# A DATABASE APPROACH TO THE SAFETY LIFE CYCLE

Michael D. Scott, P.E.
Principal Safety System Specialist
AE Solutions
P.O. Box 26566
Greenville, SC 29616

Ken O'Malley, P.E.
Principal Control System Specialist
AE Solutions
P.O. Box 26566
Greenville, SC 29616

## KEYWORDS

ANSI/ISA S84.01, Safety Instrumented Systems, Safety Instrumented Functions, Safety Integrity Levels, Safety Lifecycle

## ABSTRACT

A systematic database approach can be used to design, develop and test a Safety Instrumented System (SIS) using methodologies that are in compliance with the safety lifecycle management requirements specified in ANSI/ISA S84.01. This paper will demonstrate that through a database approach, the design deliverables and system configuration quality are improved and the implementation effort is reduced.

## INTRODUCTION

The safety lifecycle per IEC 61508/61511 and ANSI/ISA S84.01 describes the sequence of activities involved in the implementation of a SIS from conception through decommissioning. The safety lifecycle steps pertinent to the development of a SIS are the focus of this paper. Refer to FIGURE 1. Once the process risks are identified and existing protection layers are evaluated, an SIS is implemented to reduce the process risks to a tolerable level. Once installed, the SIS must be functionally tested on some specific frequency per the Safety Requirements Specification (SRS) and the calculated Safety Integrity Level (SIL) requirements. These concepts may seem straightforward enough. A common issue exists, however, in implementing the safety lifecycle on both existing grandfathered systems and on new systems. How can the lifecycle components and functionality be documented and tested with an auditable paper trail in an easy, manageable fashion that supports future Management of Change (MOC) efforts without adding excessive burden to plant staff? This paper illustrates how a database approach can be a very effective answer to this question.

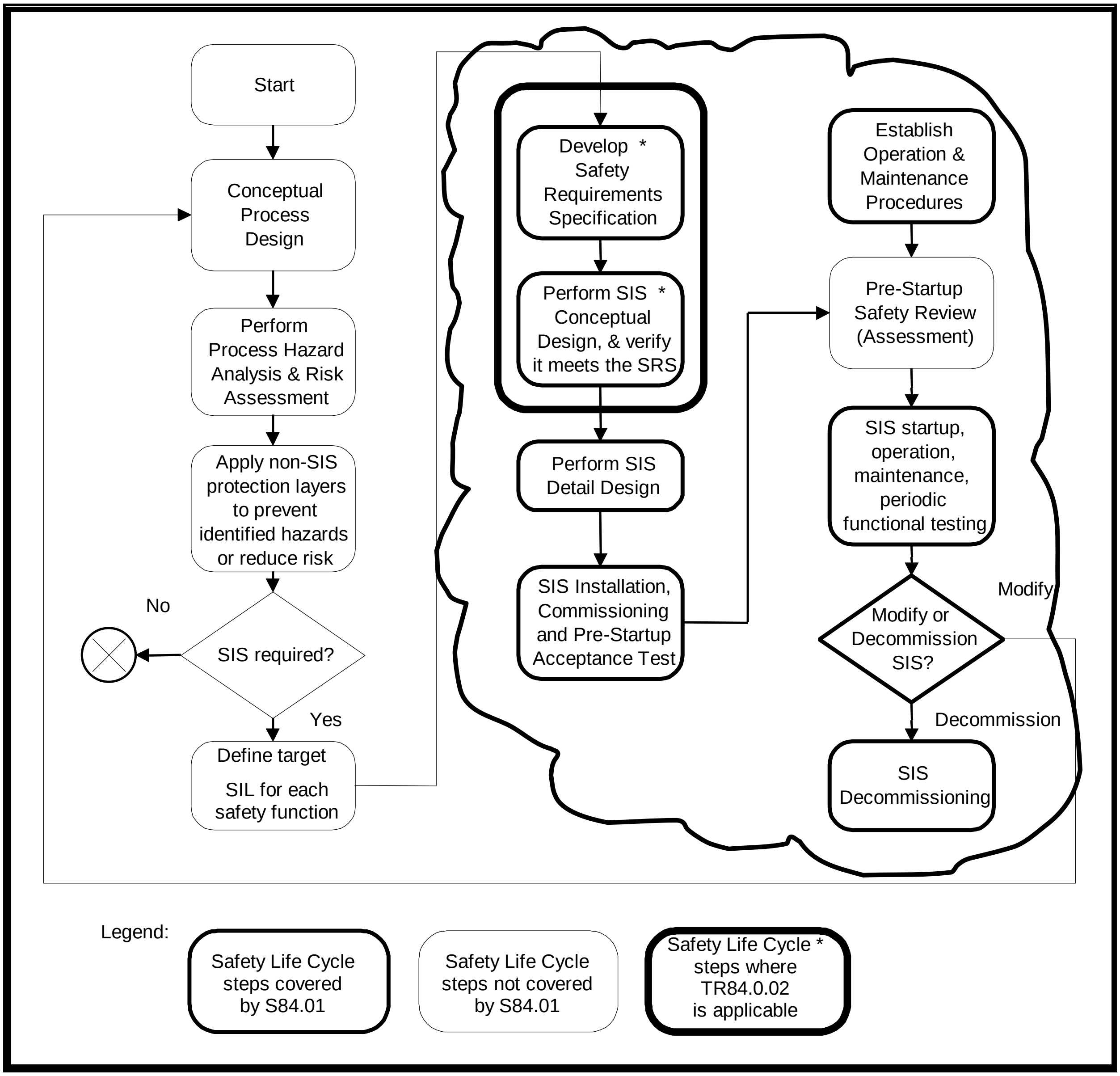

Start
Conceptual Process Design
Perform Process Hazard Analysis & Risk Assessment
Apply non-SIS protection layers to prevent identified hazards or reduce risk
No
SIS required?
Yes
Define target SIL for each safety function
Develop * Safety Requirements Specification
Perform SIS * Conceptual Design, & verify it meets the SRS
Perform SIS Detail Design
SIS Installation, Commissioning and Pre-Startup Acceptance Test
Establish Operation & Maintenance Procedures
Pre-Startup Safety Review (Assessment)
SIS startup, operation, maintenance, periodic functional testing
Modify
Modify or Decommission SIS?
Decommission
SIS Decommissioning
Legend:
Safety Life Cycle steps covered by S84.01
Safety Life Cycle steps not covered by S84.01
Safety Life Cycle * steps where TR84.0.02 is applicable

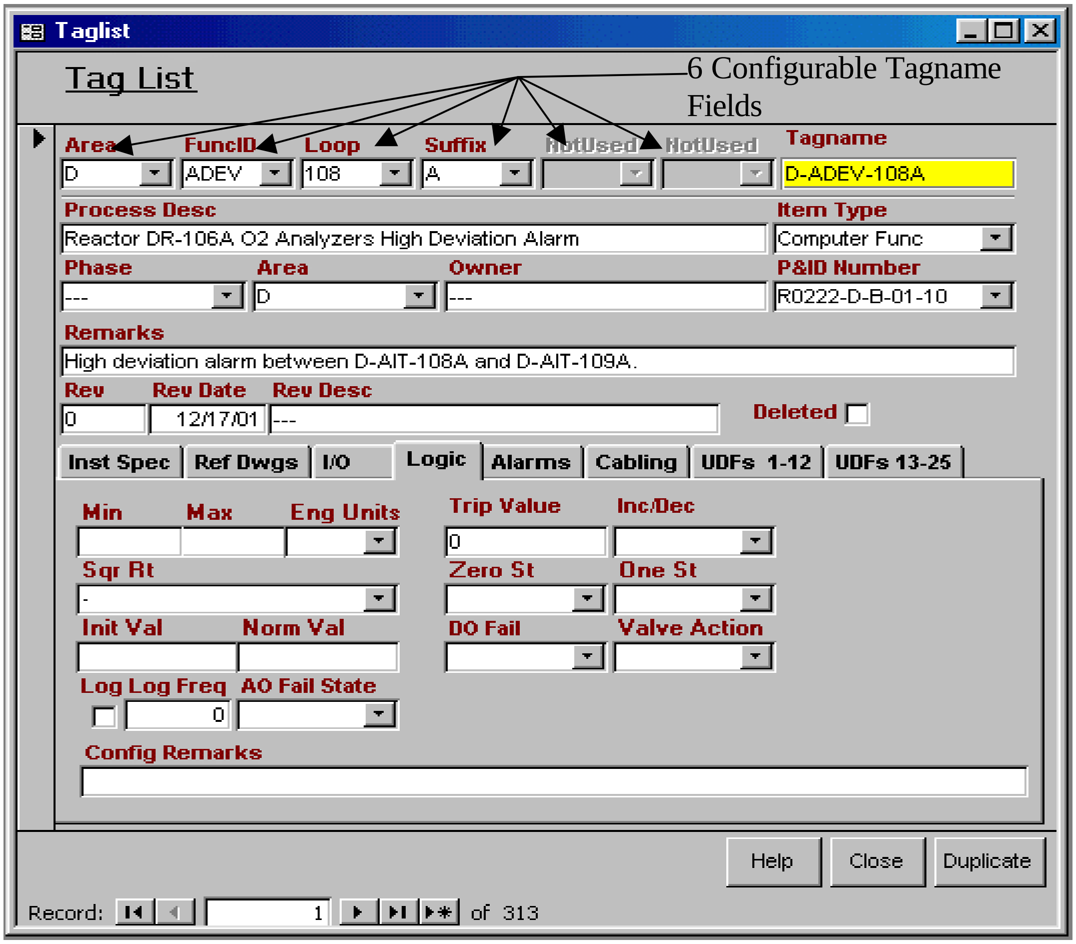
**FIG. 1 - SAFETY LIFECYCLE; STEPS PERTINENT TO SIS ARE CLOUDED (1)**

## DATABASE DESIGN CONSIDERATIONS

### FLEXIBILITY / CUSTOMIZATION

Without question, the most critical decision required when developing a new database application is how much flexibility/customization should be built into the application.  For example, an application developed for use by a system integrator dealing with different SIS manufacturers and different client standards on every project requires a great deal of flexibility and customization.  Whereas an application developed for use by a particular SIS manufacturer or a specific end-user would require less flexibility.  Keep in mind that small increases in flexibility result in exponential increases in initial development effort.  Areas where flexibility considerations should be made are:  the number of and headings of instrument tagname and SIS I/O assignment fields, Safety Instrumented Function (SIF) (also referred to as interlocks in this paper) naming/ numbering conventions, project or plant area designations, project phase designations, on-off state descriptor words, engineering units, alarm groups, and alarm priorities.

Figure 2 is a sample form for inputting information about each tag.  An example of configurable tagnaming fields is illustrated.  The figure shows that a total of 6 tagname fields available in the application but only 4 are used.  The other two are marked as “NotUsed” and are disabled.  So the number of fields used to create a complete tagnumber is configurable up to a total of 6 and the heading for each field is configurable.  The same philosophy could be applied to I/O address assignment fields.



6 Configurable Tagname Fields

Taglist

Tag List

Area: D
FuncID: ADEV
Loop: 108
Suffix: A
NotUsed:
NotUsed:
Tagname: D-ADEV-108A

Process Desc: Reactor DR-106A O2 Analyzers High Deviation Alarm
Item Type: Computer Func

Phase: ---
Area: D
Owner: ---
P&ID Number: R0222-D-B-01-10

Remarks: High deviation alarm between D-AIT-108A and D-AIT-109A.

Rev: 0
Rev Date: 12/17/01
Rev Desc: ---
Deleted □

Min:
Max:
Eng Units:
Trip Value: 0
Inc/Dec:
Sqr Rt: -
Zero St:
One St:
Init Val:
Norm Val:
DO Fail:
Valve Action:
Log □
Log Freq: 0
AO Fail State:
Config Remarks:

Record: 1 of 313

FIG.  2 - TAGLIST FORM FOR CREATING TAGGED POINTS IN THE DATABASE

Read only fields should be shown differently from Read/Write fields – notice the yellow Tagname field in Figure 2. This field is built automatically as the user enters the data for each of the individual tag fields that make up the complete Tagname. The concatenated Tagname is shown for the user's information only and is not directly accessible.

The ability to print reports on subgroups of the complete database is also an important flexibility consideration. The form in Figure 2 shows two fields, Area and Phase, which provide the flexibility search criteria for reporting.

## PICKLISTS

Picklists that limit a user's entries to predefined acceptable values should be used wherever possible. They offer numerous advantages:

- The project team agrees upon the acceptable entries before detailed work begins.
- Reduce the amount of typing required, which reduces the data entry error rate and reduces the data entry time and effort. A tagnumber, for example, is entered only one time - when it is first created.
- Inconsistencies in a multi-user environment are reduced. For example, one user might define a point's engineering units as "psi" and another user might define them as "Psig" and a third might type in all caps "PSIG". Picklists eliminate this variability.
- A listing of valid entries makes data entry for new users more intuitive.

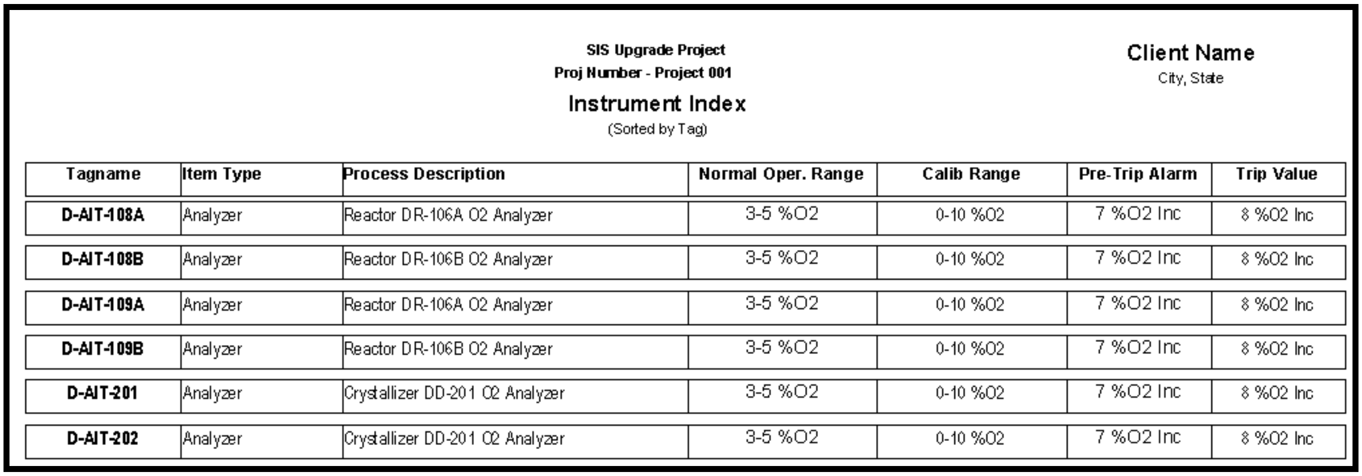
## CASCADED UPDATES AND DELETES

An efficient database application must be constructed modularly. Each module performs a specific function such as an instrument index module, an interlock list module, etc. Each module is linked to the other modules where data sharing is necessary, such as when a tag number from the instrument index module is referenced in the interlocks module. The tagnumber field is the common link between the two modules. It is important to design an application such that changes in a parent module are automatically cascaded down to the child modules. For example, a tagnumber change in the instrument index module should be automatically changed in all modules where that tag is used. Similarly, deletes should be cascaded from the parent module to the child modules. If a tagnumber is deleted from the instrument index module, it should automatically be deleted from all other modules. The user should be asked to confirm the delete before proceeding since significant work in the child modules could be lost with the deletion of the tag.

# DEVELOP SAFETY REQUIREMENTS SPECIFICATION

A database approach can be a very effective means of describing a SIS's functional requirements and the SIL requirements as mandated by S84. In the approach illustrated in this paper there are three separate documents used to comply with all SRS requirements from S84. A text based SRS document is used to define the global, system-wide requirements such as testing frequency, start-up and shutdown sequences, common cause considerations, response time requirements and a description of actions to be taken on loss of energy sources to the SIS. In addition to the textual SRS document, two reports are used to comply with the tag specific and SIF specific requirements. To illustrate how these documents work together, the text-based SRS might state that all valves are fail closed, energize to open, except where noted differently in the Interlock List report. The report then would only have to specify those valves that fail open. It is understood that all others are fail closed.

Figure 3 shows an abbreviated instrument index that includes only those fields necessary for compliance with the S84 mandated SRS, specifically the normal operating ranges and trip values for all analog signals.



SIS Upgrade Project
Proj Number - Project 001

Instrument Index
(Sorted by Tag)

Client Name
City, State

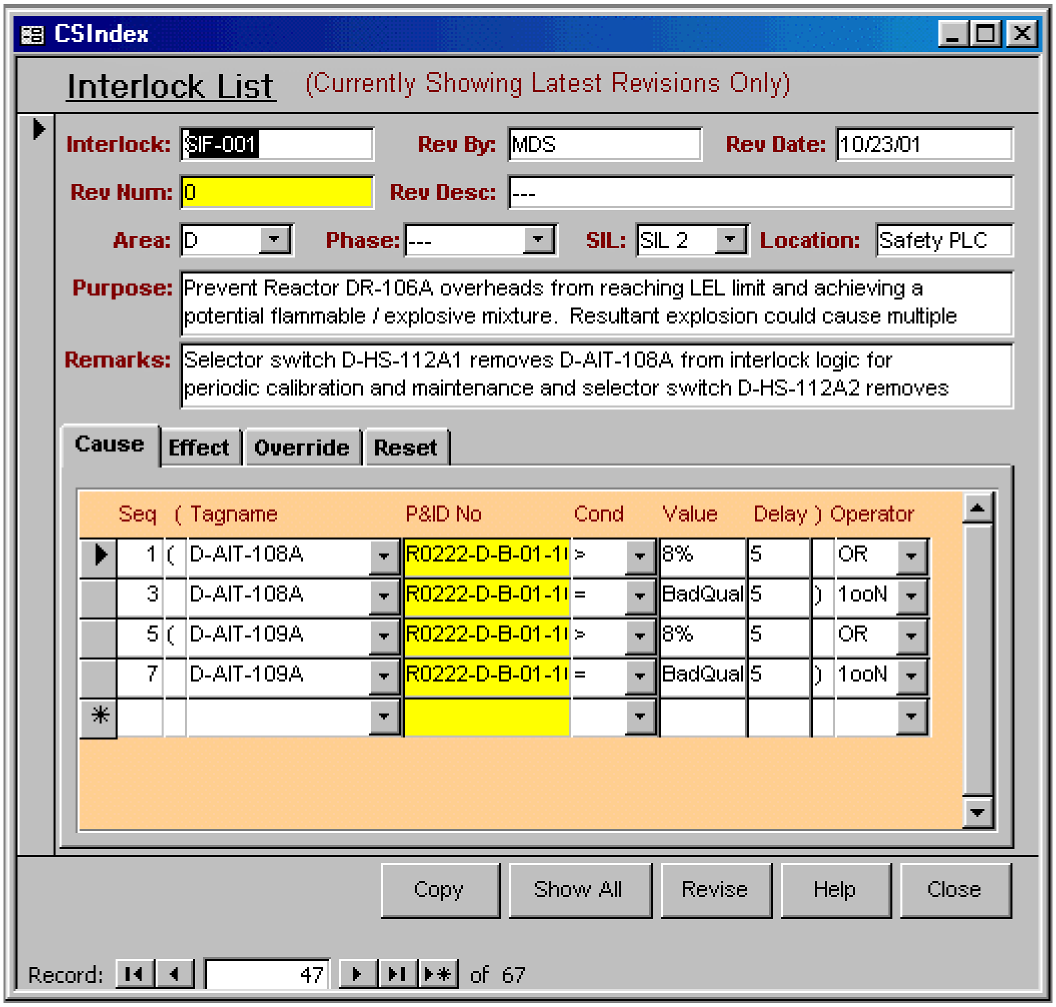
| Tagname | Item Type | Process Description | Normal Oper. Range | Calib Range | Pre-Trip Alarm | Trip Value |
|---|---|---|---|---|---|---|
| D-AIT-108A | Analyzer | Reactor DR-106A O2 Analyzer | 3-5 %O2 | 0-10 %O2 | 7 %O2 Inc | 8 %O2 Inc |
| D-AIT-108B | Analyzer | Reactor DR-106B O2 Analyzer | 3-5 %O2 | 0-10 %O2 | 7 %O2 Inc | 8 %O2 Inc |
| D-AIT-109A | Analyzer | Reactor DR-106A O2 Analyzer | 3-5 %O2 | 0-10 %O2 | 7 %O2 Inc | 8 %O2 Inc |
| D-AIT-109B | Analyzer | Reactor DR-106B O2 Analyzer | 3-5 %O2 | 0-10 %O2 | 7 %O2 Inc | 8 %O2 Inc |
| D-AIT-201 | Analyzer | Crystallizer DD-201 O2 Analyzer | 3-5 %O2 | 0-10 %O2 | 7 %O2 Inc | 8 %O2 Inc |
| D-AIT-202 | Analyzer | Crystallizer DD-201 O2 Analyzer | 3-5 %O2 | 0-10 %O2 | 7 %O2 Inc | 8 %O2 Inc |

**FIG. 3 - ABBREVIATED SIS INSTRUMENT INDEX**

Figure 4 shows the Interlock List form where SIF requirements are defined. The 1ooN notation represents 1 out of N voting scheme shutdown logic. In this example there are two analyzers so N is equal to 2. The Interlock List describes each Safety Instrumented Function (SIF) in detail. Initiators are referred to as Cause Tags. Final control elements are referred to as Effect Tags. Latched interlocks are cleared via the Reset tags, and a SIF's functionality can be bypassed using the Override tags. Parenthetical groupings of tags and operators allow fairly complex logic to be represented in a textual format. Maintaining the correct sort order in the tag listings is crucial. If the tags are listed in an order other than the one in which they were originally entered, the logic statements with the logical operators and parentheses might become nonsensical. Each tag is assigned a SEQ number to assure proper sorting on the form and the report.

Figure 5 shows the Interlock List report and Figure 6 shows a logic diagram representation of the Cause logic for SIF-001 shown in Figures 4 and 5. The reader might note that the same functional logic could have been expressed with one 4-input "OR" gate. The logic was divided into multiple operations for increased flexibility. If a third analyzer were ever added and a 2oo3 voting scheme adopted, the 1ooN operator could be changed to a 2ooN operator with minimal impact to the main logic structure.

Note that highly complex logic, though not typical in a shutdown scheme, may become difficult to represent in the report format shown. In these cases, external logic diagrams outside of the database may be employed. The SIF should still be created in the database, however, and should reference the logic diagram(s). This way, the database remains the central reference document for all SIF functionality.

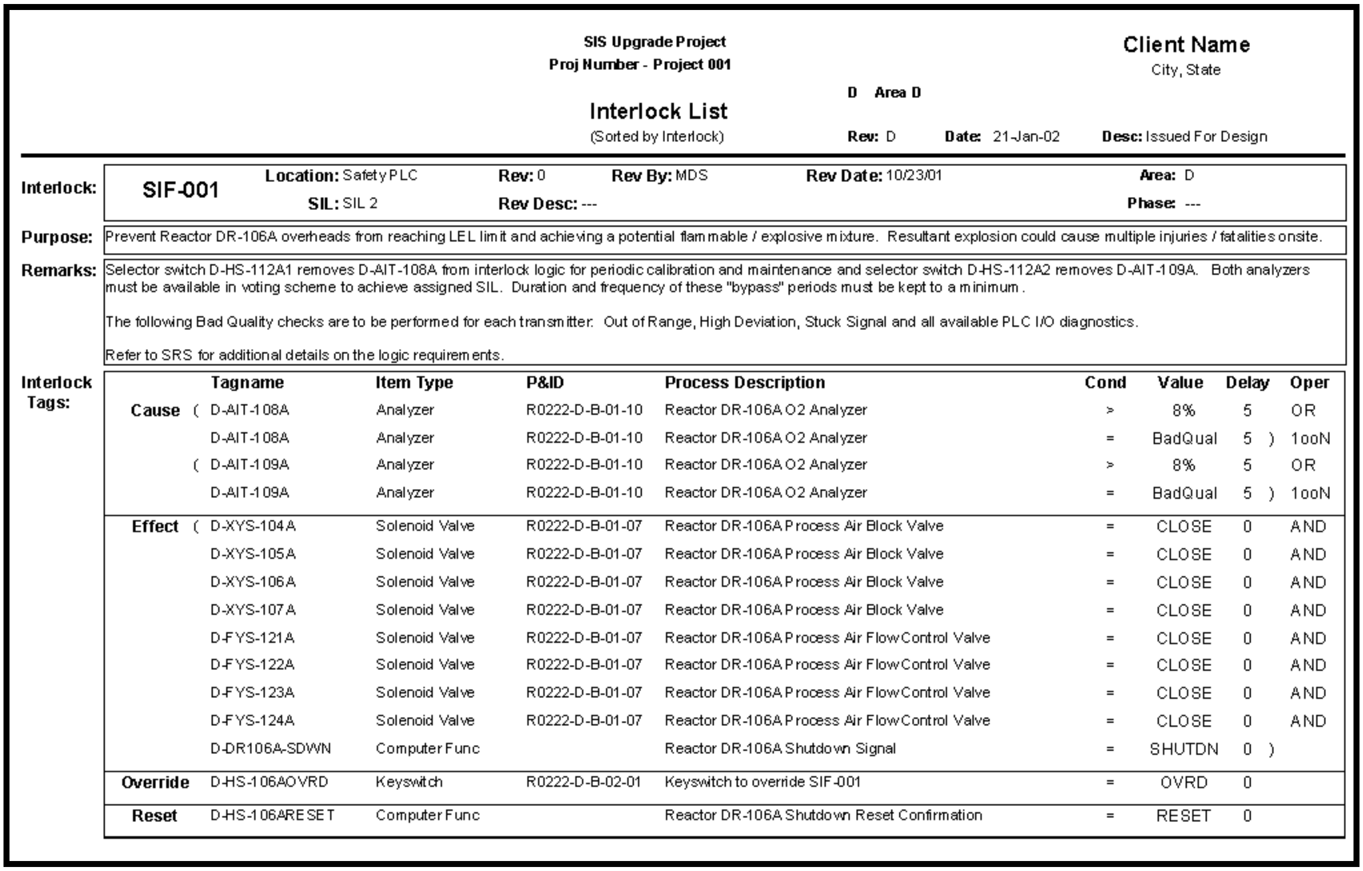


Interlock List (Currently Showing Latest Revisions Only)

Interlock: SIF-001
Rev By: MDS
Rev Date: 10/23/01
Rev Num: 0
Rev Desc: ---
Area: D
Phase: ---
SIL: SIL 2
Location: Safety PLC
Purpose: Prevent Reactor DR-106A overheads from reaching LEL limit and achieving a potential flammable / explosive mixture. Resultant explosion could cause multiple
Remarks: Selector switch D-HS-112A1 removes D-AIT-108A from interlock logic for periodic calibration and maintenance and selector switch D-HS-112A2 removes

| Seq | ( | Tagname | P&ID No | Cond | Value | Delay | ) | Operator |
|---|---|---|---|---|---|---|---|---|
| 1 | ( | D-AIT-108A | R0222-D-B-01-1 | > | 8% | 5 | | OR |
| 3 | | D-AIT-108A | R0222-D-B-01-1 | = | BadQual | 5 | ) | 1ooN |
| 5 | ( | D-AIT-109A | R0222-D-B-01-1 | > | 8% | 5 | | OR |
| 7 | | D-AIT-109A | R0222-D-B-01-1 | = | BadQual | 5 | ) | 1ooN |

FIG. 4 - INTERLOCK LIST FORM



**SIS Upgrade Project**
**Proj Number - Project 001**

**Client Name**
City, State

**D** **Area D**

**Interlock List**
(Sorted by Interlock)

**Rev:** D **Date:** 21-Jan-02 **Desc:** Issued For Design

**Interlock:** SIF-001 **Location:** Safety PLC **Rev:** 0 **Rev By:** MDS **Rev Date:** 10/23/01 **Area:** D
**SIL:** SIL 2 **Rev Desc:** --- **Phase:** ---

**Purpose:** Prevent Reactor DR-106A overheads from reaching LEL limit and achieving a potential flammable / explosive mixture. Resultant explosion could cause multiple injuries / fatalities onsite.

**Remarks:** Selector switch D-HS-112A1 removes D-AIT-108A from interlock logic for periodic calibration and maintenance and selector switch D-HS-112A2 removes D-AIT-109A. Both analyzers must be available in voting scheme to achieve assigned SIL. Duration and frequency of these "bypass" periods must be kept to a minimum.

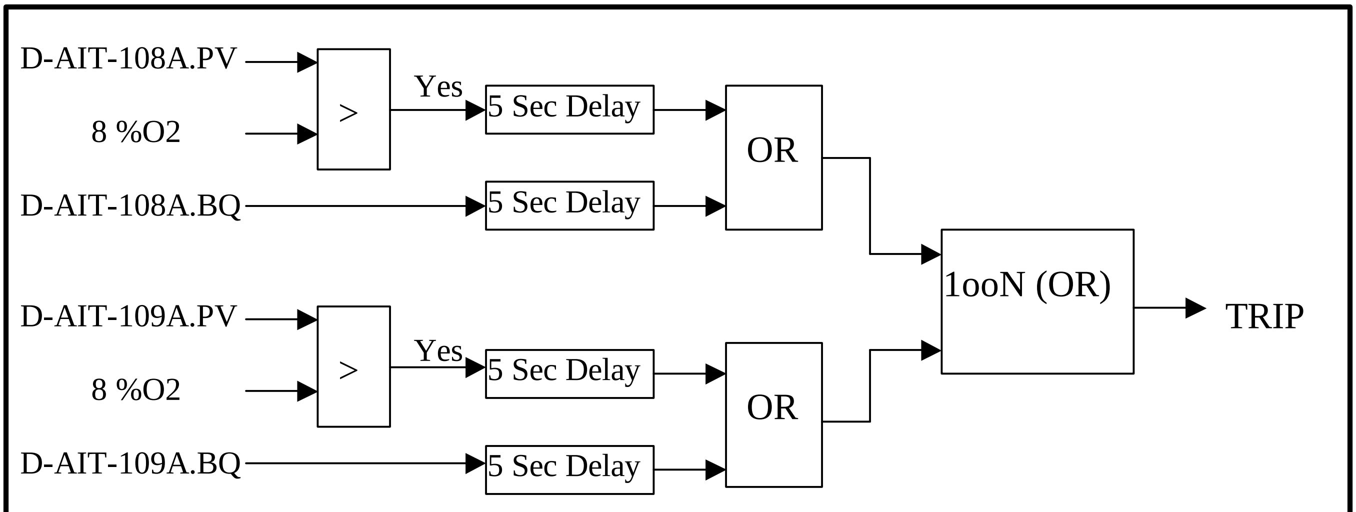
The following Bad Quality checks are to be performed for each transmitter. Out of Range, High Deviation, Stuck Signal and all available PLC I/O diagnostics.

Refer to SRS for additional details on the logic requirements.

**Interlock Tags:**

| | Tagname | Item Type | P&ID | Process Description | Cond | Value | Delay | Oper |
|---|---|---|---|---|---|---|---|---|
| Cause | ( D-AIT-108A | Analyzer | R0222-D-B-01-10 | Reactor DR-106A O2 Analyzer | > | 8% | 5 | OR |
| | D-AIT-108A | Analyzer | R0222-D-B-01-10 | Reactor DR-106A O2 Analyzer | = | BadQual | 5 ) | 1ooN |
| | ( D-AIT-109A | Analyzer | R0222-D-B-01-10 | Reactor DR-106A O2 Analyzer | > | 8% | 5 | OR |
| | D-AIT-109A | Analyzer | R0222-D-B-01-10 | Reactor DR-106A O2 Analyzer | = | BadQual | 5 ) | 1ooN |
| Effect | ( D-XYS-104A | Solenoid Valve | R0222-D-B-01-07 | Reactor DR-106A Process Air Block Valve | = | CLOSE | 0 | AND |
| | D-XYS-105A | Solenoid Valve | R0222-D-B-01-07 | Reactor DR-106A Process Air Block Valve | = | CLOSE | 0 | AND |
| | D-XYS-106A | Solenoid Valve | R0222-D-B-01-07 | Reactor DR-106A Process Air Block Valve | = | CLOSE | 0 | AND |
| | D-XYS-107A | Solenoid Valve | R0222-D-B-01-07 | Reactor DR-106A Process Air Block Valve | = | CLOSE | 0 | AND |
| | D-FYS-121A | Solenoid Valve | R0222-D-B-01-07 | Reactor DR-106A Process Air Flow Control Valve | = | CLOSE | 0 | AND |
| | D-FYS-122A | Solenoid Valve | R0222-D-B-01-07 | Reactor DR-106A Process Air Flow Control Valve | = | CLOSE | 0 | AND |
| | D-FYS-123A | Solenoid Valve | R0222-D-B-01-07 | Reactor DR-106A Process Air Flow Control Valve | = | CLOSE | 0 | AND |
| | D-FYS-124A | Solenoid Valve | R0222-D-B-01-07 | Reactor DR-106A Process Air Flow Control Valve | = | CLOSE | 0 | AND |
| | D-DR106A-SDWN | Computer Func | | Reactor DR-106A Shutdown Signal | = | SHUTDN | 0 ) | |
| Override | D-HS-106AOVRD | Keyswitch | R0222-D-B-02-01 | Keyswitch to override SIF-001 | = | OVRD | 0 | |
| Reset | D-HS-106ARESET | Computer Func | | Reactor DR-106A Shutdown Reset Confirmation | = | RESET | 0 | |

**FIG. 5 - INTERLOCK LIST SHOWING SIF FUNCTIONALITY**



Where .PV is the measured value and .BQ is TRUE when the point is in Bad Quality.

**FIG. 6 – LOGIC DIAGRAM OF CAUSE TAG LOGIC FOR SIF-001**

## COMMISSIONING / PRE-STARTUP ACCEPTANCE / PERIODIC TESTING

The project database, with input and approval from the entire project team, forms the ideal check document(s) for the SIS final design and functionality. The database reports illustrated above can all serve as check documents by adding signoff and approval fields to each record. These fields should be built into the report design and the user is prompted at report run time whether or not the check and approval fields should be "turned on". This provides a permanent, hardcopy record of the checks performed and signoff.

It was mentioned previously under the Flexible Database Design section that the ability to report on subgroups of the total database is important. Nowhere is this flexibility more important than during the testing, commissioning and acceptance phases of a project. It is crucial that the check documents contain only those portions of a project that are of interest to the check team's immediate responsibilities.

Commissioning a new or upgraded control system installation, particularly for larger systems, is simplified by dividing the process into small, independent and somewhat self-contained pieces, known as commissioning packages. The project can then be commissioned and turned over to Plant Operations in a piecemeal fashion rather than all at once. The ability to track each package independently and report on commissioning progress as percent complete is a tremendous benefit.

Meeting calculated SIL requirements usually necessitates periodic testing of SIFs. Risk reduction can be improved with more frequent testing. The sort and query features of a database make it ideal at tracking and performing periodic testing. SIFs can be grouped and sorted by testing frequency. The reports with the check and approval fields "turned on" create an effective roadmap to direct the testing efforts.

## MANAGEMENT OF CHANGE

Keeping up with the small changes made to a facility over its life is arguably one of S84's most difficult mandates. Maintaining up to date documentation is usually low on the list of priorities in the rush to correct a problem or improve a process. This situation is made worse when the data is scattered throughout multiple, independent documents that are not linked together. Conversely, a simple documentation process reduces the maintenance effort and increases the likelihood that the documentation will be kept up to date.

## CONCLUSION

With the amount of "streamlining" and outsourcing in today's market, plant staff is stretched farther than ever. The mandates of S84 will make the problem worse by placing ever-increasing demands on these overworked personnel. An intelligent method of managing the safety lifecycle has never been more important than it is today. A database approach maximizes quality and accuracy of a SIS design and minimizes the effort required both in the up front design and implementation and in the long term with periodic testing and management of change.

## REFERENCES

1. ANSI/ISA-84.01-1996, Application of Safety Instrumented Systems for the Process Industries

2. PIP PCESS001, Process Industry Practices Process Control, Safety Instrumented Systems Guidelines

3. IEC 61508, Functional Safety of Electrical/Electronic/Programmable Safety-Related Systems