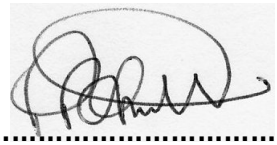
FUNCTIONAL SAFETY ASSESSMENT REPORT

for

MTM, F26, H28 and Cryogenic Series Habonim Ball Valves with Spring Return Actuator and Adaptor

Assessor:  .....

Bob Smith BA CEng FInstMC MIET
Sira Associate,
Sira Certification Service

Checked:  .....

Andrew Derbyshire IEng MIET
Functional Safety Consultant,
Sira Test & Certification

Date of issue: 09th May 2012

Customer: Habonim Industrial Valves & Actuators Ltd

Report Number: R56A27584A

CONTENTS

REVISION HISTORY

Rev	Date	Comment
0.1	07-May-12	Interim draft for internal review
0.2	08-May-12	Final draft with comments from independent check
1.0	09-May-12	Final version to be issued to the customer
1.1	20-Jul-12	Update to remove blank page at the end of the report

FUNCTIONAL SAFETY ASSESSMENT REPORT

Commercially in confidence

1 INTRODUCTION

1.1 References

Carried out by:	Sira Test & Certification, Rake Lane, Eccleston, Chester, CH4 9JN
On behalf of:	Habonim Industrial Valves & Actuators Ltd Kibbutz Kfar Hanassi Galil Elion 12305 Israel
Equipment assessed:	Habonim MTM, F26, H28 and Cryogenic series Ball valves with Spring Return Actuator and Adaptor
Date of Request for Assessment:	March 2012
Assessment standards:	IEC 61508-2:2010
Certificate number:	Sira FSP 12009 – MTM Ball Valve Series Sira FSP 12010 – F26 Ball Valve Series Sira FSP 12011 – H28 Ball Valve Series Sira FSP 12012 – Cryogenic Ball Valve Series
Assessments conducted between:	March and May 2012

1.2 Background and scope of the report

Habonim Industrial Valves & Actuators Ltd applied to Sira Test & Certification for assessment of their Valve and Actuator to the international functional safety standard IEC 61508 in late November 2009, for use in safety-related systems up to a safety integrity level of SIL3. In March 2012 Habonim requested an expansion to their existing certification requiring assessments of typical versions of four further ball valves, MTM, F26, H28 and Cryogenic. 2" versions were chosen in each case and these are assessed in the following report.

This assessment report covers the failure modes and effect analysis (FMEA) of four ball valves, manufactured by Habonim Industrial Valves and Actuators Ltd, Results are presented for valve actuator combinations using reliability data determined for the actuator in a previous report (See R56A20450A Rev 2-0 June 2010).

The lifecycle (to IEC 61508-2) and management of functional safety (to IEC 61508-1 clause 6) are reported on in a previous report and that assessment is not reported here but assumed to be fully operational and fully applicable to the lifecycle of the valves assessed here.

The valves associated with this assessment are all mature products and have been in the manufacturing phase for many years. The relevant lifecycle and management system assessment therefore applies to all relevant ongoing activities (including design modifications). This is reasonable, especially when considering that the devices qualify with the criteria for Type A components (IEC 61508-2, clause 7.4.3.1.2). The Valve and actuator combination that this report specifically supports are listed in the following table.

Valve	Description
2" T47Z with high temperature bonnet	Habonim Ball Valve body used in an automatically actuated configuration
2" F26	Habonim Ball Valve body used in an automatically actuated configuration
2" A28X	Habonim Ball Valve body used in an automatically actuated configuration
2" FCB47C Cryogenic Series	Habonim Ball Valve body used in an automatically actuated configuration

This report is only intended to support certification of the above product and products that are generically similar, i.e., the ball valve design is similar for all sizes of valve, and only materials are changed to suite different process applications.

The assessment was performed by one Sira assessor with relevant competencies in functional safety, specifically FMEA and SIL assessment.

Assessor	Company	Assessment Responsibility
Bob Smith	Sira Test and certification Ltd Associate	FMEA

1.3 Some common terms and abbreviations

E/E/PES	Electrical/Electronic/Programmable-Electronic safety-related Systems
SIL	Safety Integrity Level
UKAS	United Kingdom Accreditation Service
PFD	Probability of failure on demand
SIS	Safety Instrumented System
ESD	Emergency Shutdown
FSM	Functional safety management
SIF	Safety instrumented function
HFT	Hardware fault tolerance
SFF	Safety failure fraction
FMEA	Failure modes and effects analysis
MTTR	Mean time to repair

1.4 Overall description of the equipment

- The Valves are all mechanical devices which have metal bodies to provide mechanical integrity, compliance with the pressure vessel directive and environmental protection. These valves are intended for a variety of applications that include functional safety; they have not been designed specifically as a safety product. Application for functional safety is generally in a low demand application as an on – off valve emergency shutdown final actuator. This assessment has considered the two safety applications 'normally open' and 'normally closed' and in a 'Low Demand' mode of operation. Other functions and other modes of operation that might be required for non-safety applications have not been considered.

- Multiple valves may be used in series or parallel for increased 'reliability of trip' if required by the user.

1.5 Operating environment/constraints

The basic arrangement that has been assessed consists of a ball valve, a spring return actuator and an adaptor necessary to interface the actuator to the ball valve. It is worth explaining that the basic ball valve design is also available as a manually operated valve, hence to automate it is necessary to remove the manual handle and couple to an actuator using a specifically designed adaptor.

Four ball valves have been selected for this assessment and each is representative of a particular Habonim range. The particular ball valve part chosen is expected to be a typical of each range in terms of reliability and consequently further FMEA of other sizes should not be necessary.

Each valve actuator assembly must be provided with an associated 'restrictions in use' report constructed by the manufacturer, which will specify precisely the limits of environment and application within which the safety assessment is valid. The particular valves which are the subject of this assessment are the 2" versions of the MTM Series, F26 Series, H28 Series and Crogenic Series ball valve with adaptor to interface to a C25 4 piston actuator.

Temperature and Pressure limits are according to the restrictions in use report associated with each valve.

1.6 Identified hazards / risk reduction / SIL targets

The Manufacturer has a target of SIL3 for this product. This is defined by a perception of the market requirements and hence there are no specific identified hazards to be considered. Consequently, this assessment considers a theoretically 'ideal' application for the valve, the final decision on suitability for use in a particular safety function; environment and process application must rest with the safety loop designer as valve materials will vary considerably depending on the process application and process fluid. It is assumed that the process fluid is clean and free from all abrasive constituents that might damage the finish of the ball and the seat seal. This is in accordance with the manufacturers Installation, Operating and Maintenance Manual.

1.7 Safety functions

The safety related functions of the equipment are:

- To open on demand, OR
- To close on demand
- Low Demand mode of operation only.

2 SCOPE OF THE ASSESSMENT

2.1 Equipment and documentation assessed

This assessment is for the Habonim 2” ball valve with C25 Spring return actuator and C30 adaptor and all similar designs; representative valve part numbers are:

Ball valve part no. - 2” MTM T47Z
2” F26
2” H28
2” Cryogenic FC47C

Spring Return Actuator and adaptor failure rate data are extracted from a previous report R56A20450A Rev 2-0 June 2010.

2.1.1 Equipment Documents

The following documents define the equipment that is assessed and should be stated in any certificate that is supported by this assessment. Any changes to these drawings will require a re-assessment.

Table 1: Equipment Documents - Valve

Document no.	Pages	Rev	Date	Document description
20-TB47Z-GGGZIG-XBW	1 of 2	HA	18/04/2012	2-6” 47Z SER. FULL BORE METAL SEATED BALL VALVE EXTENDED BW ENDS
20-TB47Z-GGGZIG-XBW	2 of 2	HA	18/04/2012	2-6” 47Z SER. FULL BORE METAL SEATED BALL VALVE EXTENDED BW ENDS
20-F26-RR66FG-600-RTJ	1 of 2	HA	10/04/2012	2” F26 SER. ANSI 600 RTJ VALVE
20-F26-RR66FG-600-RTJ	1 of 2	HA	10/04/2012	2” F26 SER. ANSI 600 RTJ VALVE
20-A28X-666MWB-NPT	1 of 2	HA	10/04/2012	2” A28X SER.NPT VALVE-EXP
20-A28X-666MWB-NPT	1 of 2	HA	10/04/2012	2” A28X SER.NPT VALVE-EXP
20-FCB47C-66666PG-XBW75-6-C35	1 of 2	HAQ	11/11/2010	2” FCB47C SER. VALVE XBW75 ENDS V30, BONNET 6”
20-FCB47C-66666PG-XBW75-6-C35	1 of 2	HAQ	11/11/2010	2” FCB47C SER. VALVE XBW75 ENDS V30, BONNET 6”
TM-01-01E-12/06-HF	1 of 8	HF	None	Installation, Operating and Maintenance Manual

2.1.2 Documentation provided in support of the assessment

The following documents were assessed and or referred to during the assessment but do not require to be stated in any certificate that is supported by this assessment.

Table 2: Supporting Documents

Document number	Rev	Date	Document description
R56A20450A	2-0	June 2010	Habonim Valve-Act-AD Assessment Report

The above record does not include such documents as specifications, test plans, test procedures and test records. It should be understood that the components being assessed are established products being in production for some 2 years or more. Habonim document their valve designs under quality control procedure using 'Technical Files'. These Technical Files are effectively the valve specifications, ASME calculations, design drawings, test specs, test procedures etc. Test results are recorded during production using purpose designed test sheets which combine the test requirements with the results recorded by the tester. This is then a unique test record kept with the valve.

2.2 Assessment procedures, tools and techniques used

The assessment was carried out using the following procedures, tools and techniques:

Aspect	Procedures used	Tools / techniques used
Product assessment	• Reference was made to the relevant schedule of TOEs in The CASS Templates for Sub-Systems, rev 0, and the CASS Scheme Common Schedules in The CASS Guide, rev 2.a. • The ST&C procedures manual for functional safety assessment	• Document inspection • FARADIP.THREE, ver 5.0 • EXIDA – Final Elements & IEC61508 and IEC61511 Functional Safety Elements • Reliability Information Analysis Center Automated Databook V2.22 • ISA – Safety Instrumented Systems Verification – Practical Probabilistic Calculations.

3 SUMMARY OF ASSESSMENT

3.1 General

The CASS Templates for Sub-system Data have been used as a framework for the product assessment. The CASS Templates for the E/E/PES lifecycle and the management of functional safety that supports the product were assessed in a previous report. A summary of the safety-related qualitative and quantitative assessments follows below, based on the detailed findings in Annexes 1, 2 and 3 of this report.

3.2 FMEA exercise and determination and justification of the failure rate data used

The methodology of the FMEA process was to perform a desk based FMEA making reference to Habonim supplied valve drawings. An FMEA example is provided in Annex 6.

The components are initially listed out on the spreadsheet using a unique spreadsheet reference and also the drawing reference. Columns are added to allow Sira identified failure modes, Habonim comments/amendments and available failure rate data to be documented. Further columns are added so that failure modes can be categorised as $\lambda_{SU,}$ Safe Undetected failure rate, $\lambda_{SD,}$ Safe Detected failure rate, λ_{DU}, Dangerous Undetected failure rate, and $\lambda_{DD,}$ Dangerous Detected failure rate. Columns are included for factors such as proportion of failure rate (attributable to that mode), quality factor and environmental factor.

SIL is calculated according to the following formulae:

1. $PFD_{1oo1} = (\lambda_{DU}+\lambda_{DD}).T_1/2$ It should be noted that this equation is a simplified version of IEC61508-6 as for these simple mechanical devices λ_{DD} is always zero and Mean Time To repair (MTTR) for them is also small and has only a small effect, typically MTTR for the ball valve and actuator is 4-8 hours.

3.2.1 Quality and environmental factors

A conservative ‘Quality factor’ of unity was used, to reflect the fact that Habonim have and operate an ISO9000:2008 Quality system and carry out supplier audits to ensure a minimum quality of component materials. Almost all components are then manufactured by Habonim and are subject to the full BSI approved quality system procedures and inspections.

Initially a conservative ‘environmental factor’ of unity was used for a ‘fixed ground, (no adverse vibration, temperature cycling, etc. This factor was considered to be a reasonable factor for a normal valve application, however, it is important to note this fact in any certification and associated restriction in use; ensuring that the end user has a mechanism for adjusting the results of this report for the application cases where high vibration might significantly reduce the component reliability in practise.

3.2.2 Selection and justification of Failure Rate Data

It is a recommendation of this report that whenever a Habonim valve (or indeed any valve irrespective of manufacture) are commissioned into a safety (or environmental) service as a new and previously untried safety component, the end user must ensure that his/her own Functional Safety Management system requires the close monitoring of all such SIL equipment. In this manner site specific failure rate data may be obtained allowing a much more precise estimate of SIL to be made. This is an implicit requirement of IEC61508-2, para 7.4.7.6.

As it is completely unreasonable and impractical for Habonim to take responsibility for collecting failure rate at each and every site where their valves might conceivably be used, it is also then problematic to make an assessment of SIL in the absence of such a reliable data source. When selecting failure rate data for electrical and electronic equipment it is possible to take recourse to a generous amount of readily available data. This is not the case for mechanical components. We can easily find typical failure rates for complete valves of one type or another but it is difficult to find relevant generic data for valve components such as seals and valve stems. We have therefore used related data where available (for instance ISA, Safety Instrumented Systems Verification, a book that includes some typical data for ball valve components. We have also referenced Final Elements by EXIDA as this provides useful mechanical component failure data which might be used with care. Finally, we have viewed Habonim customer complaints for the last four years where it is possible to infer a metal casting failure rate which is consistent with the data published in reference works and also to determine a usable figure for graphite and graphite composite seals. This figure has been used as it is more pessimistic than the data for a generic seal.

It is recognised that none of these approaches to obtaining data is ideal. The most reliable data is that available to the end user, hence another requirement of this report is that Habonim attempt to establish such a co-operative relationship that component failure data of improved quality is available to enable adjustment, if necessary, of the SIL capability conclusion determined in this assessment and report.

3.2.3 Failure Data utilised

Four sources of data were used:

1 EXIDA – Final Elements & IEC61508 and IEC61511 Functional Safety Elements
2 Reliability Information Analysis Center Automated Databook V2.22
3 ISA – Safety Instrumented Systems Verification – Practical Probabilistic Calculations.
4 Faradip 3.5

This available generic data is then supported by that interpreted from Habonim NCR statistics.

The four reference generic sources provided the following data:

Table 3: Generic Failure Rate Data and Habonim NCR

Sub Component	**Failure Mode**	**Sources of Data/ Failure Rate Data**			
		Exida	**NPRD**	**ISA**	**Habonim NCR**
Castings	Porosity	1.8E-08			2.05E-08
Stem	Break/deformation	1.90E-08		1.88E-08	
Seat Ring					8.56E-09
Seal				2.00E-08	
Follower					
Disc Spring	Broken (20%)		6.00E-07	2.00E-08	
Disc Spring	Relaxation (80%)		6.00E-07	2.00E-08	
Body Bolts	Broken	1.00E-09		1.00E-09	3.42E-09 (loose)
Ball	Seizure - galling	1.3E-07		1.89E-07	8.56E-09 (leaking through)
Locking Clip					
Stem Packing				2.00E-08	1.03E-08
Stripped teeth			6.00E-07		
‘O’ ring		2.00E-07	8.55E-08	2.00E-08	
Coil Spring	Broken (20%)	8.00E-08	1.75E-06		
Coil Spring	Relaxation (80%)	8.00E-08	1.75E-06		

Actuator - whole	Worst case est.				7.5E-10
Seals – Graphite *					7.2E-8
Castings *					2.0E-08

'*' Data derived from Habonim complaints record provided 07/05/2012

In determining these failure rates the following problems were identified from NCR's:

Actuator bolts loose
Valve not closing
Leaking from stem
Valve bolts loose
Misc assy problems
Valve leaking through
Seat failure
Stem leakage
Porosity
Sticking
Failure to Open

Failure modes were considered by Habonim engineers and their comments are included within the fmeda wherever available.

3.2.5 Control of Systematic Failures

Habonim control of systematic failures was considered in January 2010 and reported in the associated report (referenced in para 2.1.2). The conclusion then that the controls in place were consistent with a Systematic SC of 3. It should be noted that Habonim customer complaints record indicates that some 30 out of 35 problems reported were systematic in nature. Habonim are therefore recommended to review their procedures and consider whether tighter procedures might be issued or additional training to ensure that existing management procedures are being followed.

3.3 FMEA RESULTS – presented as PFD/SFF

Valve type	SAFETY	SAFETY+PVST	ENVIRONMENTAL	REDUCED PROOF TEST
MTM	0.004/98%	0.003/99%	0.006/98%	0.001/98%
F26	0.003/99%	0.0008/99%	0.002/99%	0.0007/99%
H28	0.002/99%	0.0006/99.8%	0.001/99.6%	0.0006/99%
CRYOGENIC	0.004/98%	0.003/99%	0.002/99%	0.0009/99%

Summary of results

Safety	SIL2 capable (package) with a 1 year proof test interval
Environmental	SIL2 capable (package) with a 1 year proof test interval
Safety with PVST	MTM & Cryogenic – SIL2 capable with a 1 year proof test interval F26 and H28 – SIL3 capable with a 1 year proof test interval
3 month Proof Test	MTM SIL2 capable, F26, H28 and Cryogenic SIL3 capable.

Conclusion

This assessment has used worst case available data to ensure that a safe estimate of Failure rates and SIL capability has been presented.

It is recommended that this assessment is a good defendable assessment concluding that:

1. SIL2 is the safety SIL capability limit in a 1oo1 architecture and a low demand application with a one year proof test interval for all four valve series.
2. Where the use of partial stroke valve testing (PVST) is practicable SIL3 is achievable with the F26 and H28 series using a one year proof test interval though for the F26 the PFD is probably still too high for use when other loop components are included.
3. Where Environmental SIL is most important then SIL2 is the limit for a 1 year proof test interval.
4. SIL3 can be achieved for all but the MTM series when the proof test interval is reduced to 3 months, though this is only just achieved with the Cryogenic series.

In each case SIL3 may also be achieved in a 1oo2 or higher architecture.

4 CONDITIONS OF CERTIFICATION

The manufacturer of the certified equipment shall observe the following conditions of certification:

1. The manufacturer shall produce user documentation covering each product listed on the certificate that comprehensively describes the limits and conditions of safe use.

2. The manufacture shall encourage feedback of failure modes and failure rate data from their customers in order to build a library of component failure rates for each valve series.

3. Habonim shall review this data periodically to determine whether the average failure rates exceed the rates quoted in this report table 3.

4. Adequate Techniques and Measures are applied to the lifecycles of these valves to ensure that systematic failure potential is closely controlled. (A previous report reviewed Habonim's procedues and concluded that they were compatible with SIL3). Systematic failures are the most applicable to mechanical devices such as valves and consequently the close control of all lifecycle activities is the key to achieving high safety integrity.

5 CONDITIONS OF SAFE USE

The following conditions apply to the installation, operation and maintenance of the certified equipment. Failure to observe these may compromise the safety integrity of the certified equipment:

1. End users of the Habonim Valve and Actuator products must ensure that all failures are logged i.e. failure mode (safe or dangerous, component failure description if possible, date of failure, Number of hours in operation. In time this should provide useful corroborative data in support of Habonim SIL capability claims.
2. 100% Compliance with the recommendations contained in the Habonim Installation, Operating & Maintenance Manuals for the valve series concerned.
3. 100% Compliance with the Habonim document Compact II 4 Piston Pneumatic Actuator Installation, Operating & Maintenance Manual.
4. The ball valves shall not be used without complete overhaul, as recommended by Habonim, after a maximum of 4 years in use. After this time wear out mechanisms are likely to degrade the safe operation of the ball valve.
5. Unless recommended by Habonim engineering department R&D Engineering Manager, the end user shall not utilise the Habonim ball valve in such an application where abrasive solids are likely to be present. Such use will substantially increase the probability of damage to the ball or seat and may result in failure to achieve the required SIL capability.
6. The end user shall ensure that the ball valve-adaptor-actuator package is 100% proof tested in accordance with the manufacturer's recommendations and according to the proof test period used in the loop SIL calculation. This proof test shall include confirmation that the closing and opening torques are within specification, if not the valve must be returned to the manufacturers for overhaul as soon as possible. Until the valve can be removed from the safety application regular limited proof tests shall be performed to monitor the closing and opening torque. The revised proof test interval must be established by the process safety team risk assessment.
7. The end user shall ensure periodic visual checks are carried out to enable early detection of stem or body leakage and to generally check the condition of the valve body, bolts etc.
8. Only competent maintenance staff shall carry out proof testing and maintenance work.

6 OVERALL CONCLUSIONS

Conclusions

The assessment concludes that the four ball valve series concerned in this assessment achieve the requirements for SIL2 capability using the generic component data available, in both fail open and fail closed modes.
It should be noted that the assessment failure rates required by IEC61508-2 (λ_{DU}, λ_{SD}, λ_{DD}, & λ_{SU}) have no meaning for the ball valve alone, consequently all references to these failure rates are only on the basis of discrimination and action by some external means.

The assessment concludes that, with the available failure rate data, the Habonim Ball valve-adaptor-actuator package is capable of SIL2 (with a 1 year proof test interval) in both normally open and normally closed configurations.

The assessment also concludes that, with the available failure rate data, the F26, H28 and Cryogenic series ball valve-adaptor-actuator package achieve a PFD consistent with the requirements for SIL3 (when used with a proof test interval of 3 months) in both normally open and normally closed configurations.

Annex 1 – Details of the Sub-system Assessment

E/E/PES SUB-SYSTEM DATA TABLE

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508:2000 Clauses and Tables	Guidance for the assessor	Assessor's evaluation of the evidence of conformity
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.	Not checked at this time
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., • 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 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. Part of the Base Data set	Not seen at this time

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508:2000 Clauses and Tables	Guidance for the assessor	Assessor's evaluation of the evidence of conformity
3	The estimated rates of failure (due to random hardware failures) in any modes.	Required as input to the application-specific allocations of failure rates to safe and dangerous failure modes, which then permits the calculation of SFF and PFD. Proposed for these templates to be in the form of: Overall Failure Rate (all functional failures, all modes) Plus, for each failure mode: • % of overall Failure rate • function affected • consequence for the output signal • externally available diagnostic indication of the failed state	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 2/ Annex A 2/ Annexe C 7/B.6.6.1	Requires an environment context for the overall failure rate, or range of overall failure rates, which is relevant to the expected conditions of use. The use of an overall failure rate, and allocation of percentages to failure modes, presumes that the percentage allocation will be valid over the range of overall failure rates. Where that is not valid e.g. one failure mode becomes more dominant in certain conditions then that should be clear in the presented data.	Ball Valve – fail open or closed MTM $\lambda_{DU} = 9.1.10^{-7}$ /hr $\lambda_{SD} = 0$ No effects=$1.9.10^{-6}$ /hr F26 $\lambda_{DU} = 6.10^{-7}$ /hr $\lambda_{SD} = 0$ No effects=$7.5.10^{-6}$ /hr H28 $\lambda_{DU} = 4.4.10^{-7}$ /hr $\lambda_{SD} = 0$ No effects=$1.8.\ 10^{-6}$ /hr Cryogenic $\lambda_{DU} = 7.4.10^{-7}$ /hr $\lambda_{SD} = 0$ No effects=$2.5.10^{-6}$ /hr

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508:2000 Clauses and Tables	Guidance for the assessor	Assessor's evaluation of the evidence of conformity
4	diagnosed (dangerous) failure rates	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.	2/7.4.7.3 (b) 2/7.4.7.4 2/7.4.7.3.(j) 2/ Annex A	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 application context 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	The Habonim valve-adaptor-actuator has no diagnostics, it is completely mechanical. Diagnosed Dangerous failure rate = 0

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508:2000 Clauses and Tables	Guidance for the assessor	Assessor's evaluation of the evidence of conformity
5	un-diagnosed dangerous failure rates	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 undetected by diagnostic tests (see 2/7.4.7.4)	2/7.4.7.3 (c) 2/7.4.7.4 2/7.4.7.3.(j)	The referenced clauses in IEC61508 require dangerous failure rates to be defined. This is not valid at the generic sub-system level without an application context defining safe and dangerous states. The information required here is therefore described by the consequences of the failure on the critical parameters involved. (e.g. relay contact stuck closed) Categorisation into safe and dangerous states can be provided in addition, but only when accompanied by the assumptions for the application context A failure rate for each identified mode of failure. (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, and 'Proven-in-use' evidence. For 'Proven-in-use' the failure rate will include systematic failures.	MTM $\lambda_{DU} = 9.1.10^{-7}$ /hr F26 $\lambda_{DU} = 6.10^{-7}$ /hr H28 $\lambda_{DU} = 4.4.10^{-7}$ /hr Cryogenic $\lambda_{DU} = 7.4.10^{-7}$ /hr
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)		See Manufacturer IOM.

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508:2000 Clauses and Tables	Guidance for the assessor	Assessor's evaluation of the evidence of conformity
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)	consider wear out caused by design or application, e.g. capacitor or battery life, hardening of seals, run-time of bearings etc.	Wear out mechanisms are primarily soft parts, stem wear and seals. Operational restrictions are documented in the IOM, namely that pressure vessel wear should not reduce below ASMI B34. Zero stem leak is guaranteed for four years, after that full stem seal replacement is recommended.
8	proof test requirements	any periodic proof test requirements	2/7.4.7.3 (f)	• the purpose of the test, with respect to otherwise unrevealed failure modes • 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	Proof test periods are as stated
9	maintenance requirements	any periodic maintenance requirements	2/7.4.7.3 (f)	• the purpose of the maintenance • the maintenance procedure • the recommended in-service interval for maintenance.	Maintenance requirements are fully documented in the relevant IOM Manual

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508:2000 Clauses and Tables	Guidance for the assessor	Assessor's evaluation of the evidence of conformity
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	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. Annex A places constraints on the claims for diagnostic techniques. Note that failure rate of any internal or external diagnostic function is required to 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.	There is no diagnostic coverage; no failure mode is detected by automatic means.
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.	Not Applicable

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508:2000 Clauses and Tables	Guidance for the assessor	Assessor's evaluation of the evidence of conformity
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. 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 application context. Thus there may be several factors contributing to the actual MTTR as used in an application.	Not confirmed this time.
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	The requirement is for all information related to failure rate and diagnostic coverage, placed into the application context for safe and dangerous failure modes, 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. A SFF number must always be accompanied by the application context information. This relates to the inherent architecture and fault tolerance available with every instance of the sub-system, and not application-specific combinations.	SFF has no meaning for a ball valve alone. For each series build (valve – adaptor-actuator) the following were calculated: MTM=98% F26=99% H28=99% Cryogenic = 99%

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508:2000 Clauses and Tables	Guidance for the assessor	Assessor's evaluation of the evidence of conformity
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)	this relates to the inherent architecture and fault tolerance available with every instance of the defined sub-system, and not application-specific combinations.	**Fault Tolerance = 0**
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**	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. There are also constraints imposed on the highest claimable SIL by consideration of systematic faults for Proven By Design sub-systems, and those constraints may further restrict the overall claim for the sub-system.	The valve, adaptor and actuator may all be classified as Type A devices, they are simple mechanical and an FMEA has been completed of each component. There are no unpredictable aspects to failure. Though the End user must take extensive steps to ensure that restrictions in use are complied with. Habonim do not supply higher architectures though it is possible to increase the Fault Tolerance in this manner.
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)	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.	Techniques and Measures have been addressed in a previous report and concluded: A limit of SIL3 applies to Systematic failure constraints. The lifecycle (Annex 2) and management of functional safety (Annex 3) support a SIL3 (systematic) claim.

PROVEN-IN-USE SPECIFIC DATA TABLE

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508 Clauses and Tables	Guidance for the assessor	Assessor's evaluation of the evidence of conformity
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	Failure rate data is generic, reference has been made to Habonim NCR's to provide evidence that failure rate data used in the assessment is worse than Habonim NCR's suggest. This has been done to remain conservative in the assessment.
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.	Not Applicable.
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.	Not applicable

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508 Clauses and Tables	Guidance for the assessor	Assessor's evaluation of the evidence of conformity
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)	The sub system is a mechanical system to be used either for closing a process line on demand from a safety function or opening a process line. Demand Mode is Low. No other safety functions have been identified.

SUB-SYSTEM PROVEN BY DESIGN -SPECIFIC DATA TABLE

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508 Clauses and Tables	Guidance for the assessor	Assessor's evaluation of the evidence of conformity
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	See Annexe 6. Highest SIL (systematic) is SIL3.
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	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. 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.	See Annexe 6.

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508 Clauses and Tables	Guidance for the assessor	Assessor's evaluation of the evidence of conformity
23	systematic fault tolerance measures (see 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	Evidence that the features have been appropriately incorporated, consistent with the SIL claimed. 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. A16 requires aspects of redundancy, diagnostics, retry mechanisms etc. A17 requires measures against environmental hazards A18 requires consideration of operations aspects (modification, confirmation of operator action etc)	FT=0
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.	Not seen at this time

Annex 2 – Failure Mode and Effect Analysis Excel spreadsheet and mathematics

MTM - Hab TB47Z Series – safety
- - Hab TB47Z Series – Environmental
- - Hab TB47Z Series – Safety+PVST

F26 - Hab F26 Series – safety
- - Hab F26 Series – Environmental
- - Hab F26 Series – Safety+PVST

H28 - Hab H28 Series – safety
- - Hab H28 Series – Environmental
- - Hab H28 Series – Safety+PVST

Cryogenic - Hab FC47C Series – safety
- - Hab FC47C Series – Environmental
- - Hab FC47C Series – Safety+PVST