competent functional safety practitioner to determine a device's applicability in a specific safety-related application. It is best if the FMEDA report is certified by a well-qualified third-party agency that specializes in functional safety approvals.

"Logical" Logic Solvers

Until recently, the thought of a safety system conjured up images of Triple Modular Redundant (TMR) systems that represent enormous capital expenditures. Today, however, manufacturers offer a wide gamut of safety-certified devices that can be integrated into very cost-effective solutions. One simple, economical, yet highly dependable option is using a Safety Trip Alarm as a Single Loop Logic Solver (Figure 1 on Page 1).

A Single Loop Logic Solver (or Safety Trip Alarm), monitors a temperature, pressure, level, flow, position or status variable. If the input exceeds a selected high or low trip point, one or multiple relay outputs warn of unwanted process conditions or provide emergency shutdown (Figure 2), or provide on/off control, such as in a level control application (Figure 3).

Figure 2. *Single Loop Logic Solvers (Safety Trip Alarms), with selectable deadband to reduce false alarms, can be used to warn of unwanted process conditions or to provide emergency shutdown.*

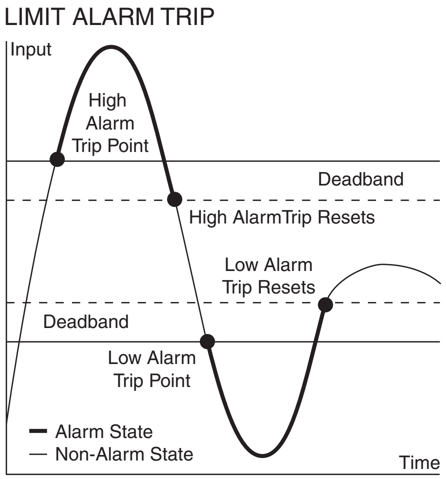
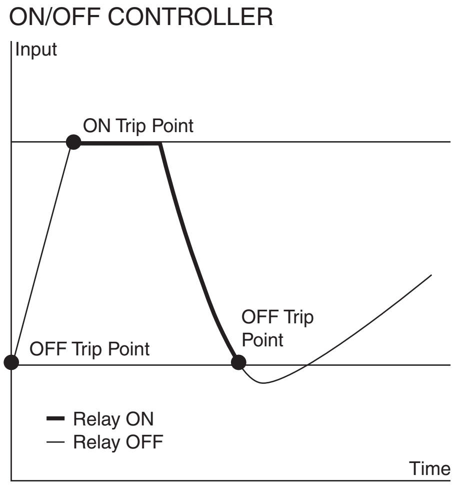


Figure 3. *Safety Trip Alarms can be used as simple on/off controllers in level applications (pump/valve control) when filling, emptying or preventing overflow of a container or tank.*



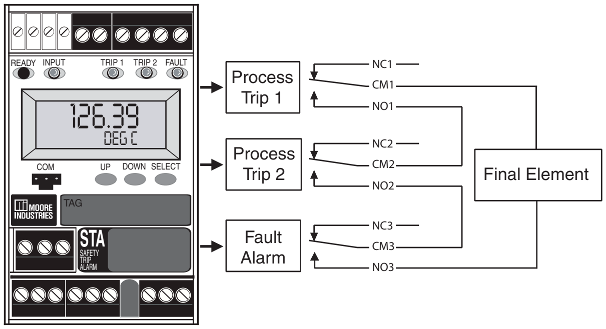
Sophisticated Advantages—The sophistication of alarm trips, and their applicability in SIS systems, has increased exponentially since their introduction. This includes programmable inputs; local configuration using on-board controls; safe password protection; a process display; transmitter excitation (the ability to power a transmitter eliminates an additional possible point of failure); and especially, comprehensive internal, input and sensor diagnostics.

Input/Instrument Diagnostics with Fault Alarm— Specially-engineered Safety Trip Alarms can check their own operation and configuration upon start up, and then continuously monitor this information, as well as the input signal. If internally diagnosed faults or external faults, such as loss of sensor or "bad quality input" occur, the alarm will trip a fault alarm.

SIL 2 and SIL 3 Applications—By using the "new generation" of Single Loop Logic Solvers, users realize many of the same advantages of larger and more expensive safety-certified PLCs at a fraction of the cost. If a microprocessor based Single Loop Logic Solver has a Safety Failure Fraction greater than or equal to 90%, and the PFDavg data falls within the required range, it is suitable for use in SIL 2 applications using a 1oo1 (no voting or redundancy required) architecture. In a 1oo2 architecture (redundancy) this same Single Loop Logic Solver could be suitable for use in a SIL 3 application provided the software is assessed and suitable for SIL 3 applications.

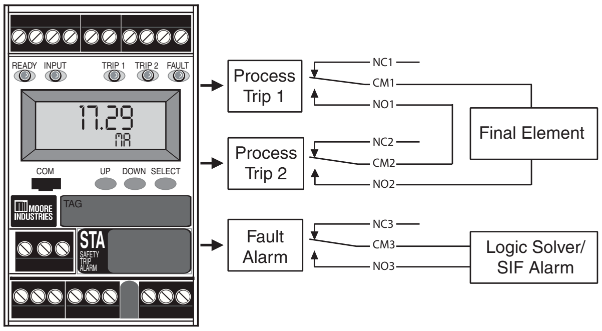
Typical examples of Single Loop Logic Solvers in Safety Instrumented Systems include:

Figure 4. *Safety Trip Alarm in a High Integrity Architecture.*



High Integrity Architecture—This configuration offers the highest trip integrity in a non-redundant application (Figure 4). Since all three relays are wired in series, any trip alarm or fault alarm will trip the final element or logic solver.

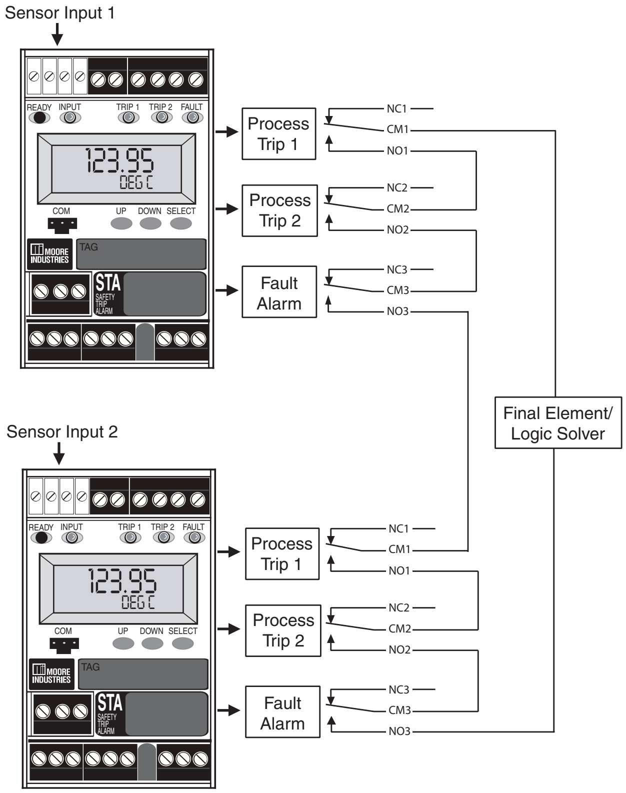
Figure 5. *Safety Trip Alarm in a High Availability Architecture.*



High Availability Architecture—In this configuration, the Safety Trip Alarm provides higher process or system availability (Figure 5). The fault alarm is wired separately to inform a safety system that there is a fault alarm and that this component’s ability to carry out its portion of the Safety Instrumented Function cannot be performed. This configuration would be used in applications where it is desirable to keep the process running should a fault occur because of a bad input or instrument fault. The output process trip relays are connected in a 1oo2 scheme to trip, providing security against a single relay failure. However, should the fault relay become active, the fault should be removed before the Safety Trip Alarm can provide proper safety coverage.

1oo2 Redundant Architecture—In this architecture, every component appears twice, and may be applicable for use in SIS systems up to SIL 3 (Figure 6). Advantages are improved reliability of trip action and reduced vulnerability to a single failure compared to a 1oo1 architecture. The logic in this configuration is an ‘OR’ statement for the safety function; if either sensor input reaches a trip condition or a fault relay is activated, the loop or function will reach a tripped state.

Figure 6. *Safety Trip Alarms in a 1oo2 Redundant/Voting Architecture Are Applicable for Use in SIS Systems Up to a SIL 3 Architecture.*



Third-Party Safety Certifications

Today, some Single Loop Logic Solvers (Safety Trip Alarms) are designed “from the ground up” in accordance with IEC 61508. An essential requirement to verify their design is a third-party certification from TÜV, Exida or a similarly accredited approval body. This certification provides unbiased, verified evidence that the unit is appropriate for use in specific SIS strategies. For example, the certification may verify that the device is appropriate for SIFs up to SIL 2 in a simplex or 1oo1 configuration. For increased process availability and/or higher SILs (such as SIL 3), the devices may be applied in 1oo2 or 2oo3 architectures (Figure 6). Hazardous area approvals, specifically Class 1, Division 2 for non-incendive (Type N) applications and Zone 2 applications are a must.

Just the Right Fit

Today, there are solutions for SIS strategies with hundreds of I/O and there are those for systems with just a handful of I/O—and everything in between. The “new generation” in safety-certified Single Loop Logic Solvers fits into this scenario nicely. They provide an extremely affordable option that delivers simple installation, easier validation and faster start-ups. Perpetual benefits that last for the life of the system include less maintenance, faster testing, easier documentation of the safety management reports and modular replacement strategies.

MOORE INDUSTRIES®
WORLDWIDE • www.miinet.com
United States • info@miinet.com
Tel: (818) 894-7111 • FAX: (818) 891-2816
Australia • sales@mooreind.com.au
Tel: (02) 8536-7200 • FAX: (02) 9525-7296
Belgium • info@mooreind.be
Tel: 03/448.10.18 • FAX: 03/440.17.97
The Netherlands • sales@mooreind.nl
Tel: (0)344-617971 • FAX: (0)344-615920
China • sales@mooreind.sh.cn
Tel: 86-21-62491499 • FAX: 86-21-62490635
United Kingdom • sales@mooreind.com
Tel: 01293 514488 • FAX: 01293 536852
Page 4
Specifications and information subject to change without notice.