
CASS TEMPLATES FOR SUB-SYSTEM DATA IN RELATION TO IEC61508 SAFETY FUNCTION ASSESSMENT

Report No. CASS2-BR-COMP-Rev0.doc
Prepared for The CASS Scheme Ltd
By Barrie Reynolds, Honeywell Control Systems Ltd

All comment or communications to:

The CASS Scheme Limited
South Hill
Chislehurst
Kent
BR7 5EH
Tel No: +44(0) 208 2951873
Fax No: +44(0) 208 4670145
Email: enquiries@cass.uk.net

©The CASS Scheme Ltd. 2004

This information is made freely available for public comment and use by The CASS Scheme Ltd, who request that appropriate acknowledgement be made when referencing the material.

CONTENTS LIST

FOREWORD	4
1 PURPOSE.....	8
2 OVERVIEW	9
3 BACKGROUND	13
4 SCOPE.....	15
4.1 Information scope	15
4.2 User Scope.....	16
4.3 Sub-system Scope.....	16
4.4 Consideration of the scope of ‘validated Data Sets’	17
5 TERMINOLOGY, DEFINITIONS, AND ABBREVIATIONS	18
6 IEC61508 SUB-SYSTEM TARGETS OF EVALUATION.....	24
6.1 REQUIRED TOES FOR ALL SUB-SYSTEMS	25
6.2 REQUIRED TOES FOR PROVEN IN USE SUB-SYSTEMS	33
6.3 REQUIRED TOES FOR ‘Proven By Design’ SUB-SYSTEMS	35
7 TEMPLATES	39
7.1 TEMPLATES - GENERAL	39
7.2 TEMPLATE STRUCTURE	39
8 EXAMPLES.....	42
8.1 CASS SUMMARY TEMPLATE FOR PRESENTING THE RESULTS OF A SUB-SYSTEM CONFORMITY ASSESSMENT.....	42
8.2 SIMPLEX/ PROVEN BY DESIGN	50
8.3 SIMPLEX/ PROVEN IN USE	60
8.4 REDUNDANT /PROVEN BY DESIGN.....	65
8.5 REDUNDANT /PROVEN IN USE.....	70
9 GUIDANCE ON FAILURE RATES AND DIAGNOSTIC COVERAGE.....	73
9.1 Failure Rates	73
9.2 Diagnostic coverage	74

CHANGE HISTORY

Version Number	Date	Principal changes since last issue
Rev 0	8 April 2004	First publication

FOREWORD

A foreword to the CASS Templates for Sub-system Data in Relation to IEC61508 Safety Function Assessment, and Product Certification.

8 April 2004

CERTIFIED PRODUCT DATA SETS AND CERTIFIED PRODUCTS, WITH RESPECT TO IEC61508.

In order to demonstrate compliance to IEC61508 for the implementation of a safety function, the safety function designer has to have access to information about the components and sub-systems which permit judgments to be made about

- failure rates in all modes which affect the integrity of the design
- the extent to which those failures are automatically detectable
- the extent to which those failures are predictable
- the extent to which the available data is representative of the intended application context
- the extent to which the criteria defined in the standard for control of systematic failures, and for avoidance of systematic failures, have already been addressed at the component/ subsystem design.

The last item is the only area which is directly addressed by IEC61508 within the context of constraints placed upon individual subsystems with respect to their use at a specified Safety Integrity Level (SIL) and is addressed by reference to TOEs #22 and #23 in the CASS Templates for Sub-system Data.

To identify the constraints placed on the subsystem SIL by the subsystem architecture, and by the PFDavg for demand mode applications, requires a knowledge of the full context of the safety function, the component or subsystem features being employed for the safety function, of the diagnostic functions actually being implemented, the operation philosophy and test regime, and the constraints imposed by the other subsystems involved in the implementation of the safety function.

Consequently, the essential requirement is to establish the fundamental failure rate and failure mode characteristics, and the available external diagnosable failure modes, and to make that available along with the supporting evidence for the robustness of the component or subsystem design. That information is considered to be a Base Data Set for any component or subsystem.

There are no IEC61508 compliance criteria associated with a Base Data Set other than those associated with systematic robustness. There will be degrees of rigour with which the validity of the information has been deemed to have been established, the highest of which is likely to involve independent assessment by bodies accredited as competent to undertake such activities. The following particular requirements for formal independent assessment have been considered:-

Specific consideration of Product Certification by Accredited Certification Bodies.

1) The assessment process and scope

Formal Product Certification is primarily concerned with ‘Proven by Design’ components placed on the market by vendors with the specific intention or expectation of those products being employed in safety applications. The vendor is expected to have certain specific recommended application configurations for the sub-system, which in most cases will define ‘safe’ and ‘dangerous’ failure modes within that context, and permit parameters other than the Base Data to also be calculated (i.e. the Application Context Data - Type A/B, SFF, and continuous mode dangerous failure rate).

The formal certification of products in the context of IEC61508 would be required to address:

	Reference
The formal structure of the product assessment and on-going surveillance process.	The CASS Scheme Common Schedules - Assessment Procedures and Assessment Techniques.
Targets of Evaluation	
The application-independent characteristics of the subsystem (e.g. failure rate, failure mode, and systematic design aspects)	a) Product Base Data, CASS Templates for Sub-Systems. b) CASS Product Template Summary (incorporated in the Example section of (a) above).
The relevant Functional Safety Management attributes related to the systematic aspects of the product design, and related to the provision of the Product Base Data.	a) The relevant parts of IEC61508 Part 1 Clause 6 b) The CASS Guide to Functional Safety Capability Assessment (FSCA) as guidance on assessment of Functional Safety Management
Optionally	
The application-context-dependent characteristics of sub-systems intended by the vendor to be applied in a specified manner, where relevant. (Validation of any vendor-provided additional Reference data for typical applications based on certain specified assumptions).	a) CASS Templates for Sub-Systems, Application Context data. b) The Functional Safety Management aspects related to the processes by which the Application Context data is derived.
Validation of the supporting field experience evidence* and correlation to Product Base Data for Proven-by-Design subsystems.	a) CASS Templates for Sub-Systems, Proven-in-Use data, and Guidance on Failure Rates and Diagnostic Coverage

*Field experience data, particularly that meeting the criteria for Proven-in-Use, is the preferred source for reliability data (IEC61508 Part 2 7.4.7.4 a) NOTE 2). It is likely that products may be submitted for certification without field experience data, and the

supporting rationale for the choice of 'generic' database from which to predict the products reliability performance will need to be appropriately robust. Significant explicit credit should be given to the reliability data which is supported by a formal field experience feedback program which is managed by the vendor, and the extent of such supporting evidence should be clear in the assessment report.

2) Proposal for Maintenance of Certification.

The extent to which re-certification is necessary as a function of design changes can be burdensome if not addressed pragmatically, and the following is provided as a proposal for general guidance on identifying significant change.

A process for maintaining certification revision in line with revised sub-system model nomenclature is required, and to that extent every design change is subject to re-certification, otherwise the referenced product on the certificate is not consistent with the current model/ revision level. Consequently the Certification Body will be notified about every change if the vendor wishes to keep the certification up to date.

The underlying principle is that the vendor should have in place a process for the management of change in compliance with IEC61508 Part 2, in order to ensure that the evidence is available for inspection. The presumption is that the Certification Body will review and normally accept vendor-supplied documented evidence of 'insignificant change', and of 'significant change' produced under a certified Functional Safety Management process, and the Certification Body will issue covering certification for the revised product without the need for detailed re-assessment or additional evidence. The Certification Body review here is primarily for compliance with the terms of the agreed process by which the evidence is compiled, and by which a new design is produced, as would be done in a 'self-certification' regime.

There is a further presumption that the vendor submits all necessary evidence, as defined in the Functional Safety Management plan for demonstration of compliance, to support the described change at the time of notification of the change.

A level of re-assessment would be the norm when the change also has impact on critical aspects of the existing Functional Safety Management processes.

Note that the requirements within IEC61508 for re-verification and re-validation by the vendor still apply, consistent with the processes identified in the vendor's compliance plans. Whether there is a need for any level of detailed re-assessment should be triggered by 'significant' change, based on Certification Body judgement of the documented evidence provided with the notification of change.

Significant change should be presumed, by the certification body:-

- Where design change is not accompanied by quantitative assessment or failure analysis, or by documented impact assessment supporting a vendor judgement of 'insignificant change'. (i.e. where an agreed process for demonstration of compliance is not in place, or the previously agreed requirements and criteria have not be complied with)

- Where design change is accompanied by a vendor impact assessment which is classed as ‘significant’ by the vendor, according to its own documented criteria for ‘significant change’. A default assumption for all software change is ‘significant’, except where explicitly addressed and agreed as documented criteria in the vendor’s functional safety compliance plan. Significant change under a well-structured functional safety management system should still not require anything other than scrutiny by the Certification Body of the evidence submitted by the vendor to ensure compliance with the requirements for necessary evidence as documented in the agreed plan.
- Where design change is predicted to result in more than 20% degradation in failure rates for any Output States expected to be assigned as ‘dangerous’, when assessed according to procedures already covered and agreed in the vendors functional safety compliance plan.
- Where design change introduces a new Output State of the sub-system which is intended for use in safety applications.
- Where the design change cannot be assessed by the vendor using the processes in the existing agreed compliance plan (e.g. new techniques, competencies, tools)
- Where design processes are significantly different and not covered by existing agreed compliance plans (e.g. 3rd party sub-contracts, different implementation technology)
- Where changes in the Functional Safety Management practices, which could result in a lower systematic SIL, have not been addressed by a specific impact assessment with respect to the existing product certification (e.g. changes of management safety policy, quality control procedures, out-sourcing, re-location, procurement and manufacturing policy etc. as referenced in the vendor’s documented processes forming part of the compliance plan).
- Note that the principles of IEC61508 Part 2 are generally applicable to most aspects of sub-system design, and clause 7.8 is appropriate with respect to change/ modification even at the sub-system level for the Base Data where compliance with the standard is being claimed.

B.Reynolds, Honeywell Control Systems Ltd. 8 April 2004.

1 PURPOSE

The purpose of 'Template Data' is to provide all necessary reference data for sub-systems/ components to support the use of them within specific applications. In CASS terminology that is the reference data set based on the essential Sub-systems ('Type 1') Base Data which is required to support the claims made in Application Specific Assessments ('Type 2') for specific safety functions.

The document is intended to be used as guidance in the consistent compilation of the evidence required by IEC61508 for a component or subsystem in a safety application, based on a common format of data template with associated reference notes.

To this extent the document is also intended to provide the basis for independent verification of the Base Data for components and subsystems (formal or informal “certified subsystem data sets”)

The document is not intended to be a work-sheet for reliability calculations, nor does it provide any reference data for use in reliability calculations. It does not replace any part of IEC61508.

The data and examples provided in this document are in no way to be regarded as relevant and appropriate examples of good engineering practice, nor as representing examples of appropriate and satisfactory evidence in support of any claim.

The CASS Scheme Ltd. offer the templates for open public comment, use, and support on the basis of achieving common understanding, common terminology, and common structuring of information.

Refer to overview diagram Figure 1.

- Areas A and B (green) represents the Base Data required for all subsystems.
- Area C (yellow) identifies those parameters which describe the Application Context within which the subsystem is intended (by the designer of the safety function) to be used on a regular basis.
- Area D (cyan) represents the particular parameters which are specific to a defined safety function.

This document is primarily concerned with the data in **Areas A and B**.

Subsystems with only one major component are represented by A, and subsystems which comprise several components or subsystems are represented by A together with B. The templates are intended to be applicable to components, and to subsystems comprising several components, as deemed appropriate when establishing the commonly used combinations of equipment(e.g. thermocouple, temperature transmitter, isolation barrier).

The data in these areas relate to failure rates, failure modes, the resulting effect on the sub-system outputs, and the extent to which those output states are inherently diagnosed or can be diagnosed if additional external diagnostic functions are implemented.

- There may be several sets of failure rate data available per subsystem, related to different operational environments.
- There may be several identifiable failure modes, each of which may have a consequential unique output state of the subsystem, or some failure modes may result in the same state.
- The failure modes of more than one component may result in the same output state.
- For each subsystem, the SIL (systematic) is established on the basis of the associated design criteria for fault avoidance and fault tolerance (except “proven in use” data).

With this data set, the extent to which the sub-system can be used appropriately in any specific Application Context, and safety function, can be fully defined.

This level is appropriate for the standardised ‘Subsystem Data Set’ for maintaining subsystem and component information, and for formal or informal “validated/certified subsystem data”.

Note that this Base Data is fully independent of the Application Context, and this subsystem has no SIL (architecture), no SIL (demand mode), no SIL (continuous mode), no PFD, no SFF, and no such information is necessary in the context of providing generic, application independent, subsystem data.

Inclusion of any claims or statements about any aspect of compliance to the application-specific functional safety criteria of IEC61508 for marketing purposes, or

internal company reference models (e.g. claims for SFF, PFD, suitability for use at SIL 2 etc...) must recognise that such statements can only be based on assumptions, or on tightly constrained conditions of use, and have little relevance or value until re-validated in the context of the implemented safety function. The information for the subsystem must include the Base Data, and all information related to the assumptions made about the Application Context and proof-test interval from which the additional claimed parameters are derived.

It is rarely, if ever, appropriate to associate a **component** (i.e. one part of an input, logic solver, or output subsystem) with a SIL (architecture), or SIL (continuous/demand mode), and never appropriate to do so outside of the application context for the entire subsystem within which it is incorporated.

Application context is known to the **safety function** designer, see Area C. The **subsystem** (and particularly the component) designer is not necessarily aware of the application context.

- A subsystem may be validated for several different Application Contexts, each with its own set of resulting Application Context calculations
- the application context defines what constitutes safe, dangerous
- defines what external diagnostic functions are implemented
- defines the operational environment
- defines the executive action philosophy (e.g. de-energised to trip)
- defines which of the subsystem functions are used for safety

The Application Context knowledge, applied to the Base Data, allows calculation of

- Type A/B
- SFF
- SIL (architecture)
- dangerous failure rate
- SIL (continuous mode)

With this data set, the extent to which the sub-system can be used appropriately in any specific Safety Function (demand mode) can be fully defined.

Where subsystems are designed for a specified Application Context, and are constrained from being applied in any other way, then the above parameters can be derived by the **subsystem designer** (e.g. subsystem supplier) provided that the intended application context is fully defined.

Without specific safety function test interval information, this subsystem in this application context has no PFD, and no SIL (demand mode)

Specific Safety Function requirements are known to the **safety function designer**, see Area D

To perform the specific Safety Function Context calculations, the safety function designer requires

- the target SIL for the function
- the target PFD for the sub-system
- all of the subsystem Base Data mapped to the specific Application Context for the safety function
- Proof Test Interval acceptable limits, and MTTR

Normally the PFD of the subsystem will be manipulated to fit the target PFD requirements by changing the Proof Test Interval as necessary, until the acceptable limits are reached.

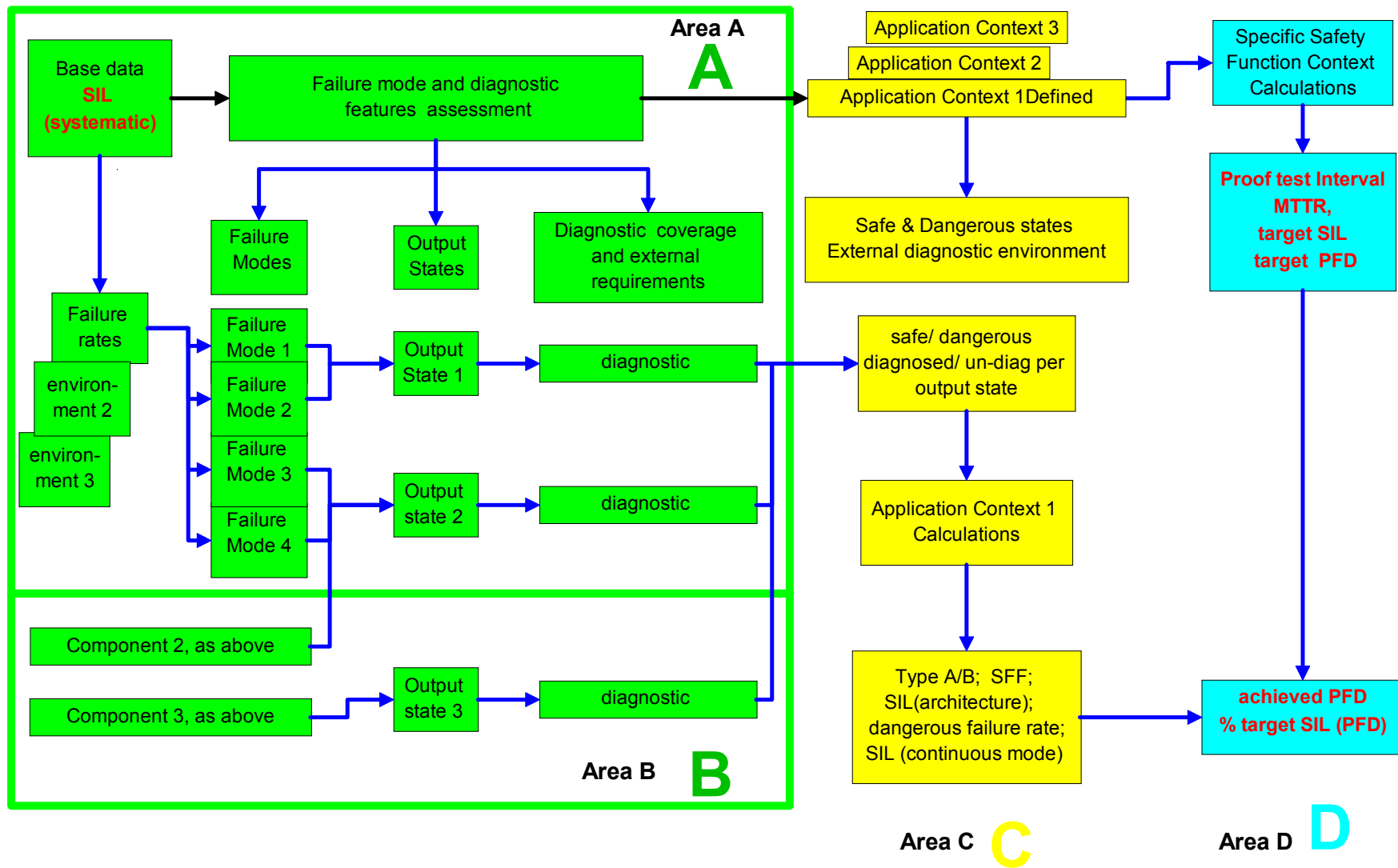


Figure 1: Base Data, Application Context, and Safety Function Calculations

CASS Templates for Sub-Systems

3 BACKGROUND

IEC 61508 Part 2 has requirements for “subsystems”, where these “subsystems” are parts of a larger system. The CASS Sub-System Templates are intended to support “subsystems” which are characterised by such terms *as application independent, generic, and proprietary*. This document uses the term “subsystem” throughout for components or sub-systems to maintain consistency with IEC 61508. Where 'components' are referenced in this document, the context is that sub-system failures take place at the component level, and that Type A , Type B, and SFF classifications (see definitions) relate to subsystems.

The use of a sub-system in a safety application requires- among other things- knowledge about failure rates, failure mode, repair rates, test rates, diagnostic coverage, and a context within which 'safe' and 'dangerous' are defined. That information rarely is available from a single source, and there is a need to structure the information such that, at any point in the life-cycle, the extent to which all of the necessary information has been addressed is clear.

The IEC61508 standard assumes a safety context and an *application context* which may not be the only way a particular sub-system is can be used, and the terminology of the standard is entirely focused on the safety context. The requirements of the standard, as expressed for subsystems, predominantly use terminology like 'dangerous failure rate', 'Safe Failure Fraction' for parameters - but those cannot be determined by the sub-system supplier without the additional *application context* information.

The way a sub-system is used in a safety application is dependent on the safety requirements and safety philosophy of the application . The concept of what is a safe failure state, and what is a dangerous failure state of a sub-system will be defined on an application basis, may vary across safety functions, and in some cases may vary within the same safety function e.g. where both 'energise- to- trip' and 'de-energise-to- trip' philosophies are used for different functional safety tasks within an output chain.

It is therefore necessary to accurately define the *failure modes* and consequences in terms which allow the sub-systems to be used appropriately, and not to assume that certain *failure modes* will always be consistent with 'safe' or 'dangerous' states. It is also important that guidance be provided to the user on the best application of the sub-system in a safety context.

A simple example illustrates the potential for confusion in the request for, and provision of, the data sufficient to support a change-over relay for safety applications.

Although there is a common preferred *application context* using normally energised coil, normally closed contacts, which is common in 'fail-safe' situations, the relay could also be used for very good reasons as

- normally energised, normally open contact
- normally not energised, normally open contact
- normally not energised, normally closed contact

CASS Templates for Sub-Systems

The manufacturer may be able to provide the relevant failure rates for each of the *failure modes*, and with guidance will be able to provide the systematic SIL information, but does not know how the relay will be used.

Only the designer of the complete safety function knows what constitutes a safe state, how the relay will be used, which failure states can be diagnosed, whether they will actually be diagnosed on this safety function, the frequency of the diagnostic, and the frequency of the proof test. He, however, wishes to capture the common implementations for his purposes, and wants to ensure that he asks the appropriate questions of the supplier.

The IEC61508 standard then places obligations

- on sub-system suppliers to provide appropriate data
- on safety function designers to use prediction data correctly in the *application context*
- on end users to continuously monitor failure rates, failure modes, and validate the achieved integrity of the safety functions (1/ 6.2.1 - j)

Additionally, the suppliers of components and subsystems wish to promote their products appropriately in a safety-systems marketplace, view independent validation of their subsystem data as commercially important to them, but have no clear guidance as to how that should be addressed in the context of IEC 61508.

The CASS templates are intended to support those involved in all of the above activities.

CASS Templates for Sub-Systems

4 SCOPE

4.1 INFORMATION SCOPE

The templates derived in this document are intended to be able to support the parameters associated with sub-systems up to and including the point at which those sub-systems become integrated into specific safety functions, i.e. the generic non-application-specific parameters, plus those parameters which are associated with the use of the sub-system in a specific *Application context*.

For example, PFD is not a property of a sub-system and is excluded since it is dependent on the test intervals used in a specific application, but the dangerous failure rate for a sub-system with the associated definitions of the operating context are included, since they will always be the same when used in the same way.

Similarly, SIL(PFD) as derived from I/ 7.6.2.9 (Table 2 for Demand Mode allocation of SIL as a function of PFD) is excluded from the primary data set since this particular parameter -in the context of a sub-system

- is only relevant when the proof-test interval is defined
- is normally manipulated by varying the proof test interval in order to comply with the specified requirements for a particular SIL
- is dependent on the proportion of the PFD allocated to other items performing the safety function.

Although popularly seen as the primary parameter associated with a sub-system (e.g. XYZ pressure sensor is suitable for SIL 2 applications) such a statement has little value, and may be grossly misleading, unless accompanied by the entire data set addressed in these templates, plus a definition of the assumptions made about the PFD of other items in the end-to-end safety instrumented system.

For consistent reference it may be appropriate for some designers or users to establish a fixed point of reference for test intervals, in which case it may be useful to include a calibrated SIL-by-PFD (Demand Mode) e.g. XYZ pressure sensor takes 25% of SIL X with 12 month proof-testing, in a defined application context. (where 'X' is no higher than the highest SIL permitted from architectural and systematic considerations in that context).

This approach is more directly relevant to the 'SIL-Continuous Mode'

There is a significant break-point in the information set for sub-systems, depending on whether the *Application context* is known, or not. The templates are intended to be applicable to both cases.

CASS Templates for Sub-Systems

4.2 USER SCOPE

It is intended that the templates be applicable for

- 1) specifying the required information when purchasing subsystems
- 2) providing the necessary information in data sheets and in responses to purchasing enquiries.
- 3) establishing databases for safety-related information for *custom-defined sub-systems* at all stages of the life-cycle, whether those sub-systems are:
 - a) considered as 3rd party commodity components.
 - b) standard assemblies of components from a supplier.
 - c) defined assemblies of components in use as 'company standards' in a design implementation or an end-user facility, with a specific *application context*
 - d) sub-systems in service, (a defined *application context*) for which safety-related performance information is to be collected
- 4) The basis of future formal sub-system assessment.

For example:

- a manufacturer of a sensor may supply a set of data with the device.
- a system integrator may combine the devices in a 'custom-defined' voting group, and apply a data comparison algorithm across all members of the group, enhancing the validation of the data integrity. The system integrator would supply an additional set of data related to that generic combination of sensors when used with that algorithm. The data set would still be generic, and not complete until the actual application-specific information is available.
- an end user may collect failure data on the individual sensor, and thereby enhance the manufacturer's generic data with site-specific 'proven in use' data
- an end user may also choose to collect data on the 'custom-defined sub-system' as implemented, with its associated logic algorithm, to create a 'proven in use' database related to the common functionality employed in his application. e.g.:
 1. valve, pilot valve, and all associated electronic signals, feedback, diagnostics
 2. a dual transmitter voting 1-o-o-2 with cross-comparison deviation alarming.

4.3 SUB-SYSTEM SCOPE

The templates are typically expected to be applicable for:

- 1) sensors and all input devices
- 2) actuators and all final elements
- 3) signal conditioning devices
- 4) isolators & barriers
- 5) simple logic modules
- 6) trip amplifiers
- 7) specific defined combinations of any of the above

No specific constraint is placed on the applicability of the templates to complex sub-systems involving software. The software within sub-systems is required to be addressed in the same way as the software for the safety function itself, i.e. by applying the full extent of the appropriate referenced clauses of the IEC61508 standard. However, the more complex the sub-system, the more likely is the possibility that the proposed template format will be insufficient as a vehicle by which to present the data and the supporting evidence.

CASS Templates for Sub-Systems

4.4 CONSIDERATION OF THE SCOPE OF 'VALIDATED DATA SETS'

This document introduces the concept of a 'Validated Data Set' which covers the scope of these templates, but is restricted in principle to the Base Data which is 'application- context -independent' data, and for which sub-system suppliers may wish to obtain an independent assessment. In this event:

the subsystem designer should ensure that the level of independence of the assessment is appropriate to the intended integrity level of the application he is considering. any assessments which cover parameters beyond the Base Data (e.g. SIL, PFD, SFF) must address in detail all of the appropriate assumptions related to test intervals, diagnostic coverage, external diagnostic facilities, etc. which characterise the appropriate application context.

Where the sub-system is specifically intended for safety applications, the sub-system supplier would be expected to define the application context in which the data is considered valid, and may restrict the information to that which is directly applicable in this case.

CASS Templates for Sub-Systems

5 TERMINOLOGY, DEFINITIONS, AND ABBREVIATIONS

An external reference to IEC61508 is presented in an abbreviated form as e.g. 2/7.4.3.2, interpreted as IEC61508 Part 2 Clause 7.4.3.2

The Definitions are provided for those terms and parameters which are not explicitly called up as Targets of Evaluation by the standard. Many of the Definitions may also be addressed in the informative parts of IEC61508 - the purpose of including them here is to provide the particular context related to sub-systems.

Definitions

Item	Definition
<i>Application context</i>	<p>The information necessary in order to assess whether the <i>Output State</i> from a <i>Failure mode</i> of a sub-system is to be classed as Safe, or as Dangerous, within a specified Safety Function. This information is normally defined by the safety function designer or end user. The application context relates directly to the implementation of the design under consideration i.e. it is project or site specific information</p> <p>Note that there may be several <i>Application contexts</i> for the same sub-system on the same project, or within the same operational environment. Separate records will be needed for each <i>Application context</i>.</p> <p>The information required specifies the safety policy and operating philosophy and any other information required to relate that philosophy to the <i>Output State</i>. It will typically address:</p> <ul style="list-style-type: none"> • energise/ de-energise to trip • normally closed/ normally open states • the inputs or outputs to be used for safety purposes • the allocation of the Output States to 'safe' and 'dangerous' states • the external diagnostic environment, so that states which are externally diagnosable (e.g. out of range) can be appropriately handled • continuous or on-demand operating scenario, to ensure that states considered as 'safe' in an on-demand mode are not assumed to be safe in a continuous mode, and that the data is not used out of context. • conditions to be achieved, for safety (e.g. gas tight closure) • timing constraints to be achieved for safety (inputs and outputs) • Assumptions or descriptions of the external diagnostic environment provided. • The assumptions or description of the operating mode of the sub-system ('on demand' or 'continuous mode') • The common cause failure factor appropriate to redundant elements within the sub-system in this <i>application context</i>. <p>Each <i>Application context</i> should be given a specific identifier or name.</p>

CASS Templates for Sub-Systems

Item	Definition
	<p>The <i>Application context</i> does not necessarily need to be supplied by the user, but can be inherent in the design concept of the sub-system where the function used for safety applications is defined fully in its safety context. This is particularly true for sub-systems with internal redundancy which is intended to provide enhanced safety, since the concepts of 'safe' and 'dangerous' must be known in order to effectively apply the redundancy. Such sub-systems will typically be marketed for safety applications, or be created as 'custom-defined sub-systems' for safety applications.</p> <p>In some cases the application context may also impact the choice of the Base Data Set to be used, and there will be a close correspondence between Base Data sets and the Application Context definition. e.g. the failure rate and failure mode characteristics for a relay in demand mode are significantly different from those which are relevant when the relay is used in a continuous mode.</p>
Context Safety State	The Safe or Dangerous classification allocated to an <i>Output State</i> for a specified <i>Application context</i> , before the application of any external diagnostic function.
Base Data	<p>The information related to the functions supported by the sub-system, the internal architecture, and systematic constraints.</p> <p>The various <i>failure modes</i>, associated failure rates, and diagnostic functions potentially available for the sub-system described in terms of the resulting <i>output states</i> for the sub-system outputs, excluding all assumptions about what constitutes 'safe' and dangerous in an application.</p> <p>There would normally be only one base set of data, but several failure rates may be available for different operational environments.</p>
Custom-defined Sub-systems	Commonly used combinations of components or sub-systems in simplex or redundant architectures which form the basis of system designs, and for which a collated set of data serves a useful purpose.
Common Cause Factor	<p>Ref 2/7.4.3.2.2 (d) and associated notes. Applicable for redundant architectures within the defined sub-system. Note that calculation of the reliability parameters for redundant architectures at all levels is subject to the general requirements of IEC 61508.</p> <p>Common cause factors are application context specific, and not normally part of the base data set of the subsystem unless all of the critical parameters of the application context are defined by one consistent packaging environment (e.g. redundant relays in a single package)</p>

CASS Templates for Sub-Systems

Item	Definition
External diagnostic possibilities	<p>A description of the diagnostic facilities supported by the sub-system which are not used internally to force a specific Output State, but which could be used by other external functions to monitor the health of the sub-system.</p> <p>Requires a description and specification of the functions supported, the associated Output State of the associated diagnostic signal, if any, and the recommendations for implementation of the diagnostic function.</p>
Failure mode	<p>A description of a component-level failure within the sub-system which results in one defined Output State. Failure modes are described in terms related to the physical cause e.g. worn bearing, open circuit input, broken armature.</p> <p>Failure modes have failure rates assigned.</p>
Failure rate fraction [%]	The summation under each Output State of the percentages of the overall failure rate assigned to the contributing Failure modes .
Fault coverage-external [%]	The diagnostic fault coverage resulting from External Automatic diagnostic tests associated with one Output State . Only applicable where a sub-system arrangement involves a defined external diagnostic function.
Fault coverage-Internal [%]	The diagnostic fault coverage resulting from Internal Automatic diagnostic tests associated with one Output State
Internal Automatic diagnostic test interval	<p>The time interval between the completion of the specified diagnostic test routine, and the completion of the same subsequent test, where such tests are always automatically carried out with every instance of the sub-system.</p> <p>See IEC61508 Part 2 / 7.4.7.3 (h) and 9.2</p>
Output State	<p>A description of the impact of one or more failure modes which result in the same condition with respect to the functional output of the sub-system. Output States are states of the sub-system expressed in terms e.g.</p> <p>for sensors: out of range -high, within range -uncertain value, short circuit,</p> <p>for actuators: open, closed, stuck midway, stopped, slow response, etc.</p> <p>One Output State can have several contributing Failure modes</p>
PBD - Proven By Design	<p>A classification of the type of claim being supported for the parameters of the sub-system, for which the evidence is based on reference to the techniques and measures employed in the design and production of the sub-system.</p> <p>see sections 7.2.1, and the examples</p>

CASS Templates for Sub-Systems

Item	Definition
PFD	<p>Probability of Failure on Demand.</p> <p>Not a property of a sub-system, but a parameter usually manipulated by selecting appropriate proof-test intervals in order to achieve a specified SIL.</p> <p>Used within the standard as one of the primary criteria for the SIL of a functional safety task, but not directly relevant for the sub-system in isolation. PFD is derived from the sub-system failure rates, <i>application context</i> of safe and dangerous <i>failure modes</i>, and the applicable proof-test interval. Addressed in IEC61508 part 6 / B1.</p>
PIU	Proven In Use. See section 6.2
proof test coverage	The extent to which the specific proof test for an un-diagnosed Output State will always reveal the fault. (percentage)
SIL	<p>Safety Integrity Level, and defined within IEC61508 Part 4 clause 3.5.6.</p> <p>Since there are several factors which contribute to, or constrain, the overall SIL it is useful to address them separately. The lowest of the SILs determined in each of the categories places a constraint on the claims which can be made for the sub-system, and on the safety function in which the sub-system is employed.</p> <p>SIL by PFD - defined in 1/7.6.2.9 Table 2. The criteria for SIL as determined for low demand mode, characterised by probability of failure on demand.</p> <p>SIL (continuous mode) - defined in 1/7.6.2.9 Table 3, characterised by dangerous failures per hour for continuous mode operations</p> <p>SIL (architecture) - defined in 2/ 7.4.3.1 and Tables 2 and 3, and characterised by Type A/ Type B properties, levels of Safe Failure Fraction, and hardware fault tolerance.</p> <p>SIL (systematic) - defined in 7.4.7.3 (m) and characterised by the levels of rigour and measures and techniques employed to prevent systematic faults being introduced, and to make the sub-system tolerant of systematic faults.</p>

CASS Templates for Sub-Systems

Item	Definition
subsystem	<p>An undefined term in IEC61508 Part 4.</p> <p>A definition is required in the context of this document, since, critically, that is the level at which Safe Failure Fraction is to be determined (2/ C 1), and the level at which Type A/ B is determined (2/ 7.4.3.1.2) .</p> <p>The relevant characteristics of a subsystem are defined by the context within IEC61508 Part 2 and include:</p> <p>2/ 7.4.2.11:</p> <ul style="list-style-type: none"> • subsystems have their own defined integration test. • can comprise a single or any group of components • are the level at which ‘verification’ should be maintained for repeated common implementations <p>2/7.4.3.1.5</p> <ul style="list-style-type: none"> • subsystems are implicitly associated with “input subsystem”, “output subsystem”, “logic subsystem” from figure 5. <p>2/7.4.3.2.3</p> <ul style="list-style-type: none"> • The level at which proof testing takes place <p>2/ 7.4.7.9</p> <ul style="list-style-type: none"> • the level at which failure rate and other data for “proven in use” claims is maintained.
systematic failure	<p>IEC61508 Part 4/ 3.6.6</p> <p>failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.</p> <p>All software failures are systematic.</p>
TOE	<p>Target of Evaluation. The term used by CASS for a specified requirement in IEC61508. All TOEs have an associated IEC61508 reference clause</p>

CASS Templates for Sub-Systems

Item	Definition
<p>Type A/ Type B Sub-systems</p>	<p>The definitions are in 2/ 7.4.3.1 - Architectural constraints on hardware safety integrity.</p> <p>The Type A/ Type B classification cannot - in principle- be done without reference to the <i>application context</i>, since the wording of the standard is such that 2/7.4.3.1.2 and 2/7.4.3.1.3 actually relate to 'field experience' and 'detected dangerous failures' in their respective sub-clauses (c), i.e. that the <i>application context</i> must be known in order to make the classification decision, when the assignment of 'safe' and 'dangerous' to the various failure states has been completed.</p> <p>In practice, the classification can frequently be undertaken in the absence of the <i>application context</i> provided that all known failure modes are defined and that all failure rates for those modes have been established to the same extent. This is normally the case for sub-systems which are PBD.</p> <p>Where different or alternative outputs are available for the implementation of safety functions, and have different Type A/ Type B classifications, then the applicable classification is not known unless the application context is fully defined.</p> <p>The final decision on Type A/ Type B classification is then a function of the evidence available to the implementer of the application, and not the sole responsibility of the sub-system supplier, unless the <i>application context</i> is also fully described.</p> <p>Accordingly, the Type A/ Type B parameter occurs in the Base Data, and is confirmed or changed at the Application Context.</p>

CASS Templates for Sub-Systems

6 IEC61508 SUB-SYSTEM TARGETS OF EVALUATION

These Tables of TOES represent the way the subsystem parameters are laid out in the standard. They are arranged here into groups of TOEs which identify:
TOES for all sub-systems

additional TOES for PIU sub-systems

additional TOES for PBD sub-systems

The TOEs represent the information required at the 'implemented safety function' level, only some of which is directly applicable to the sub-system Base Data information, and much of which is derived from that in combination with the specific *application context*

The entries in the CASS Templates are taken either from the TOES, or from the defined terms in the previous section.

All of the activity related to establishing the appropriate data to use in relation to the standard is required to be undertaken by persons who are competent to undertake those activities For subsystems specifically intended for safety applications, the obligations on suppliers, designers, and users related to the presentation and maintenance of this data are best considered within the context of IEC 61508 Part 1 clause 6, Management of Functional Safety, as addressed by CASS FSCA.

CASS Templates for Sub-Systems

6.1 REQUIRED TOES FOR ALL SUB-SYSTEMS

Object Name	Purpose of Object	IEC 61508 Ref.	Comments
E/E/PES SUB-SYSTEM DATA TABLE			
TOE 1). sub-system identification	All information which is required to identify the hardware and software configuration of the subsystem in order to enable the configuration management of the E/E/PE safety-related system in accordance with 1/6.2.1.	2/7.4.7.3(n)	typically part number, model number, revision number. Part of the Base Data set
TOE 2). a functional specification	required to define those functions and interfaces of the subsystem which can be used by safety functions.	2/7.4.7.3 (a) 2/7.4.7.4 2/7.4.7.12	e.g. <ul style="list-style-type: none"> • no functions suitable for safety applications • all functions supported by validated data • Analogue signal only (not digitally encoded communications) • signals at designated terminals only • signals within certain ranges only • primary measurement only - not the auxiliary data <p>The standard requires, implicitly, that there be a declaration made by the supplier of the data for all sub-systems as to whether they are considered to be at all suitable for use by safety functions.</p> Part of the Base Data set

CASS Templates for Sub-Systems

Object Name	Purpose of Object	IEC 61508 Ref.	Comments
<p>TOE 3). The estimated rates of failure (due to random hardware failures) in any modes.</p>	<p>Required as input to the application-specific allocations of failure rates to safe and dangerous <i>failure modes</i>, which then permits the calculation of SFF and PFD. Proposed for these templates to be in the form of: Individual Failure Rates for each failure mode</p> <p>Plus, for each <i>failure mode</i>:</p> <ul style="list-style-type: none"> • function affected • consequence for the output signal • externally available diagnostic indication of the failed state 	<p>2/7.4.7.3 (b) 2/7.4.7.3.(j) 2/7.4.7.4 2/7.4.3.2 for PFD context</p> <p>2/ Annex A 2/ Annexe C 7/B.6.6.1</p> <p>2/7.4.7.9 for PIU</p>	<p>See section 9.1, Requires an environment context for the failure rate, or range of failure rates, which is relevant to the expected conditions of use. Part of the Base Data set</p>
<p>TOE 4). diagnosed (dangerous) failure rates</p>	<p>Required as input to calculation of SFF and PFD. The estimated rates of failure (due to random hardware failures) in any modes which would cause a dangerous failure of the E/E/PE safety-related system, which are detected by diagnostic tests.</p>	<p>2/7.4.7.3 (b) 2/7.4.7.4 2/7.4.7.3.(j) 2/ Annex A</p>	<p>The referenced clauses in IEC61508 require dangerous failure rates to be defined. Categorisation into safe and dangerous states can only be provided when accompanied by the assumptions for the <i>application context</i></p> <p>Annex A places constraints on the claims for diagnostic techniques, and requires the diagnostic coverage claim to be justified for non-proven-in-use sub-systems. Not part of the Base Data set for PBD</p>

CASS Templates for Sub-Systems

Object Name	Purpose of Object	IEC 61508 Ref.	Comments
TOE 5). un-diagnosed dangerous failure rates	<p>Required as input to calculation of SFF and PFD.</p> <p>The estimated rates of failure (due to random hardware failures) in any modes which would cause a dangerous failure of the E/E/PE safety-related system, which are undetected by diagnostic tests (see 2/7.4.7.4)</p>	<p>2/7.4.7.3 (c) 2/7.4.7.4 2/7.4.7.3.(j)</p>	<p>The referenced clauses in IEC61508 require dangerous failure rates to be defined. This is not valid at the generic sub-system level without an <i>application context</i> defining safe and dangerous states.</p> <p>(see notes on 'diagnosed dangerous failures') Techniques for assessment of failure rate are referenced in 2/7.4.7.4, with guidance. The choice is between design assessment, or 'Proven-in-use' evidence. For 'Proven-in-use' the failure rate will include systematic failures. Not part of the Base Data set for PBD</p>
TOE 6). environmental limits	any limits on the environment of the subsystem which should be observed in order to maintain the validity of the estimated rates of failure due to random hardware failures	2/7.4.7.3 (d)	part of the Base Data set
TOE 7). lifetime limits	any limit on the lifetime of the subsystem which should not be exceeded in order to maintain the validity of the estimated rates of failure due to random hardware failures	2/7.4.7.3 (e)	<p>consider wear out caused by design or application, e.g. capacitor or battery life, hardening of seals, run-time of bearings etc. part of the Base Data set</p>

CASS Templates for Sub-Systems

Object Name	Purpose of Object	IEC 61508 Ref.	Comments
TOE 8). proof test requirements	any periodic proof test requirements	2/7.4.7.3 (f)	<ul style="list-style-type: none"> • the purpose of the test, with respect to otherwise unrevealed <i>failure modes</i> • the test procedure • the typical time required to perform the test • the extent to which hidden faults are revealed by the test. (see 4/ 3.8.5) • the tests associated with the diagnostic functions part of the Base Data set for PBD
TOE 9). maintenance requirements	any periodic maintenance requirements	2/7.4.7.3 (f)	<ul style="list-style-type: none"> • the purpose of the maintenance • the maintenance procedure • the recommended in-service interval for maintenance. part of the Base Data set for PBD

CASS Templates for Sub-Systems

Object Name	Purpose of Object	IEC 61508 Ref.	Comments
TOE 10). diagnostic coverage	the diagnostic coverage derived according to annex C. This information is required when credit is claimed for the action of the diagnostic tests performed in the subsystem in the reliability model of the E/E/PE safety-related system .	2/7.4.7.3 (g) 2/Annex C 2/ 7.4.3.2.2 2/Annex A and all sub-sections	<p>see note 1 under 2/7.4.7.3 (h). This data is related to the internal sub-system diagnostics available with every instance of the sub-system.</p> <p>Where the defined ID of the sub-system includes an external diagnostic function, then all relevant parameters within this template related to the external diagnostic function must also be provided. See Section 9.2</p> <p>Annex A places constraints on the claims for diagnostic techniques.</p> <p>Note that failure rate of any internal or external diagnostic function is required be included in the full assessment of diagnostic coverage, and will be captured if a separate template is used for the diagnostic function as a stand-alone sub-system.</p> <p>Annexe C only recognises diagnostic coverage in the context of dangerous failures. This document recognises the principle of generic diagnostic coverage for every failure mode, independent of the application context, which is part of the Base Data set.</p>

CASS Templates for Sub-Systems

Object Name	Purpose of Object	IEC 61508 Ref.	Comments
TOE 11). diagnostic test interval	the diagnostic test interval, when required. This information is required when credit is claimed for the action of the diagnostic tests performed in the subsystem in the reliability model of the E/E/PE safety-related system.	2/7.4.7.3 (h) 2/Annex C	see note 1 under 2/7.4.7.3 (h). This data is related to the internal sub-system diagnostics available with every instance of the sub-system. Where the defined ID of the sub-system includes an external diagnostic function, then all relevant parameters within this template related to the external diagnostic function must also be provided. See 'diagnostic coverage' in section 9.2
TOE 12). other repair constraints	any additional information (e.g. repair times) which is necessary to allow the derivation of a mean time to restoration (MTTR) following detection of a fault by the diagnostics;	2/7.4.7.3 (i)	Any maintenance, re-calibration, or other activities in addition to standard repair times and procedures should also be identified. Part of the Base Data set for PBD Note that a standard repair time given by a sub-system supplier must be qualified by the assumed context, and will not necessarily take into account the <i>application context</i> . Thus there may be several factors contributing to the actual MTTR as used in an application.

CASS Templates for Sub-Systems

Object Name	Purpose of Object	IEC 61508 Ref.	Comments
TOE 13). safe failure fraction	all information which is necessary to enable the derivation of the safe failure fraction (SFF) of the subsystem as applied in the E/E/PE safety-related system, determined according to annex C. Needed to determine the highest safety integrity level that can be claimed for a safety function according to the architectural constraints.	2/7.4.7.3 (j) 2/Annex C	<p>The requirement is for all information related to failure rate and diagnostic coverage, placed into the <i>application context</i> for safe and dangerous <i>failure modes</i>, which are then used for calculation of SFF. The calculation of SFF cannot be done without knowledge of the safe, dangerous, and external diagnostic support context.</p> <p>Not part of the Base Data set for PBD</p> <p>A SFF number must always be accompanied by the <i>application context</i> information.</p> <p>A subsystem may have more than one SFF value depending on the application context.</p>
TOE 14). hardware fault tolerance	the hardware fault tolerance of the subsystem. Needed to determine the highest safety integrity level that can be claimed for a safety function according to the architectural constraints	2/7.4.7.3 (k)	<p>this relates to the inherent architecture and fault tolerance available with every instance of the defined sub-system, and not application-specific combinations.</p> <p>Part of the Base Data set for PBD</p>

CASS Templates for Sub-Systems

Object Name	Purpose of Object	IEC 61508 Ref.	Comments
TOE 15). Highest SIL (architecture)	the highest safety integrity level that can be claimed for a safety function according to the architectural constraints, derived from the hardware fault tolerance and SFF	2/7.4.7.3 (j) 2/7.4.7.3 (k) for Type A/B 2/7.4.3.1.2 2/7.4.3.1.3	<p>This claim depends on the selection of Type A/ Type B sub-system table, and on the SFF. The Type A/Type B classification and the SFF must always consider the application context. Consequently the Highest SIL (Architecture) is always application context dependent. see: Application context SFF Type A/ Type B</p> <p>Not part of the Base Data set for PBD</p> <p>Defining the SIL (architecture) for any component within a subsystem is not appropriate, except at the subsystem level. It is possible to combine components with low failure rates (dangerous only, with a nominally unacceptable SIL (architecture)) in subsystems with other components which have high safe failure rates, and achieve a high SIL for the subsystem</p>
TOE 16). systematic failure constraints	any limits on the application of the subsystem which should be observed in order to avoid systematic failures.	2/7.4.7.3 (l)	<p>Any requirements or constraints about the way the sub-system should be employed for safety applications, or constraints related to the extent of validity of the available data. Part of the Base Data set for PBD</p>

CASS Templates for Sub-Systems

6.2 REQUIRED TOES FOR PROVEN IN USE SUB-SYSTEMS

These TOES defines the set of additional data required for “proven in use” sub-systems.
See IEC61508 Part 7 clauses B.5.4, C.2.10 for supporting definitions of Proven in Use

A previously developed subsystem shall only be regarded as proven-in-use when it has a clearly restricted functionality and when there is adequate documentary evidence which is based on the previous use of a specific configuration of the subsystem (during which time all failures have been formally recorded, see 2/7.4.7.10), and which takes into account any additional analysis or testing, as required (see 2/7.4.7.8). The documentary evidence shall demonstrate the likelihood of any failure of the subsystem (due to random hardware and systematic faults) in the E/E/PE safety-related system is low enough so that the required safety integrity level(s) of the safety function(s) which use the subsystem is achieved.

Object Name	Purpose of Object	IEC 61508 Clauses and Tables	Comments
PROVEN-IN-USE SPECIFIC DATA TABLE			
TOE 17). Evidence of similar conditions in previous use.	Demonstrates that the previous conditions of use of the specific subsystem are the same as, or sufficiently close to, those which will be experienced by the subsystem in the E/E/PE safety-related system.	2/7.4.7.7 2/7.4.7.6 2/7.4.7.10 2/7.4.7.11	2/7.4.7.10. places constraints on the acceptable sources of data, and recommends data collection standards. 2/7.4.7.11. gives guidance on the extent and degree of detail of required supporting evidence. Note that there is a requirement for the failure rates for a sub-system which is ‘Proven in-use’ as part of its failure rate data, see TOE 3
TOE 18). Evidence supporting the application under different conditions of use.	Required to justify the use of failure rates established under different operating conditions.	2/7.4.7.8 2/7.4.7.10 2/7.4.7.11	2/7.4.7.10. places constraints on the acceptable sources of data, and recommends data collection standards. 2/7.4.7.11. gives guidance on the extent and degree of detail of required supporting evidence.

CASS Templates for Sub-Systems

Object Name	Purpose of Object	IEC 61508 Clauses and Tables	Comments
TOE 19). Evidence of period of operational use	Required to support the claimed rates of failure on a statistical basis.	2/7.4.7.9 2/7.4.7.10 2/7.4.7.11 1/4.1	2/7.4.7.9 defines the appropriate statistical technique to apply, and the constraints on acceptable data sources. The notes to 2/7.4.7.9 give examples of typical calculations. 2/7.4.7.10. places constraints on the acceptable sources of data, and recommends data collection standards. 2/7.4.7.11. gives guidance on the extent and degree of detail of required supporting evidence. The degree of rigour is also addressed in Part 1, clause 4.1. There is no further quantification guidance on the degree of rigour.
TOE 20). Statement of restrictions on functionality.	Required in order to restrict the application of a 'proven-in-use' safety-related subsystem to those functions and interfaces of the subsystem which meet the relevant requirements.	2/7.4.7.12 2/7.4.7.6 to 2/7.4.7.10 3/7.4.2.11	The sub-system may have several safety-related functions described in its functional specification (TOE 2). This statement here is a declaration about which of those functions are actually supported by the evidence to the appropriate degree of rigour. The Note to 2/7.4.7.12 relates to the interpretation of this requirement for software, in which case it will be required to demonstrate that any specific application is only using features which are supported by the fore-going evidence (2/7.4.7.6 to 2/7.4.7.10)

CASS Templates for Sub-Systems

6.3 REQUIRED TOES FOR 'PROVEN BY DESIGN' SUB-SYSTEMS

These TOES define the set of additional data required for any sub-system not being regarded as proven in use.

Object Name	Purpose of Object	IEC 61508 Clauses and Tables	Comments
SUB-SYSTEM PROVEN BY DESIGN -SPECIFIC DATA TABLE			
TOE 21). highest SIL - (systematic)	the highest safety integrity level that can be claimed for a safety function which uses the subsystem on the basis of the supporting evidence for control and avoidance of systematic faults	2/7.4.7.3 (m)	The systematic SIL must be related to a specified function, and the supporting evidence from TOES 22 and 23 must relate to that same function Part of the Base Data set for PBD

CASS Templates for Sub-Systems

Object Name	Purpose of Object	IEC 61508 Clauses and Tables	Comments
TOE 22). systematic fault avoidance measures (see TOE 21)	description of those measures and techniques used to prevent systematic faults being introduced during the design and implementation of the hardware and software of the subsystem	2/7.4.7.3 (m) 2/7.4.4.1 3/7.4 2/Annexe B, Tables 2/ B2 with B6	<p>The information here is part of the mapping process between the design and testing methodologies, and the requirement in IEC61508. Evidence that the measures and techniques have been appropriately applied, consistent with the SIL claimed.</p> <p>Expecting a response directly relating the techniques employed to those defined in the table, with the identification of the SIL achieved by reference to effectiveness in Table 2/B6 or the appropriate tables from Part 3 for software. The level of compliance is best demonstrated though a combination of these specific requirements with the appropriate demonstration of compliance to 1/ 6 (Functional Safety Management) CASS FSCA</p> <p>Part of the Base Data set for PBD</p>

CASS Templates for Sub-Systems

Object Name	Purpose of Object	IEC 61508 Clauses and Tables	Comments
TOE 23). systematic fault tolerance measures (see item TOE 21)	description of the design features which make the subsystem tolerant against systematic faults	2/7.4.7.3 (m) 2/7.4.5.1 2/7.4.8 2/Annexe A3 2/Tables A16, A17, A18, in conjunction with A 19 3/7.4.3	<p>Evidence that the features have been appropriately incorporated, consistent with the SIL claimed.</p> <p>Expecting a response directly relating the techniques employed to those defined in each of the tables, with the identification of the SIL achieved by reference to effectiveness in Table 2/A19, or the appropriate tables from Part 3 for software.</p> <p>A16 requires aspects of redundancy, diagnostics, retry mechanisms etc.</p> <p>A17 requires measures against environmental hazards</p> <p>A18 requires consideration of operations aspects (modification, confirmation of operator action etc).</p> <p>The level of compliance is best demonstrated though a combination of these specific requirements with the appropriate demonstration of compliance to 1/ 6 (Functional Safety Management) CASS FSCA</p> <p>Part of the Base Data set for PBD</p>

CASS Templates for Sub-Systems

Object Name	Purpose of Object	IEC 61508 Clauses and Tables	Comments
TOE 24). validation records	documentary evidence that the subsystem has been validated according to clauses 2/7.7 and 3/7.of this standard.	2/7.4.7.3 (o) 2/7.7 3/7.7	Required as a validation statement or reference to a validation report for each parameter provided. The level of compliance is best demonstrated though a combination of these specific requirements with the appropriate demonstration of compliance to 1/ 6 (Functional Safety Management) CASS FSCA Part of the Base Data set for PBD

CASS Templates for Sub-Systems

7 TEMPLATES

7.1 TEMPLATES - GENERAL

The CASS Templates are structured to capture the basic reliability-related information, and to capture the subsequent derived information once the *application context* is known.

The parameters are presented in tables, with cross references to one of two reference sections, either

Terminology, definitions, and Abbreviations section 5

or

section 6 (TOEs).

The Terminology & Abbreviations table addresses those terms which are used by this document, and the TOE table addresses those terms used and defined in IEC61508, and carries references to the appropriate sections in the standard.

Example templates are included for use by sub-system suppliers, and for use by anyone creating sub-systems as standard assemblies of components appropriate to their needs.

7.2 TEMPLATE STRUCTURE

The templates are structured by the following primary classification criteria, below. Ideally, the information would be structured by life-cycle activity, but this is not so easy to do since there is the potential for significant overlap across the classification criteria within the life-cycle.

7.2.1 INFORMATION CLASSIFICATION CRITERIA

The primary categorisation criteria for sub-systems in the context of IEC61508 is:

a) Proven In Use / Proven By Design

Whether they are supported by comprehensive documented evidence of previous satisfactory performance (Proven In Use - PIU), or whether their satisfactory performance is being predicted on the basis of design-related characteristics (referred to here as 'Proven By Design' PBD).

b) Simplex / Internally Redundant

Whether they have internal redundancy as part of the standard configuration (i.e. inherently within every instance of the sub-system), or no internal redundancy.

This results in four primary subsystem categories:

Proven by Design-Simplex

Proven by Design-Redundant

Proven in Use-Simplex

Proven in Use-Redundant

CASS Templates for Sub-Systems

For each of these subsystems categories there is a Base Data template, plus the additional data related to the application context.

Table 1. The Primary Template Types

Template	Architecture and Type of Evidence Provided
Simplex/ PBD	The basic reference data; justification for use depends on Proven By Design characteristics; no internal redundancy.
Simplex/ PIU	The basic reference data; justification for use depends on evidence of previous satisfactory performance; no internal redundancy.
redundant/ PBD	<p>The reference data related to the inherent redundant structure; justification for use depends on Proven By Design characteristics; internal redundancy structure is intended for a specific manner of application, and hence some or all of the application context must have been defined.</p> <p>The design, and the predicted failure rates and diagnostic coverage factors must be derived according to the principles of IEC61508 for redundant combinations, which effectively means deriving the information and parameters for the simplex functions according to the simplex templates (above), and deriving the parameters for the redundant structure from that data using the appropriate methodology.</p> <p>The consequence of this approach is that the failure rate factors derived for the sub-system include all common cause failures between the internal redundant functions, and allows the sub-system to be treated as a 'black box' provided that the intended application constraints are observed.</p>
redundant/ PIU	<p>The reference data related to the inherent redundant structure; justification for use depends on evidence of previous satisfactory performance; internal redundancy structure is employed in a specific manner, i.e. some or all of the <i>application context</i> is known or implicit.</p> <p>Output States will include, but not be limited to:-</p> <ul style="list-style-type: none"> • modes resulting in failure of Simplex components • modes resulting in subsystem failure due to independent Simplex failures • modes resulting in subsystem failure due to common cause factors

CASS Templates for Sub-Systems

The templates are organised by sets of data, see Table 2.

Table 2. **The Sets of Data within each Template**

Data Set	Description of Data Set
Base data	The information required for all sub-systems, see <i>Base Data</i> .
Application context information	A description of each of the specific <i>Application contexts</i> which are relevant for this subsystem, and the associated context-specific derived parameters. see definition.
Specific Safety Function calculation parameters	The sub-system parameters required by IEC61508 for the calculation of the PFD for one specific end-to-end safety function, for which the Base data, and <i>Application context</i> information are all required, plus the operational data and implementation data associated with that particular safety function.

In general, for PBD sub-systems, the complete data set for an installed safety system will be derived progressively from Base data by the addition of the *Application context* information, and applying the appropriate methodology to derive the actual parameters used in any specific safety function.

Where the templates are used to collect PIU data, then the actual conditions of service, the diagnostic environment, and the operational context are all known and the data is fed back to the Base data and the *Application context* data for the individual sub-systems and to any associated 'custom-defined sub-systems'.

CASS Templates for Sub-Systems

8 EXAMPLES

The examples are presented as small tables, for reference. In practice it would normal to combine several , as relevant, into a composite spread-sheet. The generic template is relevant to most sub-systems for formal product certification purposes, and provides a cross reference between the Data, The IEC61508 clause, and the CASS TOEs.

8.1 CASS SUMMARY TEMPLATE FOR PRESENTING THE RESULTS OF A SUB-SYSTEM CONFORMITY ASSESSMENT

Table 1. Sub-system data set

Object name	IEC 61508 Part 2 7.4.7.3	CASS TOE	Purpose of object	Data for Situation 1	Data for Situation 2	Data for Situation 3 etc.....
Sub- System ID	n)	1	All information which is required to identify the hardware and software configuration of the subsystem in order to enable the configuration management of the E/E/PE safety-related system in accordance with 1/6.2.1.			
Functional Specification	a)	2	Required to define those functions and interfaces of the subsystem which can be used by safety functions			
Environment/ stress criteria	d)	6	Any limits on the environment of the subsystem which should be observed in order to maintain the validity of the estimated rates of failure due to random hardware failures			

CASS Templates for Sub-Systems

Object name	IEC 61508 Part 2 7.4.7.3	CASS TOE	Purpose of object	Data for Situation 1	Data for Situation 2	Data for Situation 3 etc.....
Environmental limits	d)	6	As above			
Lifetime limits	e)	7	Any limit on the lifetime of the subsystem which should not be exceeded in order to maintain the validity of the estimated rates of failure due to random hardware failures			
Maintenance requirements	f)	9	Any periodic maintenance requirements			
Repair constraints	f)	12	Any additional information (e. g. repair times) which is necessary to allow the derivation of a mean time to restoration (MTTR) following detection of a fault by the diagnostics			
Hardware fault tolerance	k)	14	The hardware fault tolerance of the subsystem. Needed to determine the highest safety integrity level that can be claimed for a safety function according to the architectural constraints			
Systematic failure constraints	l)	16	Any limits on the application of the subsystem which should be observed in order to avoid systematic failures.			

CASS Templates for Sub-Systems

Object name	IEC 61508 Part 2 7.4.7.3	CASS TOE	Purpose of object	Data for Situation 1	Data for Situation 2	Data for Situation 3 etc.....
Proven in use only						
Evidence of similar conditions in previous use	7.4.7.6	17	Demonstrates that the previous conditions of use of the specific subsystem are the same as, or sufficiently close to, those which will be experienced by the subsystem in the E/ E/ PE safety- related system.			
Evidence supporting the application under different conditions of use	7.4.7.8	18	Required to justify the use of failure rates established under different operating conditions.			
Evidence of period of operational use	7.4.7.9	19	Required to support the claimed rates of failure on a statistical basis			
Statement of restrictions on functionality	7.4.7.1 2	20	Required in order to restrict the application of a 'proven- in- use' safety- related subsystem to those functions and interfaces of the subsystem which meet the relevant requirements.			

CASS Templates for Sub-Systems

Object name	IEC 61508 Part 2 7.4.7.3	CASS TOE	Purpose of object	Data for Situation 1	Data for Situation 2	Data for Situation 3 etc.....
Proven by design only						
Highest SIL (systematic)	m)	21	The highest safety integrity level that can be claimed for a safety function which uses the subsystem on the basis of the supporting evidence for control and avoidance of systematic faults			
Systematic fault avoidance measures	m)	22	Description of those measures and techniques used to prevent systematic faults being introduced during the design and implementation of the hardware and software of the subsystem			
Systematic fault tolerance measures	m)	23	Description of the design features which make the subsystem tolerant against systematic faults			
Validation records	o)	24	Documentary evidence that the subsystem has been validated according to clauses 2/ 7.7 and 3/ 7. of this standard.			

CASS Templates for Sub-Systems

Object name	IEC 61508 Part 2 7.4.7.3	CASS TOE	Purpose of object	Data for Situation 1	Data for Situation 2	Data for Situation 3 etc.....
Type A/ Type B	k)	15	<p>The appropriate classification of the subsystem with respect to Part 2 Tables 2 and 3, and the associated supporting evidence.</p> <p>Frequently, but not always, requires the application context to be known.</p> <p>See comments to TOE 15, and CASS Type A/B definition for explanation</p>			
Failure mode* * see Table 2	b), c), j)	3	<p>Required as input to the application-specific allocations of failure rates to safe and dangerous <i>failure modes</i>, which then permits the calculation of SFF and PFD.</p> <p>Proposed for these templates to be in the form of:</p> <p>Individual Failure Rates for each failure mode Plus, for each <i>failure mode</i>:</p> <ul style="list-style-type: none"> • Function affected • Consequence for the output signal • Externally available diagnostic indication of the failed state 	*	*	*

CASS Templates for Sub-Systems

Object name	IEC 61508 Part 2 7.4.7.3	CASS TOE	Purpose of object	Data for Situation 1	Data for Situation 2	Data for Situation 3 etc.....
Output State Failure rate (failures per million hours)* * see Table 2	b), c), j)	3	As above	*	*	*
Internal Automatic diagnostic test interval* * see Table 2	g), h)	10, 11	The diagnostic coverage derived according to Annex C. This information is required when credit is claimed for the action of the diagnostic tests performed in the subsystem in the reliability model of the E/ E/ PE safety-related system .	*	*	*
External diagnostic possibilities* * see Table 2	g), h)	10, 11	A description of the diagnostic facilities supported by the sub-system which are not used internally to force a specific Output State , but which could be used by other external functions to monitor the health of the sub-system. Requires a description and specification of the functions supported, the associated Output State of the associated diagnostic signal, if any, and the recommendations for implementation of the diagnostic function.	*	*	*

CASS Templates for Sub-Systems

Object name	IEC 61508 Part 2 7.4.7.3	CASS TOE	Purpose of object	Data for Situation 1	Data for Situation 2	Data for Situation 3 etc.....
Proof test requirements* * See Table 2	f)	8	The diagnostic test interval, when required. This information is required when credit is claimed for the action of the diagnostic tests performed in the subsystem in the reliability model of the E/ E/ PE safety-related system.	*	*	*

CASS Templates for Sub-Systems

Table 2 Failure mode data

The table records the results of the supplier's Failure mode and Effect Analysis, with the assigned failure rates, and identifies the possible techniques by which to increase the diagnostic coverage of those *failure modes*. Note that the information here is generic and not yet related to safe/ dangerous. Where several failure modes have a common output state they should be grouped together for reference to simplify the summation of failure rates per Output State.

	Failure mode	Output State	Failure rate (failures per million hours)	Internal automatic diagnostic test interval	External diagnostic possibilities	Proof test requirements	Notes
Data for Mode 1							
Data for Mode 2							
Etc.....							

CASS Templates for Sub-Systems

8.2 SIMPLEX/ PROVEN BY DESIGN

8.2.1 BASE INFORMATION

Sub-System ID	Flow sensor XYZ		
Functional Specification	Electronic differential pressure transmitter measuring air flow		
Environment/ stress criteria	Mil Handbook 217 F, Ground Benign, 50 deg C	Mil Handbook 217 F, Ground Fixed, 50 deg C	Mil Handbook 217 F, Ground Fixed, 100 deg C
environmental limits	-20 C to 150 C, 100% RH (or - refer to spec sheet xyz)		
lifetime limits	none		
maintenance requirements	annual calibration		
repair constraints	none		
hardware fault tolerance	none		
systematic failure constraints	not suitable for xxx applications		
highest SIL -(systematic)	SIL 2		
systematic fault avoidance measures	see report xyz-validation		
systematic fault tolerance measures	see report xyz-validation		
validation records	see report xyz-validation		
Type A/Type B	Type A, see wx123 validation report, supported by FMEA report XY123, and field experience data for very similar designs.		

CASS Templates for Sub-Systems

8.2.1.1 Example of part of a Validation Report

Note that the example conformance statements are not intended to be definitive of acceptable responses, and are not necessarily sufficient on their own to demonstrate compliance with the claimed SIL.

The table gives the mandatory techniques, and the selected optional technique, as required by the Table B2, with the accompanying statement by which the claim for compliance is made (and for which further supporting evidence is assumed to be available)

The manufacturer here has reproduced a table, with the requirements for SIL2 identified in column 3, taken from the Table B2. The claims in this case would relate to a relatively minor modification or enhancement of a 'standard' sub-system, and the 'Systematic SIL' claimed in this respect would be SIL2.

Table B2 Compliance			(Fault Avoidance)
Conformance for Highest SIL systematic failure, from Part 2 Table B2			Manufacturers Conformance Statement
Technique/measure	See IEC 61508-7	SIL2	
Observance of guidelines and standards	B.3.1	HR mandatory	ABC Ltd standard design, quality, and manufacturing disciplines under ISO9001.
Project management	B.1.1	HR low	ABC Ltd standard design, quality, and manufacturing disciplines under ISO9001.
Documentation	B.1.2	HR low	ABC Ltd standard design, quality, and manufacturing disciplines under ISO9001.
Structured design	B.3.2	HR low	Based on existing well established proven design. (same for all XYZ family)
Modularisation	B.3.4	HR low	Based on existing well established proven design (same for all XYZ family).
Use of well-tried components	B.3.3	R low	Based on existing well established proven design. (same for all XYZ family)

A similar table would be expected to be constructed from IEC61508 Part 2 Tables A16, A17, and A18 with A19 (see the TOEs for the techniques and measures implemented for systematic fault tolerance.

The Type A/Type B validation report needs to address the requirements of 2/ 7.4.3.1.2 for Type A, provide the necessary evidence, and define the assumptions made in the allocation of safe and dangerous failures. Note that factors in the application context may require this to be re validated for each specific application context.

CASS Templates for Sub-Systems

8.2.1.2 *Validation Records*

An example of the evidence a supplier may turn to for quality control and related assessment of performance characteristics of his sub-system. He would need to show which aspects of the sub-system functions were addressed by this evidence.

Validation of all design and specification as per ABC Ltd design procedures under ISO9001 for product certifications under CSA, FM, BASEEFA, EN50178, IEC721, EN50081-2, EN50082-2, & NAMUR NE21 as per ABC Ltd data sheet.

CASS Templates for Sub-Systems

8.2.2 FAILURE MODE DATA, PART OF BASE BATA

The table would convey the results of the supplier's Failure mode and Effect Analysis, with the assigned failure rates, and identify the possible techniques by which to increase the diagnostic coverage of those *failure modes*. Note that the information here is generic and not yet related to safe/ dangerous. Where several failure modes have a common output state they should be grouped together for reference to simplify the summation of failure rates per Output State.

Failure mode	Output State	Failure rate (failures per million hours)	Internal Automatic diagnostic test interval	External diagnostic possibilities	proof test requirements	Notes
component failures	Max. output, >20 mA	3	no	detect out of specified range - above 20mA		
component failures	Fixed output within range	1.3	No	monitoring of output for change consistent with other variables	annual calibration recommended	
component failures, calibration drift	false output within range	2.2	no	comparison with similar or inferred measurement;	annual calibration recommended	
component failures, broken connections	output below 4 mA	3.6	no	detect out of specified range - below 40mA		
component fault	Slow response	0.5	no	monitoring of output for change consistent with other variables	annual calibration recommended	Blocked external process connections would give the same result but must be addressed separately.

CASS Templates for Sub-Systems

8.2.3 FAILURE MODE DATA RELATED TO APPLICATION 1 CONTEXT (**HIGH FLOW TRIP**)

This takes the failure mode data from 8.2.2, and relates it to a specific *application context*.

Application context Statement

<i>Application context</i> Name	High Flow Trip HFT1
<i>Application context</i> descriptor	trip on High Flow, with out-of- range detection, no value comparison
Safety Policy	Fail Safe/ de-energise to trip/ on-line repair allowed on loss of instrument signal, with time-out
operating philosophy	normally mid range, high to trip
operating scenario	on-demand
safe conditions to be achieved	Response within 10 seconds of occurrence high flow.
Assumptions or descriptions of the external diagnostic environment provided.	detection of 'low out of range' by logic in the safety system.
Common Cause failure factor	not applicable for Simplex Systems

contd:

CASS Templates for Sub-Systems

The Output State, Failure Rate, and External diagnostic possibilities columns are taken from the Base Data, for reference here.

The last line is derived from knowledge of which failure rates are relevant in this context.

The Dangerous undiagnosed failure rate (column 8) is derived from mapping the Failure Rate to the implemented diagnostic functions, diagnostic coverage, and application context safety state

Output State	Failure rate	Context safety state HFT1	External diagnostic possibilities	Diagnostic coverage-external [%]	Notes *	Dangerous undiagnosed	Dangerous undiagnosed failure rate	proof test requirements	proof test coverage
Max. output, >20 mA	3	Safe	detect out of specified range - above 20mA	0	no external diagnostic implemented, accept spurious trip	no	0		
Fixed output within range	1.3	Dangerous	monitoring of output for change consistent with other variables	0	no comparison implemented	yes	1.3	validate full range excursion ref test procedure #xx1	100%
false output within range	2.2	Dangerous	comparison with similar or inferred measurement;	0	no comparison implemented	yes	2.2	validate accuracy across range ref test procedure #xx2	100%
output below 4 mA	3.6	Dangerous	detect out of specified range - below 4mA	100%	*1	no	0	no separate proof test required, covered by on-line diagnostics and the proof-test of the PLC input function.	
Slow response	0.5	Dangerous	monitoring of output for change consistent with other variables	0	*2	yes	0.5	validate accuracy across range ref test procedure #xx2	100%
	10.6						4.0		

* The notes here could be extensive, or refer off to an implementation guidance note. e.g.

*1) Dangerous unless detected by safety PLC standard algorithm, or by linked low alarm logic. Ensure the option is available and configured. Diagnostic action fails at the same rate as the PLC functional task, hence 100%.The on-line repair criteria, as opposed to forcing an immediate trip, requires a repair timer.

*2) The allocated failure rate relates only to the identified component fault. Blocked external connections are not included and must be addressed as a separate component.

CASS Templates for Sub-Systems

8.2.4 APPLICATION-CONTEXT CALCULATED PARAMETERS

This table would be typical of the data derived from all of the foregoing data, and consolidated for a specific application context.

Refer to	Parameter	Data Source
	<i>Application context</i> Name	e.g. High Flow Trip HFT1 from (8.2.3)
	<i>Application context</i> descriptor	e.g. trip on High Flow, with out-of- range detection, no value comparison ; from (8.2.3)
Type A/ Type B	Type A/ Type B classification	derived from Base data (8.2.1), Failure mode (8.2.2), and <i>Application context</i> (8.2.3) when evaluated against the requirements of the standard.
	overall relevant Failure rate	from application context specific subtotal (8.2.3)
	diagnostic test interval	from (8.2.2)
	automatic diagnostic coverage percentage of dangerous failures	derived from (8.2.1),(8.2.2), 8.2.3
	automatically diagnosed (dangerous) failure rate	derived from (8.2.1),(8.2.2), 8.2.3
	Dangerous failure rate detected by proof tests	derived from (8.2.1), 8.2.3
	Dangerous failure rate undetected by proof test	from 8.2.3 to explicitly recognise that all proof tests may not be 100% effective
	failure rate of safe detected failures	
	failure rate of safe undetected failures	
	SFF	derived from (8.2.1),(8.2.2), 8.2.3 and the diagnosed failure information derived above
	Application-specific repair constraints	derived from(8.2.1)
7.4.3.2.2 (d)	Common Cause factor	taken from 9.1.3 when applicable
	highest SIL by architecture	derived from (8.2.1),(8.2.2), 8.2.3, the SFF, the Type A / B classification, and the criteria in the referenced Part 2 table
	highest SIL -systematic for Proven By Design sub-systems	from (8.2.1)
1/ 7.6.2.9	Percentage SIL X -Continuous Mode	As applicable from the operating scenario (9.1.3); dangerous failure rate as determined in 9.1.3 when considering a continuous mode of operation, as a percentage of the permitted maximum dangerous failure rate for SIL X where 'X' is no higher than the highest SIL permitted from architectural and systematic considerations.

CASS Templates for Sub-Systems

8.2.5 SAFETY FUNCTION CALCULATED PARAMETERS

When the above Application Context parameters have been defined, the actual PFD for a specific functional safety task can be established.

Refer to	Parameter	Data Source
	MTTR	specified on an application specific basis, taking into account the constraints identified in the generic data from (8.2.1) base data and the actual operational environment.
	Proof Test Interval	specified on an application specific basis, taking into account the SIL required, and the unrevealed dangerous failure rates from 8.2.3 The proof test interval is manipulated until the resulting PFD for the sub-system is at the required level within the end-to-end functional safety task.
2/7.4.3.2	PFD	derived from (8.2.1),(8.2.2), 8.2.3, and the test interval parameters
1/ 7.6.2.9	Percentage SIL X -Demand Mode at defined test interval.	As applicable from the operating scenario (9.1.3). Dangerous failure rate as determined in 9.1.3 when considering a demand mode of operation, combined with the defined test interval to derive PFD, and expressed as a percentage of the permitted maximum PFD for SIL X , where 'X' is no higher than the highest SIL permitted from architectural and systematic considerations in the specified application context. e.g. XYZ flow sensor takes 25% of SIL X with 12 month proof-testing, in this application context.

CASS Templates for Sub-Systems

8.2.6 FAILURE MODE DATA RELATED TO APPLICATION 2 CONTEXT (TRIP ON LOW FLOW)

This set of data uses the base data from 8.2.1 in a different named *application context*. The significance here is that 'Safe' and 'Dangerous' are not assigned to the same *Output States* as in the previous example.

Application context Statement

<i>Application context</i> identifier	Low Flow trip LFT1
<i>Application context</i> descriptor	trip on Low Flow, with out-of- range detection, with value comparison , 50% effectiveness
Safety Policy	Fail Safe/ de-energise to trip/ no on-line repair allowed on loss of instrument signal
operating philosophy	normally mid range, low on demand
operating scenario	on-demand
safe conditions to be achieved	(only applicable for output devices)
Assumptions or descriptions of the external diagnostic environment provided.	detection of out of range by logic in the safety system. Deviation monitoring from adjacent process transmitter, 5% limit process excursion through hysteresis limit at least once per day will detect stuck value. Methodology and effectiveness covered by report XYZ.

CASS Templates for Sub-Systems

Output State	Failure rate	Context safety state LFT1	External diagnostic possibilities	Diagnostic coverage-external [%]	Notes *	Dangerous un-diagnosed	Dangerous un-diagnosed failure rate	proof test requirements	proof test coverage
Max. output, >20 mA	3	Dangerous	detect out of specified range - above 20mA	100	*1	no	0		
Fixed output within range	1.3	Dangerous	monitoring of output for change consistent with other variables	50%	comparison implemented with claim for 50% effectiveness	yes	0.65	validate full range excursion ref test procedure #xx1	100%
false output within range	2.2	Dangerous	comparison with similar or inferred measurement;	50%	comparison with similar or inferred measurement	yes	1.1	validate accuracy across range ref test procedure #xx2	100%
output below 4 mA	3.6	Safe	detect out of specified range - below 4mA	100%	No specific diagnostic action - system will trip anyway.	no	0		
Slow response	0.5	Dangerous	monitoring of output for change consistent with other variables	50%	comparison implemented *2	yes	0.25	validate accuracy across range ref test procedure #xx2	100%
	10.6						2.0		

*1 Dangerous unless detected by safety PLC standard algorithm, or by linked High Alarm logic. Ensure the option is available and configured. Diagnostic action fails at the same rate as the PLC functional task, hence 100%

*2 The allocated failure rate fraction relates only to the identified component fault. Blocked external connections are not included and must be addressed as a separate component.

8.2.7 APPLICATION-SPECIFIC CALCULATED PARAMETERS

A table for this *Application context*, as per 8.2.4, based on the data from 9.1.6

CASS Templates for Sub-Systems

8.3 SIMPLEX/ PROVEN IN USE

8.3.1 BASE DATA (GENERAL)

Arranged as several columns representing data from different conditions of use. Here segmented by different Environment/ Stress criteria which are process criteria relevant to the user, but which could also be characterised by measurable parameters (temperature, pressure, viscosity, acidity etc), or by operational (continuous, batch, on-demand) characteristics

Sub-System ID	valve ABC		
Functional Specification	4" Ball valve in ESD service, air to open, spring return, normally open, close on demand, with limit switches.		
Environment/ stress criteria	clean steam.	hot hydrocarbon fluid, clean *4	cool viscous hydrocarbon fluid, dirty *4
environmental limits	the environmental data from the application	the environmental data from the application	the environmental data from the application
lifetime limits	recommendation based on records of experience of wear-out and replacement times	recommendation based on records of experience of wear-out and replacement times	recommendation based on records of experience of wear-out and replacement times
maintenance requirements	3 year full service	2 year full service	1 year full service
repair constraints	none identified		
hardware fault tolerance	0	0	0
systematic failure constraints	none identified		
Evidence of period of operational use	pointer to records	pointer to records	pointer to records
Statement of restrictions on functionality.	Not validated for use as 'open-on-demand'		
For each intended application-specific environment:	*1		
Evidence of similar conditions in previous use.	*2		
Evidence supporting the application under different conditions of use.	*3		

* 1: depends here whether this column is for collection of data, or for prediction from other PIU data. Only valid for predictions; collection uses the 'Evidence of Use' records above, which become the reference data for predictions)

*2: pointer to records, for this sub-system in similar environments, or similar sub-system in this environment, and the assumptions made.

*3: pointer to records, for this sub-system in other environments, or similar sub-system in other environments, and the assumptions made.

*4: the different conditions of use considered as significantly affecting reliability performance

CASS Templates for Sub-Systems

8.3.2 FAILURE MODE DATA FOR THE DEFINED FUNCTIONALITY

Note: for PIU sub-systems the data will have normally been obtained with respect to a specified *Application context*. It may not be possible to identify all possible *failure modes*/ failure rates of the sub-system from one specific *Application context* - consequently it may not be possible to maintain a table of failure mode data independent of the *Application context*.

Failure mode	Output State *3	Failure rate per million hours	Internal Automatic diagnostic test interval	External diagnostic possibilities	proof test requirements
valve stuck closed, loss of air connection, other spurious closure, diagnosed	valve fails closed limit switch true	4	Whenever Limit switch is exercised *1	monitor limit switch *1 detect lack of flow	
valve stuck closed, loss of air connection, other spurious closure, undiagnosed	valve fails closed limit switch false	0.2	none	detect lack of flow	
seat obstructed, bad seal	Leakage internal (passing) when closed	2	No, only proof testing.	none	
valve stuck open, failed spring, diagnosed	valve fails open limit switch true	3	Whenever Limit switch is exercised *1	monitor limit switch *1 partial closure testing	
valve stuck open, failed spring, undiagnosed	valve fails open limit switch false	0.15	none	none	
flange seal failure	Leakage external *2	1	No	none	

Note that the following two factors are picked up later when the *application context* is known:

*1 the limit switch has no diagnostic value except as information after the demand or test, and the inclusion of the diagnostic is entirely dependent on whether the valve is periodically automatically exercised in addition to the proof testing.

*2 the listing of the 'leakage external' from the flange seal failure here may seem appropriate, but in this context may have no relevance to the actual safety function being considered. It may- however- be contributing to another potential hazard.

*3 Note that there are two output states, the valve state and the limit switch state, and consequently the four possible combinations of these states has been addressed.

CASS Templates for Sub-Systems

8.3.3 APPLICATION CONTEXT STATEMENT FOR 'CLOSE ON DEMAND, PARTIAL CLOSURE TEST'

Application context Statement

Application context identifier	ESDV A1
Application context descriptor	Close on demand, with partial closure test
Safety Policy	Fail Safe/ de-energise to trip/ loss of instrument air is safe
operating philosophy	normally open, close on demand
operating scenario	on-demand
safe conditions to be achieved	gas tight closure
Assumptions or descriptions of the external diagnostic environment provided.	limit switches, combined with automated partial closure testing, all logic in the safety system. Partial closure test methodology described and validated in XYZ report, 80% diagnostic coverage. *

*Note that there may be limitations in the effectiveness of the external test, and limitations imposed by the failure rate of the limit switches which form part of the diagnostic hardware. The presentation of the information in this template make it clear that, in this case, the limitations imposed by the failure rate of the limit switches has already been taken into account in the base data for the subsystem.

CASS Templates for Sub-Systems

Output State	Failure rate	External diagnostic possibilities	Diagnostic coverage-external [%]	context safety state ESDV A1	Notes *	Dangerous undiagnosed	Dangerous undiagnosed failure rate	proof test requirements	proof test coverage
valve fails closed limit switch true	4	monitor limit switch detect lack of flow	0	Safe	no explicit diagnostic required. accept as spurious closure.	no	0		
valve fails closed limit switch false	0.2	detect lack of flow	0	Safe	no explicit diagnostic required. accept as spurious closure.	no	0		
Leakage internal (passing) when closed	2	none	0	Dangerous		yes	2	*3	100%
valve fails open limit switch true	3	monitor limit switch partial closure testing	80%	Dangerous	*1	yes	0.6	*4	100%
valve fails open limit switch false	0.15	none	0	Dangerous	*1	yes	0.15	*4	100%
Leakage external	1	none	0		*2		0	*5	90%
	9.35 (flange seal excluded) *2						2.75		

*1 The limit switch provides no diagnostic unless partial closure testing is implemented. Both are to be implemented via safety PLC. Diagnostic fails at same rate as functional task in the PLC. Partial closure test does not assure full closure on demand, so less than 100% claimed

*2 Noted as a potential contribution to a new hazard. (Assessed as not relevant to this function -excluded from calculations)

Proof test for leakage does not use process fluid as part of standard test, estimated 90% effective as a test.

*3 validate full closure to specified tolerances ref test procedure #xx3

*4 validate full valve excursion and limit switch operation ref. test procedure #xx4

*5 verify no leakage under closed, max pressure conditions

CASS Templates for Sub-Systems

8.3.4 APPLICATION-SPECIFIC CALCULATED PARAMETERS

A table for this *Application context* ESDV A1, as per 8.2.4

CASS Templates for Sub-Systems

8.4 REDUNDANT /PROVEN BY DESIGN

Notes.

1. There is significant scope here for confusion in terminology, when dealing with duplex systems. If a dangerous failure in one half is unrevealed, but the voted consequence is 'safe', do you best classify the fault as unrevealed/ safe (for the sub-system) or as unrevealed dangerous in this type of table? The recommendation is to use unrevealed - safe, and explain that the second fault is required to make it dangerous
2. care is needed about using (asking for) supplier data for duplex sub-systems where the response is conditional on whether certain externally available diagnostic features are actually used on an application. Can affect PFD and SFF

8.4.1 BASE DATA

Sub-System ID	SAFETY RELAY ABC		
Functional Specification	Dual separate double pole-guided contact relays in one assembly, coils in parallel, contacts in series. Intended for normally energised coil, normally closed contact safety applications: de-energise coil to open relay contact.		
Environment/ stress criteria	Mil Handbook 217E, Ground Benign	Mil Handbook 217E, Ground Fixed	
Type A/ Type B classification	Type A		
environmental limits			
lifetime limits			
maintenance requirements			
repair constraints			
hardware fault tolerance			
systematic failure constraints			
highest SIL -(systematic)			
systematic fault avoidance measures			
systematic fault tolerance measures			
validation records			

As a redundant subsystem the failure rate data will represent the results of the appropriate calculations related to the internal series and parallel architecture of the subsystem. The associated failure rate and failure mode table does not show the underlying failure rate information related to a single relay.

CASS Templates for Sub-Systems

8.4.2 FAILURE MODE DATA

Failure mode*	Output State for subsystem	Failure rate per million hours	Internal Automatic diagnostic test interval	External diagnostic possibilities	proof test requirements
for any one of two relays: open or short circuit in coil; open circuit in relay contact connections; contacts become high resistance or fail to remain closed when energised for both relays: open or short circuit in common energising circuit; open circuit in sub-system output contact connections	output circuit open	0.5	no	none	
for any one relay: short circuit across relay contacts; contacts welded together; contacts jammed together. Contacts of 1 relay remain closed when de-energised	Output remains closed when energised. Output circuit opens when de-energised, due to second relay. Diagnosed	.04	(the same frequency as demand or test)	(monitor the second pole of both relays during proof test and demands. Only revealed after demand or test)	Ref. Manufacturers Application Note Ap xxx for testing via second contact
as above, undetected by second contact, which cannot monitor all identified fault states	Output remains closed when energised. Output circuit opens when de-energised, due to second relay. undiagnosed	.0004	none	none	
concurrent on both relays: short circuit across relay contacts; contacts welded together; contacts jammed together; short circuit across output terminals Includes internal common mode	Output circuit remains closed when de-energised. diagnosed	0.005	(the same frequency as demand or test)	(monitor the second pole of both relays during proof test and demands. Only revealed after demand or test)	Ref. Manufacturers Application Note Ap xxx for testing via second contact
as above, undiagnosed. (2 nd contact cannot monitor all the potential faults)	Output circuit remains closed when de-energised. undiagnosed	0.0005	none	none	

* Detailed description of failure modes would normally be covered in the accompanying report.

CASS Templates for Sub-Systems

8.4.3 *APPLICATION CONTEXT DATA*

Application context Statement

Application context identifier	FSD1
Application context descriptor	Fail Safe, Open on demand
Safety Policy	Fail Safe/ de-energise to trip
operating philosophy	normally energised, normally closed, open on demand
operating scenario	on-demand
safe conditions to be achieved	(only for output sub-systems)
Assumptions or descriptions of the external diagnostic environment provided.	Assumes second pole is available off each relay, to permit monitoring of stuck contacts, and that monitoring is implemented.

contd.

CASS Templates for Sub-Systems

Output State	Failure rate	External diagnostic possibilities	Context safety state FSD1	Diagnostic coverage-external [%]	Notes *	Dangerous undiagnosed	Dangerous undiagnosed failure rate	proof test requirements	proof test coverage
output circuit open	0.5	none	Safe	0	accept as spurious closure.	no	0		
Output remains closed when energised. Output circuit opens when de-energised, due to second relay. Diagnosed	.04	revealed after a demand or test by monitoring second contact	safe, loss of limited functionality	0	*1	no	0	monitor the second pole of both relays during proof test and demands. Only revealed after demand or test. See procedure xxx5	100
Output remains closed when energised. Output circuit opens when de-energised, due to second relay. undiagnosed	.0004	none	safe, loss of limited functionality	0	*1	no	0		
Output circuit remains closed when de-energised. diagnosed by contact	0.005	revealed after a demand or test by monitoring second contact	Dangerous	0	*2	yes	0.005	verify correct action when de-energised ref test procedure xxx5	100%
Output circuit remains closed when de-energised. undiagnosed	0.0005	revealed after a demand or test by monitoring the output signal	Dangerous	0	*2	yes	0.0005	verify correct output when de-energised ref test procedure xxx6	100%
Total relevant failure rate	0.5459						0.0055		

*1 This information relates to an internal single relay only, and is required for the redundancy calculation. Safe at the sub-system level. The redundancy equation is significantly affected if the second pole is not monitored in testing.

*2 second contact is not accepted as a diagnostic in this context, and only assists in the proof testing of the relay.

CASS Templates for Sub-Systems

8.4.4 APPLICATION-SPECIFIC CALCULATED PARAMETERS

A table for this *Application context*, as per 8.2.4

CASS Templates for Sub-Systems

8.5 REDUNDANT /PROVEN IN USE

8.5.1 BASE DATA (GENERAL)

Sub-System ID	SAFETY RELAYS- GENERIC		
Functional Specification	Dual separate double pole-guided contact relays in one assembly, coils in parallel, contacts in series. Used for normally energised coil, normally closed contact safety applications: de-energise coil to open relay contact.		
Environment/ stress criteria	Offshore - ref# xx report	Onshore-ref # xy report	
Type A/ Type B classification	Type A		
environmental limits	the applicable range for this set of data		
lifetime limits	recommendation based on records of experience of wear-out and replacement times		
maintenance requirements	3 year maximum between proof tests		
repair constraints	none identified		
hardware fault tolerance	1		
systematic failure constraints	none identified		
Evidence of period of operational use	pointer to records		
Statement of restrictions on functionality.	Not validated for use as 'energise to trip'		
For each intended application-specific environment		*1	
Evidence of similar conditions in previous use.	pointer to records, for this sub-system in similar environments, or similar sub-system in this environment, and the assumptions made.		
Evidence supporting the application under different conditions of use.	pointer to records, for this sub-system in other environments, or similar sub-system in other environments, and the assumptions made.		

*1: depends here whether this column is for collection of data, or for prediction from other PIU data. Only valid for predictions; collection uses the 'Evidence of Use' records above, which become the reference data for predictions

CASS Templates for Sub-Systems

8.5.2 FAILURE MODE DATA

Failure mode *1	Output State for subsystem	Failure rate per million hours	Internal Automatic diagnostic test interval	External diagnostic possibilities	proof test requirements
	output circuit open	0.5	none	none	
	Output remains closed when energised. Output circuit opens when de-energised, due to second relay. Diagnosed	.04	(the same frequency as demand or test)	(monitor the second pole of both relays during proof test and demands. Only revealed after demand or test)	Ref. Corporate Application Engineering Practice CAE P xxxx for testing by a second contact
*2	(Output remains closed when energised. Output circuit opens when de-energised, due to second relay. undiagnosed)	0	none	none	cannot be detected
	Output circuit remains closed when de-energised. diagnosed	0.005	(the same frequency as demand or test)	(monitor the second pole of both relays during proof test and demands. Only revealed after demand or test)	Ref. Corporate Application Engineering Practice CAE P xxxx for testing by a second contact
	Output circuit remains closed when de-energised. undiagnosed	0.0005	none	none	

*1 Unless the end user has the facilities for detailed failure mode investigation, the Output State becomes the practical level at which failure rate information is maintained.

*2 This state is included for reference (only) from the previous PBD for example. It is actually a state which cannot be identified without detailed product analysis since it represents a short-circuit across an otherwise normally functioning relay, and cannot be diagnosed externally. This class of output state would not normally appear in a P IU table.

CASS Templates for Sub-Systems

8.5.3 APPLICATION CONTEXT DATA

Application context Statement

Application context identifier	FSD1
Application context descriptor	Fail Safe, Open on demand
Safety Policy	Fail Safe/ de-energise to trip
operating philosophy	normally energised, normally closed, open on demand
operating scenario	on-demand
safe conditions to be achieved	(only for output sub-systems)
Assumptions or descriptions of the external diagnostic environment provided.	Assumes second pole is available off each relay, to permit monitoring of stuck contacts, and that monitoring is implemented.

The context, and the context related data is the same as the previous Redundant PBD example.

CASS Templates for Sub-Systems

9 GUIDANCE ON FAILURE RATES AND DIAGNOSTIC COVERAGE

9.1 FAILURE RATES

Note that the standard actually calls for "diagnosed (dangerous) failure rates" and un-diagnosed dangerous failure rates, which are sub-sets of the information defined here. The standard does not call for 'all failure rates in all failure modes' since it presumes a pre-allocation and knowledge of the safe and dangerous modes.

That knowledge of safe and dangerous failure modes is only achievable with a clear *application context*, and before that is available, then the failure rate and failure mode data must be expressed in functional consequence terms for the output of the subsystem.

Where a subsystem fault has no consequence for the safety-related outputs of the subsystem which are relevant in the Application Context, then the failure rate associated with that failure mode should not be taken into account.

Where the failure rates are being considered within an explicit *application context*, then it may be acceptable to only have the data classified into safe/ dangerous failures. Where - in addition, external diagnostic functions are being applied, it is preferable to have the full failure mode information available to facilitate the appropriate implementation of the diagnostic.

Failure modes are classified as diagnosed, and non-diagnosed. A failure rate for each identified mode of failure is required which includes the extent to which it can be diagnosed, along with the states of the associated parameters, and the extent to which that diagnostic is inherent in the sub-system or dependent on additional application-level support. It will require further qualification, when placed into a specific *application context*, as to whether the external diagnostic support is to be implemented in this instance, or not. Since the templates in this document are intended also for structuring PIU information, it is important in that case that the diagnostic context is fully described i.e. whether the potential diagnostic function actually being exercised in this case.

Where the definition of failure is not clear, then a default assumptions should be made that a five percent deviation from normal expected performance constitutes a subsystem fault.

The choice for assessment of failure rates is between design assessment using reliability prediction techniques, or 'Proven-in-use' evidence, with a preference for site-specific 'proven in use' in the standard.

Techniques for prediction of failure rate are referenced in 2/7.4.7.4, with guidance. There is further guidance in Annexe C.1 (a) related to FMEA, and in Part 7 bibliography.

The guidance also relates to the classification of the data by the intended operating environment.

The IEC61508 assessor should expect to see a reference to a formal methodology underlying the assembly of the data, the allocation of the failure rates of each failure mode to an *Output State*, and be provided access to the evidence that the methodology has been appropriately and competently applied.

The assessor, and data supplier, should note that there has been significant activity in international standards related to predicting equipment reliability, and in particular note that the MIL Handbook 217 database is no longer being maintained. Draft Standard IEEE 1413 is under review (2001) and prediction methodologies based on assessment of similarity (to earlier models)

CASS Templates for Sub-Systems

and on 'physics of failure' are gaining ground. The Avionics Working Group (CA-AWG) CA-AWG/2/D is re-defining collection methodologies, and IEC 62308, Ed.1: Reliability assessment and durability analysis, has progressed to Committee Draft stage (2003).

There is no single definitive methodology recommended in IEC61508, other than the clearly expressed preference for site-specific proven-in use data.

- The more the *application context* deviates from the site-specific operational criteria, the more conservatism the assessor should expect to see in the use of the data.
- Extrapolation from data collected on one particular model and applied to another will require justification.
- Extrapolation from data collected on one particular model and applied to another from a different supplier will require additional justification since the detail of design characteristics may not be known to both parties.

For 'Proven-in-use' the failure rate will include systematic failures. Clauses 2/7.4.7.5 through to 7.4.7.12 address the criteria for 'Proven in Use' data. Note that 'Proven In Use' in the context of IEC61508 relates to a specific hardware or software configuration which is managed under version control, and is in no way generic to a class of sub-systems which may (or may not) have similar characteristics. Thus, industry specific and application specific reliability databanks (e.g. OREDA for Offshore Oil & Gas subsystems) which are generic, and not manufacturer/ model specific, are to be used in support of 'Proven By Design' sub-systems, and not in support of 'Proven In Use' arguments for sub-systems.

The primary reference for the collection of reliability data is IEC 60300-3-2:1993 (BS5760-11), Dependability management – Part 3: Application guide – Section 2: Collection of dependability data from the field, but the user must be aware that the methodologies are not specific to safety-systems, and the focus on the need for recording failure mode, output state, and common cause factors for redundant sub-systems is not addressed. Further practical guidance is available in: D.J. Smith -Reliability, Maintainability, and Risk. Ed 5 (ISBN 0-7506-3752-8)

There is an increasing interest in formal application of FMEA with extension to specifically address the diagnostic capabilities of a subsystem, with reference to MIL -STD-1629A, but the relative merits of that against similar extensions to other standards on FMEA such as BS 5760-5 and IEC 812 and the current status of those standards is not reviewed here.

9.2 DIAGNOSTIC COVERAGE

The methodology for assessment of diagnostic coverage is given in Part 2 Annex C, in which it is presumed that the 'safe' and dangerous context is known. For the generic sub-systems, the diagnostic coverage data is applicable for each identified *Output State*.

Note that diagnosed failures may implicitly require some level of application support. It is important that the diagnostic functions inherent in the standard sub-system, and those functions which are dependent upon external support be clearly identified. The IEC61508 standard is explicit about the diagnostics being part of the standard sub-system. This CASS document goes beyond that simplistic view and recognises that external supporting diagnostics can be applied to form useful standard configurations as Template items (e.g. a transmitter with out-of-range monitoring by the safety logic) but when that is done then all of the information related to the *application context* and the implementation and integrity of the external diagnostic function must also be available.

CASS Templates for Sub-Systems

Essentially, when an 'external diagnostic' (external to the original sub-system) is applied and a high level of diagnostic coverage is claimed, then the diagnostic function itself cannot be considered to be 'external' to the requirements of IEC61508, and the combination of the sub-system with the diagnostic function must be considered as the 'Identified Sub-system' in the Template. In such cases it may be useful to collect the data for the sub-system alone, and the external diagnostic function alone, as separate templates and create a dedicated composite sub-system template representing the 'standard implementation'.

In particular, the 'Notes' to Annex C.2 are important, and Notes 4 and 5 set the guidance for the diagnostic function to be "within the E/E/PE safety-related system", and to be automatic (independent of human intervention).

Where only modest claims are made for diagnostic coverage, sufficient perhaps to raise a Safe Failure Fraction from 40% to over 60% (a critical target in the architecture constraint tables in IEC61508 Part 2), it should be noted that there are still limits to the value which can be claimed, and to the techniques employed in achieving that value. The limitations are discussed in general in IEC61508 Part 2 Annex A.1, and the tables A14 and A15 address sensors and actuators with guidance for other sub-assemblies in Tables A1 to A13.

Diagnosed *Failure modes* are characterised by:

a) **Diagnosed fault, and forced sub-system state.**

Diagnosics which are always performed by the sub-system, on itself, which result in defined states being forced by internal active functions which are independent of applications. The resulting state is not a normal operational state. (Typically forced default output states, mechanically or electrically locked states). The effectiveness of such internal diagnostic functions is always reflected in the failure rate for the associated forced output state.

b) **Diagnosed loss of limited functionality, with continued normal sub-system operation.**

Failure modes which result in diagnostic status signals being generated by the sub-system which require that the status normally be used to invoke other application specific actions. A continued operational state of the sub-system is maintained due to internal redundancy, or the fault involves only partial loss of functionality, but for which repair is required. (E.g. loss of an internal diagnostic capability which does not force a defined output state; loss of one member of a voted standard arrangement within the sub-system)

c) **Diagnosed Loss of a specified function; no forced sub-system output state.**

Standard internal diagnostics which result in an externally available diagnostic status, but for which the resulting sub-system state is not (or can no longer be) forced to a default state. e.g.

- detected loss of electrical continuity, and no facility to force the sub-system output state
- diagnosed calibration error, with continued operation
- diagnosed communication error, with output frozen
- confirmation of physical actuation e.g. by a limit switch which is a defined part of the subsystem

Note that when this internal diagnostic is less than 100 percent effective, there will always be at least two separate failure rates associated with the diagnosed and undiagnosed output state.

CASS Templates for Sub-Systems

d) **Externally detectable abnormal sub-system signals; no internal separate diagnostic function, and no automatic response.**

Sub-system signals or other externally detectable abnormal characteristics which are outside of a defined range, but for which no diagnosed status is developed by the sub-system itself.(e.g. signal below 4 mA; signals more than 5% different in a voting set). May require guidance from the supplier for the technique to be employed for detection of the abnormal states, and will require assessment of the associated failure rate of the external diagnostic function whenever it is used and for which a claim is made.