MANUAL

CLASSIFICATION AND IMPLEMENTATION OF INSTRUMENTED PROTECTIVE FUNCTIONS

DEP 32.80.10.10-Gen.

July 1996

DESIGN AND ENGINEERING PRACTICE

PREFACE

DEP (Design and Engineering Practice) publications reflect the views, at the time of publication, of:

Shell International Oil Products B.V. (SIOP)
and
Shell International Exploration and Production B.V. (SIEP)
and
Shell International Chemicals B.V. (SIC)

The Hague, The Netherlands,

and other Service Companies.

They are based on the experience acquired during their involvement with the design, construction, operation and maintenance of processing units and facilities, and they are supplemented with the experience of Group Operating companies. Where appropriate they are based on, or reference is made to, national and international standards and codes of practice.

The objective is to set the recommended standard for good design and engineering practice applied by Group companies operating an oil refinery, gas handling installation, chemical plant, oil and gas production facility, or any other such facility, and thereby to achieve maximum technical and economic benefit from standardization.

The information set forth in these publications is provided to users for their consideration and decision to implement. This is of particular importance where DEPs may not cover every requirement or diversity of condition at each locality. The system of DEPs is expected to be sufficiently flexible to allow individual operating companies to adapt the information set forth in DEPs to their own environment and requirements.

When Contractors or Manufacturers/Suppliers use DEPs they shall be solely responsible for the quality of work and the attainment of the required design and engineering standards. In particular, for those requirements not specifically covered, the Principal will expect them to follow those design and engineering practices which will achieve the same level of integrity as reflected in the DEPs. If in doubt, the Contractor or Manufacturer/Supplier shall, without detracting from his own responsibility, consult the Principal or its technical advisor.

The right to use DEPs is granted by SIOP, SIEP or SIC, in most cases under Service Agreements primarily with companies of the Royal Dutch/Shell Group and other companies receiving technical advice and services from SIOP, SIEP or SIC. Consequently, three categories of users of DEPs can be distinguished:

1) Operating companies having a Service Agreement with SIOP, SIEP, SIC or other Service Company. The use of DEPs by these Operating companies is subject in all respects to the terms and conditions of the relevant Service Agreement.

2) Other parties who are authorized to use DEPs subject to appropriate contractual arrangements.

3) Contractors/subcontractors and Manufacturers/Suppliers under a contract with users referred to under 1) or 2) which requires that tenders for projects, materials supplied or - generally - work performed on behalf of the said users comply with the relevant standards.

Subject to any particular terms and conditions as may be set forth in specific agreements with users, SIOP, SIEP and SIC disclaim any liability of whatsoever nature for any damage (including injury or death) suffered by any company or person whomsoever as a result of or in connection with the use, application or implementation of any DEP, combination of DEPs or any part thereof. The benefit of this disclaimer shall inure in all respects to SIOP, SIEP, SIC and/or any company affiliated to these companies that may issue DEPs or require the use of DEPs.

Without prejudice to any specific terms in respect of confidentiality under relevant contractual arrangements, DEPs shall not, without the prior written consent of SIOP and SIEP, be disclosed by users to any company or person whomsoever and the DEPs shall be used exclusively for the purpose for which they have been provided to the user. They shall be returned after use, including any copies which shall only be made by users with the express prior written consent of SIOP and SIEP. The copyright of DEPs vests in SIOP and SIEP. Users shall arrange for DEPs to be held in safe custody and SIOP or SIEP may at any time require information satisfactory to them in order to ascertain how users implement this requirement.

All administrative queries should be directed to the DEP Administrator in SIOP.

NOTE: In addition to DEP publications there are Standard Specifications and Draft DEPs for Development (DDDs). DDDs generally introduce new procedures or techniques that will probably need updating as further experience develops during their use. The above requirements for distribution and use of DEPs are also applicable to Standard Specifications and DDDs. Standard Specifications and DDDs will gradually be replaced by DEPs.

TABLE OF CONTENTS

APPENDICES

1. INTRODUCTION

1.1 SCOPE

This DEP, which is a revision of the DEP of the same number dated December 1994, specifies requirements and gives recommendations for classifying Instrumented Protective Functions and implementing them.

1.2 DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS

Unless otherwise authorised by SIOP and SIEP, the distribution of this DEP is confined to companies forming part of the Royal Dutch/Shell Group or managed by a Group company, and to Contractors and Manufacturers/Suppliers nominated by them (i.e. the distribution code is "F" as defined in DEP 00.00.05.05-Gen.).

This DEP is intended for use in oil refineries, chemical plants, oil and gas production facilities and supply/marketing installations.

If national and/or local regulations exist in which some of the requirements may be more stringent than in this DEP the Contractor shall determine by careful scrutiny which of the requirements are the more stringent and which combination of requirements will be acceptable as regards safety, environmental, economic and legal aspects. In all cases the Contractor shall inform the Principal of any deviation from the requirements of this DEP which is considered to be necessary in order to comply with national and/or local regulations. The Principal may then negotiate with the Authorities concerned with the objective of obtaining agreement to follow this DEP as closely as possible.

1.3 DEFINITIONS

1.3.1 General definitions

The **Contractor** is the party which carries out all or part of the design, engineering, procurement, construction, commissioning or management of a project or operation of a facility. The Principal may undertake all or part of the duties of the Contractor.

The **Manufacturer/Supplier** is the party which manufactures or supplies equipment and services to perform the duties specified by the Contractor.

The **Principal** is the party which initiates the project and ultimately pays for its design and construction. The Principal will generally specify the technical requirements. The Principal may also include an agent or consultant authorised to act for, and on behalf of, the Principal.

The word **shall** indicates a requirement.

The word **should** indicates a recommendation.

1.3.2 Specific definitions

Demand
A process or equipment condition or event which requires the Instrumented Protective Function to take action to prevent a Hazardous Situation.

Failure
Actual performance falls short of specified performance.

Final Element
A device or combination of devices that manipulate a process variable or attract the attention of the operator to achieve risk reduction. The Final Element includes output cards or output relays, solenoid valves and cabling. Examples are valves, switchgear (rotating equipment stop circuits) and alarms.

NOTE: In the first issue of this DEP the term Actuator was used, but this caused confusion with valve actuators.

Frequency of Demand
The frequency at which Demands occur. Dimension ($time^{-1}$).

Hazardous Situation
The potential to cause harm, including ill health and injury, damage to property, products or the environment, production losses or increased liabilities.

Hazard Rate
The frequency at which Hazardous Situations occur. Dimension ($time^{-1}$).
Hazard Rate = Frequency of Demand * Probability of Failure on Demand

Initiator
A device or combination of devices that indicates whether a process or equipment item is operating outside the operating envelope. The Initiator includes input cards and input relays. Examples are manual switches, position switches and measurement systems (including process connections, sensors, transmitters, cabling, trip amplifiers or input cards etc.).

Instrumented Protective Function
A function comprising the Initiator function, Logic Solver function and Final Element function for the purpose of preventing or mitigating Hazardous Situations.

Instrumented Protective Function Class
Unrevealed Failure class I, II, III, IV, V, VI and X, plus Revealed Failure class F or N detailing the requirements for an Instrumented Protective Function.

Instrumented Protective System
The electromechanical, electronic and/or programmable electronic Logic Solver component of the Instrumented Protective Function, complete with input and output equipment.

Logic Solver
The portion of an Instrumented Protective Function which performs the application logic function. The Logic Solver excludes trip amplifiers, input cards and output cards. Examples are electromechanical relays, solid-state/magnetic-core logic and the Central Processing Unit (CPU) section of programmable electronic systems.

Mitigation
Makes a consequence less severe or relieves consequences.

Permissive
The result of a check on whether or not a combination of conditions is healthy, to allow the Logic Solver to proceed with the next step in a sequence.

Probability of Failure on Demand
The probability of the Instrumented Protective Function failing to respond to a Demand. Dimensionless.

Process Safety Time
The period of time in which the process can be operated without protection and with a demand present, without entering a Hazardous Situation. Dimension (time).

Revealed Failure
A failure whose occurrence is inherently apparent.

Revealed Failure Robust
A configuration in which plant availability is not jeopardised by the Revealed Failure of a single IPF component.

Risk
The Hazard Rate multiplied by the consequence of a Hazardous Situation.

Trip
An Instrumented Protective Function action to bring the Final Element(s) to a safe state.

Unrevealed Failure
A failure which is dormant in the Instrumented Protective Function and can only be revealed when the system has to perform a certain action or through testing.

Unrevealed Failure Robust
A configuration in which plant safety is not jeopardised by the Unrevealed Failure of a single IPF component.

1.4 ABBREVIATIONS

AK	Anforderungsklasse (requirement class)
CAPEX	Capital expenditure
CPU	Central processing unit
DCS	Distributed control system
DIN	Deutsche Industrie Norm (German industrial standard)
ESD	Emergency shutdown
FGS	Fire gas and smoke detection and protection system
FLD	Functional logic diagram
HAZOP	Hazard and operability study
HSE	Health, safety and environment
IEC	International Electrotechnical Commission
IPF	Instrumented protective function
IPS	Instrumented protective system
MOS	Maintenance override switch
MVC	Measurement validation and comparison
NDE	Normally de-energised
NE	Normally energised
NRV	Non-return valve
OOS	Operational override switch
OPEX	Operational expenditure
PC	Personal computer
PEFS	Process engineering flow scheme
PFD	Probability of failure on demand
PLC	Programmable logic controller
SER	Sequence of events recorder
SIL	Safety integrity level
TSO	Tight shut off
TÜV	Technischer Überwachungsverein (German body, translates to Technical Inspection Agency).
	NOTE: Throughout this DEP, reference to TÜV means either TÜV Bayern or TÜV Rheinland.
USD	United States Dollars
UZ	Tag numbering system to indicate IPF group
VDU	Visual display unit

1.5 CROSS-REFERENCES

Where cross-references to other parts of this DEP are made, the referenced section number is shown in brackets. Other documents referenced in this DEP are listed in (10.).

2. GENERAL

Instrumented Protective Functions are implemented on the basis of:
- the requirements laid down in design books;
- proper and proven engineering design;
- experience;
- results of HAZOP studies and technical desk HSE reviews.

A formal classification method is required to:
- Remove uncertainties regarding the safety integrity, cost effectiveness and availability of IPFs for present and new designs and installations.
- Provide an audit trail and thus traceability.
- Ensure that designs are of a suitable technical standard but not over-engineered.
- Form a basis for maintenance strategies such as test frequencies.

Summarising, this DEP is intended to guide users to a safe, cost effective and consistent design, implementation and maintenance strategy for IPFs.

Application of the IPF classification methodology should, for existing plants, be justified by a management directive to have fit-for-purpose IPFs with minimum manpower. For new projects it is justified by the project requirement to have a fit-for-purpose, cost effective design.

For existing plants, it is not possible to justify a classification exercise on the basis of reduction in manpower as it is impossible to indicate before performing the exercise whether or not the existing installation is fit-for-purpose in terms of safety.

The classification methodology described in this DEP is developed based on the German standard DIN V 19250 and the work done by IEC Sub-Committee 65A, see IEC/65A draft 1508, and has been tested by SIOP and SIEP on real process unit cases. For a report of this test, see MF 95-0020.

Where applicable, local authority or insurance company approval shall be obtained to apply the method of classification and implementation described in this DEP.

This DEP shall not be used to justify replacement of relief valves by IPFs.

The term "safeguarding" is used in this DEP only when it relates to Instrumented Protective Functions as well as to protective equipment of a mechanical nature such as non-return valves, relief valves and bursting disks.

3. INSTRUMENTED PROTECTIVE FUNCTIONS CLASSIFICATION METHODOLOGY

3.1 BACKGROUND

The initial risk in operating a process unit or a piece of equipment can be reduced by facilities other than an IPF, such as increased wall thickness for high pressure protection, resulting in an intermediate risk. See Figure 1. If this intermediate risk is lower than a tolerable risk, an IPF is not required. If the intermediate risk is higher than a tolerable risk, an IPF is required to reduce the risk. Such a tolerable risk level is determined by sound current practice.

A protection system can be mechanical (relief valves, bursting discs, etc.) and/or instrumented (IPF). In most SIOP and SIEP designs both types of protection systems are applied, with the mechanical system being the last line of defence wherever possible.

The requirement for an IPF results from proper design practices which are checked by the technical desk HSE review or the HAZOP study. This DEP provides a methodology to classify these IPFs. It is not intended to replace the quantitative risk assessment, technical desk HSE review or the HAZOP study.

The consequence of an IPF failing on demand is discussed during a technical desk HSE review or a HAZOP study and is also one of the basic inputs to the classification methodology. The classification exercise could therefore be an extension of a technical desk HSE review or a HAZOP study.

The full process of classification and implementation of IPFs is indicated in Figure 2 and Figure 3. Comparison of these two figures shows that the classification methodology described in this DEP removes the requirement to provide a tolerable hazard rate for each IPF, and removes the requirement for accurate calculation of the frequency of demand on each IPF.

3.2 THE CLASSIFICATION PROCESS

3.2.1 General

The IPF classification and implementation methodology should be applied during development of the PEFSs and the safeguarding narratives, i.e. during the Basic Design and Engineering Package (BDEP) or Project Specification phase.

Following the technical desk HSE review or HAZOP study, a comprehensive IPF classification exercise shall be performed.

The IPF classification and implementation methodology can also be applied to existing plants, generating the benefits as described in (2.).

A well-developed issue of the following documents shall be available to the team performing the classification:
- process and utility engineering flow schemes (PEFSs);
- safeguarding memorandum with process safeguarding flow schemes (PSFSs);
- safeguarding narratives;
- cause and effect matrices.

Controls which protect process units or equipment from operating outside the operating envelope, such as minimum flow control and maximum or minimum pressure control, are not IPFs. It is therefore not required to classify these controls. If present, alarms and switch functions related to these controls shall be classified.

Appendix 1 gives suggestions on how to set up a classification exercise.

3.2.2 IPF classification team

The team performing the IPF classification shall be kept small. Competent personnel responsible for the subjects of process technology, process safety, operations and process control shall form the team. Other disciplines, e.g. rotating equipment specialists, shall be consulted as required, e.g. when the IPFs of a compressor are classified.

A facilitator shall be appointed. The task of the facilitator is to guide the team through the classification steps and to ensure that every step is recorded to the satisfaction of all team members before the next step is dealt with.

The facilitator shall be familiar with the classification methodology as described in (3.) and (4.).

3.2.3 IPF and loop

An IPF consists of the initiating, logic solver and final element functions. Alarms, not related to automatic trips, and switching functions are also considered IPFs.

An IPF loop consists of the hardware, initiator, IPS or, in the case of alarms, DCS and final element and the utilities such as power and instrument air supply required to perform the IPF.

NOTES:
1. The hardware and software implementation of the IPF is by one or more IPF loops.
2. An IPF may consist of a combination of IPF loops. For example a backflow protection function may consist of low flow and low differential pressure initiators and two valves.
3. For permissives, valves or rotating equipment stop circuits are not necessarily the final element; the logic solver may be the final element.
4. In the first issue of this DEP the term IPF loop was used for both IPF and IPF loop.

The classification shall be performed for each IPF. For an IPF consisting of one initiator and one final element this is straightforward. Functions shall be extracted as indicated in Figure 4 and Figure 5. With more than one initiator function and more than one final element function, a combination of these two figures shall be applied.

Independent functions with a common initiator or a common final element shall be classified

individually assuming the other functions are operating properly.

It shall be noted that the logic solver may consist of more than one UZ block. For example, a recycle gas low flow trip that trips the compressor and, via the compressor and feed pump UZ blocks, also trips the feed pump.

As a starting point it may be taken that, in addition to alarms, every 'x' on the cause and effect matrix is a function. This is not valid for functions consisting of more than one initiator or more than one final element. To ensure that all functions have been classified, the classification report shall be checked against the final functional logic diagrams.

To save time required for classification, the IPFs to be classified should be identified and the IPF identification section of the classification report, see Figure 8, should be completed before the team convenes for the classification exercise.

The number of IPFs to be classified if UZs are connected together as shown in Figure 6, can grow dramatically. Figure 6 also shows how the classification effort can be reduced. It is beneficial to prepare this type of diagram, known as a "spider diagram", giving an overview of all IPFs in a unit, as preparation for a classification exercise.

3.2.4 IPF classification procedure

3.2.4.1 General

The classification methodology is split into two parts:
- classification of IPF unrevealed failures (failures on demand, which are safety related);
- classification of IPF revealed failures (often called 'nuisance' or 'spurious' failures, which are related to economics).

The classification of IPF unrevealed failures is further split into:
- consequences related to personnel safety;
- consequences related to production and equipment loss;
- consequences related to the environment.

The basis of the classification methodology is the risk diagram related to personnel safety published in DIN V 19250. Applying this risk diagram to an IPF results in a requirement class (AK class) for that function. AK classes, however, are not easily translated to implementation requirements for IPFs.

The DIN risk diagram was adopted by IEC/SC65A draft 1508, in informative annex D, which uses Safety Integrity Levels (SILs) as the result of applying this diagram. These SILs are related to Probability of Failure on Demand ranges. These PFD ranges can be applied to calculate whether the implementation and maintenance strategy results in an IPF of sufficient integrity.

NOTE: The informative annex D in IEC/SC65A draft 1508 indicates a general risk graph implementation and an example. The example is the same as the DIN V 19250 version but with heavier weighting of the more severe consequences, and has been selected for this DEP with minor changes.

The IEC/SC65A draft 1508 relates the SIL not only to probabilistic PFD requirements, but also gives deterministic requirements which, as far as applicable, have been incorporated in this DEP.

Risk diagrams have been added in this DEP for production and equipment loss and for environmental consequences. Although the added risk diagrams are not related to IEC/SC65A draft 1508, they shall not be changed without the approval of the Principal.

In line with the risk diagrams, diagrams to classify IPF revealed failures are also included in the methodology promoted in this DEP.

The full IPF classification methodology is indicated in Figure 7.

All IPFs, including alarms, shall be classified.

Classification of pre-alarms is not required. For pre-alarms it shall be confirmed that corrective operator action to avoid the IPF action is feasible. If this is not the case, the pre-alarm may be deleted. The result of this confirmation shall be recorded, preferably in the classification report.

NOTE: It may not always be apparent that operator action is feasible. If, for example, an IPF action (pre-alarm) would occur if a controller setpoint is increased too much, operator action to avoid another IPF action (shutdown) is feasible by reducing the setpoint again.

3.2.4.2 Consequences

The consequences of IPF failure on demand and IPF revealed failure shall be recorded as general descriptions. The descriptions shall be clear and unambiguous, such that another expert is able to follow the reasoning for selecting the routes in the risk diagrams described in the next sections.

If the failure on demand of an IPF has multiple consequences, all consequences shall be classified and the most stringent IPF class shall be selected for that function. If the demand has different causes, the consequences of failure on demand will usually be different as well, requiring a classification for all causes and consequences.

Attention shall be paid to the fact that the location of a plant may have an impact on the consequences, e.g. the difference between onshore and offshore production installations, manned and unmanned operation, close to or far from the fence.

For permissives used in batch processes and sequences, two types of failures are relevant:
- The permissive indicates that the conditions are safe to proceed while the actual conditions are not safe to proceed. This failure is an unrevealed failure in terms of classification. The consequence shall be described under consequence of failure on demand.
- The permissive indicates that the conditions are not safe to proceed while the actual conditions are safe to proceed. This failure is a revealed failure in terms of classification. The consequence shall be described under consequence of revealed failure.

3.2.4.3 Unrevealed failures

3.2.4.3.1 Frequency of demand

A demand on an IPF may be caused by instrument malfunction, operator error, etc.

After recording the consequences, the first question to be answered by the classification team is: how often is the IPF activated (W classification)? The IEC/SC65A draft 1508 describes the frequency of demand in qualitative terms: very low, low and relatively high. This DEP has added quantitative demand frequencies.

The following rules are applicable:
- With proper control and when the dynamic behaviour of the process is known, the frequency of demand may be taken as W2.
- A classification of W1 requires a special justification describing why it is so low. IEC/SC65A draft 1508 indicates that the control system that is the basis of such a low frequency of demand shall be a safety-related system fulfilling all requirements laid down for these systems in IEC/SC65A draft 1508. This is not the case for SIOP or SIEP supported DCS systems. Effective W reduction as described below does not fall under this rule.
- Another description for W1 is that a demand on the IPF may happen, but in a typical unit it is unlikely to happen during the lifetime of the unit.
- In batch processes valves are closed and opened frequently by the batch controller. Situations exist where a certain valve position is a permissive to proceed with a next step, because starting the next step with the valve in another position would give a hazardous situation. The frequency of demand is not the frequency of the valve close commands, because a real demand is present only when the batch controller fails to signal the valve to move to the safe position or the valve fails to move to the safe position. The frequency of demand shall therefore be taken as W2.
- It may be taken into account that one NRV used in a clean and non-corrosive duty reduces the frequency of demand on a backflow protection system typically by a factor of 10, and two different makes and types of NRVs in series reduce the frequency of demand typically by a factor of 50. The latter is not a factor 100 because of common mode failures not related to make and type. Note that NRVs are considered safety-related, but the IEC/SC65A draft 1508 does not detail requirements for these external risk reduction facilities.

NOTE: It is assumed that the small leakage of an NRV can be accommodated by e.g. a fire relief valve.

- If the potential consequence occurs in less than one in ten of the demand cases the frequency of demand may be reduced by one level. The maximum number of effective W reduction steps is 1.

  EXAMPLE: A furnace explosion due to sub-stochiometric firing occurs in less than 10% of the demand cases; the frequency of demand on the sub-stochiometric firing IPF is W2, which may effectively be reduced to W1.

3.2.4.3.2 Personnel safety

To classify the IPF related to personnel safety, the following three questions shall be answered:

(i) What is the potential extent of human injury per demand if the IPF fails on demand, i.e. when a hazardous situation occurs? If there is no injury (S0), the IPF is not required regarding personnel safety and this part of the classification is finished. Any other S-value leads to a next step in the personnel safety risk diagram. If there is the remotest chance that two persons may die (i.e. if it cannot be excluded that the person may be accompanied by a second person), S2 should be selected.

(ii) What is the duration of presence of the person(s) who may be injured in the area affected by the possible hazardous situation? A2 shall be selected when the person(s) are likely to be present at the time of the hazardous situation, e.g. the demand occurs during local manual start or the hazardous situation may occur after the person(s) have arrived on the scene to investigate a developing abnormal situation. For S1 and S4 this step is not required.

(iii) What are the possibilities for the person(s) who may be injured to avert the hazardous situation? This step is only required for S2. Note that the possibility to avert a hazardous situation should not be uprated from G2 to G1 on the assumption that the person will wear personal protective equipment, unless it is certain that the protective equipment will be worn. Usually, systems are designed on the assumption that the use of such equipment is not absolutely required to achieve a sufficient degree of safety, although it is recognised that it can improve safety still further.

If the result of the classification is S0, the IPF is not required for personnel safety. For other results, following the risk diagram along the lines of S, A and G, the IPF class for the function related to personnel safety can be obtained from the relevant W column.

3.2.4.3.3 Production and equipment loss

A diagram is provided in Figure 7 to classify production and equipment loss.

A more detailed description of the potential production and equipment loss (L) selections is indicated below. Damage refers to direct hardware replacement and repair cost and also to consequential losses due to down time.

L0 - No operational upset or no damage to equipment.
Not sufficient upset or damage to justify an alarm, e.g.:
  - Little or no upset or damage at all.
  - A failure of the controller will result in an alarm elsewhere.

L1 - Minor operational upset or minor damage to equipment.
Minor operational upset, e.g.:
- Off-spec product.
- Relief case of medium quantity.

Minor damage to equipment, e.g.:
- Cavitation of a conventional pump on low suction level.
- Longer term moderate or major damage to essential or non-essential equipment, allowing ample time (minimum one day) for operator action.

L2 - Moderate operational upset or moderate damage to equipment.
Moderate operational upset, e.g.:
- Upset in a utility affecting other units such as liquid in an off-gas stream to the fuel gas system.
- Relief case of a large quantity or relief case of medium quantity of highly valuable products.

Moderate damage to equipment, e.g.:
- Overpressure resulting in minor loss of containment (e.g. gasket leaks) if the IPF is the final protection because the installation of a mechanical relief device is not possible or practical.
- Cavitation of a spared high speed or multi-stage pump.

L3 - Major operational upset or major damage to equipment.
Major operational upset, e.g.:
- An immediate large relief case that would cause violent high energy release such as vapour breakthrough from high to low pressure, e.g. hydroprocessing units, high pressure solvent treating units etc.
- Process fluid overflow.
- Solidification of product in a large unheated piping system requiring major corrective action.
- Non-costly repair required of essential unspared equipment.

Major damage to equipment, e.g.:
- Costly repair required of major spared equipment or non-essential equipment.

L4 - Damage causing major loss of containment or damage to essential equipment causing major economic loss.
Damage causing major loss of containment (rupture), e.g.:
- Excessive over-temperature such as exotherms and runaway reactions.
- Over-pressure resulting in major loss of containment if the IPF is the final protection because the installation of a mechanical relief device is not possible or practical.

Damage to essential equipment which from a damage point of view is similar to L1, L2 or L3, but could cause a major economic loss (millions of US Dollars) due to the disabling of essential unspared equipment for an extended repair or replacement period, e.g.:
- Suction vessel high level IPF on a recycle gas compressor.
- Low suction level IPF of a multistage, high speed HCU feed pump.
- Furnace or boiler protection.

NOTE: For extreme economic losses, the IPF class may be increased by one step to ensure an appropriate cost-benefit ratio.

If the result of the classification is L0, the IPF is not required for production and equipment loss. For other results, the IPF class can be obtained from the diagram by selecting the point corresponding to the L and W.

3.2.4.3.4 Environment

A diagram is provided in Figure 7 to classify environmental consequences.

A more detailed description of the potential environmental consequence (E) selections, is indicated below:

E0 - No release or release with negligible damage to the environment.
No release at all or a very minor release that is below the environmental quality standard, not even justifying an alarm, e.g.:
- A very small release from a flange gasket or from a valve stem seal without blow-

out of gasket/seal material.

E1 - Release with minor damage to the environment that should be reported.
A release that is not very severe but is large enough to be reported to plant management or to local authorities, e.g.:
- A moderate leak from a flange gasket, a valve stem seal, a pump or compressor seal, a small bore connection, a relief valve blowing hydrocarbons into the atmosphere.
- Small-scale liquid spill contained on the location or platform.
- Small-scale soil pollution without affecting ground water.

E2 - Release within the fence with significant damage to the environment.
Significant loss of containment that damages the environment on the premises but not outside the fence, e.g.:
- A cloud of obnoxious vapour travelling beyond the unit limit following flange gasket blowout, compressor seal failure etc.
- A liquid release that is not collected in the drain system and could affect ground water locally or could spill into a river or sea.

E3 - Release outside the fence with temporary major damage to the environment.
Major loss of containment travelling outside the premises causing environmental damage that can be cleaned up without lasting consequences, e.g.:
- A vapour or aerosol release with or without liquid fallout that causes temporary damage to plants, fauna or property, following venting to atmosphere, liquid entrainment from flare, etc.
- Solids (dust, catalyst, soot, ash) fallout following an operational plant upset.
- Liquid spill into a river or sea.

E4 - Release outside the fence with permanent major damage to the environment.
Major loss of containment travelling outside the premises causing environmental damage that cannot be cleaned up without lasting consequences, e.g.:
- A vapour or aerosol release with or without liquid fallout that causes lasting damage to plants, fauna or property, following venting to atmosphere, liquid entrainment from flare, etc.
- Solids (dust, catalyst, soot, ash) fallout following an operational plant upset.
- Liquid spill into a river or sea.
- Liquid release that could affect ground water outside the fence.

IPFs that prevent relieving to the atmosphere should be classified according to this category as well.

Flaring, venting and noise may have an impact on public image and should therefore be addressed when performing environment classification.

The following additional rules apply:
- If flaring is within the allowable environmental limits as set by the local authorities it shall be considered for the classification as having no environmental consequences. If flaring or venting is above these limits it shall be considered for the classification as production loss, e.g. cost of shutdown, fine.
- If the classification team decides that, for a certain consequence, the related public image is a very sensitive issue, E shall be increased by one level.

If the result of the classification is E0, the IPF is not required for environmental protection. For other results, the IPF class can be obtained from the diagram by selecting the point corresponding to the E and W.

3.2.4.3.5 Synergetic Consequences

For architectures where one initiator function activates more than one final element function, the individual classifications only classify final element failure on demand because the assumption is made that, when classifying one function, the other functions, and thus the initiator, function properly. An additional classification, initiator failing on demand, is therefore required. A check shall be performed whether initiator failure on demand, and consequently none of the final elements operate on demand, has synergetic consequences, i.e. consequences in addition to those caused by the failure of the individual final elements. If that is the case, the initiator shall be classified accordingly.

NOTES: 1. As an example, assume one fuel gas knock out drum and more furnaces. Individual IPF classifications of high level to fuel gas shut off may result in S2. In this case we assume that only one function fails and the others still function, which is only possible in case the initiator functions. Check on synergetic consequences when initiator fails gives S3 because in this case in all furnaces an uncontrolled fire or explosion may occur, hence the higher classification for the level trip initiator.

2. The consequence of initiator failure on demand could also result in a lower IPF class compared to the highest class resulting from the individual classifications of functions containing that initiator. This is the case for e.g. oxygen and natural gas shut-off in a Shell Gassification Process (SGP) where the consequence of leaving the oxygen valve only open is more severe than to leaving both valves open. Hence the class for the function initiator to oxygen valve is higher than the result of the synergetic consequence of initiator failing classification. The latter determines the required initiator class.

The above is not relevant for final elements because, for architectures where more initiators activate one final element, final element failure is classified for each function and as a minimum the most stringent classification is selected for the final element, see also (4.3).

3.2.4.3.6 Interpretation of the results and general rules

The highest class resulting from the three types of consequences shall be selected for the IPF.

An IPF shall not be removed when the classification results in unclassified, without feedback to the HAZOP study and/or technical desk HSE review. If an IPF is not required, it shall be deleted before the next IPF is classified.

If more IPFs protect against the same consequences, the classification may indicate that all but one can be deleted. In this case a reiteration process shall take place to ensure that the IPF which remains is the most suitable one.

If the classification method indicates that the IPF class is X, the design without the IPF shall be made safer such that the IPF is either not required or is classified lower than X. This rule shall be applied in the majority of cases. Under special circumstances, to be decided by the Principal and on a case-by-case basis, the decision could be taken to have a third party perform a full safety and reliability assessment and, if required, request approval of the design from the authorities.

NOTE: As an example of the type of analysis which should be carried out in such cases, reference is made to the EP application of design of multi-well systems for which full flow relief is not possible/desirable. This is documented in EP 95-1745. Although this report is specific to multi-well design, the methodology is generally applicable. When such analysis has been carried out, the resulting design will fall outside the scope of this DEP and no attempt should be made to reclassify using this DEP.

For IPF classes II to VI a pre-alarm shall be implemented unless corrective operator action to avoid the IPF action is not feasible.

Automatic start-up overrides with a duration of 5 seconds above the minimum time required for start-up, or based on process or equipment conditions, are preferred to manual start-up overrides because they will have a positive impact on the overall IPF PFD by removing the risk associated with human error of leaving on, or switching on again, a manual start-up override.

To achieve the requirements of an IPF class, unrevealed failure robustness may be required. This is implemented in a 1oo2 (one-out-of-two) configuration, meaning that if one of the two initiators or final elements has an unrevealed failure, the IPF action will be taken by the second initiator or final element, respectively.

If a manual trip switch is installed to allow the operator to react to unforeseen events, the classification of this switch shall be same as the classification of the most stringently classified final element activated by the manual trip switch.

NOTE: The manual trip switch could be a furnace trip switch, but also a plant emergency trip switch.

In combined IPF and sequence control systems (e.g. furnace start-up), each step may have to be classified separately because the frequency of demand and the consequences may be different. This is also valid for different phases of plant operation.

For fire detection and protection classification, only the incremental consequence of IPF failure on demand shall be taken into account, not the full consequence of a fire. The fire is

assumed to be there already and the IPF is installed for mitigation purposes, e.g. an automatically triggered water deluge system or facility ESD.

3.2.4.4 Revealed failures

3.2.4.4.1 General

The revealed failure classification should be performed after the unrevealed failure class implementation has been decided, because implementation of the requirements related to the unrevealed failure class may impact the revealed failure rate of initiator or final element configurations.

The revealed failure classification diagrams given in Figure 7 are based on:
- A pay-out period of 1 year.
- The assumption that the revealed failure robustness will reduce the revealed failure rate to a negligible figure.
- Minimum CAPEX.

The classification diagrams should be applied; detailed calculations to justify revealed failure robustness requirements should not be made.

Initiators and final elements should be classified separately, due to the possible significant difference in cost of revealed failure robustness for initiators and final elements.

NOTE: The revealed failure robustness classification diagrams may also be applied to parts of function components. Report OH 96/30180 gives details on the impact of IPF PFD and revealed failure rate calculations when part of a function component is implemented robust, in this case a solenoid valve.

3.2.4.4.2 Cost of robustness

Three diagrams are indicated in Figure 7 for different costs of revealed failure robustness. The cost of robustness shall be determined and the related diagram selected.

Data on the cost of revealed failure robustness shall be obtained from competent personnel responsible for instrumentation.

3.2.4.4.3 Frequency of revealed failure

The frequency of revealed failure for the IPF component under classification shall be determined (R classification).

The default failure rates for single initiators and single final elements, as given in report OH 96/30180, both translate to R1.

Unrevealed failure robustness increases the revealed failure rate by up to a factor of two compared to a single configuration.

3.2.4.4.4 Cost of revealed failure

The cost of revealed failure related to the consequences described in (3.2.4.2) shall be determined (C classification).

NOTES:
1. The cost of revealed failure for all IPFs with the same final element shall be the same.
2. If the cost of an initiator revealed failure differs significantly from the cost of actuator revealed failure due to e.g. longer plant down time, the C classification may be different for initiator and actuator.
3. The cost of revealed failure should take into account potential consequential damages or loss e.g. where thermal shocks may lead to premature furnace tubes material fatigue.

3.2.4.4.5 Revealed failure class

If the result of the classification is C0, the IPF is not required to be revealed failure robust. For other results, the revealed failure class can be obtained from the diagram by selecting the point corresponding to R and C.

3.2.4.4.6 Interpretation of the results and general rules

The result of the revealed failure classification for initiators and final elements is N or F. N indicates that revealed failure robustness is not required, F indicates that revealed failure robustness is required.

3.2.5 Documentation

The classification results shall be documented as part of the safeguarding narratives or as a separate document.

The classification report shall be such that it shows that the classification was made on objective and reasonable grounds, by a team with members qualified to perform the classification. This can be achieved as follows:

- Build-up the team as indicated in (3.2.2).
- A short statement indicating the consequences of IPF failure on demand and IPF revealed failure shall be documented.
- If the team is unable to reach a consensus, the issue should be raised to a higher level of management, again with all necessary disciplines represented and, if applicable, the Principal shall be consulted.

To enable consistency checks and easy handling of data, classification results shall be entered into a database. It shall be possible to search on any word in any field. As an example, a print-out of a database record is given in Figure 8. Items in bold are the field headings, the remainder are the database entries. For more examples see MF 95-0020. Figure 9 provides a blank classification form that may be used during the classification exercise.

This database may also be used to enter the implementation data such as test frequency etc.

For authority approval purposes, classifications where personnel or environment consequences are above S0 and E0 respectively should be documented separately.

The question on the IPF classification form, 'is it a pre-alarm', shall be answered with yes or no. If corrective operator action to avoid the IPF trip action is not feasible, a note shall be made that the pre-alarm can be deleted.

If one of the selections made during the classification is W0, W1, W3, A2 or G1, an explanatory note shall be recorded.

The classification report shall be updated as part of each plant change such that the requirements for each IPF are at all times auditable and traceable.

A summary of the unrevealed failure classification results may be shown in a cause and effect matrix, as shown in the example in Table 1, using the existing cause and effect matrices.

Table 1 Cause and effect matrix summarising the unrevealed failure classification

Cause ↓ Effect →	Close Fuel Gas Valve	Stop Compressor	Initiator Failure	Overall Class Initiator
High Fuel Gas Pressure	IV		N/A	IV
Low Air Fuel Ratio	IV		N/A	IV
Flame Failure	IV		N/A	IV
Furnace Feed	IV		N/A	IV
High Furnace Outlet Temperature	III		N/A	III
High Speed	-	V	N/A	V
Low Lub-Oil Pressure	-	III	N/A	III
High Compressor Outlet Temperature	III	IV	V	V
Overall IPF Class Final Element	IV	V		

NOTES:
1. Empty entries are also empty in the original cause and effect matrix.
2. Entries '-' have been classified as unclassified, and the IPF can be deleted.
3. The row 'Overall IPF Class Final Element' and the columns 'Initiator Failure' (synergetic consequences) and 'Overall IPF Class Initiator' are additional to the original cause and effect matrix.

4. IMPLEMENTING THE CLASSIFICATION RESULTS

4.1 INTRODUCTION

This Section deals with general rules related to the implementation of the classification results obtained as described in (3.). This Section indicates the basic implementation steps that shall be taken to arrive at a test interval and to select the architecture.

The details of implementing the classification results are dealt with in (5.) to (9.).

An important group of IPFs that will often be deleted after classification are those IPFs which protect against events that are already covered by other IPFs. This will reduce the complexity of the functional logic diagrams.

EXAMPLE: The IPF action following high-high level in a recycle gas compressor suction vessel should only be to stop the compressor. Any subsequent actions, such as stop feed, stop furnace, open low rate depressuring valve, should be initiated by recycle gas low flow alone. Without the IPF classification methodology described in this DEP, these cascading IPFs were common because of the traditional dictum: "if you know it already, take the action and do not wait for subsequent initiators".

Deletion of the cascading IPFs does not necessarily reduce the potential for revealed failures. Only the deletion of an entire initiator will help to achieve better plant availability.

4.2 GENERAL RULES

For IPF class III, control valves and IPF valves may be combined only if the demand on the IPF cannot be caused by a malfunction of the control valve and the IPF valve has no requirements for leakage class V or VI TSO according IEC 534-4. In this way the common mode element is virtually eliminated.

NOTES:
1. The requirement for leakage class V or VI TSO according to IEC 534-4 is often over-stressed because the term TSO valve is incorrectly used instead of IPF valve. The TSO requirement should be challenged during design.

2. As an example where the valves may not be combined, consider flow streams A and B, each with their own flow control, being mixed and reacted. A TZA-HH should stop flow A to kill an exothermic reaction. The flow control valve of A could well be the root cause of too much A, so tripping it may not be effective, hence a separate IPF valve is required.

3. In batch processes valves are closed and opened frequently by the batch controller. Situations exist where a certain valve position is a permissive to proceed with a next step, because starting the next step with the valve in another position would give a hazardous situation. A malfunction of the valve may be the cause of the demand. A separate means of stopping the batch, such as with a separate valve, shall therefore be provided when the IPF is classified as IPF class III or higher.

Because the operator has more information about the overall plant and evacuation situation than any IPF, IPF class IV fire, gas and smoke detection functions may be implemented with the operator as one link of the IPF chain, provided that:
- The control room is a safe area and continuously manned by competent personnel;
- The operator has time to take action, i.e. the process safety time exceeds the sum of the IPF response time and the operator response time.

If an IPF operates a valve when activated, this action shall be communicated to the DCS, triggering an action in the DCS to automatically switch the related controller to manual and drive the output to the safe position, either zero or maximum, if this can be done at acceptable cost. This DCS action shall only be triggered on receipt of the change of state from normal to trip, without preventing the operator from changing the controller state and output at any other time.

If an unrevealed failure robust initiator is required for one function, while the classification of a second function with the same initiator requires a single configuration, one initiator of the unrevealed failure robust set may be used for that function. See Figure 10. This implementation reduces the revealed failure rate of the second function.

If one function is classified as IPF class I or II while others with the same initiator are classified as IPF class III or higher, the former may be implemented in the DCS. Implementing the IPFs in this manner requires separate initiators for the IPF class I or II functions than for the IPF class III functions. This will only be cost effective if a separate measurement for control or indication is available to be used for the IPF class I or II IPF. If

an IPF classified as IPF class I or II is implemented as IPF class III, testing requirements for this function remain those for IPF class I or II, see (7.).

Pre-alarms should be obtained from the control transmitter signal in the DCS if this is available.

The following documents shall be provided to specify the requirements and organisation for implementation of IPFs:
- functional logic diagrams (FLDs);
- IPF classification results;
- typical block schemes;
- typical loop diagrams;
- DEP 32.80.10.30-Gen.;
- completed data requisition sheets DEP 32.80.10.93-Gen.

4.3 IPF CLASS OF INITIATOR, LOGIC SOLVER AND FINAL ELEMENT

The IPF class for those initiators and final elements which are part of only one IPF can be obtained directly from the classification report.

If one initiator activates more than one final element, the highest of all IPF classes related to that initiator, including the result of the check on synergetic consequences (3.2.4.3.5), shall be selected for the initiator.

If one final element is activated by more than one initiator, the IPF class of all functions of which the final element is part shall be added to arrive at the classification of the final element. This shall be done as follows:
- Count the number of IPFs for each class.
- If the number of times a class appears is 10 or more, each full number of 10 classes shall be taken as one occurrence of the next higher class.
- Repeat the exercise until there are not more than 9 occurrences of any class.
- Take the highest class that remains.

EXAMPLE: Assume 31 functions having the same final element, 22 of which are IPF class III and 9 of which are IPF class IV. The method is shown in table 2.

Table 2 Example of the adding rule

Start	→ Equivalent To	Leaving	→ Equivalent To	→ Overall Final Element Classification
22 x III	2 x III 2 x IV	2 x III	2 x III	V
9 x IV	9 x IV	11 x IV	1 x IV 1 x V	

The same adding rule applies to logic solver components that are common to more than one function, unless the functions are independent.

The adding rule is not valid for IPF class I (alarm only) functions because the operator decides how he will act and he usually has more than one option in a particular situation.

4.4 BASIC IMPLEMENTATION STEPS

4.4.1 General

Applying (3.), (4.2), and (4.3) will result in an IPF class for each initiator, the logic solver and each final element. These classes shall be translated to implementation requirements as explained below.

From IEC/SC65A draft 1508 and DIN V 19250 the relation between IPF class, SIL, required PFD and required AK class (from DIN V 19250) can be obtained as shown in Table 3.

Table 3 Relation between IPF class, SIL, required PFD and required AK class

IPF Class	Safety Integrity Level (SIL)	Required PFD	IPS Approval according AK Class
I	-	$\geq 10^{-1}$	-
II	a	$\geq 10^{-1}$	1
III	1	$\geq 10^{-2}$ - $<10^{-1}$	2-3
IV	2	$\geq 10^{-3}$ - $<10^{-2}$	4
V	3	$\geq 10^{-4}$ - $<10^{-3}$	5
VI	3	$\geq 10^{-4}$ - $<10^{-3}$	6
X	4	$\geq 10^{-5}$ - $<10^{-4}$	7
X	b	Not Indicated	8

A deterministic requirement of IEC/65A draft 1508 is that IPF class V and VI initiators and final elements shall be unrevealed failure robust.

Table 3 shows that the PFD requirement does not differ for IPF classes V and VI. However, because the consequences resulting in class V or VI can be very different and the calculation methodology does not take common mode failures and software failures into account, the following additional requirements shall apply for IPF class VI functions:
- The initiator shall be diverse.
- The IPF shall not contain software.
- The final element shall be diverse.

4.4.2 IPF implementation

Pre-alarms and IPFs with an IPF class I require no special equipment and shall be implemented as alarm only. The control loop measurement and the DCS may be used for implementation.

If operator action cannot be relied upon, IPF class I functions shall be classified and implemented as IPF class II.

IPF class II functions require no special equipment and shall be implemented as a switching function. The control loop measurement and the DCS may be used for implementation.

All initiations by IPF class II, III, IV, V and VI functions shall be announced by an alarm.

For IPF class III to VI functions, the required PFD as indicated in table 3 in (4.4.1) is one of the governing requirements. This PFD can be obtained in various ways:
- Using equipment with a lower unrevealed failure rate will reduce the PFD of the IPF.
- Reduction of the test interval and increase of test coverage (7.2) will reduce the IPF PFD.
- Applying unrevealed failure robustness, i.e. one-out-of-two (1oo2), for final element and/or initiator will reduce the IPF PFD.

See (8.) for details on how to calculate PFD and the effects of equipment failure rate, test philosophy and architecture implementation.

For IPF class V and VI functions, the initiator and final element shall be unrevealed failure robust, irrespective of the PFD. For IPF class VI functions, the initiator and final element shall be unrevealed failure robust and diverse and the logic solver shall not be microprocessor based.

Where unrevealed failure robust valves are required and in the absence of leakage class V or VI TSO requirements, one of the two valves may be the control valve.

The required AK class for the logic solver can be obtained from table 3 in (4.4.1).

The result of the revealed failure classification for initiators and final elements is N or F. N indicates that revealed failure robustness is not required, and F indicates that revealed failure robustness is required.

If the result of the classification does not require unrevealed failure robustness but does require revealed failure robustness for an IPF initiator or final element, the relevant component shall be executed in a two-out-of-two (2oo2) configuration. The effect of this architecture on the PFD may be such that equipment, test philosophy and/or architecture requires adjustment in order to fulfil the PFD requirements related to the IPF class.

If both revealed and unrevealed failure robustness is required for initiators and for relay type final elements, they shall be implemented in a two-out-of-three (2oo3) configuration. Valve type final elements shall in this case be implemented as indicated in Figure 11, the '2oo4' configuration.

Figure 12 shows a possible implementation of the various classes.

5. IMPLEMENTATION OF PROCESS UNIT RELATED INSTRUMENTED PROTECTIVE FUNCTIONS

5.1 GENERAL

The requirements given in this and the following chapters are based on the assumption that a DCS is available. If this is not the case, the Principal shall be consulted for the human-machine interface requirements.

The normally energised (fail-safe) design concept shall be implemented. For certain process applications, however, a normally de-energised (non-fail-safe) design concept for IPF final elements may be required. In such cases approval of the proposed implementation shall be obtained from the Principal.

Requirements detailed in the technical specification of the IPS, see DEP 32.80.10.30-Gen., are as far as possible not repeated in this DEP.

IPF loops class III and higher shall function independently of process control systems, without any mutual influence, except where explicitly indicated in this DEP.

The separation between IPF and process control system is recommended in IEC/SC65A draft 1508 and can be justified as follows:

- Assume that with a combined control and IPF measurement, 50% of the unrevealed initiator failures will cause a hazardous situation because the process is out of control in the hazardous direction. At the same time the IPF does not function.
- The default unrevealed failure rate of an IPF initiator is for example 0.024 per year.
- The number of hazardous situations caused by combining control and IPF measurement is therefore 0.012 per year.
- A conservative estimate of the cost of one hazardous situation is USD 1,000,000.
- The cost of the hazardous situation caused by combining control and IPF measurements is therefore USD 12,000 per year.
- The estimated cost of one IPF measurement is USD 10,000.
- The payback of separating control and IPF measurements is therefore approximately one year.

If sequential functions and IPFs are difficult to split, the IPS shall also take care of sequential control functions (e.g., for fired heaters).

5.2 INITIATOR

IPF class III and higher initiators shall have their own process tappings, impulse lines, sensors, utilities (power fuses, air supply branch-offs), etc. Only elements such as orifice plates and bluff bodies of vortex meters may be shared with control measurements.

Intelligent sensors with 4-20 mA output signals are preferred to discrete, direct mounted, field switches because they have lower failure rates, better accuracy, better stability and allow sensor signal analysis and measurement comparison. These sensors shall communicate with the IPS in 4-20 mA signal mode. Digital communication protocols for sensors are not yet acceptable. Use of hand-held communicators on intelligent sensors shall, for reasons of integrity, be restricted and may only be applied if tests have proven that their use will not cause adverse consequences regarding revealed or unrevealed failures. Additional line resistors may be required to permit communication with the sensor.

Manual switches shall be normally closed.

IPF initiators, except high liquid level IPF initiators, should have the same range and accuracy as neighbouring process sensors in order to facilitate measurement comparison as described in MF 94-0495. See also (7.). High liquid level displacer and dP cell IPF initiators should have vessel connections at 80% and 100% to ensure proper functioning under varying density conditions compared to design.

Where possible, separate trip amplifiers shall not be applied. Sensor signals shall be connected directly to input cards integrally available in IPSs.

In case input cards are not available for signals used in the field, these signals shall be converted in the field.

If intrinsically safe electrical equipment is applied in hazardous areas, isolation barriers are required. To minimise the number of components in the IPF loop, ex 'n' , ex'e' or ex 'd' type sensors should be applied in zone 2 or in zone 1 (except ex 'n') hazardous areas.

For analogue inputs and for Normally Open contact inputs, open or short circuit cable faults or sensor faults shall, as far as possible, be detected via line monitoring and self testing features. Operators shall be informed in case of fault detection and maintenance shall be initiated immediately. Revealed failure actions (spurious trips) may be avoided in such cases provided that the following requirements are met:

- A second or back-up indication shall be available to the operator.
- The control room shall be continuously manned by competent personnel.
- An alarm shall be generated and annunciated on the DCS indicating that the IPF trip measurement is faulty.
- Other ways to trip or stop the process shall be available to the operator.
- A maintenance override for that IPF should be available.
- The process dynamics shall be such that the operator has time to act.
- This automatic override functionality is time restricted, i.e. the trip measurement shall be taken in maintenance override before a pre-set time of one hour has elapsed. In case an MOS is not available, the fault will cause a spurious trip after the pre-set time has elapsed.

For an implementation of the automatic override, see Figure 14.

It is recognised that it may not always be possible to avoid spurious trips under open circuit or short circuit conditions. The possibility to implement automatic overrides does not imply that time delays should be applied to IPS inputs to avoid revealed failure actions under such circumstances. Time delays for this purpose shall not be applied if the sum of the required delay time and the IPF response time (including the IPS response time which shall be taken as two times the IPS cycle time) exceeds the process safety time and shall be approved by the Principal. The process safety time shall be determined by Process Control and Technology departments.

If the IPS has line monitoring facilities, analogue sensors shall have "direct" output signals only. If this is not the case, high trip sensors shall have "reverse" output.

For IPF loops class III and higher, the initiators should have a red colour and should have a red nameplate with black lettering.

If diverse initiators are required, diverse measuring principles shall be applied. These diverse measuring principles shall, where possible, include different types of process connections. An example of a diverse measuring principle is ultrasonic and dP cell level measurements. An example of a non-diverse measuring principle is displacer and dP cell level measurements, because in both cases the tappings may block.

NOTE: Diverse measuring principles shall not be applied when this would result in an increased unrevealed failure rate as would be the case when a pressure transmitter is replaced by a pressure switch.

5.3 INSTRUMENTED PROTECTIVE SYSTEM

IPSs shall be based on either:
- electromechanical relays;
- solid-state/magnetic-core technology;
- microprocessor technology (PLCs).

Pneumatic and hydraulic relay based IPSs shall not be used for new or re-instrumentation projects and are therefore not dealt with in this DEP.

For new or re-instrumentation projects, particular attention shall be paid to electromechanical relay-based IPSs as they may not fulfil the requirements of IPF class V and higher.

The IPS, including the IPS-PLC to IPS-PLC communication link for IPF class III and higher safety related signals, shall fulfil the requirements of the DIN V 19250 risk class (AK class) related to the IPF class resulting from the classification and shall be certified by TÜV.

In case an IPS-PLC is applied, the complete IPS, including system software versions and releases, shall be evaluated and certified by TÜV.

To avoid unexpected failures of software and/or hardware, only proven releases of software and hardware shall be used. The release of the system should not be upgraded after order placement for functionality enhancements. Upgrades to fix bugs that jeopardise safety or plant availability shall be implemented but only after certification by TÜV.

The majority of the IPFs will be IPF class V or below; however, it is preferred to purchase, as a minimum, AK class 5 TÜV-certified IPSs so that the majority of plant changes can be incorporated in the same IPS.

Although solid-state/magnetic-core and PLC-based systems are preferred, relay-based systems may be selected for certain applications. Relay-based systems have the disadvantages that no self-diagnostics are available, troubleshooting and making modifications can be difficult and communication to a DCS is only possible for the output signals. The DCS shall not be connected in series with the trip amplifiers that are required to input analogue initiators into a relay based IPS.

Only IPS suppliers or system builders (integrators) which are accepted by the Principal shall be used for IPS engineering, construction, wiring, testing, etc.

The IPS-PLC to IPS-PLC communication link shall be fail safe and revealed failure robust, and the signals transmitted over this link shall be NE such that IPF trip actions are taken when the link fails.

IPSs supported by SIOP and SIEP require no further quantitative reliability assessment studies since these have already been done. These studies have shown that, in order to obtain revealed failure rates equal to or better than relay based IPSs, IPS-PLCs are only acceptable when fail safe, revealed failure robust input and output cards and processors are used. Output cards driving non-critical indication or alarm lamps should be single and non-fail-safe.

When making a selection between solid-state/magnetic-core technology and PLCs, the following shall be considered:
- actual field experience (installed base);
- requirements of national and/or local regulations;
- application complexity;
- level of automation;
- skills required.

Advantages of PLCs are:
- faster engineering, through configuration techniques;
- ease of FLD simulation, off-line on a PC;
- ease of logic modifications;
- ease of commissioning;
- ease of monitoring the integrity of field devices and their wiring;
- fewer different hardware cards;

- self-documenting facilities.

Disadvantages of PLCs are:
- special skills required;
- possible bugs in the software;
- higher revealed failure rates;
- protection against (on-line) logic modifications requires strict procedures.

IPS systems shall be as simple as possible and shall have a minimum number of components.

IPS-PLCs shall not be applied when an IPF class VI integrity is required because the software contribution to the unrevealed failure rates of PLCs is unknown, and therefore not taken up in the IPF calculation methodology. Only in very exceptional cases, and with the approval of the Principal, may PLCs be considered for class VI loops.

If a classification results in a number of IPF class VI loops and the remainder of the IPFs implemented in the same IPS-PLC are IPF class V or lower, the IPF class VI loops may be implemented in the IPS-PLC making use of the secondary means of de-energisation functionality which bypasses all microprocessors in the system. In this case the IPS-PLC shall comply with the requirements of IPF class V and the secondary means of de-energisation facility shall be TÜV certified according to DIN V 19250 AK class 6.

Process units should be allocated to IPSs with due consideration to IPS failure. For details regarding the allocation of process units to Input and Output cards, see DEP 32.80.10.30-Gen.

To ensure suitable response time for activation and sufficiently accurate time stamping, the scan or cycle time of IPS-PLCs shall be less than 300 ms.

For each piece of rotating equipment, it shall be checked whether a 300 ms cycle time is sufficient to protect the equipment, i.e. confirm that the process safety time of the equipment exceeds 600 ms. If this is not the case, an IPS-PLC is not suitable.

If PLC based IPSs are considered for equipment packages, for reasons of integration, spare parts, training and maintenance, the same IPS should be selected as those applied in the remainder of the plant or project. It should be realised that doing this may complicate the factory acceptance test of these equipment packages. For more details, see DEP 32.31.09.31-Gen.

Time synchronisation between IPSs, SERs and DCS, shall be applied from an external clock.

Initiator or final element and IPS robustness implementation shall be independent. For example, assume a 2oo3 initiator has to be routed to an IPS with revealed failure robust inputs. In that case each initiator is connected to one point of each of the dual input cards, resulting in a total of 6 routes. A different set of dual input cards shall be used for each initiator. See Figure 15.

On-line changes to tuning parameters may be made provided they are tested before taking the loop into service. On-line logic changes and operating system software upgrades should not be performed unless full functional tests can be performed with the process unit in operation. If on-line changes are to be made then a thorough analysis shall be made and agreed with Operations, addressing the following:
- What has to be changed?
- How and when is it to be changed?
- What are the contingencies for errors?
- What risk assessment will be made?
- What fall-back scenarios are in place?

IPS systems shall be fed via two separate power feeders, with at least one of them connected to a vital uninterrupted power supply system (UPS), with automatic change-over facilities and remote alarm in case of single failure. For details, see DEP 33.64.10.10-Gen. and Standard Drawing S 67.006.

To facilitate long term reliable operation of IPSs, this equipment shall be installed inside (field) auxiliary rooms. These rooms shall have temperature and humidity control facilities fulfilling the requirements stated in DEP 32.80.10.30-Gen.

In order to reduce down-time and override time, 'card' or 'complete component' replacement techniques shall be applied.

As a minimum a common cabinet utility alarm and a common system alarm shall be transmitted to the DCS for the attention of the operator. When the alarm occurs the operator shall contact the responsible maintenance person for further action.

Engineers should be trained before and during the factory acceptance test. Mechanics and technicians should be trained during site acceptance testing and commissioning activities. If own personnel are not properly trained and kept up-to-date, modifications shall be left to the Supplier.

5.4 FINAL ELEMENT

Where a control valve also functions as an IPF class III or higher IPF valve, the IPF shall have priority over the process control function. Where the control valve is fitted with a positioner, the solenoid valve driven by the IPS shall be fitted between the positioner and the actuator diaphragm or piston. A digital output shall not be routed from the IPS to the DCS with the DCS configured to drive the valve to the safe position, since in that case the IPF class II DCS would be part of the IPF class III loop.

If diverse unrevealed failure robust valves are required, the valves shall be of a different make and/or type (model).

IPF valves classified as IPF class III or higher shall not be provided with a hand wheel or a bypass as these increase the unrevealed failure rate of the final element.

IPF class III or higher valve type final elements should be air operated and spring loaded. Hydraulically operated valves are less suitable due to the complexity of the hydraulic system. For hydraulic actuator requirements see DEP 31.36.10.30-Gen. Electric motor operated valves without spring return shall not be used for IPF class III or higher valve type final elements.

For IPF loops class III and higher, the valve actuator should have a red colour and should have a red nameplate with black lettering.

For NDE IPF final elements, automatic wiring tests such as line monitoring and earth fault and automatic test of the availability of instrument air shall be implemented on each loop. Regular functional testing shall also be performed. The IPS-PLCs are designed, especially with respect to the internal diagnostics, for the de-energised signal being the safe state of inputs and outputs. For NDE applications which do not apply an external inverter such as a relay, the IPS-PLC shall also be designed for the energised signal being the safety related input or output state. This is not the case for many of the TÜV certified IPS-PLCs. If this is not the case, inverter relays with the appropriate classification shall be applied.

Power and air supply for NDE final elements shall be such that the impact of supply failure on the IPF PFD is negligible, e.g. by means of an alarm in case the supply fails.

For instrument air supply requirements for depressurising systems, see DEP 32.45.10.10-Gen.

For valve type IPF final elements, see DEP 32.36.01.17-Gen.

Rotating equipment stop circuit type IPF final elements should be implemented by a 24 V(dc) output connected to the coil of an interposing relay. A contact of this relay should be wired into the motor switchgear. This implementation is referred to as 'no special equipment' in Figure 12.

5.5 CABLING

For certain applications, special cabling is required. For details, see DEP 32.37.20.10-Gen. and DEP 32.45.10.10-Gen.

The maximum allowable distance between the IPS and the solenoid valve shall be checked.

5.6 HUMAN-MACHINE INTERFACE

5.6.1 Operator interface

Process alarms and IPS system and utility alarms shall be presented to the operator via the DCS operator workstations. Resets shall be operated from the DCS.

ESD, OOS and MOS enable switches shall be mounted on a blank section of the operator console.

For complex logics, one or both of the following should be displayed on the DCS screen in addition to the information displayed on the process graphics:
- 'live' cause and effect matrices;
- help text.

The DCS system shall be used to perform all IPS alarm handling, indication, annunciation, logging and printing.

For IPS system alarms and IPS utility alarms, more (or all) diagnostic information may be transmitted from the IPS to the DCS in addition to the common alarms. Alarms can then be shown individually or combined, depending on the action to be taken by the operator. Help screens should be provided to indicate causes and actions associated with the alarms. The necessary actions shall be taken to ensure that mean time to repair figures of the IPS do not deteriorate so as to prevent jeopardising plant safety or plant availability.

Time stamps should not be sent from the IPS to the DCS. The SER time stamping shall be used for post mortem analysis.

Any time delay, due to system constraints, between (IPS) trip initiation and (DCS) alarm presentation shall be less than 3 seconds.

If technically possible, full SER functionality should be provided in the DCS, i.e. integration of SER lists with DCS alarms lists and functionality presently available in the SERs also in the DCS.

For a list of signals to be transmitted to the DCS for operator interface, see DEP 32.80.10.30-Gen. In addition, the signal to switch automatically the related controller to manual and drive the output to a safe position may be transmitted to the DCS.

The first trip action occurring in each UZ group (first failure) shall be detected by the IPS. A first-up flag shall be transmitted to the DCS and the DCS screen shall display the first-up alarms differently from the subsequent alarms, until the first-up reset is activated from the DCS and the first-up flag removed by the IPS.

OOSs, see (5.9), shall be implemented as a hardwired switch with a yellow back-lit handle; the light shall be on when the override is switched on. ESD switches shall be implemented hardwired, with a red handle without back-light. For MOS enable switches, see (5.8.3).

The normal position of all switches on the console shall be horizontal.

5.6.2 Sequence of event recorder

Plant events, utility events, operator actions (overrides and manual trips) and IPS failures shall be logged and stored on the SER for incident analysis purposes.

The SER network should be revealed failure robust. This network may be combined with the maintenance / engineering network.

If the SER functionality resides in a PC, site procedures shall ensure that the SER cannot be infected by viruses.

For a list of the type of events and signals to be recorded on the SER, see DEP 32.80.10.30-Gen.

5.6.3 Maintenance and engineering interface

The maintenance and engineering interface shall give details of all IPS failures (card failures, cable faults etc.).

The maintenance and engineering interface should consist of one or more (PC based) workstations. Site procedures shall ensure that these workstations cannot be infected by viruses.

A workstation shall only be used as an on-line diagnostic tool whilst connected to a 'live' operating system.

'Forced' or software overrides on input and output channels of IPS-PLCs shall be enabled and disabled by means of a key lock and/or password facility. Procedures shall be in place that during and after plant start-up all such overrides on input and output channels are removed. Presentation of 'forced' overrides to the operator shall be similar to MOS presentation.

A revealed failure robust IPS-PLC network should be used for the maintenance and engineering workstation functionality. This network may be combined with the SER network. In addition to this network, individual engineering workstation connections, one per IPS-PLC, shall be provided. These can be used when the maintenance/engineering network fails.

5.7 COMMUNICATION INTERFACES WITH OTHER SYSTEMS

5.7.1 Interface with DCS

In order to monitor IPS related events on the DCS screens and to activate resets and MOSs, there shall be communication between DCS and IPSs. Therefore the IPS shall be linked with the DCS. The link shall be by point-to-point DCS gateways or serial links and should be revealed failure robust. The revealed failure robustness is required because of the MOS and reset control from the DCS, and not for safety purposes. IPS to DCS connections via integrated IPS-PLC networks should be avoided because of gateway or serial communication port loading and additional time delays.

Failure of serial links shall not cause nuisance trips. IPF class III to VI signals shall not be transmitted over this link because the highest IPF class in which a DCS may be part of the IPF loop is class II. If the communication link between DCS and IPS fails, an alarm shall be generated in the DCS.

Interfaces between DCS and IPS systems shall be such that upon any failure of the link the protection functionality of the IPS system will not be defeated, except for MOS and reset signals from the DCS that may be routed through this interface and therefore cannot be operated when the link fails.

All serial links shall comply with MF 91-0885.

For a list of the type of signals to be communicated between IPS and DCS, see DEP 32.80.10.30-Gen.

5.7.2 Interfaces with other systems

There shall be no communication interfaces between the IPS and systems other than DCS. Interfaces between IPS and other systems shall be hard-wired.

5.8 MAINTENANCE OVERRIDES

5.8.1 General

The preferred and TÜV-approved (see TÜV document "Maintenance Override") implementation is described in this Section.

Maintenance override switches (MOSs) are used to override IPF initiators to enable maintenance or on-line functional testing. It shall be considered during the basis of design (BOD) phase whether MOSs are required in those cases where spare process units or equipment are available.

Maintenance override facilities may be provided only for those IPF initiators where a second or back-up indication, and a means to stop the process, are available to the operator. Furthermore, the process dynamics shall be such that the operator has time to act.

Therefore, MOSs shall not be provided on, for example:
- flame sensors;
- (axial) displacement type sensors;
- manual ESD inputs.

A maximum of one trip initiator may be overridden per protection group (UZ group) at any one time.

To reduce the number of MOSs, an MOS shall not be applied for 2oo3 IPF initiator configurations. To reduce the IPF PFD, an MOS function shall be provided for each of the initiators of 2oo2 IPF initiator configurations. Setting of one MOS shall create a situation such that, during the time the override is switched on, the configuration automatically functions as a 1oo2 system.

Outputs shall not be overridden because, within one protection group (UZ group), they are usually the result of more than one input.

An MOS override shall not inhibit the alarm function.

For an implementation example, see Figure 16.

5.8.2 Operational considerations

Operations personnel shall be solely responsible and authorised to switch an IPF initiator into override.

Before an MOS is activated, all work and permit procedures shall be followed, such that a record is available indicating the name of the person who switched on the override.

When the IPF initiator is in override, the operator shall check the related control or indicating transmitter measurement frequently such that manual actions (removal of the override or manual ESD) can be taken if the process moves out of the operating envelope.

The proposed set-up requires optimum (radio) communication between the operator and the technician. A separate radio channel should be provided for this.

MOSs shall be activated for as short a time as possible.

5.8.3 Implementation

An MOS shall be activated from the DCS VDU/keyboard. When an MOS is activated, the appropriate override signal shall be sent via the communications link to the IPS.

A hard-wired, yellow, back-lit MOS enable switch shall be provided on the DCS console. At least one switch shall be provided per process unit. Only when this switch is in the enable position is the MOS signal accepted by the actual protection logic. Because this switch is hardwired, the operator has the possibility to de-activate any override when the communication link fails.

The status of the MOS enable switch shall be read by the DCS via the serial link for event logging purposes.

The logic to activate only one override per protection group (UZ group) shall be implemented in the IPS.

In case the DCS to IPS communication link fails, the overrides shall remain as they were before the failure and when the link is re-established there shall be no status change.

5.8.4 Human-machine interface related to maintenance overrides

The process graphics on the DCS VDUs should indicate (grouped together):
- the control measurement/pre-alarm;
- the trip alarm;
- the MOS activate command switch;
- the MOS activated indication.

A dedicated overview graphic should be provided on the DCS to enable the operator to quickly find trip initiators in override without searching for the correct process graphic.

In the DCS optimum use should be made of units or compounds to convey MOS related information to the operator.

The MOS activated indication will only come on when an MOS command is issued and the enable switch is turned to the enable position and the override logic is performed in the IPS.

A yellow, common (minimum one per process unit), hardwired MOS indication lamp driven from the IPS shall be provided on the DCS console to indicate that at least one override is set in the relevant process unit. This shall be implemented by applying an MOS enable switch with a yellow back-lit handle, the lamp in the handle functioning as the MOS indication lamp.

All MOS related events shall be recorded on the SER with a time stamp and shall also be printed on the DCS printer. The service description which is also printed shall include the tag name of the initiator being overridden.

MOS activation shall generate a (low priority) alarm on the DCS. If the MOS is not removed the alarm shall be repeated every 4 hours.

The operator shall check, when switching on an override, that the indications described above function properly.

5.9 OPERATIONAL OVERRIDES

Operational overrides should be avoided by implementing automatic start-up overrides, see (3.2.4.3.6), in the FLD design.

Operational overrides shall not be provided on manual ESD inputs.

Operational override switches shall be located on the DCS console and hardwired to the IPS. The switch shall have a yellow, back-lit handle.

6. IMPLEMENTATION OF FIRE GAS AND SMOKE DETECTION INSTRUMENTED PROTECTIVE FUNCTIONS

6.1 GENERAL

For active fire protection equipment, see DEP 80.47.10.31-Gen.

The Contractor shall check local regulation requirements related to the FGS, and if these are more stringent than the requirements of this DEP, they shall prevail. In these instances, the Principal shall be informed.

This section deals only with FGS IPF and IPS requirements which are additional to or different from process unit IPF and IPS requirements as described in (5.).

FGS IPFs shall be separate from the process IPFs because the FGS IPFs shall remain operable during plant shutdown.

6.2 INITIATOR

DEP 32.30.20.11-Gen. details the requirements for the sensor part of the FGS IPF loops. In case of conflict between DEP 32.30.20.11-Gen. and the IPF class requirements of the initiator, the Principal shall be consulted. The interface between the sensor and the FGS IPS input card is either a 4-20mA signal or a potential free contact.

If the initiators are of the normally open (quiescent current) design, continuous line monitoring facilities capable of detecting open loops and short circuits shall be applied and an alarm raised if a fault is detected. No protective action shall be taken if such a fault in the initiator circuit is detected.

6.3 INSTRUMENTED PROTECTIVE SYSTEM

The FGS IPS should operate independent from any other instrumentation system, such as DCS and process unit related IPS, except for the DCS human-machine interface. Combining FGS related IPS and process unit related IPS requires the approval of the Principal.

The maximum cycle time of the FGS shall be 500 ms.

The battery back-up time shall be as required by DEP 33.64.10.10-Gen.

6.4 FINAL ELEMENT

The automatic output actions performed by the FGS shall be entirely independent of the DCS.

If the process unit or rotating equipment will be tripped by the FGS, the FGS final element shall be implemented as a potential free contact output which is routed to a digital input of the relevant process IPS. For equipment packages that are fully self-contained, see DEP 32.31.09.31-Gen.

Final elements that constitute a personnel hazard when actuated, such as extinguishing agent release systems, shall have safety features to ensure evacuation of personnel before release.

6.5 CABLING

For special requirements regarding cabling, refer to DEP 80.47.10.30-Gen. and DEP 80.47.10.31-Gen.

7. TESTING

7.1 CLASSIFICATION RESULTS AND TEST PHILOSOPHY

To achieve the PFD related to an IPF class, the loop architecture may be changed (impact on CAPEX), hardware with a lower unrevealed failure rate may be installed (impact on CAPEX) or the test interval may be reduced (impact on OPEX and/or CAPEX).

The relation between the IPF class and the testing frequency is given by the PFD formulae described in (8.). Figure 17 shows the basic relationship between test frequency, IPF loop unrevealed failure rate, architecture, PFD and IPF class using simplified formulae and a zero test duration. The relationship can be obtained by means of the IPF calculation methodology as described in OH 96/30180, see (8.).

For manual testing, experience has shown that it is very difficult to keep up with a test interval of less than 6 months.

As can be seen in Figure 17, large reductions in IPF PFD are possible by testing the loop automatically, around once per day to once per week. For more details on automatic testing, see (7.6).

To enable manual testing without the requirement to shut the process unit down, use can be made of MOSs for initiator testing. For IPF final element testing, however, additional equipment may have to be installed, such as an additional valve in parallel to the valve to be tested. In that case, precautions shall be taken that the additional equipment is not in use during normal operation as this would increase the unrevealed failure rate of the IPF final element.

IPF class I and II functions, including alarms and pre-alarms, shall be tested once every 4 years.

For IPF class III to VI functions, two types of tests can be identified:
- Regular proof tests with a certain test interval (maximum 4 years) and coverage factor.
- Tests during planned shutdown with a maintenance interval (the time between planned shutdowns) and a coverage factor as close as possible to 1. The maintenance interval shall be maximum 4 years if the planned shutdown cycle exceeds 4 years.

A demand is not necessarily initiated for safety reasons, it may be caused for example by an operator wanting to stop a furnace by means of the furnace ESD switch. If such a demand occurs with an interval shorter than the test interval, the test interval used in the PFD calculations may be reduced provided that a proper coverage factor is used and a test record is made.

If, for existing installations, the IPF classification and implementation methodology results in a significantly increased test interval, this test interval shall not be increased in one step because of the possible effect of time-based maintenance on unrevealed failure rates. If, for example, the test interval of a valve was 6 months with an observed failure rate of 0.047 unrevealed failures per year, an increase in test interval to two years will dramatically increase the unrevealed failure rate of the valve if the valve tends to stick after 9 months. In this case, time-based maintenance (stroking or greasing of the valve) shall be applied at an interval of less than 9 months and the valve shall be tested every 2 years. The maximum test interval step increase is 6 months.

For new installations the initial test interval shall be 6 months, which can be increased, in case of satisfactory test results, in steps of 6 months to the calculated test interval.

7.2 TEST COVERAGE FACTORS

An important factor in the IPF calculation methodology (8.) is the test coverage factor. This factor is a measure on a 0-1 scale of how well the test is performed, i.e. which proportion of the unrevealed failures possibly present in the IPF loop will be found by the test.

7.3 INITIATOR TESTING

To achieve the highest possible coverage factor, initiators shall be tested by simulating, as close as possible to the process, a change in process condition exceeding the limit. If the

impulse lines are not included in the test, the coverage factor shall be reduced accordingly.

Irrespective of the IPF class, initiators shall be tested with a coverage factor of as close as possible to 1 during planned shutdowns (maintenance interval), i.e. maintain in the workshop and clean the impulse lines, such that PFD calculations may be performed with a coverage factor of 1. The maintenance interval shall be maximum 4 years if the planned shutdown cycle exceeds 4 years.

Proper functioning of line monitoring, if implemented, shall be tested during every planned shutdown. The interval of these tests shall be maximum 4 years in case the shutdown cycle exceeds 4 years.

7.4 LOGIC SOLVER TESTING

Relay-based IPSs shall be fully tested during every planned shutdown (maintenance interval). The maintenance interval shall be maximum 4 years if the planned shutdown cycle exceeds 4 years.

Solid-state/magnetic-core and PLC based IPSs do not require to be tested manually, unless the user decides to test for human induced errors. The maintenance interval as used in (8.) shall be set equal to the life time of the IPS, usually 10 years.

7.5 FINAL ELEMENT TESTING

To achieve the highest possible coverage factor, NE final elements shall be tested by forcing the IPS output.

Irrespective of the IPF class, final elements shall be tested with a coverage factor of as close as possible to 1 during planned shutdowns (maintenance interval), i.e. maintain in the workshop, such that PFD calculations may be performed with a coverage factor of 1. The maintenance interval shall be maximum 4 years if the planned shutdown cycle exceeds 4 years.

Proper functioning of loop monitoring, if implemented, shall be tested during every planned shutdown. The interval of these tests shall be maximum 4 years if the planned shutdown cycle exceeds 4 years.

If the valve action is monitored by the DCS by monitoring the effect of the valve moving to the safe position and the DCS generates a report, this report may be considered as a test provided that the valve has no TSO requirement. The valve closing time should also be checked such that incipient problems (valve becoming sticky) are also detected.

NOTE: The valve moving to a safe position is not necessarily detected by a position switch; the reduction of flow to zero, if a closed valve is the safe position, is also a detection possibility.

In batch processes valves are closed and opened frequently by the batch controller. Situations exist where a certain valve position is a permissive to proceed with a next step, because starting the next step with the valve in another position would give a hazardous situation. If the movement to the safe position of the valve during the batch is checked by the batch controller and a report indicating functioning of the valve is generated, the test interval may be assumed to be the time between the (batch controlled) movements to the safe position.

7.6 AUTOMATIC TESTING

7.6.1 General

Automatic functional testing is one way to reduce the test interval and at the same time reduce human-induced unrevealed failures and nuisance trips caused by human errors during manual testing.

Irrespective of the automatic tests performed, manual testing with a coverage factor of as close as possible to 1 shall be performed during planned shutdowns (maintenance interval). The maintenance interval shall be maximum 4 years if the planned shutdown cycle exceeds 4 years.

7.6.2 Process IPF initiators

Research is in progress to determine whether one or a combination of the following methods is a suitable replacement of manual initiator testing:
- continuous comparison of initiator signals, e.g. IPF initiator versus DCS control measurement;
- continuous analysis of initiator signal noise for analogue measurements;
- analysis of measurement rate of change.

Algorithms for these tests have been included in the supported DCSs under the Shell MVC package; see MF 94-0495.

The coverage factor of comparison tests is 0.99 according to IEC/SC65A draft 1508.

7.6.3 Flammable or toxic gas initiators

To enable one-man testing of flammable or toxic gas detectors the following system shall be implemented if specified by the Principal:
- A test button and lamp connected to the FGS IPS shall be provided near each detector and a common test enable switch shall be mounted on the mimic.
- The panel operator enables the test by means of the test enable switch. Enabling the test is recorded on the SER.
- The tester presses the button and the lamp will come on when the IPS has taken the detector in override. Pressing the button is recorded on the SER.
- The tester presents the test gas to the detector head and the HH level shall be detected within a set time. HH level detection or non-detection within the set time is recorded on the SER.
- If the HH level is not detected within 4 minutes or when the level returns to normal, the override shall be removed automatically. Removal of the override is recorded on the SER.
- The SER printout functions as the test record.

NOTE: The Principal may decide to use another testing method.

7.6.4 Final elements

For IPF final elements, automation of valve testing may be applied. Performing this test by partial valve stroking has not always been successful. The coverage factor of partial valve stroke testing is 0.5 according IEC/SC65A draft 1508. Partial valve stroking should therefore not be applied.

Semi-automatic full valve stroking may be used as a substitute for manual testing provided that it is acceptable to Operations to operate the valve for a short period.

If semi-automatic full valve stroke testing is applied to valves with leakage class V or VI TSO requirements, the coverage factor shall be determined together with the discipline responsible for stating the TSO requirement.

The basic testing principle for semi-automatic full valve stroke testing shall be as follows:
- The tester initiates the test from the DCS.
- The command to close the valve should be transmitted via the communication link from the DCS to the IPS.
- The IPS sends the close command to the valve for a period exceeding the valve travel time (such that the DCS can detect the safe position) after which it returns the valve again to the position it had before the test.
- A valve safe position indication shall be available in the DCS.
- The test result shall be recorded by the DCS automatically.
- The consequence of the valve failing in the safe position as a result of this test should be considered.

Another automatic test which may be implemented is to monitor stroking times during each operation of the valve and raise an alarm when the stroking time exceeds a specified limit.

8. IPF CALCULATION METHODOLOGY

8.1 GENERAL

The details of the IPF calculation methodology are described in OH 96/30180. The purpose of this calculation methodology is:
- To calculate required test intervals to fulfil the probabilistic IPF class requirements taking into account unrevealed failure rates, test coverage factor, etc.
- To calculate the IPF revealed failure rate.

8.2 ASSUMPTIONS

The probabilistic calculations used in the calculation methodology do not take into account common mode and systematic failures, nor are human errors taken into account in the version of the calculation methodology available at the time of issue of this DEP.

The failure rates used in the calculation methodology are assumed to be constant over time. Failures that are expressed as failures per million operations, (operating) time based failures, systematic failures and human errors, have to be converted to failure rates constant over time. This can be done by making use of the test results, e.g. 1,000 solenoid valves proof tested with a regular interval over a period of 10 years yield a number of failures per 10,000 'solenoid valve years' which can be converted to failures per year for a solenoid valve.

NOTE: Preventive maintenance will reduce time dependent failures, resulting in lower converted unrevealed failure rates.

For NDE output circuits the failure rate of cables and connections, power supply, instrument air supply, etc. shall be included in the unrevealed failure rate of the final element, while for NE output circuits they shall be included in the revealed failure rate.

8.3 INPUTS INTO THE CALCULATION METHODOLOGY

8.3.1 Instrumented protective system

A selection is to be made between:
- relay system;
- solid-state/magnetic-core system;
- IPS-PLC system;
- other, in which the user is free to enter the failure rate data required.

8.3.2 IPF architecture

The architecture for the initiator and final element components of the IPF are not necessarily the same.

The following initiator architectures are covered by the calculation methodology:
- non-robust, for both revealed and unrevealed failures, i.e. 1oo1;
- unrevealed failure robust and non-robust for revealed failures, i.e. 1oo2;
- revealed failure robust and non-robust for unrevealed failures, i.e. 2oo2;
- unrevealed failure robust and revealed failure robust, i.e. 2oo3.

The calculation methodology covers the following architectures for final elements:
- non-robust, for both revealed and unrevealed failures, i.e. 1oo1, for rotating equipment stop circuits and valves;
- unrevealed failure robust and non-robust for revealed failures, i.e. 1oo2, for valves;
- revealed failure robust and non-robust for unrevealed failures, i.e. 2oo2, for valves;
- unrevealed failure robust and revealed failure robust, i.e. '2oo4', for valves.

8.3.3 Failure rates

Both unrevealed and revealed failure rates of the following loop components shall be entered into the calculation methodology:

- The initiator, excluding the IPS input. For those cases where no failure rate data are available from local records, the calculation methodology provides default failure rates.
- IPS input. For PLC type IPSs, this is the (robust) input card. For other IPSs this is the trip amplifier and the first relay, solid-state module or magnetic-core. Except for 'other' types of IPS systems, failure rates are fixed in the calculation methodology.
- Logic solver. Except for 'other' logic solver types, failure rates are fixed in the calculation methodology.
- IPS output. For PLC type IPSs, this is the (robust) output card. For other IPSs this is the last relay, solid-state module or magnetic-core. Except for 'other' types of IPS systems, failure rates are fixed in the calculation methodology.
- The final element, excluding the IPS output. For those cases where no failure rate data are available from local records, the calculation methodology provides default failure rates.

The failure rates for the initiator and IPS input are added to give the total initiator failure rate because it is assumed that both the initiator and the IPS input are tested during the regular manual or automatic proof test. For similar reasons, the failure rates for the IPS output and final element are added to give the total final element failure rate.

An upgrade or new version of the IPS may necessitate an update of the failure rates mentioned above.

8.3.4 Testing

The following types of information related to testing are required:

- Test interval for the initiator and IPS input combination, and for the IPS output and final element combination. These two test intervals are not necessarily the same. The logic solver is assumed to be tested only during the maintenance interval.
- Coverage factors with which these tests are performed.
- Test duration. It is assumed that the initiator is on maintenance override and the final element is either mechanically prohibited from moving fully or bypassed. Hence during the test both inputs and outputs are in the unrevealed failure condition. For tests where this is not the case, e.g. automatic testing of initiators by MVC, the test duration should be set to zero.
- Maintenance interval or lifetime. Both the input and the output combinations will be tested during planned shutdown (maintenance interval) with a coverage factor as close as possible to 1, see (7.). The maintenance interval shall be maximum 4 years if the planned shutdown cycle exceeds 4 years. Relay type logic solvers shall also be tested during the planned shutdown, hence the maintenance interval is also applicable to this type of logic solvers. Solid-state/magnetic-core and IPS-PLC logic solvers do not require testing during planned shutdowns, hence the lifetime of this type of equipment shall be taken into account.
- Repair time shall be taken into account for all components of the loop. The calculation methodology assumes that the loop stays in override when an unrevealed failure is found during the test. Repair times for both revealed and unrevealed failures are assumed to be the same.

8.4 OUTPUTS OF THE CALCULATION METHODOLOGY

The calculation methodology provides the following outputs:

- PFD of the initiator and IPS input combination;
- PFD of the logic solver;
- PFD of the IPS output and final element combination;
- PFD of the IPF, assuming the initiator and final element are in override during repair and assuming the initiator and final element are not in override during repair;
- IPF class of the IPF, assuming the initiator and final element are in override during repair and assuming the initiator and final element are not in override during repair;
- revealed failure rate of the above mentioned IPF components.

NOTE: IPF class V or VI cannot be obtained when the initiator or final element are single (1oo1) or revealed

failure robust (2oo2), irrespective of the PFD.

The PFD of the IPF loop components are given to enable test interval optimisation.

The IPF PFD shall be lower than the PFD required for the IPF class related to the IPF. If this is not the case, test intervals, architecture or function components shall be changed such that the PFD is sufficiently reduced.

8.5 CALCULATION OF TEST INTERVAL - SPECIAL CASES

8.5.1 Initiator or final element part of more functions

If an initiator or final element is part of multiple IPFs, the test interval for the initiator or final element shall be the shortest of the initiator or final element test interval calculated for the IPFs.

8.5.2 Adding rule

The simple rule given in (8.5.1) is not valid when the adding rule is applied, see (4.3), e.g. 13 initiators and 1 final element. If all functions are IPF class III, the adding rule results in final element implementation requirements as per class IV. A class IV final element may be implemented single (1oo1) and, if no additional steps are taken, the test interval for the final element would be the same as in the case of the final element being part of only the most stringent IPF class III function.

The steps to be taken to determine the test interval taking into account the more stringent final element requirements are:

(i) Calculate the PFD for each loop and take the most stringent final element PFD.
(ii) Reduce the test interval of the final element such that the PFD obtained in the previous step is reduced by a factor 10.
(iii) Use this test interval as the final element test interval.

If in the example above all individual functions would have been class IV, the final element shall be implemented as class V which, according to the deterministic class V requirements, would mean unrevealed failure robust. The test interval shall be calculated following the steps indicated above, with the addition that in step (ii) the unrevealed failure robustness is incorporated.

NOTE: The addition of unrevealed failure robustness may result in an increased test interval.

8.5.3 Synergetic consequences

The following steps shall be taken to determine the test interval taking into account the more stringent initiator requirements if synergetic consequences (3.2.4.3.5) are applicable:

(i) Calculate the PFD for each function and take the most stringent initiator PFD.
(ii) If the initiator IPF class resulting from the check on synergetic consequences is one IPF class above the highest IPF class of that initiator for the classifications excluding the synergetic consequences, reduce the test interval of the initiator such that the PFD obtained in the first step is reduced by a factor 10.
(iii) If the initiator IPF class resulting from the check on synergetic consequences is two IPF classes above the highest IPF class of that initiator for the classifications excluding the synergetic consequences, reduce the test interval of the initiator such that the PFD obtained in the first step is reduced by a factor 100.
(iv) Use this test interval as the initiator test interval.

If all individual functions are class IV or lower and due to synergetic consequences the initiator shall be implemented as class V, the initiator shall be unrevealed failure robust. The test interval shall in this case be calculated following the steps indicated above, with the addition that in step (ii) or (iii) the unrevealed failure robustness is incorporated.

NOTE: The addition of unrevealed failure robustness may result in an increased test interval.

9. MAINTENANCE

9.1 INTEGRITY

Integrity of IPFs shall be managed by applying the following:
- Modifications shall be carried out following plant change procedures.
- Temporary modifications, e.g. defeat of an IPF loop, shall be separately identified within the plant change procedure.
- For software based IPSs, principles of system management shall be applied.
- A focal point for Manufacturer/Supplier maintenance and support shall be appointed.
- System revision and upgrades shall be avoided, see also (5.3). In case a revision or upgrade is required, procedures as described by the Manufacturer/Supplier shall be adhered to. All revisions and upgrades shall be documented.
- Software back-ups shall be made at regular intervals.
- Security and access rights shall be documented.
- A system logbook shall be available for recording all systems modifications.
- System documentation shall be available.
- Adherence to strict security procedures when remote maintenance is applied.
- Follow-up of pending repairs.

9.2 TEST PROCEDURES

Procedures and test sheets for periodic functional testing and inspection shall be available and used.

It shall be clear to the users which part of the intended (by design) protection functionality is covered by the test procedures.

Testing shall be carried out according to a pre-defined planning schedule, based on test intervals calculated according to (8.). The schedule status shall be reported.

Manual testing of IPFs shall be performed by a qualified team having dedicated procedures, reports, data bases, etc. This team shall work in close relation with operational, mechanical and electrical testing teams, as well as with the instrument maintenance team.

The team shall ensure that unrevealed failures are not introduced by the tests (e.g. by leaving impulse lines closed).

IPF testing may be subcontracted, depending on local circumstances.

9.3 TEST RESULTS

Test results and details of corrective actions or preventive maintenance activities shall be recorded, preferably in coded form, in a database for future reference and statistical analysis.

Coding should be as follows:
- Failure mode which indicates the problem as found by the technician, e.g. impulse line closed.
- Failure causes indicating the causes of the problems (if known), e.g. human error.
- Failure type (unrevealed).
- Corrective maintenance and preventive actions taken.
- Time spent and manning required on the various activities.

These results shall be analysed, reported and used to optimise test frequencies or to modify the system where necessary. Test frequencies should be adjusted to reflect actual data available from the database.

Test reports shall be archived for at least ten years or for the life of the IPF, whichever is longer.

9.4 SCHEDULED MAINTENANCE

Apart from functional test and inspection procedures, time and condition based maintenance schedules such as periodic calibrations, valve stroking or periodic valve overhaul may also be required.

9.5 TRIP REPORTS

Trip reports should be stored, preferably in coded form, in the same database as the database referred to in (9.3).

The coding should be as follows:
- real demand;
- system (instrumentation) failure;
- human error;
- unknown.

Trip reports shall be analysed and used to optimise test frequencies or to modify the system where necessary.

9.6 MODIFICATIONS

Modifications shall follow the same IPF classification and implementation procedures as applied to new designs.

9.7 AUDITS

A yearly audit should be carried out to confirm compliance with:
- change procedures;
- test procedures;
- test schedule;
- recording and analysis of results;
- integrity management such as:
  - changes made to the logics performed by the IPS;
  - no 'forced' inputs or outputs present in the IPS;
  - adherence to restrictions imposed by the IPS type approval.

10. REFERENCES

In this DEP, reference is made to the following publications:

NOTE: Unless specifically designated by date, the latest edition of each publication shall be used, together with any amendments/supplements/revisions thereto.

SHELL STANDARDS

Index to DEP publications and standard specifications	DEP 00.00.05.05-Gen.
Requisitioning (binder)	DEP 30.10.01.10-Gen.
Hydraulic systems for operation of valves	DEP 31.36.10.30-Gen.
Fire, gas and smoke detection systems	DEP 32.30.20.11-Gen.
Instrumentation for equipment packages	DEP 32.31.09.31-Gen.
Instrument signal lines	DEP 32.37.20.10-Gen.
The instrumentation of depressuring systems	DEP 32.45.10.10-Gen.
Control valves - selection and specification	DEP 32.36.01.17-Gen.
Instrumented protective systems	DEP 32.80.10.30-Gen.
Data/requisition sheet for instrumented protective systems NOTE: Data/requisition sheets are contained in a binder, DEP 30.10.01.10-Gen.	DEP 32.80.10.93-Gen.
Electrical engineering guidelines	DEP 33.64.10.10-Gen.
Requirements for fire protection in onshore oil and gas processing and petrochemical installations	DEP 80.47.10.30-Gen.
Active fire protection systems and equipment for onshore facilities	DEP 80.47.10.31-Gen.
Communication between DCS and micro-processor based sub-systems	MF 91-0885
Measurement validation and comparison	MF 94-0495
Instrumented Protective Functions - Test of classification methodology	MF 95-0020
Instrumented Protective Functions - PC Software	OH 96/30180
Instrumentation for Ultimate Safeguarding Protection Philosophy and Application Guidelines	EP 95-1745

STANDARD DRAWINGS

Typical instrument electricity supply systems with static components	S 67.006

GERMAN STANDARDS

Control Technology; Fundamental Safety Aspects to be Considered for Measurement and Control Equipment.	DIN V 19250

Issued by:
Beuth Verlag GmbH
Burggrafenstrasze 6
Postfach 11 07
D-1000 Berlin 30
Germany.

Wartungseingriffe/Maintenance Override,
Version 2.2, 08. September 1994.

Issued by:
TÜV Rheinland
ISEB
Am Grauen Stein
D-51105 Cologne
Germany.
or:
TÜV Bayern
IQSE
Ridlerstrasse 31
D-80339 Munich
Germany.

INTERNATIONAL STANDARDS

Draft. Functional safety of safety related systems. Parts 1-7. — IEC/SC65A draft 1508

Industrial Process Control Valves
Part 4: Inspection and routine testing. — IEC 534-4

Issued by:
Central Office of the IEC
3, Rue de Varembé
CH 1211 Geneva 20
Switzerland.
Copies can also be obtained from national standards organisations.

APPENDIX 1 SUGGESTIONS ON HOW TO SET UP A CLASSIFICATION EXERCISE

Introduction

For the IPF classification exercise it is essential to set up a structure to optimise team productivity and quality of output. This Appendix gives guidelines for the organisation of an IPF classification exercise.

Planning

A planning schedule should be set up, detailing the individual team members by name and discipline. No more than 5 hours per day should be spent on classification because otherwise motivation and concentration may fall and the quality of team output may reduce dramatically. Each function requires equal attention. Regular breaks should be planned. The team members should not be disturbed during classification. Specialists such as rotating equipment or furnace specialists should be on call and available when their input is needed.

Team

The composition of an IPF classification team is defined in (3.2.2). Efficiency will be increased considerably by appointing a secretary who records the discussion in the IPF database. The secretary role can be fulfilled by a junior technologist or engineer. It is essential that the secretary has a technical background. The facilitator shall ensure that the discussions are sufficiently detailed without losing the objectives of the classification. Time keeping and preventing procedural errors are two important tasks for the facilitator.

Preparation

To minimise delays, all preparatory work shall be done prior to classification. Once the team has started the classification process no time should be lost doing work that could have been done in advance.

The following should be available before the start of the classification exercise:
- Copies of the documents which contain input information for the discussion.
- PC, including IPF classification database and IPF calculation software, overhead projector, LCD panel screen etc. shall have been set up and tested.
- Identification of the IPF loops and the creation of records in a database. The order in which they are going to be discussed shall have been fixed.

The following documents and office equipment should be available:
- Process and Utility Engineering Flow Schemes (PEFSs);
- Process Flow Schemes (PFSs), Process Safeguarding Flow Schemes (PSFSs), cause and effect matrices, process safeguarding memoranda and IPF & control narratives;
- overhead projector;
- projection screen or equivalent;
- LCD panel screen for use on the overhead projector;
- PC installed in the meeting room (connected to LCD panel);
- software package to store the classification results in a database, installed on the PC.

APPENDIX 2 FIGURES

FIGURE 1 RISK REDUCTION - GENERAL CONCEPTS

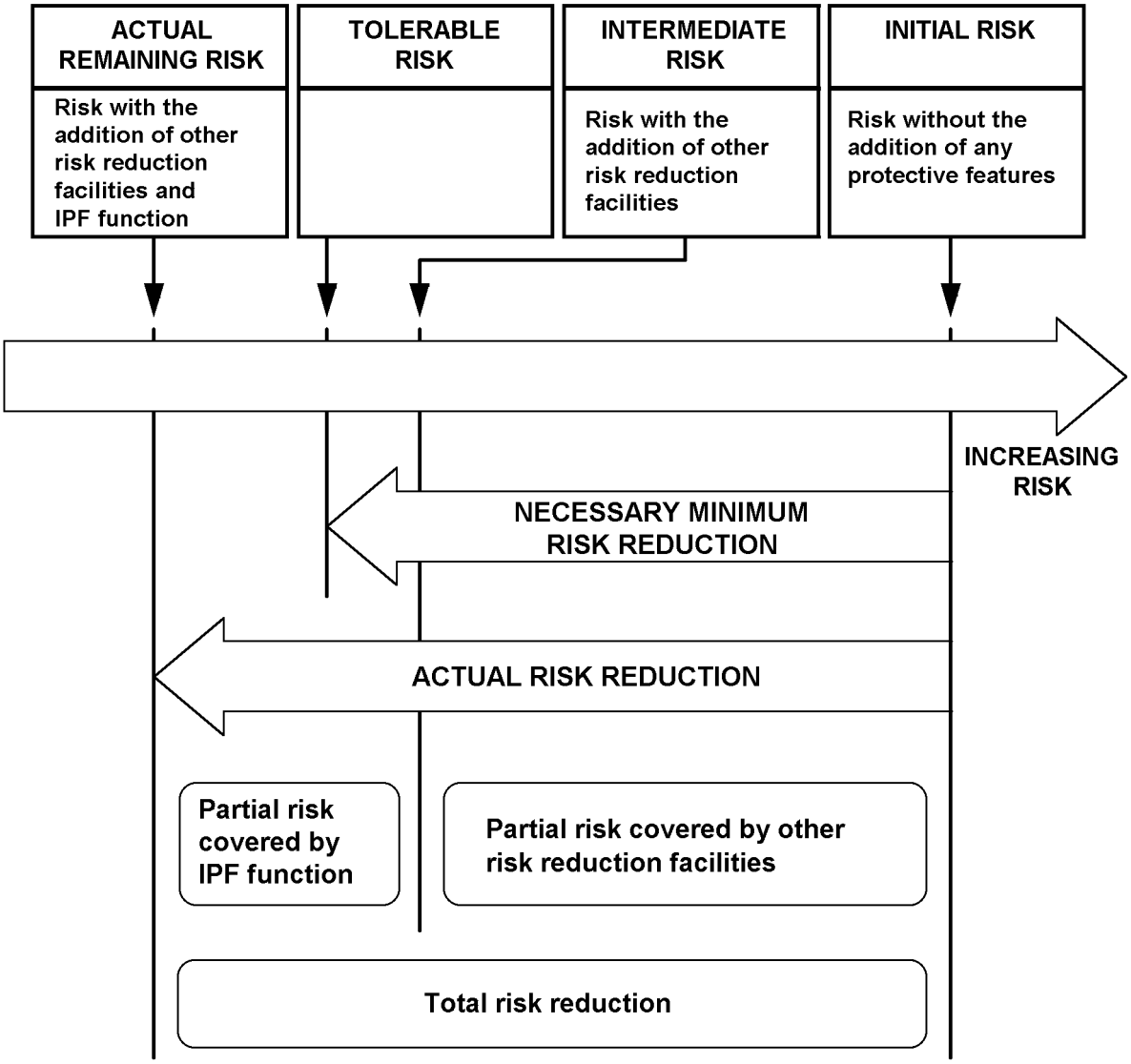


FIGURE 2 IPF CLASSIFICATION AND IMPLEMENTATION WITHOUT METHODOLOGY OF THIS DEP

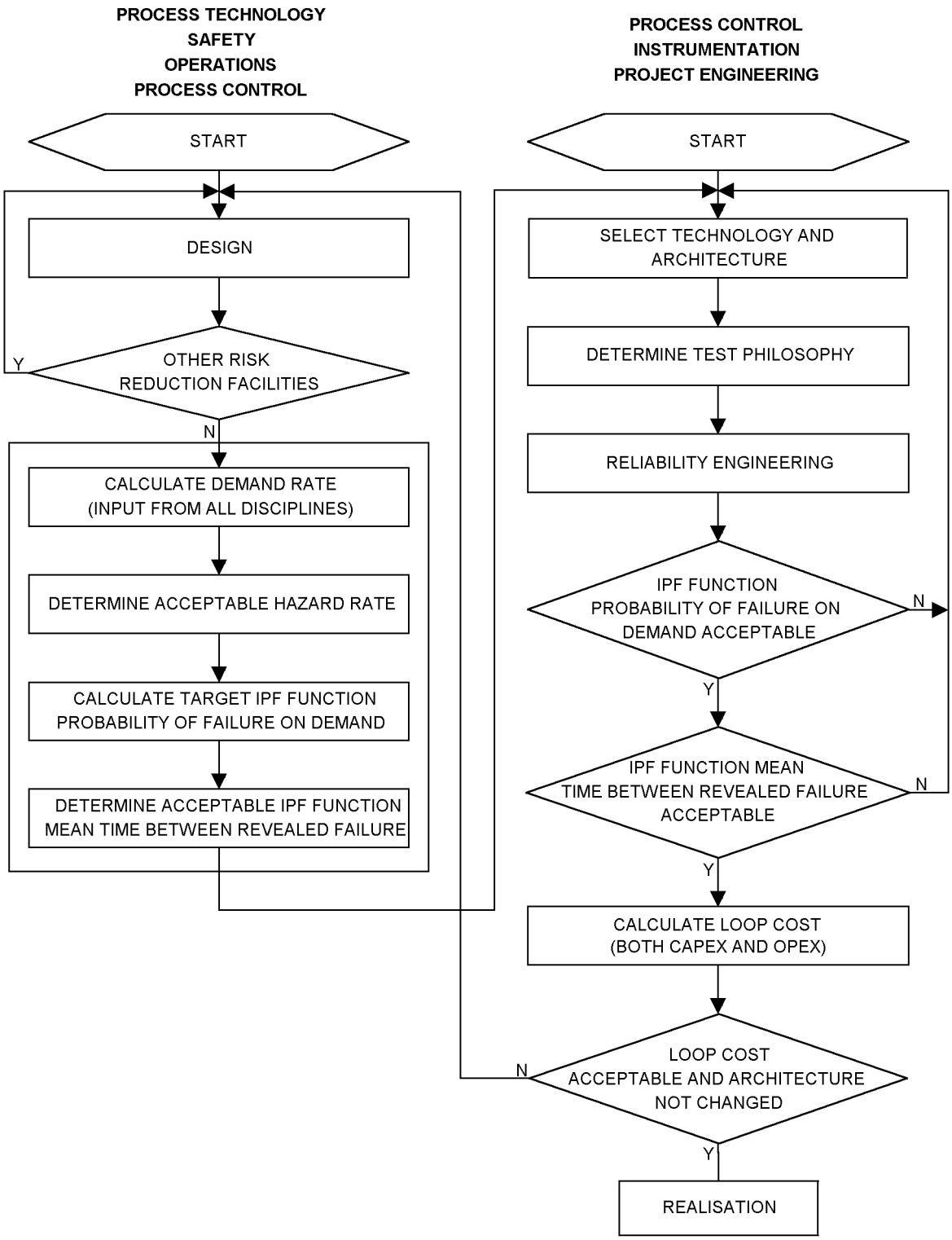


FIGURE 3 IPF CLASSIFICATION AND IMPLEMENTATION WITH METHODOLOGY OF THIS DEP

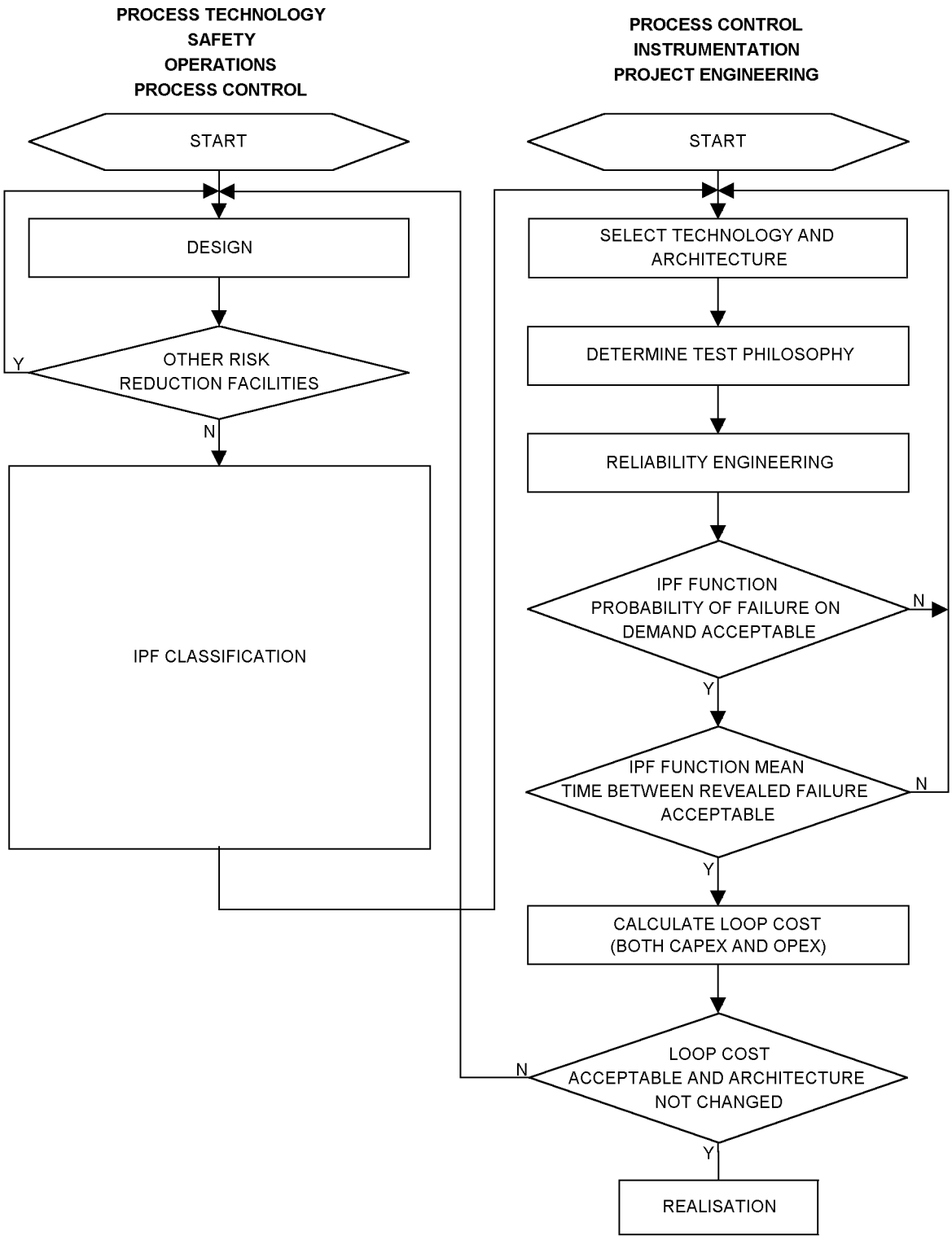


FIGURE 4 MULTIPLE INITIATORS RELATED TO ONE FINAL ELEMENT

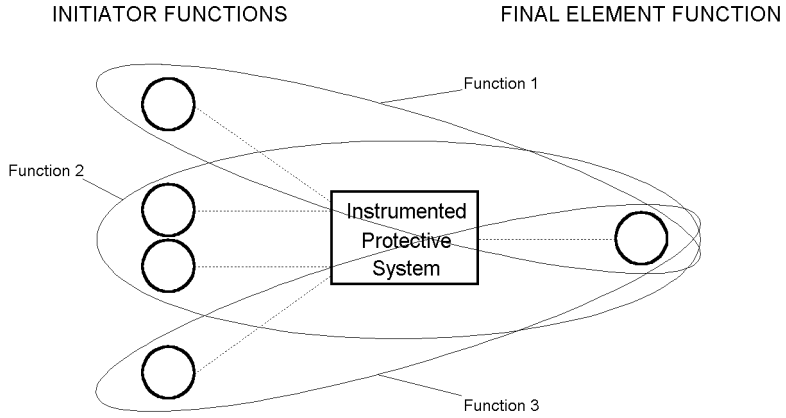


FIGURE 5 ONE INITIATOR RELATED TO MULTIPLE FINAL ELEMENTS

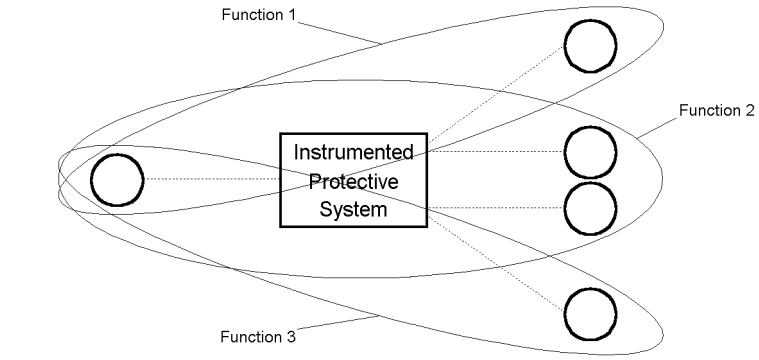
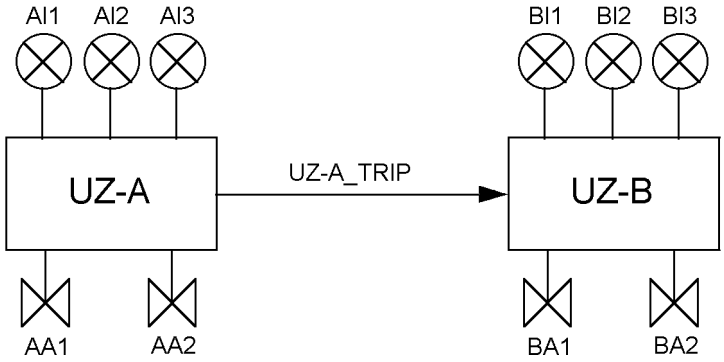


FIGURE 6 REDUCTION OF CLASSIFICATION EFFORT

SPIDER DIAGRAM



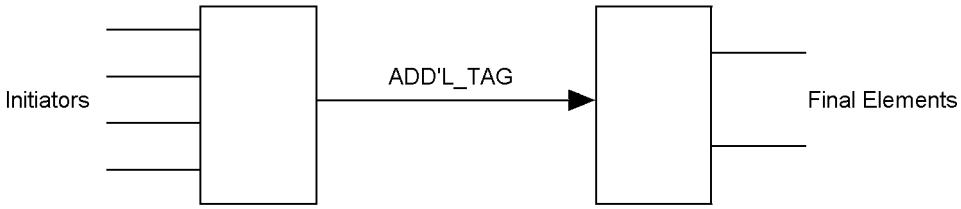
Without reduction of classification effort, a total of 24 IPFs would have to be classified, including the synergetic consequences classification. To reduce the classification effort, follow these steps:

1. Assign a temporary tag number to the connection UZ-A to UZ-B, in the sketch 'UZ-A_TRIP'.
2. Classify all 9 UZ-B functions BI1-BA1; BI1-BA2; BI2-BA1; BI2-BA2; BI3-BA1; BI3-BA2 and initiators failure
3. Classify UZ-A_TRIP-BA1 and UZ-A_TRIP-BA2 and UZ-A_TRIP initiator failure
4. Classify all 9 UZ-A functions AI1-AA1; AI1-AA2; AI2-AA1; AI2-AA2; AI3-AA1; AI3-AA2 and initiators failure
5. If the AI initiator classes resulting from step 4 are equal to or exceed the UZ-A_TRIP IPF class resulting from step 3, the classification is finished. The total number of classifications performed is 21.
6. If step 5 is not true for one or more AIs, one of the following options shall be selected:
   - Accept the UZ-A_TRIP IPF class for all those AIs. The classification is finished and the total number of classifications performed is 21, but the IPF class for those AIs is too high.
   - Classify those AIs to all BAs functions. The classification is finished and the total number of classifications performed is between 21 and 27.

NOTE: If UZ-A_TRIP is classified equal to the highest BI, a check shall be done whether the adding rule, see (4.3), has any effect on BA1 or BA2.

FULL CAUSE AND EFFECT MATRIX

The classification effort can also be reduced when all the possibilities in a cause and effect matrix are implemented, i.e. each initiator trips all final elements. In this case the IPFs can be split as follows:



To classify, follow these steps:

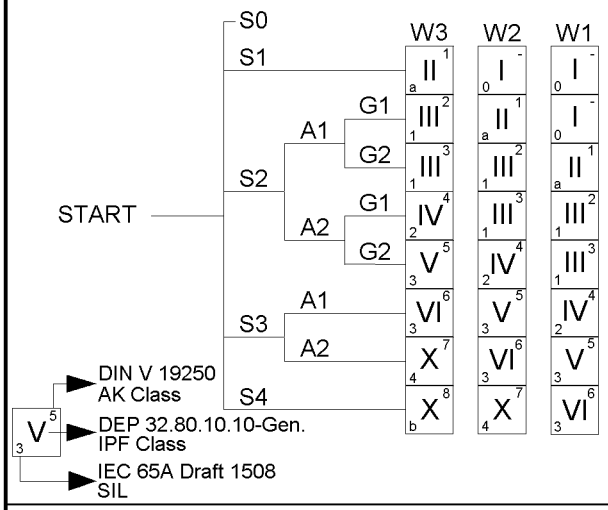
1. Classify each initiator to ADD'L_TAG function, the latter shall also be given a description, e.g. plant trip. This results in the required initiator class.
2. Classify each ADD'L_TAG to final element function. The demand rate (W) on ADD'L_TAG can be determined by summating the initiator Ws (10 or more W1s result in W2 and 10 or more W2s result in W3 with the W never above W3) or from experience. This results in the required final element class.

NOTE: The synergetic consequence check on initiator failure is not required because it is embedded in step 1.

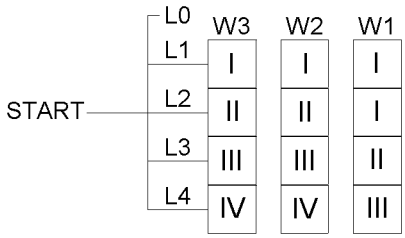
FIGURE 7 IPF CLASSIFICATION RISK DIAGRAMS

CLASSIFY IPF UNREVEALED FAILURES FOR THE THREE CATEGORIES AND SELECT THE MOST STRINGENT IPF CLASS

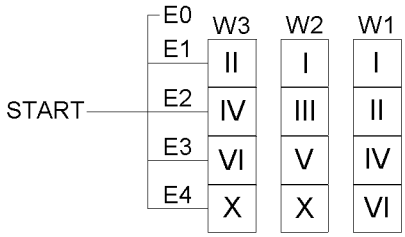
PERSONNEL SAFETY



PRODUCTION AND EQUIPMENT LOSS



ENVIRONMENT



(W) Frequency of demand
- W0 = Unclassified
- W1 = Very low (demand rate once per 10-100 years)
- W2 = Low (demand rate once per 1-10 years)
- W3 = Relatively high (demand rate more than once per year)

(S) Potential extent of human injury per demand if Instrumented Protective Function fails on demand
- S0 = No injury
- S1 = Slight injury, non-permanent
- S2 = Severe injury, death of one person
- S3 = Death of several persons
- S4 = Catastrophe, many casualties

(A) Duration of presence in danger zone
- A1 = Seldom to frequently (at time of demand)
- A2 = Frequently to continuously (at time of demand)

(G) Possibility to avert hazard
- G1 = Under certain conditions
- G2 = Hardly possible

(L) Potential production and equipment loss per demand if Instrumented Protective Function fails on demand
- L0 = No operational upset; no damage to equipment
- L1 = Minor operational upset; minor damage to equipment
- L2 = Moderate operational upset; moderate damage to equipment
- L3 = Major operational upset; major damage to equipment
- L4 = Damage to essential equipment causing major economic loss; major loss of containment

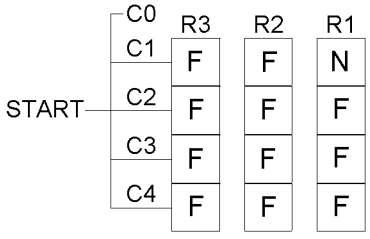
(E) Potential environment consequences per demand if Instrumented Protective Function fails on demand
- E0 = No release or release with negligible damage to the environment
- E1 = Release with minor damage to the environment that should be reported
- E2 = Release within fence with significant damage to the environment
- E3 = Release outside fence with temporary major damage to the environment
- E4 = Release outside fence with permanent major damage to the environment

Note: Take public image damage into account when classifying environment consequences.

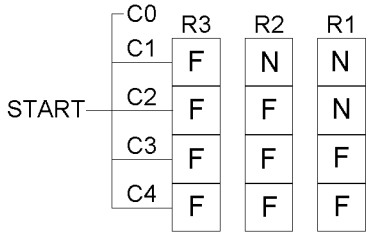
CLASSIFY IPF REVEALED FAILURES

COST OF REVEALED FAILURE ROBUSTNESS (CR)

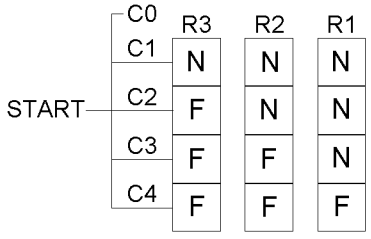
CR ≤ USD 1,000



USD 1,000 < CR ≤ USD 10,000



USD 10,000 < CR ≤ USD 100,000



(C) Potential production loss per occurrence if Instrumented Protective Function takes action without a demand
- C0 = Cost ≤ USD 1,000
- C1 = USD 1,000 < Cost ≤ USD 100,000
- C2 = USD 100,000 < Cost ≤ USD 1,000,000
- C3 = USD 1,000,000 < Cost ≤ USD 10,000,000
- C4 = USD 10,000,000 < Cost

(R) Frequency of revealed failure
- R1 = Very low (revealed failure rate once per 10-100 years)
- R2 = Low (revealed failure rate once per 1-10 years)
- R3 = Relatively high (revealed failure rate more than once per year)

FIGURE 8 IPF CLASSIFICATION RESULTS - DATABASE PRINT-OUT - EXAMPLE

IPF CLASSIFICATION

PEFS Initiator Tag:	T-2.665.807-C		
Initiator Tag:	17PDZA-002LL 17FZA-012LL	**Service Desc.:**	Backflow Detection R-1701 Feed
Related UZ1:	17UZ-020	**Service Desc.:**	HC Feed Backflow IPS
Related UZ2:		**Service Desc.:**	
Related UZ3:		**Service Desc.:**	
Intermediate Tag1:	17UZ-021 17UZ-022		
Intermediate Tag2:			
Intermediate Tag3:			
Final Element Tag:	17FCV-011 17UZ-021	**Service Desc.:**	Feed To Reactor R-1701
Is It A Pre-Alarm:	N		

Consequence Of Failure On Demand:
Case 'a'. The consequences are backspinning of pump and rupture of vessel V-1701 since it is impractical or impossible to protect it with a relief valve (too hot material). Vessel rupture is much more severe than pump backspinning, therefore the latter is not dealt with in detail any further.
Case 'b'. The pump will be stopped by 17FZA-012LL or, if the trip level is not reached, the operator will stop the pump as soon as he recognises the situation. If the backflow protection system fails, the flare system will be over loaded both in terms of temperature and in terms of flow, but the flare system will not be ruptured.

Consequence Of Revealed Failure:
The pump will stop. The unit will be out of feed for 7 hours. At end of run the chances of the reactor temperature runaway protection system 17TZA-HHs activating are reasonably high which would cause an outage of 24 hours. The cost of a revealed failure is 5,600 t/d*45 USD/t*1d~USD 250,000.

Demand	**W:** 1 / 0					
Personnel Safety	**S:** 3 / 2	**A:** 2 / 1	**G:** - / 2	**Personnel Safety Class**	:	V / -
Loss	**L:** 4 / 4			**Production And Eq't Loss Class**	:	III / -
Environment	**E:** 1 / 0			**Environment Class**	:	II / -
				Overall Unrevealed Failure Class	:	V
Cost C: 2						
CR Initiator: USD 7,500		**Rate R:** 1		**Revealed Failure Class**	:	N
CR Final Element: USD 42,500		**Rate R:** 2		**Revealed Failure Class**	:	N

Note 1
There are more than one initiator and valve in the same function, but from the classification it will be clear that these are provided to implement unrevealed failure robustness.
There are two occurrences that can cause backflow: a. Pump stoppage. and b. Inadvertent opening of 17RV-002. These cases are indicated before and after the '/' respectively, i.e. a / b.

Note 2
For case 'a', every time the pump stops the possibility of backflow is present. This would result in a frequency of demand of more than once per year. However, two non-return valves (NRVs) are installed to reduce the frequency of demand on the IPF. One NRV reduces the frequency of demand by a factor 10 and two different makes and types of NRVs reduce the frequency of demand by a factor 50. The latter is not a factor 100 because of common mode failures not related to make and type. Because of the NRVs the classification of the frequency of demand on the IPF is reduced from W3 to W1.

Note 3
Inadvertent opening of 17RV-002 will happen very infrequently, W1. However, because NRVs are installed the frequency of demand on the IPF valves reduces to W0.

Note 4
For case 'a', the most dangerous time is when the pump is started because a stop frequently occurs just after a start. The pump has a local start. This means that more than one person will be present during the most dangerous time and the classification shall therefore be A2.

Note 5
Two valves in a 1oo2 configuration results in R2.

FIGURE 9 IPF CLASSIFICATION - BLANK FORM

IPF CLASSIFICATION

PEFS Initiator Tag:

Initiator Tag: **Service Desc.:**

Related UZ1: **Service Desc.:**

Related UZ2: **Service Desc.:**

Related UZ3: **Service Desc.:**

Intermediate Tag1:

Intermediate Tag2:

Intermediate Tag3:

Final Element Tag: **Service Desc.:**

Is It A Pre-Alarm:

Consequence Of Failure On Demand:

Consequence Of Revealed Failure:

Demand	**W:**				
Personnel Safety	**S:**	**A:**	**G:**	**Personnel Safety Class**	**:**
Loss	**L:**			**Production And Eq't Loss Class**	**:**
Environment	**E:**			**Environment Class**	**:**
				Overall Unrevealed Failure Class	**:**

Cost C:

CR Initiator: **Rate R:** **Revealed Failure Class :**

CR Final element: **Rate R:** **Revealed Failure Class :**

Note 1

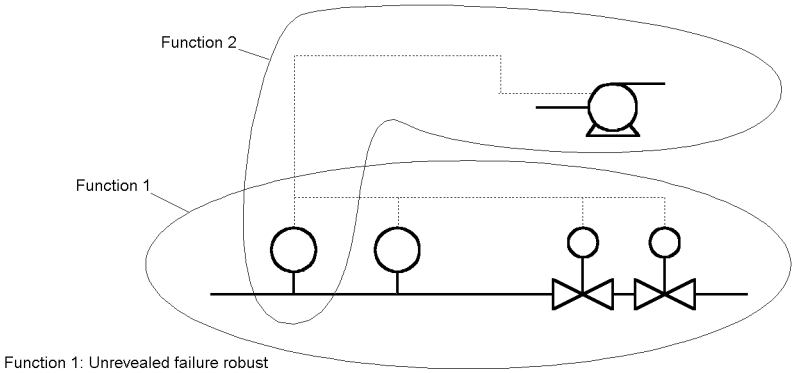
Note 2

Note 3

Note 4

Note 5

FIGURE 10 ONE INITIATOR CONNECTED TO MULTIPLE FINAL ELEMENTS



Function 1: Unrevealed failure robust
Function 2: No additional requirements for robustness

FIGURE 11 COMBINATION OF UNREVEALED AND REVEALED FAILURE ROBUST VALVES

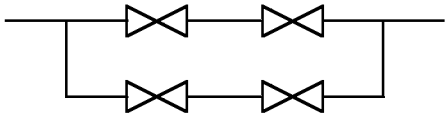


FIGURE 12 POSSIBLE IMPLEMENTATION OF IPF CLASSES

Instrumented Protective Function Classes Related to Unrevealed Failures

X = Change to safer design
, possible implementation:

VI = $PFD < 10^{-3}$
- Initiator: Separate from control; unrevealed failure robust; diverse
- IPS: Solid-state/magnetic-core hardware (TÜV approved AK6)
- Final element:
  Valve: Separate from control; unrevealed failure robust; diverse (if no TSO leakage class V or VI requirements, second valve may be a control valve tripped by a solenoid valve)
  Rotating equipment stop circuit: No special equipment, unrevealed failure robust

, possible implementation:

V = $PFD < 10^{-3}$
- Initiator: Separate from control; unrevealed failure robust
- IPS: Relay / IPS-PLC / solid-state/magnetic-core hardware (TÜV approved AK5)
- Final element:
  Valve: Separate from control; unrevealed failure robust (if no TSO leakage class V or VI requirements, second valve may be a control valve tripped by a solenoid valve)
  Rotating equipment stop circuit: No special equipment, unrevealed failure robust

, possible implementation:

IV = $PFD < 10^{-2}$
- Initiator: Separate from control
- IPS: Relay / IPS-PLC / solid-state/magnetic-core hardware (TÜV approved AK4)
- Final element:
  Valve: Separate from control; unrevealed failure robust (if no TSO leakage class V or VI requirements, second valve may be a control valve tripped by a solenoid valve)
  Rotating equipment stop circuit: No special equipment

, possible implementation:

III = $PFD < 10^{-1}$
- Initiator: Separate from control
- IPS: Relay / IPS-PLC / solid-state/magnetic-core hardware (TÜV approved AK3)
- Final element:
  Valve: Separate from control, unless the demand on the IPF cannot be caused by a malfunction of said control valve and the valve has no TSO leakage class V or VI requirements
  Rotating equipment stop circuit: No special equipment

, possible implementation:

II = $PFD \geq 10^{-1}$
- No special equipment
- Switching function

, possible implementation:

I = $PFD \geq 10^{-1}$
- No special equipment
- Alarm only, if operator action can be relied upon, otherwise classify and implement as II

For all classes II-VI a pre-alarm shall be included, provided corrective operator action to avoid the IPF action is feasible.
All actions for classes II-VI shall be announced by an alarm.
Revealed failure robustness may be added to all possible implementations without degrading the IPF class, provided the test and maintenance intervals are selected according Figure 13.
In case the class already requires unrevealed failure robustness, the combination revealed and unrevealed failure robustness shall be implemented.

NOTES:
1. Class V/VI requires unrevealed failure robustness.
2. The test and maintenance intervals related to the selected architectures can be obtained from Figure 13.
3. The AK classes given above refer to DIN V 19250 requirement classes.
4. Underlined items are mandatory minimum requirements.

Instrumented Protective Function Classes Related to Revealed Failures

F = Revealed failure robust
N = No additional requirements for robustness

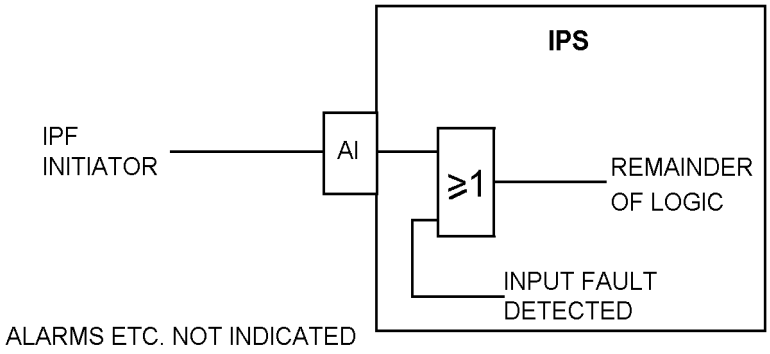
NOTE: The 'F' originates from fault tolerant. R has not been used in order to avoid confusion with the revealed failure rate classification.

FIGURE 13 POSSIBLE IMPLEMENTATION OF IPF CLASSES ARCHITECTURES AND MAXIMUM TEST AND MAINTENANCE INTERVALS

IPS Type	Final Element Type	Initiator Architecture	Final Element Architecture	Test and Maintenance Interval (years) Using Default Failure Rates and Coverage Factors see (8.)											
				IPF Class III				IPF Class IV				IPF Class V/VI			
				I	LS	F	PFD	I	LS	F	PFD	I	LS	F	PFD
PLC	Rot. Eq't	S	S	4	10	4	5.15E-02	0.5	10	0.5	9.44E-03	N/A	N/A	N/A	N/A
PLC	Rot. Eq't	UFR	S	4	10	4	7.92E-03	4	10	4	7.92E-03	N/A	N/A	N/A	N/A
PLC	Rot. Eq't	RFR	S	4	10	4	9.34E-02	0.17	10	0.5	9.78E-03	N/A	N/A	N/A	N/A
PLC	Rot. Eq't	UFR/RFR	S	4	10	4	1.22E-02	3	10	4	9.59E-03	N/A	N/A	N/A	N/A
PLC	Valve	S	S	4	10	2	9.17E-02	0.17*	10	0.17*	9.46E-03	N/A	N/A	N/A	N/A
PLC	Valve	S	UFR	4	10	4	5.37E-02	0.5	10	1.5	9.73E-03	N/A	N/A	N/A	N/A
PLC	Valve	S	RFR	4	10	1	9.24E-02	0.04	10	0.04	9.62E-03	N/A	N/A	N/A	N/A
PLC	Valve	S	UFR/RFR	4	10	4	6.11E-02	0.5	10	1	9.63E-03	N/A	N/A	N/A	N/A
PLC	Valve	UFR	S	4	10	4	8.87E-02	3	10	0.25	9.25E-03	N/A	N/A	N/A	N/A
PLC	Valve	UFR	UFR	4	10	4	1.01E-02	4	10	3	7.01E-03	1	10	1	9.95E-04
PLC	Valve	UFR	RFR	4	10	2	8.94E-02	4	10	0.08	8.09E-03	N/A	N/A	N/A	N/A
PLC	Valve	UFR	UFR/RFR	4	10	4	1.75E-02	4	10	2	6.72E-03	1.5	10	0.5	9.23E-04
PLC	Valve	RFR	S	2	10	2	9.39E-02	0.08*	10	0.08*	9.64E-03	N/A	N/A	N/A	N/A
PLC	Valve	RFR	UFR	4	10	4	9.55E-02	0.17	10	1	9.41E-03	N/A	N/A	N/A	N/A
PLC	Valve	RFR	RFR	2	10	1	9.46E-02	0.04	10	0.04	9.62E-03	N/A	N/A	N/A	N/A
PLC	Valve	RFR	UFR/RFR	4	10	3	9.69E-02	0.17	10	0.75	9.49E-03	N/A	N/A	N/A	N/A
PLC	Valve	UFR/RFR	S	4	10	4	9.30E-02	2	10	0.25	9.82E-03	N/A	N/A	N/A	N/A
PLC	Valve	UFR/RFR	UFR	4	10	4	1.44E-02	2	10	4	9.74E-03	0.75	10	0.75	9.38E-04
PLC	Valve	UFR/RFR	RFR	4	10	2	9.37E-02	3	10	0.08	9.76E-03	N/A	N/A	N/A	N/A
PLC	Valve	UFR/RFR	UFR/RFR	4	10	4	2.18E-02	3	10	2	8.39E-03	0.75	10	0.5	9.07E-04
Relay	Rot. Eq't	S	S	4	4	4	8.36E-02	0.25	0.25	0.25	9.24E-03	N/A	N/A	N/A	N/A
Relay	Rot. Eq't	UFR	S	4	4	4	1.69E-02	2	4	2	9.37E-03	N/A	N/A	N/A	N/A
Relay	Rot. Eq't	RFR	S	2	4	4	8.70E-02	0.04*	0.04	0.04*	9.39E-03	N/A	N/A	N/A	N/A
Relay	Rot. Eq't	UFR/RFR	S	4	4	4	2.72E-02	1.5	4	1.5	9.83E-03	N/A	N/A	N/A	N/A
Relay	Valve	S	S	2	4	2	8.98E-02	0.08	0.08	0.08	8.35E-03	N/A	N/A	N/A	N/A
Relay	Valve	S	UFR	4	4	4	8.42E-02	0.25	0.5	0.5	9.60E-03	N/A	N/A	N/A	N/A
Relay	Valve	S	RFR	2	4	1	9.05E-02	0.04*	0.04	0.04*	8.48E-03	N/A	N/A	N/A	N/A
Relay	Valve	S	UFR/RFR	4	4	4	9.19E-02	0.25	0.5	0.5	9.75E-03	N/A	N/A	N/A	N/A
Relay	Valve	UFR	S	4	4	4	9.74E-02	0.5	0.5	0.25	8.49E-03	N/A	N/A	N/A	N/A
Relay	Valve	UFR	UFR	4	4	4	1.76E-02	2	4	2	7.89E-03	0.5	0.5	0.5	8.77E-04
Relay	Valve	UFR	RFR	4	4	2	9.82E-02	2	2	0.08	9.39E-03	N/A	N/A	N/A	N/A
Relay	Valve	UFR	UFR/RFR	4	4	4	2.53E-02	2	2	2	8.06E-03	0.25	0.25	0.25	4.44E-04
Relay	Valve	RFR	S	1	4	2	9.34E-02	0.02*	0.02	0.02*	9.97E-03	N/A	N/A	N/A	N/A
Relay	Valve	RFR	UFR	2	4	4	8.77E-02	0.02	0.5	0.5	9.14E-03	N/A	N/A	N/A	N/A
Relay	Valve	RFR	RFR	1	4	1	9.41E-02	-	-	-	-	N/A	N/A	N/A	N/A
Relay	Valve	RFR	UFR/RFR	2	4	4	9.53E-02	0.02	0.5	0.5	9.30E-03	N/A	N/A	N/A	N/A
Relay	Valve	UFR/RFR	S	2	4	4	9.66E-02	0.75	0.75	0.25	9.55E-03	N/A	N/A	N/A	N/A
Relay	Valve	UFR/RFR	UFR	4	4	4	2.79E-02	2	2	2	9.12E-03	0.25	0.25	0.25	5.76E-04
Relay	Valve	UFR/RFR	RFR	4	4	1.5	8.83E-02	1	1	0.08	8.25E-03	N/A	N/A	N/A	N/A
Relay	Valve	UFR/RFR	UFR/RFR	4	4	4	3.56E-02	1.5	1.5	1.5	7.07E-03	0.25	0.25	0.25	6.11E-04
SS/MC	Rot. Eq't	S	S	4	10	4	5.11E-02	0.5	10	0.5	9.20E-03	N/A	N/A	N/A	N/A
SS/MC	Rot. Eq't	UFR	S	4	10	4	7.52E-03	4	10	4	7.52E-03	N/A	N/A	N/A	N/A
SS/MC	Rot. Eq't	RFR	S	4	10	4	9.29E-02	0.17	10	0.5	9.54E-03	N/A	N/A	N/A	N/A
SS/MC	Rot. Eq't	UFR/RFR	S	4	10	4	1.18E-02	3	10	4	9.18E-03	N/A	N/A	N/A	N/A
SS/MC	Valve	S	S	4	10	2	9.13E-02	0.17*	10	0.17*	9.25E-03	N/A	N/A	N/A	N/A
SS/MC	Valve	S	UFR	4	10	4	5.34E-02	0.5	10	1.5	9.51E-03	N/A	N/A	N/A	N/A
SS/MC	Valve	S	RFR	4	10	1	9.21E-02	0.04	10	0.04	9.41E-03	N/A	N/A	N/A	N/A
SS/MC	Valve	S	UFR/RFR	4	10	4	6.08E-02	0.5	10	1	9.42E-03	N/A	N/A	N/A	N/A
SS/MC	Valve	UFR	S	4	10	4	8.83E-02	3	10	0.25	9.03E-03	N/A	N/A	N/A	N/A
SS/MC	Valve	UFR	UFR	4	10	4	9.87E-03	4	10	4	9.87E-03	1.5	10	1	9.90E-04
SS/MC	Valve	UFR	RFR	4	10	2	8.90E-02	4	10	0.08	7.88E-03	N/A	N/A	N/A	N/A
SS/MC	Valve	UFR	UFR/RFR	4	10	4	1.73E-02	4	10	2	6.50E-03	2	10	0.5	9.83E-04
SS/MC	Valve	RFR	S	2	10	2	9.35E-02	0.08*	10	0.08*	9.43E-03	N/A	N/A	N/A	N/A
SS/MC	Valve	RFR	UFR	4	10	4	9.52E-02	0.17	10	1	9.20E-03	N/A	N/A	N/A	N/A
SS/MC	Valve	RFR	RFR	2	10	1	9.43E-02	0.04	10	0.04	9.40E-03	N/A	N/A	N/A	N/A
SS/MC	Valve	RFR	UFR/RFR	4	10	3	9.65E-02	0.17	10	0.75	9.28E-03	N/A	N/A	N/A	N/A
SS/MC	Valve	UFR/RFR	S	4	10	4	9.26E-02	2	10	0.25	9.60E-03	N/A	N/A	N/A	N/A
SS/MC	Valve	UFR/RFR	UFR	4	10	4	1.42E-02	2	10	4	9.50E-03	0.75	10	1	9.74E-04
SS/MC	Valve	UFR/RFR	RFR	4	10	2	9.34E-02	3	10	0.08	9.54E-03	N/A	N/A	N/A	N/A
SS/MC	Valve	UFR/RFR	UFR/RFR	4	10	4	2.16E-02	3	10	2	8.16E-03	1	10	0.5	9.23E-04

*	Actual trip to test, test duration 1E-15	Test / maintenance intervals (years) used:					
-	Required PFD cannot be obtained by reducing test interval	10	0.75	(9 months)	0.08	(4 weeks)	
F	Final Element (related interval is test interval, maintenance interval is 4 years)	4	0.5	(6 months)	0.04	(2 weeks)	
I	Initiator (related interval is test interval, maintenance interval is 4 years)	3	0.25	(3 months)	0.02	(1 week)	
LS	Logic Solver (related interval is maintenance interval)	2	0.17	(2 months)			
MC	Magnetic-Core	1.5					
N/A	Not Applicable (unrevealed failure robust required for IPF class V/VI)	1					
Rot. Eq't	Rotating Equipment Stop Circuit	PFD	Probability of Failure on Demand				
RFR	Revealed Failure Robust	S	Single				
SS	Solid-State	UFR	Unrevealed Failure Robust				

FIGURE 14 AUTOMATIC MAINTENANCE OVERRIDE



Acceptable provided the following is adhered to:

- A second or back-up indication shall be available to the operator.
- The control room shall be continuously manned.
- An alarm shall be generated and annunciated on the DCS indicating that the IPF trip measurement is faulty.
- Other ways to trip or stop the process shall be available to the operator.
- The process dynamics shall be such that the operator has time to act.
- This functionality is time restricted, i.e. the trip measurement shall be taken in maintenance override before a pre-set time of one hour is elapsed. In case an MOS is not available, IPF action shall be taken after the pre-set time has elapsed.

FIGURE 15 2oo3 INITIATOR AND DUAL INPUT CARD

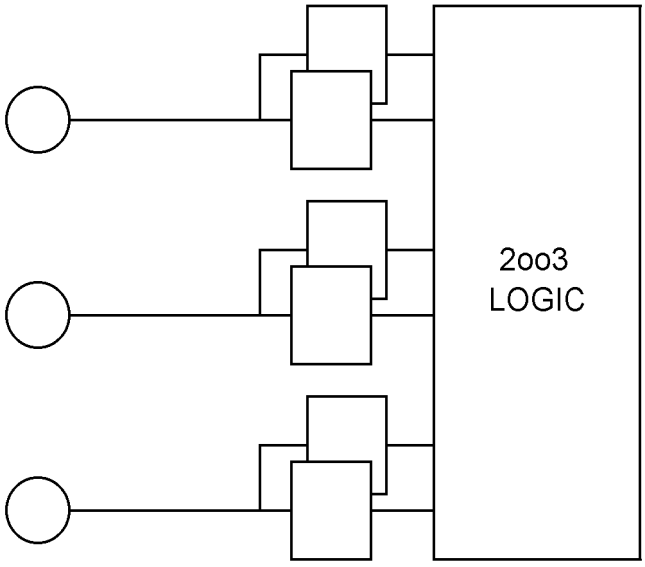


FIGURE 16 MOS IMPLEMENTATION

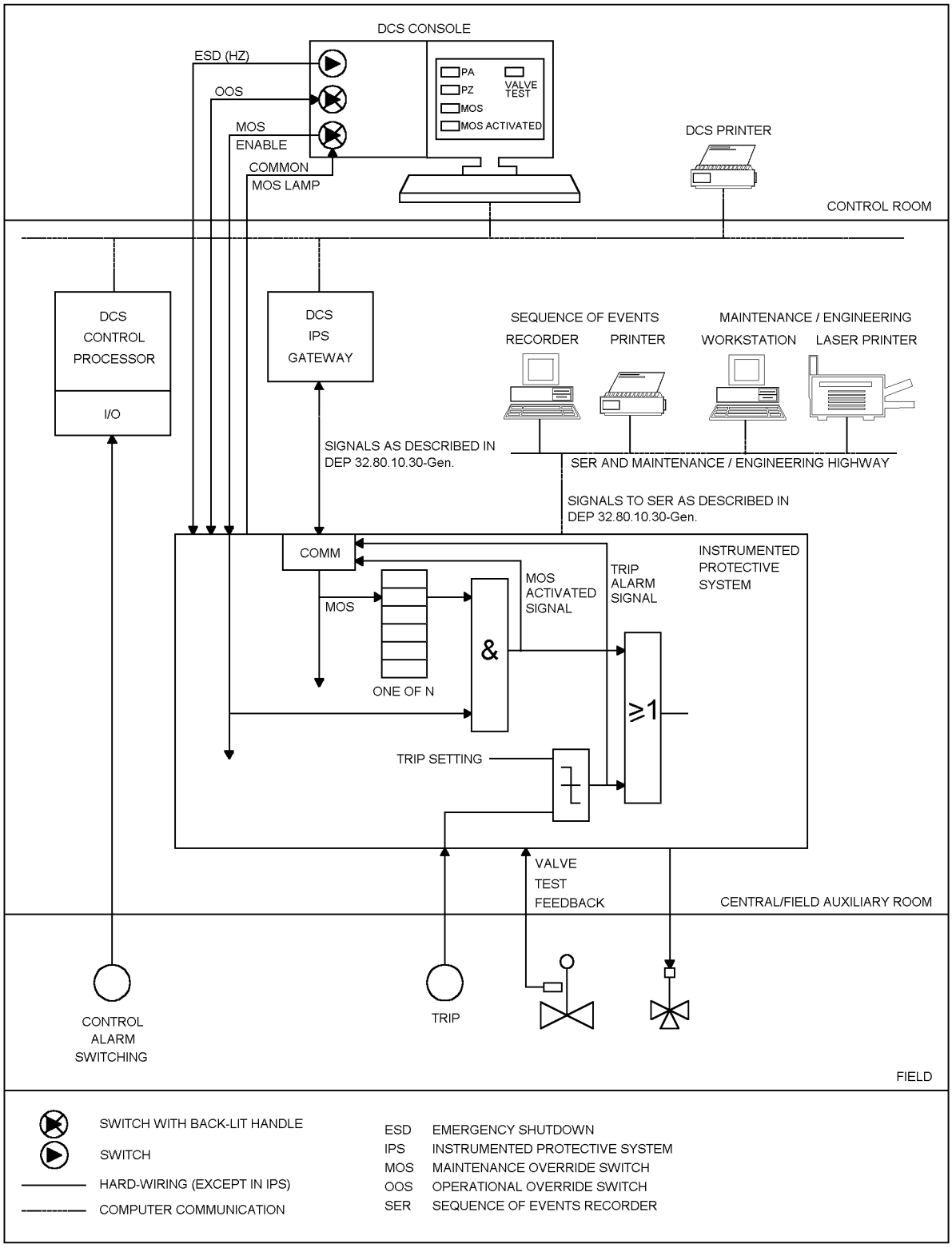
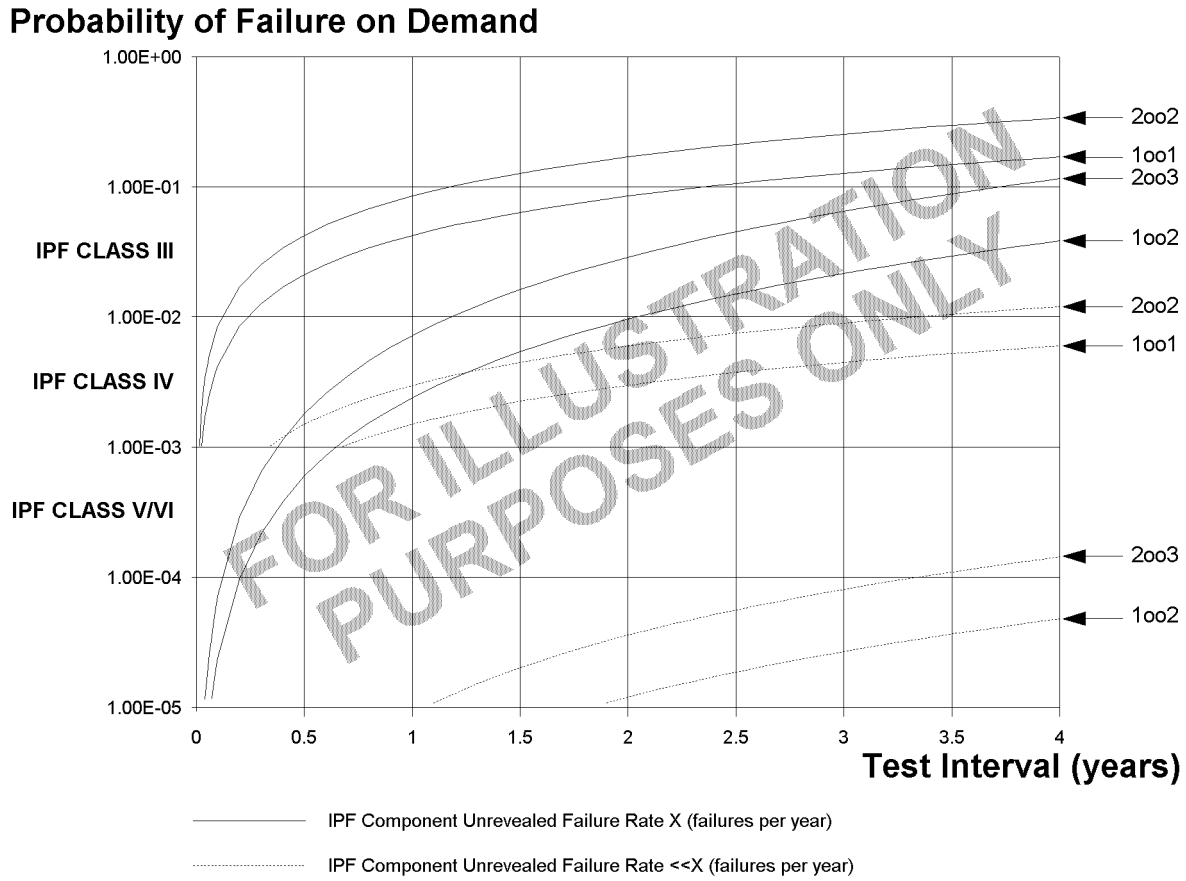


FIGURE 17 RELATION IPF PFD AND IPF CLASS - TEST INTERVAL



NOTE: For 1oo1 and 2oo2 configurations, the PFD vs. Test Interval lines stop at a PFD of 1.00E-3 because of the deterministic requirement that for IPF class V and VI the configuration shall be unrevealed failure robust.