

Estimation and Evaluation of Common Cause Failures in SIS

Angela E. Summers, Ph.D., Director
Kimberly A. Ford, Senior Risk Analyst, and Glenn Raney, Technical Specialist
Premier Consulting + Engineering, Triconex Corporation

Published in Chemical Engineering Progress, November 1999.

ANSI/ISA S84.01-1996 and drafts IEC 61508/61511 are standards covering the design, operation, maintenance, and testing of safety instrumented systems (SIS). The standards stress the importance of minimizing potential faults in the SIS through good design and engineering practice. These faults include random hardware, systematic, and common cause faults. Common cause faults occur when a single fault results in the corresponding failure of multiple components, such as a miscalibration error on a bank of redundant transmitters. The frequency of common cause faults is difficult to estimate. The modeling techniques and available failure rate data make the predictive calculations of these failures cumbersome and, sometimes, the results obtained are questionable.

This paper will discuss the methodologies that are currently used to assess common cause faults in SIS. These include qualitative techniques for identifying and reducing the potential for common cause failures and quantitative techniques for including CCF in SIS performance calculations.

Introduction

The new ANSI/ISA S84.01-1996⁽¹⁾ and draft IEC 61508⁽²⁾ standards establish the concept of the safety lifecycle model for designing **safety instrumented systems** (SIS). The SIS consists of the instrumentation or controls that are installed for the purpose of mitigating a hazard or bringing the process to a safe state in the event of a process upset. A SIS is used for any

process in which the process hazards analysis (PHA) has determined that the mechanical integrity of the process equipment, the process control, and other protective equipment provide insufficient risk reduction.

The SIS should be designed to meet the required safety integrity level as defined in the safety requirement specification⁽¹⁾ (safety requirement allocation⁽²⁾). Moreover, the SIS design should be performed in a way that minimizes the potential for common mode or common cause failures (CCF). A CCF occurs when a single fault results in the corresponding failure of multiple components. Thus, CCFs can result in the SIS failing to function when there is a process demand. Consequently, CCFs must be identified during the design process and the potential impact on the SIS functionality must be understood.

Unfortunately, there is a great deal of disagreement among the experts on how to define CCF and what specific events comprise a CCF. The following are often cited⁽²⁾ as examples of common cause faults:

- Miscalibration of sensors
- Pluggage of common process taps for redundant sensors
- Incorrect maintenance
- Improper bypassing
- Environmental stress on the field device
- Process fluid or contaminant plugs valve

But the examination of these faults, in light of any SIS design, will indicate that any of these six examples can disable single I/O systems, as well as redundant I/O systems. However, many of the proposed methodologies^(2,4) for assessing CCF ignore this fact and only penalize redundant sensors and final elements.

For example, miscalibration of redundant sensors is often cited as an important CCF to consider. The miscalibration of a single sensor will cause the SIS to fail just as seriously as the miscalibration of redundant sensors. If the miscalibration is examined from a failure rate standpoint, the following issues would need to be addressed:

- Is the miscalibration a common cause failure? If so, the proposed techniques explicitly account for it only in the case of redundant devices.
- Is this type of failure included in the failure rate data provided in the published databases or in User databases? Miscalibration is already included in the covert, as well as catastrophic, failure rate provided in some published databases. Analysts must be careful not to double-count the associated failure probability.
- Is this a failure that is independent of the device and should be discussed as a separate procedural failure? There are many procedural errors that could be listed, including bypassing, poor maintenance practice, poor testing, etc. The explicit consideration of all of these failures is time consuming and the failure rate data for these is generally non-existent.

The most critical failure is that the safety requirement specification (SRS) is incorrect at the beginning of the design process and the SIS cannot effectively detect the potential incident. This is a most disastrous common cause failure that can directly lead to the hazardous incident that the designer is seeking to prevent. Improper system specification can compromise the entire SIS and is a failure potential that most of the proposed methodologies ignore.

In an effort to ensure that CCFs had been properly addressed in the standard, the IEC 61508 (draft) committee requested an independent evaluation of the current theories on common cause modeling and the availability of failure rate data. This evaluation was performed by Dr. A.M. Wray of the Health and Safety Laboratory, an agency of the Health and Safety Executive. Dr.

Wray concluded in a 1996 report⁽³⁾ to the IEC 61508 committee that “Although IEC 1508 already has mechanisms in place which deal with common-cause failures, it is considered that the current approach is insufficient on its own. It is considered that a more-rigorous qualitative approach, possibly in the form of checklists will make a more viable alternative to modeling.”

The IEC 61508 (draft) committee has taken a quantitative approach to Dr. Wray’s checklist recommendation by developing, with Dr. Wray’s assistance, a methodology for relating specific measures used to reduce potential common cause faults to quantitative factors. While the experts on the standards committee are working to craft a quantitative technique for assessing CCF, the SIS designers need a methodology that does not depend upon the definition of various types of failures. Further, the SIS designer needs techniques that can be readily applied at various stages of the SIS design. The numerical techniques cannot be applied until after most design details have been finalized. Qualitative techniques should be established within a corporation, facility, or design team to ensure that a rigorous, comprehensive review is performed on the SIS design. This review can be performed on a proposed SIS design or on an operational, installed SIS. The primary goal of the review is to ensure that adequate measures have been employed to reduce the potential for failure of the SIS, including failure due to systematic or common cause failure.

Techniques for Evaluating SIS Designs for Common Cause Failure (CCF)

The choice of the evaluation technique is typically dependent on experience of the User with the particular SIS design. This would include documented historical performance of instruments, installation details, and design engineering teams. Experience with the specific application environment is also required, because a device or installation detail that works well in one type of application may not work well in another. For example, standard taps into a vessel for mounting a transmitter may work extremely well in clean service, but may plug very quickly in a

service where solids can deposit. Three qualitative techniques are often used to assess SIS designs:

- 1) Industrial Standards
- 2) Corporate Engineering Guidelines and Standards
- 3) Qualitative Hazard Identification

An overview of each of the techniques is provided below.

Industrial Standards

ANSI/ISA S84.01-1996⁽¹⁾ provides specific SIS design requirements in the mandatory portion of the document. It also provides guidance in the informative annexes in the non-mandatory portion of the document. In addition, draft IEC 61508⁽⁶⁾ provides specific design requirements for safety related systems. The draft standard provides specific measures and techniques that must be applied. Proposed or installed SIS designs can be assessed for agreement with these specific requirements.

While these standards represent a major step forward for the process industry, no general, broad industry standard can incorporate all of the potential caveats in a specific application. The comparison with standards is important, but it is often insufficiently rigorous to ensure that all potential failures in the SIS design are addressed.

Corporate Engineering Guidelines and Standards

To assist the design engineer, many Users develop engineering guidelines and standards (EGS) for the SIS design. The level of detail involved in an EGS is entirely dependent on the commonality involved in the various processes within the User company. The EGS may include approved architectures, device types, vendors, testing frequencies, and installation details. The

EGS should address what is considered good engineering and design practice within the User company.

For Users who have many of the same types of process units, the EGS may be extended to include application standards that list specific architectures, voting, devices, and installation details for each safety function. For example, for a process furnace in a refinery, the trip for low fuel gas pressure may be completely specified in the standard from the use of 2oo3 voting pressure transmitters to a double block and bleed. The architecture description could be enhanced with installation details showing accepted practice for transmitter installation and provisions for maintenance bypassing and testing.

The proposed or installed SIS design can be compared to these internal standards. Deviation from the internal standard can be corrected through revised design or justified through documentation that addresses why this specific application has different requirements. Generally, internal standards are an excellent way to address SIS design, since the User can account for its particular application environment and risk tolerance. The reality is that many Users find it difficult to get agreement within their own company as to what is an acceptable design. After all, someone always seems to have a way to improve on the previous design. There must be a strong internal champion for the EGS to be developed. There must also be a strong ally in upper management to support the auditing process that will be required to ensure that the EGS are used.

Qualitative Hazard Identification Techniques

Qualitative Hazard Identification Techniques have been used for many years to identify potential sources of risk in process units. These techniques require experts, who have extensive experience with the process as well as those with expertise in conducting the various analysis

methods. Typical hazard identification techniques include checklists, what-if analysis, hazard and operability studies (HAZOP), and failure mode and effect analysis (FMEA). Each of these techniques has distinct advantages and disadvantages. Any of the techniques can be modified for use in assessing the SIS. Of the qualitative assessment techniques, the checklist is the most easily adaptable to SIS design evaluation. In fact, checklists are incorporated into many international standards, such as API 14C for the design of safety systems on off-shore platforms.

Checklists

Checklists are simply a list of questions that are answered with “yes,” “no,” or “not applicable” responses. A checklist analysis will identify specific hazards, deviations from standards, design deficiencies and potential incidents through comparison of the design to known expectations, which have been expressed in the checklist questions.

Checklists have historically been used to improve human reliability with respect to design and to ensure compliance with various regulations and engineering standards. Where the quantitative analysis is typically done after the P&IDs are nearly complete, the checklist technique can be applied at any stage of design, e.g. conceptual design, detailed design, or field construction. Checklists can be established for SIS evaluation in general or can be developed for specific applications. Checklists provide the simplest method for the identification of design inadequacies.

While all of these areas cannot be addressed in complete detail in the contents of this paper, an example of a checklist is provided at the end of the paper. This checklist was developed based on the following key areas:

- Engineering Design

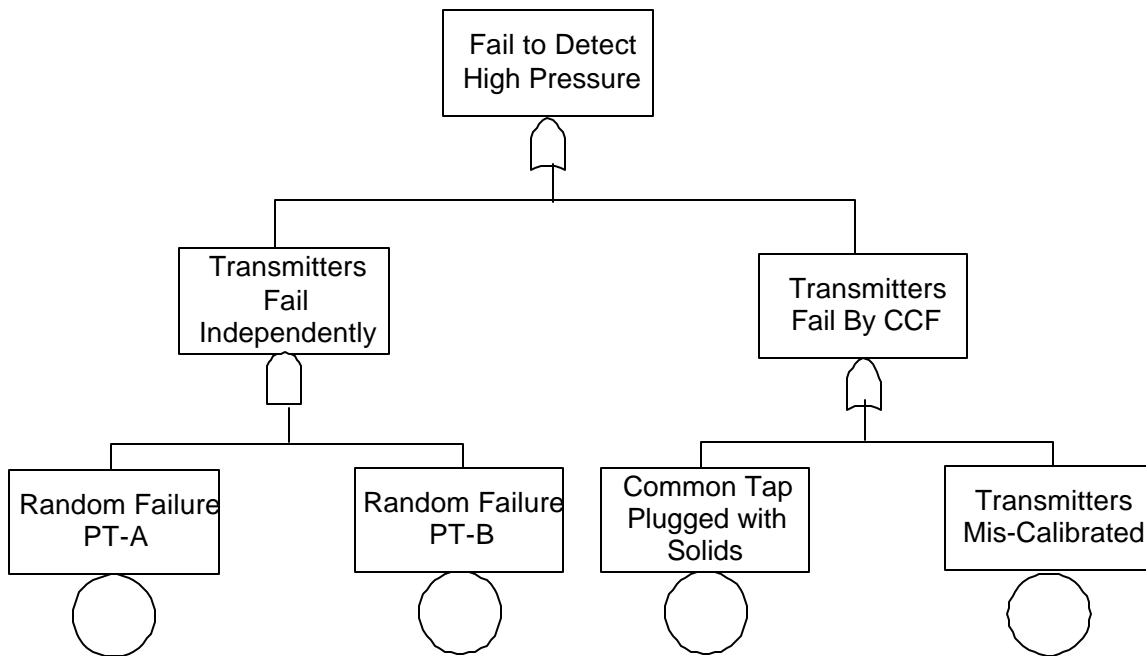
- Safety Requirement Specification⁽¹⁾ (Safety Requirement Allocation⁽²⁾)
- Conceptual Design⁽¹⁾ (Safety Requirement Realisation⁽²⁾)
- Detail Design
- Application Software Design
- SIS Components
 - Logic Solver
 - User Interface
 - Sensors
 - Actuators
 - Final Elements
 - Process Connections
 - Electrical Connections/Conduit/Wire-tray/Junction Boxes
 - Electrical Power
 - Pneumatic Supply
 - Hydraulic Supply
- Environmental
 - Manufacturer's specifications or tolerances
 - Operating specifications
- Operation
- Installation/Maintenance
 - Installation
 - Inspection
 - Testing
 - Maintenance
- Training
- Modification

Quantitative Evaluation of Common Cause Failures

In some cases, it may be necessary to consider the impact of potential common cause failures on the SIS performance. In such cases, the potential common cause failures will need to be considered in the systems quantitative performance evaluation. There are two approaches for addressing CCF, the explicit model and the approximation method.

The Explicit Model is used for common cause failure sources that are specific and well understood. These specific sources of common cause failure are modeled as explicit basic

events during an evaluation using fault tree analysis. The failure rates for these events are estimated using internal data, published data (where available), or a conservative failure rate estimate. Typical examples of CCF, which can be modeled using the explicit approach include loss of shared utilities and the plugging of process taps. The figure below illustrates the use of the explicit model in the evaluation of CCF associated with a set of redundant transmitters.



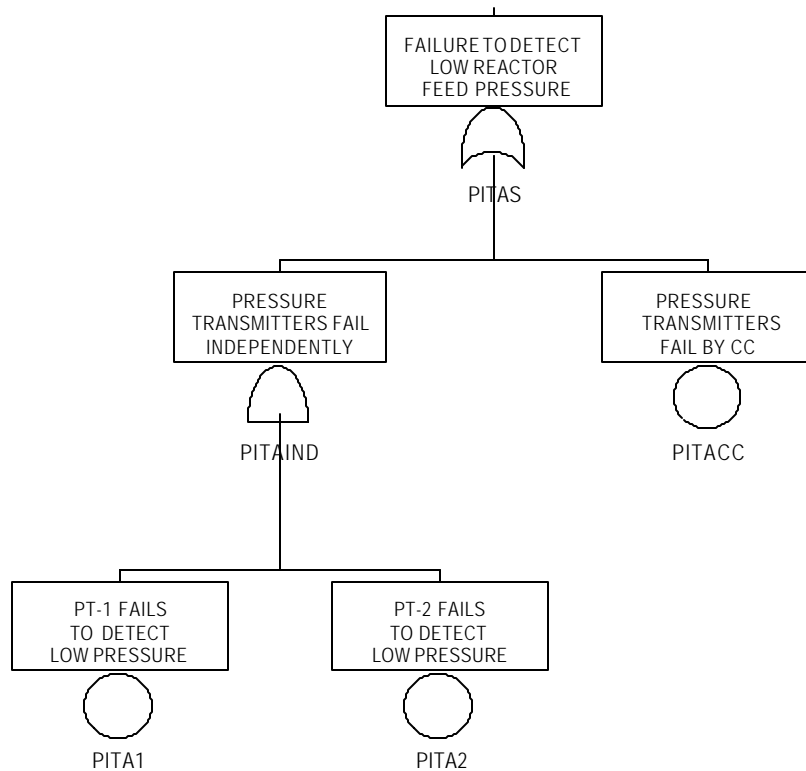
Example of CCF Explicit Model

The approximation method is the more commonly used approach to the quantitative evaluation of common cause failures. In the application of this method, typically called the β Factor Method, the likelihood of a common cause failure is related to the random failure rate for the device. This method makes it possible to evaluate CCFs without identifying the specific sources of dependent failures and their associated probability. The β Factor can be estimated as follows:

- 1) Identify the total failure rate for the device from published or internal data
- 2) Review the failure modes to determine the portion that is expected to have a common cause affect
- 3) Calculate/estimate the percentage of the failure rate that can be associated with CCF (β Factor)
- 4) Use the β Factor to calculate the dependent and independent failure rates for the device.

The figure below illustrates the fault tree model for a set of transmitters when using the approximation method.

Example of Approximation Method



The β Factor can range from nearly zero to up to 25%, depending upon the device and the particular common cause issues under consideration. The estimation of the β factor can be accomplished through either quantitative or qualitative methods. Plant experience can be used to calculate a β factor for a particular device, when good maintenance and inspection records are available. In such instances, the following equation can be used:

$$\mathbf{b} \text{ Factor} = \frac{m}{n + m}$$

where:

n = number of challenges or instances where only a single component failed,

m = number of devices which failed in a set of challenges of instances where multiple similar components have failed.

In instances where sufficient plant data is not available, qualitative methods can be used to estimate the β factor. A number of published sources provide limited guidance on the selection of the β factor based upon expert judgment. These include references (6), (7), (8), and (9). There are also methods for qualitatively estimating a β factor based upon the presence of various common cause concerns. The IEC 61508 (draft) committee has developed a methodology for relating specific measures which may reduce or increase the potential for common cause faults to quantitative factors, X and Y. These X or Y factors are used to determine the overall beta factor for each component. The beta factor is used in conjunction with the random hardware failure rate to calculate a CCF rate for a set of redundant devices. This checklist methodology has been incorporated into draft ISA TR84.0.02 Part 1 Annex A, where it is referenced to IEC 61508. The proposed methodology is still under development and numerous changes are expected prior to final issuance.

Common cause failures can be very significant in the overall system performance evaluation, therefore great care and expert judgment must be used in selecting an appropriate β factor. If the effect of common cause failures is so significant that the overall system performance fails to meet the desired performance target, the techniques discussed earlier in this paper can be employed to identify specific sources of failure and methods to eliminate them.

Conclusions

The new SIS design standards, ANSI/ISA S84.01 and draft IEC 61508, have changed the rules for the design, operation, maintenance, and testing of safety instrumented systems. The consideration of potential common cause failures in sets of redundant devices is an important element which must be addressed in all phases of the SIS life cycle. Qualitative techniques can be applied to evaluate the system design and the procedures associated with the SIS in order to identify and eliminate CCF sources. If significant CCF potential remains, quantitative techniques can be applied to include the effect of dependent failures on the overall SIS performance. It is important that common cause failures are evaluated and eliminated where ever possible, because if overlooked, the protection of the SIS can be compromised.

References

- 1) ANSI/ISA-S84.01-1996 "Application of Safety Instrumented Systems for the Process Industries," Instrument Society of America S84.01 Standard, Research Triangle Park, NC 27709, February 1996.
- 2) IEC 1508, 65A/255/CDV, "Functional safety of electrical/ electronic/ programmable electronic safety related systems—Part 6: Guidelines to the application of parts 2 and 3," International Electrotechnical Commission, Draft, April 13, 1998.
- 3) "Common-Cause Failures in Relation To Programmable Electronic Systems Used for Protection," A. M. Wray, Health and Safety Laboratory, Report to IEC 1508 Committee, August 1996.
- 4) ISA TR84.0.02, "Safety Instrumented Systems (SIS)—Safety Integrity Level (SIL) Evaluation Techniques, Part 1: Introduction," Version 4, Draft, March 1998.
- 5) "Common Cause and Common Sense: Designing Failure Out of Your SIS," A.E. Summers and G. Raney, ISA EXPO 1998, Houston, Texas, October 1998.
- 6) Guidelines for Chemical Process Quantitative Risk Analysis, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, 1989.

- 7) Loss Prevention in the Process Industries, Lees, F.P., Butterworth-Heinemann, Oxford, 1996.
- 8) “Common Cause Fault Rates for Valves: Estimates,” J.A. Steverson and C.L. Atwood, Idaho National Engineering Laboratory, 1982.
- 9) Reactor Safety Study, WASH-1400 (NUREG-75/014), United States Nuclear Regulatory Commission, October 1975.

Example Checklist

Engineering/Design

Safety Requirement Specification (SRS)

Have individuals involved in developing SRS been trained to understand the consequences of common-cause failures?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Was the SRS reviewed by members of the PHA or SIL assignment team?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Was the SRS checked against known standards? (Corporate, domestic and/or international)	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Has the safety integrity level been assigned qualitatively or quantitatively for each safety function?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Was the SRS reviewed by an independent assessor?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA

Conceptual Design

Have individuals involved in developing the conceptual design been trained to understand the consequences of common-cause failures?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Was the conceptual design verified for compliance with the SRS?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Was the conceptual design checked against known standards?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Has the safety integrity level been verified qualitatively or quantitatively for each safety function?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Was the conceptual design reviewed by an independent assessor?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA

Detail Design

Have individuals involved in developing the detail design been trained to understand the consequences of common-cause failures?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Was the detail design developed in accordance with the SRS?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Was the detail design checked against known standards?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are design reviews carried out which include the identification and elimination of common-cause failures?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Has the safety integrity level been verified qualitatively or quantitatively for each safety function?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Was the detail design reviewed by an independent assessor?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA

Application Software

Have individuals involved in developing the application software been trained to understand the consequences of common-cause failures.	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
--	------------------------------	-----------------------------	-----------------------------

Application Software (continued)

Is the final program checked against the SRS?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Is the final program verified through factory acceptance testing that includes fault simulation?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Is the final program verified through complete site acceptance testing that includes verification of startup, operation, and testing algorithms?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA

Safety Instrumented System Components

Logic Solver

Does the logic solver have methods to protect against fail-dangerous faults?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Is the logic solver a fault-tolerant device?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Is the logic solver separated from the Basic Process Control System?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are all SIS functions combined in a single logic solver?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Is the logic solver TUV certified for the application?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Is the application software protected from unauthorized changes?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA

Operator Interface

Is the SIS operation consistent with existing systems and operator experience?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Is adequate information about normal and upset conditions displayed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Do separate displays present consistent information?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are critical alarms obvious to an operator?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are related displays and alarms grouped together?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA

Sensors

Have instrument specification sheets been verified by another party?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Is sensor redundancy employed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
If identical redundancy is employed, has the potential for CCF been adequately addressed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are redundant sensors adequately physically separated?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Does each sensor have dedicated wiring to the SIS I/O modules?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Does each sensor have a dedicated process taps?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Does the configuration allow each sensor to be independently proof tested?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Can redundant sensors be tested or maintained without reducing the integrity of the SIS?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Is diversity used?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are diverse parameters measured?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are diverse means of processing specified?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Is there sufficient independence of hardware manufacturer?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Is there sufficient independence of hardware test methods?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are sensor sensing lines adequately purged or heat traced to prevent plugging?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are SIS sensors clearly identified by some means (tagging, paint, etc.) as components of the SIS?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA

Actuators

Are backup power sources provided?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are manual actuators safely and easily accessible?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA

Final Elements

Have the final elements been checked to ensure proper sizing and application?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Have the final elements been checked to ensure that the device achieves the fail safe condition?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA

Process Connections

Are process connections properly installed to prevent process fouling?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are process connections installed correctly for the device type and process?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are sensor process isolation valves associated with SIS properly marked?			

Electrical Connections/Conduit/Wire-tray/Junction Boxes

Are electrical connections properly made and inspected?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are all SIS conduits/wire-trays properly marked?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are all SIS conduits/wire-trays adequately segregated from non-SIS conduits/wire-trays?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are flexible conduit/cable connections properly made and inspected?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are all conduit covers and gaskets in place?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are all seals poured?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are all SIS junction boxes properly marked?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are all SIS terminations in shared junction boxes adequately segregated from non-SIS terminations?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA

Electrical Power

Is the electrical power source reliable?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Has the consequences of loss of instrument power been considered?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Is there an uninterruptible power supply UPS for the SIS?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Is it periodically tested under load?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are primary and backup supplies powered from independent busses?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Can redundant supplies be taken out of service for maintenance without interrupting SIS operation?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Is the SIS properly grounded?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Is the SIS hardware consistent with the area electrical classification?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are the power supplies adequately protected from ground faults or other voltage disturbances?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA

disturbances?

Pneumatic Supply

- | | | | |
|---|------------------------------|-----------------------------|-----------------------------|
| Is the pneumatic supply source clean and reliable? | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> NA |
| Has the consequences of loss of pneumatic supply been considered? | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> NA |

Hydraulic Supply

- | | | | |
|--|------------------------------|-----------------------------|-----------------------------|
| Is the hydraulic supply source clean and reliable? | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> NA |
| Has the consequences of loss of hydraulic power been considered? | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> NA |

Environmental

- | | | | |
|--|------------------------------|-----------------------------|-----------------------------|
| Have the effects of RFI on the SIS devices been considered? | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> NA |
| Are the devices being used within the manufacturer's environmental specifications? | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> NA |
| Have sources of excessive vibration been eliminated or mitigated? | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> NA |
| Have sources of excessive temperature been eliminated or mitigated? | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> NA |
| Have all SIS component environmental requirements been achieved? | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> NA |

Operation

- | | | | |
|---|------------------------------|-----------------------------|-----------------------------|
| Are the SIS functions in an area that requires frequent operator attention? | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> NA |
| Are operators provided separate, specific SIS procedures? | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> NA |
| Are operators provided specific training relative to the SIS? | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> NA |
| Are operators being evaluated for competency in SIS operation on a regular basis? | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> NA |

Installation/Maintenance

Installation

- | | | | |
|--|------------------------------|-----------------------------|-----------------------------|
| Are the individuals performing the installation trained to understand the consequences of common-cause failures? | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> NA |
|--|------------------------------|-----------------------------|-----------------------------|

Have external causes of CCF been identified (e.g. fire, vehicle impact, lightning, etc.)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are installation procedures in place, followed and supervised?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are SISs segregated from other systems to minimize the probability of external influences causing a simultaneous failure of the systems?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Is there sufficient separation in the installation of diverse equipment?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are special requirements of the design strictly observed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA

Inspection

Are the individuals performing the inspection trained to understand the consequences of common-cause failures?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are the SIS devices being inspected on a regular basis?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are SIS devices being verified against device specification sheets?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA

Testing

Have individuals involved in testing been trained to understand the consequences of common-cause failures?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
If a component fails under test, is the failure cause established to identify manufacturing or design defects?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
If a redundant element fails, do procedures require the inspection of other elements for similar faults?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Is there adequate independence of testing methods for diverse systems?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA

Maintenance

Are the individuals involved in maintenance of the SIS aware of the meaning and importance of common-cause failures?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are maintenance procedures specific to each SIS device used?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are maintenance bypasses alarmed to the control room?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are operators trained on what to monitor when maintenance bypasses are used?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Are maintenance activities related to the SIS prioritized?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA

Training

Have operation and maintenance staff been given SIS specific training?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Were examinations used to verify competency?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Is training updated relative to changes in operation and maintenance procedures?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA

Modification

Is the modification of any part of the SIS covered under management of change procedures?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
Do MOC procedures include the evaluation of how the change could affect the SIL?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA