

# **A Supplier Perspective on Tendering for Industrial Process Safety Systems, and the Role of Standards**

**The OGP Workshop on Instrumentation and Automation Standards.  
London Nov 2006**

**Barrie Reynolds, Honeywell Process Solutions  
Chairman, BSI GEL 65/1 (UK committee for IEC SC65A)  
Chairman, The CASS Scheme Ltd.**

**Honeywell**

- **The Marketplace, procurement practices, and structure**
- **The Standards, and their role in procurement.**
- **The Main Issues, and the Industry-led initiatives to address them.**
- **Examples of ‘difficult’ requirements**
- **Pointers to Best Practice**
- **Potential new standards development areas**

# Abbreviations

<b>FEED</b>	<b>Front End Engineering Design, before award of contract.</b>
<b>F&amp;G</b>	<b>Fire &amp; Gas Detection system</b>
<b>MTTR</b>	<b>Mean Time To Repair a diagnosed fault and return to service</b>
<b>PFDavg</b>	<b>Average Probability of Failure on Demand; one of the primary criteria in achieving IEC61508 SIL compliance</b>
<b>SFF</b>	<b>Safe Failure Fraction; a measure of the diagnostic coverage for dangerous failure states</b>
<b>SIL</b>	<b>Safety Integrity Level, as per IEC61508</b>
<b>SIS</b>	<b>Safety Instrumented System, from IEC61511</b>

# The Marketplace



Licenced processes		
Corporate, International & Other standards		(review of corporate standards, by invitation) Support IEC Standards Development
Process requirements		
HAZOP	(HAZOP)	(Hazop Support in FEED)
Safety Requirements	(Safety Requirements)	
Safety System Specification	(Safety System Specification)	(Safety System Specification in FEED)

# The Marketplace- End Users

- **Multiple End Users**

- No common corporate standards
- No common mandatory safety compliance standard
- Some have aligned corporate standards to IEC61508
- Many are merged conglomerates, merged standards
- many are global companies, local variations
  
- limited resources & expertise to review/ revise corporate standards and procurement processes
- more reliance on contracted services
- significant re-use of previous project documents in procurement processes, without review
- tendency to accumulate legacy and conflicting standards

# The Marketplace- Contractors

- **Multiple Contractors**
  - **Apply client's requirements**
  - **May be involved in Front End Engineering Design studies to develop the project safety system requirements.**
  - **May develop detail SIS requirements**
  - **Undertake the procurement process**
  
  - **No review/ revision of client's requirements**
  - **significant re-use of previous project documents in procurement processes**

# The Marketplace- Suppliers

- **Major suppliers aligned to IEC 61508/ 61511 requirements**
  - **Safety PLCs, Sensors, Valves, Pumps, Relays, Signal conditioning**
  - **Safety System Application Software**
  - **Man-Machine Interface (annunciators & CRT Display)**
  - **Diverse technology solutions (relay/ solid state/ software)**
  - **Installation and commissioning**
  - **Reliability and SIL Compliance consultancy**

# Suppliers

- Unusual to source all field devices, logic solver, application software from one supplier
- May be involved in Front End Engineering Design studies to develop the project safety system requirements.
- May further sub-contract some safety systems to 3<sup>rd</sup> parties, or procure field devices, signal interfacing components etc.
- May also supply the Process Control System

# The Standards, and their role in procurement.

Honeywell

- **IEC61508. Functional Safety, E/E/PES. (1998-2000)**
  - An end-to-end 'Safety Function' oriented standard, generic.
  - **Essentially a project standard**, whole lifecycle, for the **End User, Contractor, and Supplier**
  - **Not a component compliance standard.**
  - **Generic component/ sub-system reliability and design integrity criteria defined.**
  - **Requires knowledge of the specific application context and safety function in order to specify the components**
  - **currently being revised**

# IEC61511 Functional Safety, Process Industries

- **IEC61511 Functional Safety, Process Industries.**
- **Specific implementation of IEC61508.**
  - **End-to-end task oriented.**
  - **Excludes new hardware design, and system software design**
    - ◆ refers to IEC61508
  - **Provides selection criteria for 'Prior Use' components**

# IEC61508 and Procurement

- The IEC61508 SIL compliance criteria apply to the entire function, and the industry is still learning how to best deal with procurement of components, sub-systems, application software, and services to support overall compliance.
- Still on a learning curve
- The majority of the issues arise from lack of experience with the IEC61508-related standards in the client procurement specification.

# IEC61508 – Components & Sub-systems -1

Honeywell

- The compliance criteria in the standard are only for the implemented end-to-end safety functions
- Defines characteristics of sub-systems and components which *potentially* make them suitable for use at a particular SIL
  - Systematic design properties,
  - failure rate
  - failure mode
  - diagnostic coverage

# IEC61508 – Application Software & Services

- **Compliance criteria are systematic**
  - processes and procedures
  - methods & tools
  - competency
  - evidence-based assessment
- **Purchase specification frequently include requests for evidence of compliance, e.g. competency schemes, but are unsure of how to phrase the requirement, and the purchaser is probably unable to judge the adequacy of the response.**

# The Main Issues -1 - Conflicts

- **Conflicting requirements**
  - Availability, PFDavg, SIL, SFF, Failure Rate frequently **ALL used concurrently as criteria**, often without definition [safe, unsafe etc]
- **Conflicting standards**
  - ‘Applicable Standards List’ frequently **also** include older legacy standards, standards not intended for the current application, or contain philosophical conflicts.

# The Main Issues -2 Technical

- **Confusion of safety, security, environmental, and asset protection requirements**
  - Applying the IEC61508 criteria in all cases can be expensive
- **Inadequate/ Inappropriate Requirements**
  - Requiring IEC61508 SIL compliance for components, without the associated context information.
  - **Inappropriate/ impossible targets** set for sub-systems
- **Lack of understanding of constraints imposed by the standards on repair times, overrides, inhibits**
  - results in heated discussions, additional activities, modifications.

# The Main Issues -3 –Procurement Lifecycle

- **Procurement Timing**

- Procurement Phase is frequently **out of synchronisation** with the detail definition of the SIS
- Problem with detailed design data being required for SIS definition.
- Results in inadequate definition of SIS.
- **Normally suppliers do not receive detailed SIL allocation information at the time of the bid**
  - ◆ *typically affects the application software complexity, additional diagnostics etc.*
  - ◆ *can affect hardware quantity and architecture, once the field device characteristics are known.*
    - More valves required
    - more sensors required
    - more diagnostics and logic required

# Responding to the Issues –Industry Initiatives-CASS

Honeywell

- **The CASS Scheme Ltd. (<http://www.cass.uk.net>)**
  - UK initiative with broad industry backing, and HSE support
  - Register of Assessors & Accredited Certification Bodies
  - UKAS Accredited ‘**Approved Company**’ assessment criteria for capability to comply with the IEC61508 **Functional Safety Management** requirements
  - **End Users – Contractors –Suppliers –Safety Assessors**
    - ◆ addresses the systematic issues of **competency**, tools, procedures
    - ◆ provides confidence of a **company capability** to operate in compliance with the standard **for their scope of activity**.

- **CASS Templates for Sub-system Data**
  - aimed at providing a consistent format for **component and sub-system data** at the different stages from purchasing to in-service record keeping
  - suitable as a basis for independent assessment and validation of the basic data & characteristics of subsystems for safety applications
  - **Being used as template for 'Product Assessment' by Certification Bodies** for validated safety-related data to address the so-called 'SIL Compliance' requirements
  - Under continuing development, a 'Product Procurement' view, to address the education and 'inadequate/inappropriate' procurement specification issues.

# CASS - Value to Honeywell

- **Gained CASS Certification through SIRA in 2003**
- **CASS Functional Safety Capability Assessment**
  - 'Approved Company' status
  - UK Safety Project Implementation Group
  - + Honeywell India sub-contract services
- **Addresses our equipment selection, competency, and project engineering procedures.**
  
- **CASS Certificate submitted with the bid**
- **CASS is a key part of proposal presentation**
- **Value to Honeywell is the independence and UKAS accreditation.**
- **Well received and accepted by clients & contractors.**

# CASS - Value to End Users & Contractors

- **Demonstrates that the compliance requirements are addressed by the company procedures**
- **Equipment selection, competency, and project engineering procedures will be in place to ensure that purchase specifications have the appropriate integrity for the system being purchased**
- **Forms part of the evidence of compliance for safety regulators where formal demonstration of compliance to IEC61508 is a client requirement for the overall project.**

# Industry Initiatives-61508 Association

Honeywell

- **61508 Association** (<http://www.61508.org>)
  - Bring together end users and all links in the functional safety system supply chain
  - Identify and remove obstacles to profitable application of IEC 61508
  - Facilitate improvement in understanding of and competence in use of IEC 61508
  - Promote the CASS route for demonstrating compliance to IEC 61508 and related standards

- **Certification Bodies**

- Proprietary assessment scheme to address the independent review of Functional Safety Management requirements
- Detailed independent assessment of components and complex programmable Safety PLCs against their own IEC61508 compliance criteria

- **Consultants**

- Some consultants are establishing a recognised credibility in the market-place for independent failure mode, failure rate, and diagnostic coverage assessment of field devices and other common sub-systems.
- Several consultancy firms, including **Honeywell**, offer SIL Assessment and end-to-end functional task validation services.

# Examples of 'difficult' requirements-1

- **Major Chemicals Company**
  - involved heavily in development of the IEC standards
- **Evidence of lack of review/ resource**
  - **If two or more standards conflict, the more stringent standard shall apply.**
- **The system **availability** shall be > 99.998%.**
  - Availability in context of safety systems needs to be defined
  - Assumption is Operational Availability (Spurious Trip)
  - No repair time criteria specified, so the vendor is free to choose whatever he likes to meet the criterion.

# Examples of 'difficult' requirements-1a

- From the **same** requirements document section:
  - For the PLC system meet appropriate IEC requirements and Provide SIL certificate (Minimum **SIL2**) **up till** risk reduction factor of 1000 ( SIL 3 ).
  - The PLC shall have a Risk Reduction Factor of **better than** 1000 in order to achieve a **SIL of 3** for individual PSC functions.
  - The PLC shall be considered to operate in the **High Demand Mode**.
  - The **PFD** for the PLC will be better than  $1.5 \cdot 10^{-4}$ .

# Examples of 'difficult' requirements-1b

- **“For the PLC system meet appropriate IEC requirements and Provide SIL certificate (Minimum SIL2) up till risk reduction factor of 1000 ( SIL 3 ).”**  
(sic)
  - *meaning ??*
  - *1000 is the SIL2/ SIL3 border. Any PLC operating in SIL3 will need to be near to 10,000 risk reduction factor to accommodate field devices*

# Examples of 'difficult' requirements-1c

- **The PLC shall have a Risk Reduction Factor of better than 1000 in order to achieve a SIL of 3 for individual PLC functions.**
  - *Internally contradicts the previous requirement*
  - *1000 would still be 100% of SIL3 and makes no allowance for field devices*
  - *what is required here is either a specific failure rate target, or a specific PFDavg target with a mandated Proof Test Interval*

# Examples of 'difficult' requirements-1d

- **The PLC shall be considered to operate in the High Demand Mode.**
  - ***That is highly unusual for a SIS in the Chemical industry***
  - ***SIS operating in Demand Mode cannot have a Risk Reduction Factor, they only have a dangerous failure rate.***
  - ***The only applicable target criterion is tolerable dangerous failure rate.***

# Examples of 'difficult' requirements-1e

- The PFD for the PLC will be better than  $1.5 \times 10^{-4}$ .
  - *PFD is not relevant for High Demand/Continuous Mode*
  - *Target criterion is 15% of SIL3 for Demand Mode which would be sensible but*
  - ***No Proof Test Interval specified**, so it is a numbers game*
  - *conflicts with other requirements*
  
  - *Responses by suppliers have to be clause by clause, positive, compliant, without emphasising the errors in the requirements !*

# Examples of 'difficult' requirements-2

- **Major Offshore Operator**

- The ESD/F&G system architecture shall be designed and built to provide availability of **99.999** per cent.

- ◆ *Availability is undefined*

- ◆ *If 'Operational Available/ Spurious Trip' related it is a target of ~100years for Spurious Trip with 8 hour MTTR*

- ◆ *if 'Safety Availability' then it represents a PFD of 1 E-05, or 10% of SIL4, and is significantly over-specified. It can only be achieved through redundant diverse technology solutions.*

# Examples of 'difficult' requirements-2a

- **Major Offshore Operator**

- The ESD/F&G system architecture shall be designed and built to provide availability of 99.999 per cent.

- ◆ *The solution included a diverse relay system for **manual call button activation only**. The target Safety Availability of the SIS is only met for those functions. We claim compliance on a specific basis. The client is either happy, or didn't notice, or ticked the box anyway*
    - ◆ ***Fire & Gas systems**, overall, struggle to meet SIL1 and are unclassified as protection systems by many users.*

# Examples of 'difficult' requirements-2b

- **Major Offshore Operator**
  - The complete system shall meet the BS EN 61508/61511 SIL requirements **appropriate to this application.**
    - ◆ *but no SIL is specified in the procurement documentation*

# Pointers to Best Practice -1

- **Review current procurement practices**
  - align with IEC61508
  - **aim to provide a 61508-compliant requirements spec**
  - **develop a compliance tick-list for the completeness of the procurement specification**
  - **(note that IEC 61508 Edition 2 will have a specific section for assessment of the content of the requirement specification)**
  - **seek appropriate independent review- IEC61508 applies to the entire lifecycle, including procurement.**
  - **eliminate conflicting standards and legacy references**
- **Encourage the development of ‘typical’ safety functions as standard procurement templates**
  - **pre-qualified as compliant for specified SILs employing specified devices and architectures.**
  - **avoid the surprises during detailed design.**

# Pointers to Best Practice -2

- **Seek competent clarification & review from suppliers through FEED or similar studies**
- **Seek Supplier feedback after contract award**
  - **Less than 10% of client requirements specifications are seen as competent engineering documents by vendors**
  - **The same mistakes are repeated and passed around the industry. Find a way to break the cycle.**

# Pointers to Best Practice -3

- **Review the supporting material available from CASS**
  - public domain, free
  - available from CASS and 61508 Association
- **Join 61508 Association or other User + Supplier + Assessor organisations and work in a non-confrontational forum to develop the guidance you need.**

# **A Supplier Perspective on Tendering for Industrial Process Safety Systems, and the Role of Standards**

**The OGP Workshop on Instrumentation and Automation Standards.  
London Nov 2006**

**Barrie Reynolds, Honeywell Process Solutions  
Chairman, BSI GEL 65/1 (UK committee for IEC SC65A)  
Chairman, The CASS Scheme Ltd.**

**Honeywell**