Summary

Emerson has requested that Lloyd's Register (LR) provide evidence to show that the above actuators are capable of meeting a Safety Integrity Level (SIL) 3 requirement. This is calculated from an Average Probability of Failure on Demand (PFDavg) and Architectural constraint perspective. Also, they require a certificate confirming these requirements.

Conclusions

From the failure data provided by Emerson, LR has confirmed that the above SIL 3 requirements have been met as follows:
PFDavg SR/FS = $3.24\text{x}10^{-4}$ = SIL 3.
PFDavg DA = 1.72×10^{-4} = SIL 3
Safe Failure Fraction (SFF) = >90% with Hardware Fault Tolerance (HFT) of zero and equipment type 'A' = SIL 3.

It must be demonstrated that each Safety Instrumented Function (SIF) that this actuator is used in can meet the SIL 3 requirements for all the sub-systems in the SIF. The onus is on the system designer to provide this evidence via calculation.

Details

A conservative estimate has been assumed of one operation per year for each of the supplied valves, with the data since the beginning of 2005 being included. This gives a figure of:

Model	Supplied Actuators	Number of Operations	Operational Hours	Operational Years
GVO-**-SR-**	203	732	$6.4\text{x}10^{6}$	730.6
GVO-**-FS-**	226	1130	$9.9\text{x}10^{6}$	1130.1
GVO-**-DA-**	883	3492	$30.6\ \text{x}10^{6}$	3493.1
Totals	**1312**	**5354**	**$46.9\text{x}10^{6}$**	**7414.5**

SINTEF Reliability Data for Safety Instrumented Systems PDS Data Handbook 2010 edition suggests using 2.5 million hours as a minimum aggregated time for claiming “proven in use”. The above figures are well in excess of this value. This statement holds true even considering an assumed 20% of the supplied parts may be backups, and therefore are not in use.

No dangerous undetected failures have been found however the 2.5 million hours figure is quoted as being sufficient to make a “proven in use” calculation.

In the document other rules suggested are:

- “Operational data should be available from at least two installations with comparable operational environments.” - The oil and gas industry is where most of the units are employed, therefore this condition is being met.
- “The data should be collected from the useful period of life of the equipment (typically this implies that the first 6 months of operation should be considered

excluded)." - The data being used is from the past 7 years of operation, while the device has been manufactured for over 30 years. It can therefore be assumed that the infantile mortality rate has been overcome in the earlier years of production.

- "A systematic data collection and reporting system should be implemented to ensure that all failures have been formally recorded." – This rule is being put into practice, with this document created using the collected data.

- "It should be ensured that all equipment units included in the sample have been activated (i.e. tested or demanded) at least once during the observation period (in order to ensure that components that have never been activated are counted in)". As stated above, the number of operational hours is far in excess of that required even with an assumed 20% backup rate.

These statements are based on IEC 61508 and IEC 61511, in which the required amount of operational experience is not stated, however the SINTEF document gives the above values as a guideline.

The failure analysis describes two detected failures:

"Two units of GVO since 2005: Slight leakage due to drive rod surface corrosion, but actuator performance still okay."

These occurred on the double acting (DA) actuator and were described as dangerous detected failures. Due to the nature of the failures (slight leakage) and the fact that the actuator performance was still "okay", we consider this a safe failure. Therefore we will assume two safe failures and zero dangerous detected failures. There have also been zero dangerous undetected failures.

Safe Failures	Dangerous Detected Failures	Dangerous Undetected Failures
2	0	0

For the following calculations, the failsafe and spring return actuator data has been combined due to their similar design and operation.

Chi-Square Test

It is possible to calculate a value for the failure rate of a device using a Chi-Square distribution, using a confidence level and assuming constant failure rate (random failures).

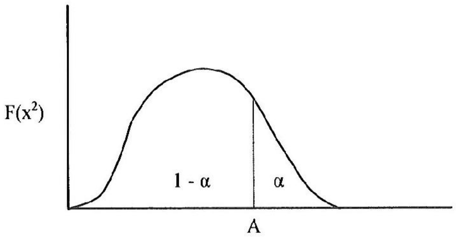

Figure 1 – Chi-Square Distribution

Figure 1 illustrates the distribution, where “A” is the confidence level, hence, the area marked α is the probability of χ^2 randomly rising above that particular value.

FAILURE RATE (FS/SR)

‘Reliability Maintainability and Risk – Practical Methods for Engineers’ Eighth Edition by Dr David J Smith shows us that for random failures, the failure rate is given by:

$$\lambda = \frac{\chi^2}{2T}$$

And outlines the method used in the following calculation.

Combining the operational hours for the FS and SR actuators, we find the accumulated test time, T, to be 16.3×10^6 hours and we take k to be 0 as there have been zero dangerous undetected failures.

Entering these values into the equation for n we find:

$$n = 2(k+1) = 2 \ \textit{degrees of freedom}$$

The number of degrees of freedom is the number of variables in a statistic that are variable. It describes the shape of the chi-squared distribution curve.

For a 70% confidence level (IEC 61508: Part 2 2010 requirement),

$$\alpha = 1 - 0.7 = 0.3$$

For the χ^2 value, we use a χ^2 distribution table, reading the value for α and n, producing:

$$\chi^2 = 2.41$$

Appling these values to the following equation, we find the failure rate.

$$\lambda_{70\%}(FS/SR) = \frac{\chi^2}{2T} = \frac{2.41}{2(16.3\times10^6)} = 7.39\times10^{-8}\text{failures per hour}$$

Using this method, we have therefore inferred an underlying dangerous undetected failure rate without any "real" failures. This figure should be treated as being conservative, as with more testing hours, this value will improve.

FAILURE RATE (DA)

Repeating this calculation for the double acting actuators, we find:

$$\lambda_{70\%}(DA) = 3.94\times10^{-8}\text{ failures per hour}$$

PFD average (Probability of Failure on Demand)

Calculating the PFD average, we can find how likely the device is to fail when it is required to operate.

$$PFD_{avg} = 0.5\lambda_{DU}T + \lambda_{DD}MTTR$$

(Equation from EEMUA 222 July 2009 App. F)

Where:

λ_{DU} =Dangerous Undetected Failure Rate
λ_{DD} =Dangerous Detected Failure Rate
T = Proof Test Interval (including restoration)
MTTR = Mean Time to Restore

The testing is done with a yearly interval, giving T = 8760 hours. The mean time to restore is taken to be 8 hours. Since there have been no dangerous detected failures, the failure rate is zero.

PFD$_{\text{AVG}}$ (FS/SR)

Inputting these figures into the above equation for the SR/FS actuator, we find:

$$PFD_{avg}(FS/SR) = \left(0.5\times7.39\times10^{-8}\times8760\right) + \left(0\times8\right) = 3.24\times10^{-4}$$

This value is solely for the actuator, other loop elements must be considered for the PFD of the full assembly.

PFD$_{\text{AVG}}$ (DA)

Repeating this calculation for the DA actuators, we find:

$$PFD_{avg}(DA) = 1.72 \times 10^{-4}$$

Safe Failure Fraction (SFF)

To find the SFF we require the failure rates of the device. No failures have occurred in the data for the SR or FS actuators so the SFF will be calculated for the DA actuators only. Since we only have safe failures, we take the dangerous failure rates to be zero.

We find the safe failure rate as follows:

$$\lambda_S = \frac{SafeFailures}{OperationalHours} = \frac{2}{30.6 \times 10^6} = 6.54 \times 10^{-8} \text{ failures per hour}$$

This can then be used to calculate the Safe Failure Fraction:

$$SFF = \frac{\lambda_{DD} + \lambda_S}{\lambda_{DD} + \lambda_S + \lambda_{DU}} = \frac{0 + 6.54 \times 10^{-8}}{0 + 6.54 \times 10^{-8} + 0} = 100\%$$

To meet a SIL 3, we must have an SFF of 90% or greater. For the given value this requirement is met.

Safe Failures	Dangerous Detected Failures	Dangerous Undetected Failures	Safe Failure Fraction
2	0	0	100.00%

The 100% value for safe failure fraction is due to the lack of dangerous failures. The SINTEF document advises this is acceptable due to the number of operational hours the products have experienced.
To meet a SIL 3, we must have an SFF of 90% or greater. For the calculated value, this requirement is met.

PREPARED BY:
Finlay Caird **Signature** *Finlay Caird* pp IH
Date 27 Aug 2012

APPROVED BY:
Ian Harris **Signature** *Ian Harris* Ian Harris.
Date 27 Aug 2012