Standardised Failure Reporting and Classification of Failures of Safety Instrumented Systems

Stein Hauge
Software Engineering, Safety and Security, SINTEF Digital, Norway. E-mail: stein.hauge@sintef.no

Solfrid Håbrekke
Software Engineering, Safety and Security, SINTEF Digital, Norway. E-mail: Solfrid.haabrekke@sintef.no

Mary Ann Lundteigen
Department of Engineering Cybernetics, NTNU, Trondheim, Norway. E-mail: mary.a.lundteigen@ntnu.no

Lars Bodsberg
Software Engineering, Safety and Security, SINTEF Digital, Norway. E-mail: lars.bodsberg@sintef.no

Safety instrumented systems (SISs) implemented on petroleum installations must be highly reliable to protect human life and environment. As of today, monitoring and follow-up of technical status of SIS components require considerable manual effort by extracting and interpreting maintenance and failure data from various systems and sources. Digitalization and increased automation may provide more cost-effective solutions for data collection and thereby provide more time for assessment and implementation of long-term reliability improvement measures. The collection of maintenance and failure data is often subject to concerns about the adequacy, quality, and uncertainty of the data. An important starting point for addressing these concerns is to ensure that failures are registered in a consistent way, with a high level of precision about failure mode, detection method, and failure cause. This paper provides guidance on how to report and classify failure data for follow-up of safety-integrity level (SIL) and possible automation. Suggested standardized taxonomies are given, e.g. by reducing possible choices in reporting and classification. The paper also briefly discusses possible automation possibilities related to failure reporting and classification.

Keywords: Industry 4.0 Reliability and Safety, Safety Instrumented System (SIS), Failure data collection, Oil and gas industry

1. Introduction

Safety instrumented systems (SISs) implemented on petroleum installations must be highly reliable to protect human life, assets and the environment. The collection and application of relevant maintenance and failure data are essential parts of SIS follow-up. The data is used to estimate failure rates for safety-critical equipment for use with quantitative analyses of safety-integrity level (SIL) performance, including the optimizing of proof test intervals. The most suited measures to correct and remove future failures are also decided with basis in information from the failure data collection and classification.

The collection of maintenance and failure data is often subject to concerns about the adequacy, quality, and uncertainty of the data. Furthermore, the failure reporting and classification require considerable manual resources; Hauge et al. (2020). An important starting point for addressing these concerns is to ensure that failures are registered in a consistent way, with a high level of precision about failure mode, detection method, and failure cause. To enable more consistent failure registration and classification, it is important to have a common structure for classification of safety critical equipment.

As a starting point, the ISO 14224 (2016) standard has been applied. The focus of ISO 14224 is on standardized data collection, and different taxonomies for e.g. detection method, failure mode, failure cause and common definitions of safety critical failures are given. The standard however includes limited guidance, examples and explanations on selection of the different parameters, e.g. what is the criteria for choosing a specific failure mode?, what are the suggested failure modes for specific equipment?, how shall the different failure modes be interpreted operational wise? A main objective is therefore to operationalize and simplify the different taxonomies and to provide examples, descriptions and illustrations related to parameter choices.

Whereas some operators apply the standard ISO 14224 codes (with some modifications), other operators have simplified their reporting system by e.g. just applying two different detection methods (e.g. "hidden" versus

Proceedings of the 30th European Safety and Reliability Conference and
the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN: 978-981-14-8593-0; doi:10.3850/978-981-14-8593-0

"revealed") and two different failure modes (e.g. "impaired safety function" versus "other maintenance related failures").

2 Scope

This paper suggests simplified taxonomies and compares these taxonomies with ISO 14224 and other industry practices. The paper suggests a detailed standardised taxonomy for: 1) grouping and classification of SIS equipment and 2) associated attributes that affect the reliability such as failure mode, detection method, and failure cause.

The results are based on work performed as part of an ongoing joint industry project called "Automized process for follow-up of safety instrumented systems" (APOS). A main purpose of this project is to simplify and standardise reporting and classification of SIS failures and to provide a basis for increased automatization and standardisation of SIS follow-up. Important inputs and sources have been reviews of existing reporting practices as well as workshops and meeting with industry experts.

3 Standardised equipment group taxonomy

An equipment group is a collection of equipment types with some common characteristics, such as comparable functionality, design, failure rate, etc. Examples of equipment groups are smoke detectors or blowdown valves.

3.1 Why group equipment?

A grouping of equipment with comparable characteristics into equipment groups is necessary for:

- structuring of failure data; the equipment groups define which failures that can be aggregated and merged for the purpose of estimating equipment failure rates.
- enabling standardised (and equipment specific) taxonomies and automized registration and classification of failures of equipment within a group.
- enabling effective SIL follow-up on a facility (and on a suitable level).
- comparing, merging and analysing data from different facilities and/or operators.
- input to a standardized object model and standardized Information Management System (IMS) applications.

3.2 How to group equipment?

There are two common criteria for defining equipment groups:

- Function of the equipment, i.e. what is the main function of this type of equipment, such as to detect fire or gas, to blow down a vessel, to shut down the well-stream, to measure the level in a tank or to cut the power to normally energized equipment.
- Design of the equipment, i.e. particular design or principle of the type of equipment under consideration, such as sensor diagnostic capabilities, measuring principle (e.g. catalytic or IR detector, displacement or radar level measurement) or valve design (e.g. ball or gate valve).

These two criteria have been aligned to already established industry practices. This means that many equipment groups are organized mainly by function, while others also consider the equipment design.

In addition, the criteria have been aligned with the main principles in ISO/IEC 81346 (2009), which promotes the usage of three main aspects: (1) the function aspect (what the object does or is intended to do), (2) the location aspect (where the object can be found) and (3) the product aspect (how the object is constructed). Aspect (1) and (3) correspond with the two main criteria discussed above (function and design), whereas the location aspect is partly captured by the tag number of the equipment itself, and partly by defining location as a separate level 3 attribute (see next section).

For the purpose of data collection, a practical criterion may also be the need for an adequate size of the equipment group population, since the ability to take decisions based on quantitative analysis, e.g. to update test intervals, relies on statistical confidence of the data.

When estimating failure rates we distinguish between 1) *Site-specific*; calculated for single equipment group at a facility, 2) *Equipment specific*; aggregated for specific equipment models, manufacturer, design principle, etc., across multiple facilities with similar operation and maintenance environment, and 3) *Generic*; aggregated from similar equipment groups at multiple facilities.

3.3 Equipment group hierarchy and attributes

This paper suggests a three-level hierarchy of equipment. (see Table 1). The proposed structure has been derived from analyses of current industry practices, international standards, expert judgements and the identified needs and requirements to the subsequent use of data (e.g. as input to a standardized object-model).

3.3.1 Main equipment groups – level 1 (L1)

L1 represents the grouping of equipment typically sharing a common main functionality. Examples of such functionality are to detect a process upset, to detect hydrocarbons or a fire, to stop the process flow or to facilitate evacuation. This paper suggests a set of predefined detection methods and failure modes for each L1 group.

Typical application for L1: Data collected for equipment groups at L1 may be applied when a rather coarse analysis is needed, but current industry practice does not usually rely on L1 data when evaluating whether the reliability performance and associated functional test intervals are adequate. Instead, L2 (or even L3) data is normally applied, to capture the differences in reliability performance that are due to differences in e.g. design principles and other characteristics.

3.3.2 Safety critical elements – level 2 (L2)

L2 represents the most important characteristics of the L1 equipment groups. For example, the most important characteristics for the gas detectors is what is being measured, is it point or line measurement and what measuring principle is applied? As compared to the L1 group, these safety critical elements (SCEs) will therefore often have a further specified (sub)functionality, e.g. to detect H2S gas, to detect smoke or to shut in and isolate the riser, and some additional design characteristics, e.g. a diesel engine or an electric engine.

Note that barrier elements, equipment (sub-groups), and equipment types are terms often used with the same meaning as SCE.

Typical applications for L2: Failure rates of equipment units within a L2 group will normally be comparable and this level is therefore often appropriate for determining test intervals and performing SIS follow-up. This level of refinement roughly corresponds to the defined barrier elements used by Petroleum Safety Authority Norway (2020) (except for gas detection and fire detection – which corresponds to L1).

3.3.3 Equipment attributes – level 3 (L3)

For additional detailing of the SCE, L3 is represented by a common set of attributes with a foreseen potential to impact the performance and reliability of the equipment within an L2 group. For example, among topside valves, there can be ball valves, globe valves, and gate valves handling fluids of different types, and there are gas detectors located in air intakes versus gas detectors located in open process areas.

For each identified attribute, a list of suggested categories is given. (see rightmost column of Table 1). The attributes considered or expected to have the most impact on the equipment reliability are defined and ticked off for each defined SCE.

Note that the defined L3 attributes also serve the purpose of future data collection and as input to a standardized object-model. As per today it is often difficult to document differences in reliability for specific attributes. For example, for shutdown valves, reliability performance can differ between valves in dirty service and clean service, but sufficient data is often unavailable to quantify such differences. By having designated and predefined attributes for each type of SCE, such reliability differences will be easier to document in the future, e.g. by being able to extract all valves in dirty service (without having to know each specific tag number).

Typical applications for L3:

In many cases it may be desirable with more detailed/differentiated failure rates, both to optimize test intervals and to target preventive measures. L3 enables analysis of possible reliability differences due to the specified attributes and thereby facilitates further differentiation of failure rates (given enough operational experience / size of the L3 group). The specific attributes can be applied as "identifiers" for limited populations of equipment that requires special follow-up.

Definition/description of L3 attributes:

- *Model/manufacturer*: This is considered as a general L3 attribute relevant for all L1/L2 elements
- *Measuring principle:* How the physical entity in some form (e.g. gas, flame, force, mass, volume, etc.) is measured. IEC 61987-1 (2006) has the following general definition of measuring principle "Phenomenon serving as the basis of a measurement".
- *Design/mounting principle*: Design or mounting characteristics related to the SCE, e.g. Thermowell or clamp-on for a temperature transmitter.
- *Actuation principle:* Type and/or design of actuator, e.g. hydraulic or pneumatic, single acting or double acting, etc.
- *Medium properties:* Characteristics/ properties related to the medium that the equipment handles. Three classes of medium properties are considered: Clean service, medium service and dirty service. Examples of dirty services can be scaling, acidity, hydrates, wax, sand, cryogenic, etc.
- *Dimension:* For some equipment types, typically valves, the dimension may

impact on the performance, e.g. large bore valves versus small bore valves.

- *Location/environment:* Physical location/ type of environment in which the SCE operates, e.g. a gas detector located in a weather exposed versus a shielded area, or a manual push button located indoor versus outdoor.
- *Application:* Functional use or purpose of the SCE, e.g. a valve used in emergency shutdown system versus combined emergency/process shutdown system, or an optical point smoke detector used as a pure smoke detector or in combination with a temperature sensor as a multidetector.
- *Diagnostics/configuration:* Describe type of diagnostics implemented and/or how the SCE is configured. Examples are line monitoring (or not) for an instrument, discrepancy alarm (or not) for transmitters, or a circuit breaker with external energy supply to move to safe position versus internally stored mechanical energy (spring forces).
- *Test, maintenance & monitoring strategy:* Type of maintenance, testing and monitoring of SCE (beyond standard functional testing), e.g. if a valve is leakage tested or not, partial stoke tested or not, or if a valve is equipped with condition monitoring facilities (e.g. valve watch) or not.

4 Suggested detection method taxonomy

4.1 Assumptions and justifications

The classification of detection method serves two main purposes:

i. to distinguish between a detected failure and an undetected failure. A detected failure is revealed upon occurrence, typically by online diagnostics or condition monitoring, whereas an undetected failure is a hidden or latent failure that has occurred sometimes in the past and is revealed either by a scheduled activity (e.g. upon testing), or during an unscheduled activity (such as a shutdown or a casual observation).

ii. to consider the effectiveness of different monitoring regimes, e.g. to assess the proportion of failures detected upon testing, the proportion of failures detected by self-diagnostics or to estimate how many failures are detected upon demand.

Note that the first purpose strictly speaking only requires two categories, whereas the second purpose requires a further division of detection method categories.

ISO 14224 has identified ten categories of detection methods. As per today, most petroleum companies apply the ISO 14224 taxonomy (or variants of this) for classifying detection method. This approach suits both purposes, but it has been pointed out that determining the correct ISO category may be difficult. As a result, some companies have implemented simplified schemes, e.g. to classify failures as either "hidden" or "revealed" (corresponding to an undetected or detected failure).

4.2 Suggested taxonomy

In this paper we suggest a flexible taxonomy that serves both detection purposes mentioned above, different company practices and at the same time is compatible with ISO 14224. Based on company needs and preferences, it is possible to either implement several levels (e.g. level D1 and D2), only level D0 (as some companies have already implemented), or only the ISO 14224 taxonomy. (see Figure 1). Note that the greyed-out level D1 and D2 is the preferred solution in this paper, but the suggested taxonomy also includes a mapping towards the hidden/revealed categorisation and the ISO 14224 categories.

5 Suggested failure mode taxonomy

5.1 Introduction

In IEC 61511 (2017), failure mode is defined as the "manner in which failure occurs". A SIS equipment can have several failure modes, either resulting in loss of the safety function of the equipment (e.g. fail to start of a fire pump), a spurious trip (e.g. spurious operation of a gas detector), a degradation of the equipment function where the safety function is however still intact (e.g. a minor internal leakage of an ESD valve), or a failure mode with no (immediate) effect on the equipment function (e.g. noise when closing a valve). In this paper, special attention is given to the failure modes that imply a loss of the defined safety function, but other failure modes are also discussed.

For completeness, failure modes related to loss of containment and loss of Ex-integrity have also been included. It is standard practice in companies to consider such failures as critical, although not critical for the safety function of the equipment as such. An example is a moderate external leakage from a process shutdown valve. The valve may perform its safety function and close upon a demand, but due to the external leakage, the valve will need immediate repair.

5.2 Suggested taxonomy

This paper suggests a taxonomy with limited number of failure modes for each equipment group, i.e. the taxonomy is equipment specific. The idea is that the use of a few, carefully selected failure modes, considered as being the most relevant for an equipment group, will simplify reporting and thereby improve both the amount and quality of failure mode reporting in notifications. Some important premises for the suggested taxonomy include:

i. As for detection method, the suggested failure modes have been arranged at two levels; F1 and F2.
ii. When selecting a level 1 failure mode, the number of relevant failure modes at level 2 will be limited.
iii. The level 2 list of failure modes shall be complete in the sense that the failure modes "Other" or "Unknown" is avoided. If correct failure mode is not found, only the L1 failure mode is reported.

5.2.1 Suggested failure mode hierarchy

Three basic failure modes are suggested at the higher level (F1): (see Figure 2).

- *Dangerous failure – Safety function impaired (SFI)*: Covers all safety critical (i.e. dangerous) failure modes. SFI does not give any detailed information about how the failure occurred, and thus, level 2 (F2) failure modes are necessary to specify more information.
- *Safe/spurious failure (SF):* Covers the failure modes that either causes a spurious operation of the equipment and/or maintains the equipment in a safe state. Note that these failures are not dangerous with respect to the safety function of the equipment but may often be critical for production. To enable more detailing of how these failures appeared, it is necessary to further define level 2 failure modes.
- *Non-critical failure (NONC):* Covers all failure modes that are not safety critical, not safe/spurious (production critical) or do not imply loss of containment or impaired EX protection. They include:
  - *Degraded failure:* The ability of the equipment to carry out the required safety function (or maintain production) is reduced, but still intact. May develop into SFI or SF failure modes.
  - *No effect failure:* No direct effect on the equipment function.

In addition, two "non-functional-safety" related level 1 failure modes have (as discussed above) been included:

- *Loss of containment failure (LOC):* Covers failure modes that are not directly critical for the defined safety function but is however considered critical since loss of containment represents a hazard by itself.
- *Loss of EX protection failure (LEX):* Covers failure modes that are not directly critical for the defined safety function but is critical due to increased ignition hazard.

Note that an additional level 0 (F0) has been added to illustrate the main division between dangerous failures that imply loss of the equipment's main safety function and all other failures. This division also reflects the reporting practice in some companies where focus is mainly on reporting at this level.

Note that it will be fully possible to *only* implement the suggested level 2 in the failure mode hierarchy. This is comparable to the ISO 14224 approach, however with the exception that the number of level 2 choices have been reduced for each equipment group.

5.2.2 Selection of failure mode level 1 – user aid

The selection of correct failure mode at level 1 (F1) is essential to identify the dangerous failures (see Figure 2). To simplify user selection of correct failure mode at this level, a flow diagram / decision tree has been suggested (see Figure 3).

A similar flowchart could be implemented in the maintenance system where the failure modes are registered. Note that when using such a flowchart, the number of failure modes that the user must choose between, will be narrowed down significantly (max. five in this gas detector case).

6 Potential for automation

For failures detected by testing, demands, self-diagnostics, condition monitoring alarms and/or other type of instrument readings, there will be a potential for automatic registration of detection method and failure mode. E.g. for shutdown valves, the valve can be set in test mode and it can automatically be registered whether the valve fails to close (FTC) or whether the response time is excessive (DOP). Similarly, feedback from the limit switches can be used to register 1) a failure to close or open upon demand, and 2) to register spurious operations (SPO) (combined with the cause and effect). Figure 4 illustrates such potential for shutdown valves ("green" failures modes can be automatically registered). Note that with additional instrumentation such as acoustic noise detectors and valve watch to monitor flow characteristics, additional failure modes (e.g. NOI and LCP may be detected (or even predicted in advance).

The failure modes for each equipment group can at level 1 be categorised into dangerous (SFI), safe/spurious (SF) and non-critical (NONC) in addition to LOC failure mode and LEX failure mode. (see Figure 2). By combining this with registered detection method, the failure class dangerous detected (DD), dangerous undetected (DU), safe (S) or non-critical (NONC) can be automatically determined (see Table 2).

Table 2. Determination of failure class

Failure mode (F1)	Detection method		
	Undetected		Detected
	Scheduled activity	Unscheduled activity or event	Diagnosed / immediately detected event
SFI	DU	DU	DD
SF	S	S	S
NONC	NONC	NONC	NONC

Further discussion of automatized determination of failure mode and class is presented by Hauge et al. (2020).

Acknowledgement

The paper presents results from APOS, a joint industry project on automized process for SIS follow-up. The project is supported by the Norwegian Research Council (Project no. 295902) and 11 industry partners representing oil companies, engineering, consultants and vendors of control and safety systems.

References

APOS, https://www.sintef.no/prosjekter/automatisert-prosess-for-oppfolging-av-instrumenterte-sikkerhetssystemer

Hauge, S., S. Håbrekke and M.A. Lundteigen (2020). *Standardised failure reporting and classification of SIS failures in the petroleum industry.* SINTEF Report.

Hauge, S. and M. A. Lundteigen (2008). G*uidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase*. SINTEF Report A8788.

Hauge, S., T. Kråkenes, P. Hokstad, S. Håbrekke and H. Juin (2013). *Reliability Prediction Method for Safety Instrumented Systems, PDS Method Handbook*. SINTEF Report A24442.

Håbrekke, S., S. Hauge, and T. Onshus (2013). *Reliability Data for Safety Instrumented Systems, PDS Data Handbook.* SINTEF Report A24443.

ISO 14224 (2016). *Petroleum, petrochemical and natural gas industries — Collection and exchange of reliability and maintenance data for equipment,*

IEC 61511 (2017). *Functional safety - Safety instrumented systems for the process industry sector*

IEC 61987-1 (2006). *Industrial-process measurement and control - Data structures and elements in process equipment catalogues*

IEC 81346 (2009). *Industrial systems, installations and equipment and industrial products - Structuring principles and reference designations*

Rausand, M (2014). Reliability of Safety-Critical Systems. Theory and Applications. John Wiley & Sons.

Petroleum Safety Authority Norway, *Trends in risk level (RNNP).* https://www.ptil.no/en/technical-competence/rnnp/. Accessed 2020-02-05

Table 1. Example of Equipment grouping for process transmitters, extract from Hauge et al. (2020)

Main Equipment groups – L1	**Safety Critical Elements (subgroups) – L2**	**Equipment attributes – L3**									**Equipment attribute categories and *Comments***
		Measuring principle	**Design/mounting principle**	**Actuation principle**	**Medium properties**	**Dimension**	**Location/ Environment**	**Application**	**Diagnostics / Configuration**	**Test, maintenance & monitoring strategy**	
Process transmitters	General – all process transmitters				x				x		**Medium properties:** clean service, medium, dirty service **Diagnostics:** Internal diagnostics: Range checking Y/N, Input filtering Y/N, Trip point HH; LL or HH&LL. External diagnostic Y/N: discrepancy alarm with reference transmitter vs no external diagnostic
	Pressure transmitters	x	x								**Measuring principle:** Capacitance, inductance, strain gauge, frequency, force, displacement, etc. **Design/mounting principle:** Absolute (bara), gauge (barg), differential (bar).
	Level transmitters	x	x								**Measuring principle:** gamma, capacitive, weight, hydrostatic, displacement, buoyancy, ultrasonic, radar, laser/optical, capacitive, vibration, etc. **Design/mounting principle:** Direct mounted, capillary, measurement chamber (float), line of sight (radar), rod (profiler), off-vessel (gamma), etc.
	Temperature transmitters	x	x								**Measuring principle:** Resistance, thermocouple, expansion, etc. **Design/mounting principle:** Thermowell, clamp-on
	Flow transmitters - volume	x	x								**Measuring principle:** Displacement, turbine, ultrasonic, differential pressure (flow orifice, venturi), rotameter, electromagnetic, vortex shedding, coriolis, etc. **Design/mounting principle**: Inline, off-line

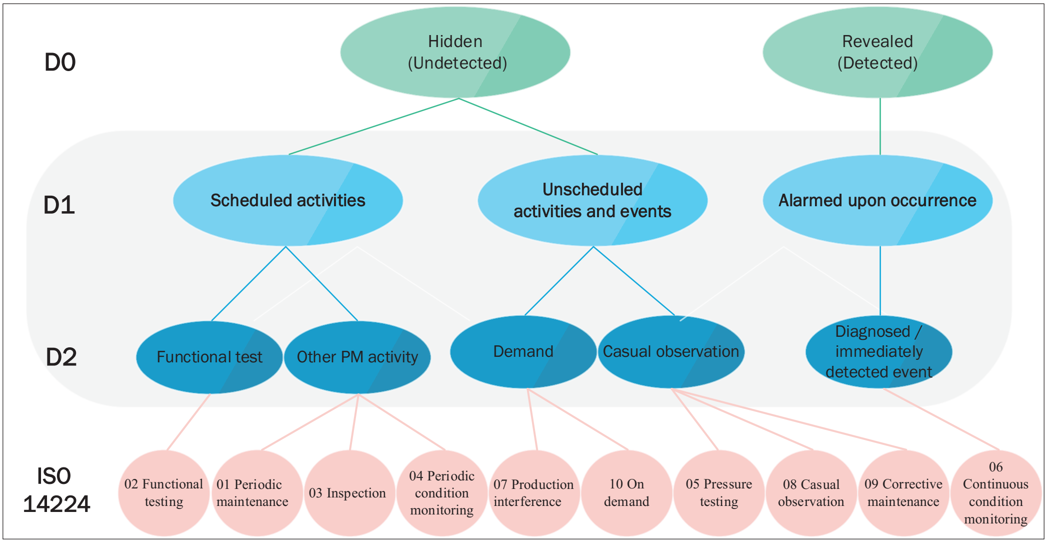


Fig. 1. Suggested (in grey) detection method hierarchy and mapping towards alternative categorisation schemes

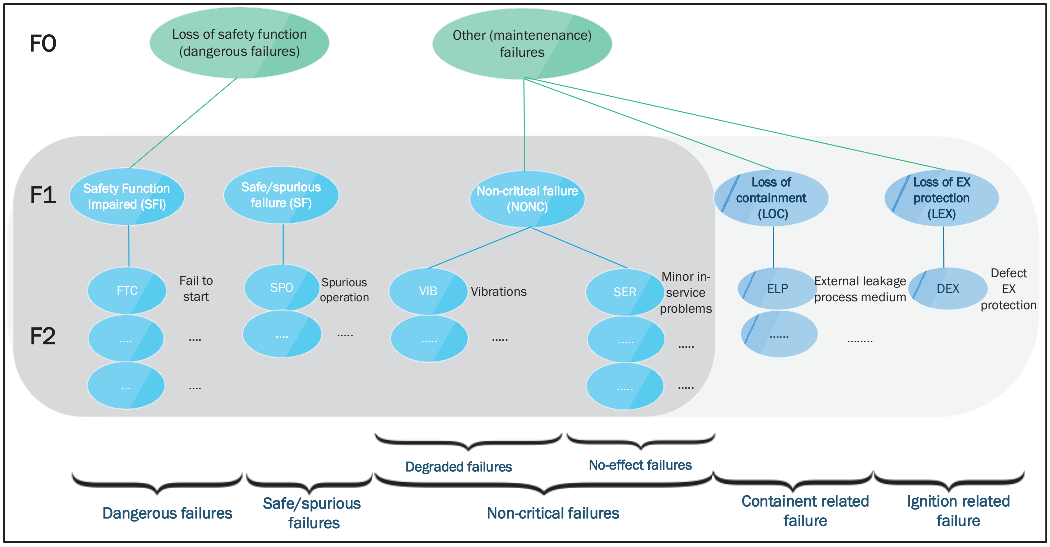
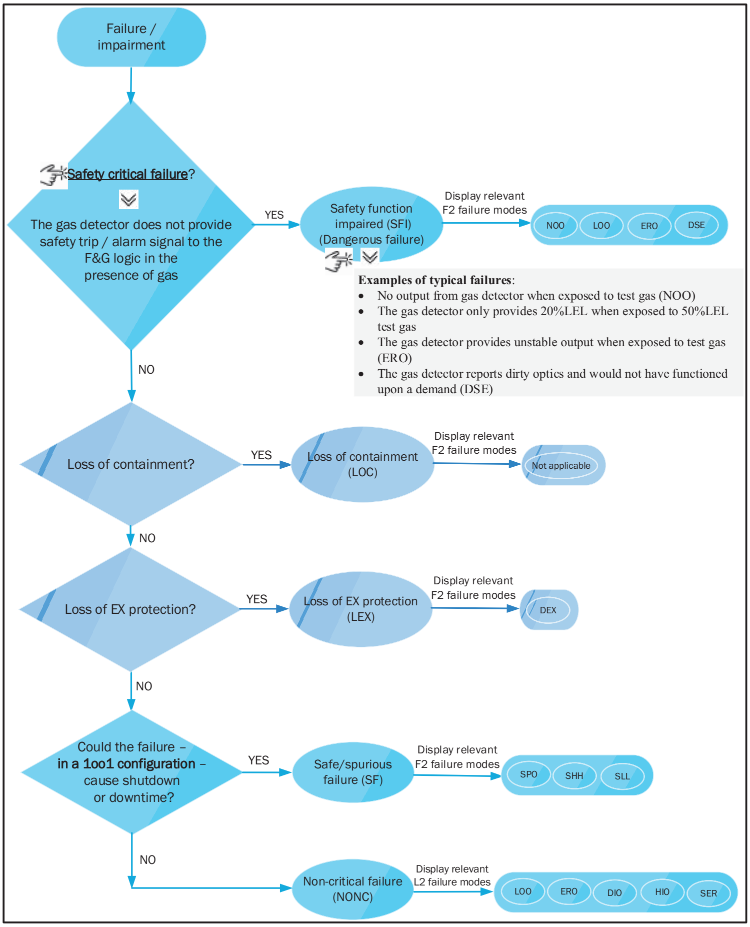

F0
Loss of safety function (dangerous failures)
Other (maintenance) failures
F1
Safety Function Impaired (SFI)
Safe/spurious failure (SF)
Non-critical failure (NONC)
Loss of containment (LOC)
Loss of EX protection (LEX)
F2
FTC
Fail to start
SPO
Spurious operation
VIB
Vibrations
SER
Minor in-service problems
ELP
External leakage process medium
DEX
Defect EX protection
Degraded failures
No-effect failures
Dangerous failures
Safe/spurious failures
Non-critical failures
Containent related failure
Ignition related failure

Fig. 2. Suggested (in grey) failure mode hierarchy – general illustration applicable to safety instrumented systems


Failure / impairment
Safety critical failure?
The gas detector does not provide safety trip / alarm signal to the F&G logic in the presence of gas
YES
Safety function impaired (SFI) (Dangerous failure)
Display relevant F2 failure modes
NOO
LOO
ERO
DSE
NO
Loss of containment?
YES
Loss of containment (LOC)
Display relevant F2 failure modes
Not applicable
NO
Loss of EX protection?
YES
Loss of EX protection (LEX)
Display relevant F2 failure modes
DEX
NO
Could the failure – in a 1oo1 configuration – cause shutdown or downtime?
YES
Safe/spurious failure (SF)
Display relevant F2 failure modes
SPO
SHH
SLL
NO
Non-critical failure (NONC)
Display relevant L2 failure modes
LOO
ERO
DIO
HIO
SER

Examples of typical failures:

- No output from gas detector when exposed to test gas (NOO)
- The gas detector only provides 20%LEL when exposed to 50%LEL test gas
- The gas detector provides unstable output when exposed to test gas (ERO)
- The gas detector reports dirty optics and would not have functioned upon a demand (DSE)

Fig. 3. Flow diagram for determination of failure mode at level 1 (IR gas detector example)

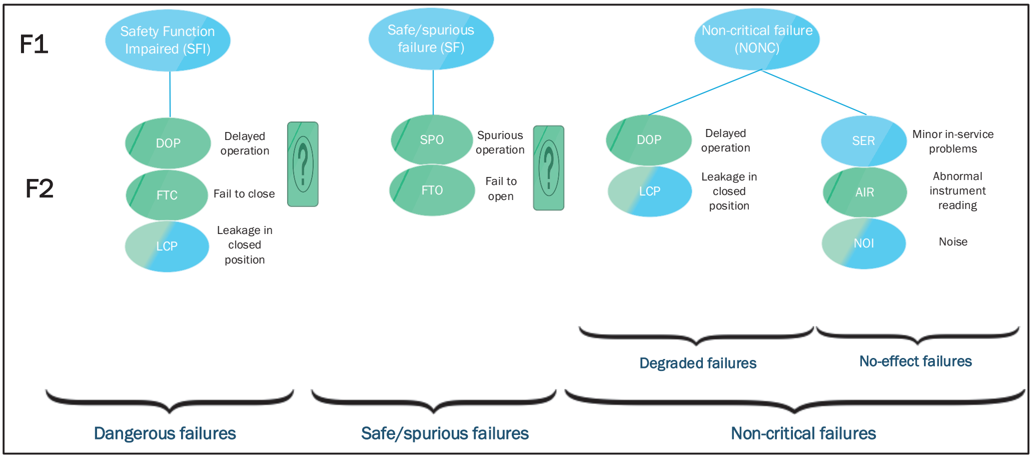


Fig. 4. Illustration of potential for automatic registration of shutdown valve failure modes