



excellence in dependable automation

More accurate failure metrics – FMEDA Techniques for Mechanical Instrumentation

Dr. William M. Goble, P.E., CFSE

exida.com

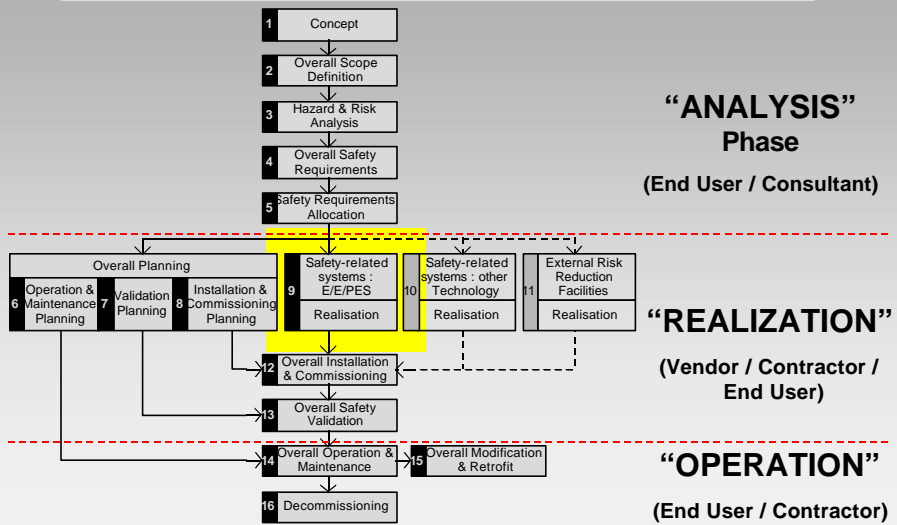
+215-453-1720

wgoble@exida.com



excellence in dependable automation

Safety Life Cycle - IEC61508



Safety Integrity Levels

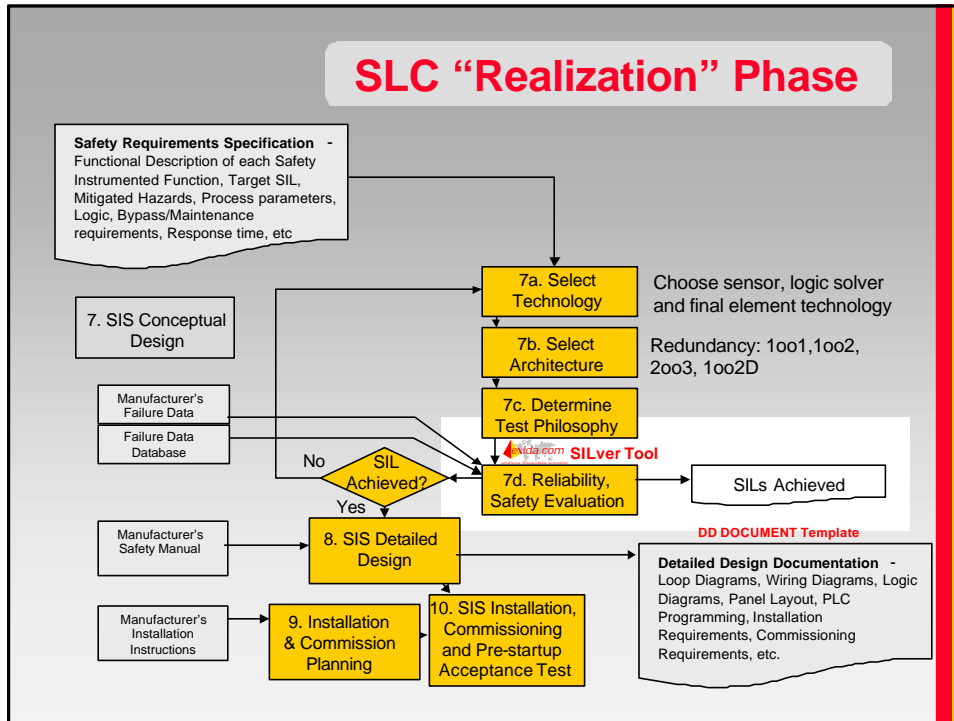
Safety Integrity Level	Probability of failure on demand (Demand mode of operation)	Risk Reduction Factor
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	100000 to 10000
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	10000 to 1000
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	1000 to 100
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	100 to 10

IEC61508 Safe Failure Fraction

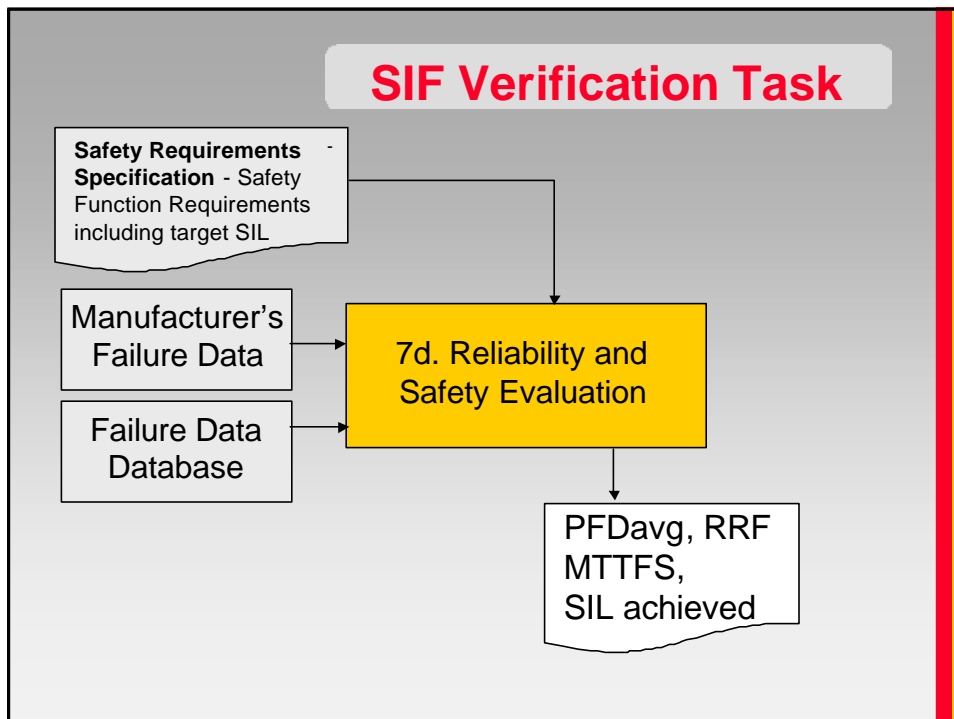
TYPE B

Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
< 60 %	Not Allowed	SIL1	SIL2
60 % < 90 %	SIL1	SIL2	SIL3
90 % < 99 %	SIL2	SIL3	SIL4
< 99 %	SIL3	SIL4	SIL4

SLC "Realization" Phase



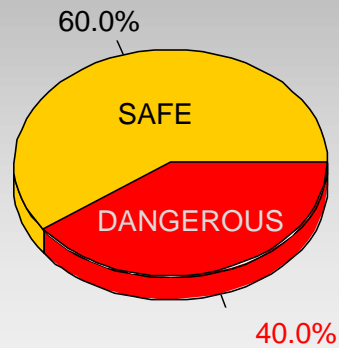
SIF Verification Task



IEC61508 part 6 - ISATR84.02 Method

- Divide failure rate into failure modes

$$\lambda = \lambda^S + \lambda^D$$



SD/SU/DD/DU

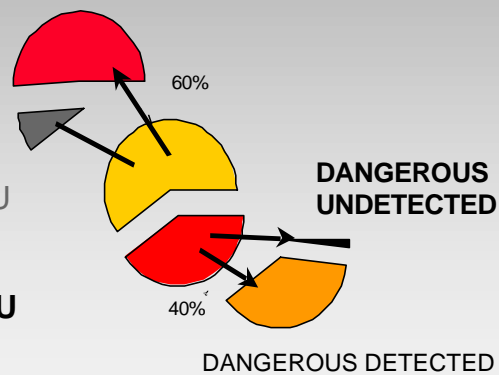
- Divide each failure rate into “detected” and “undetected” (by on-line tests)

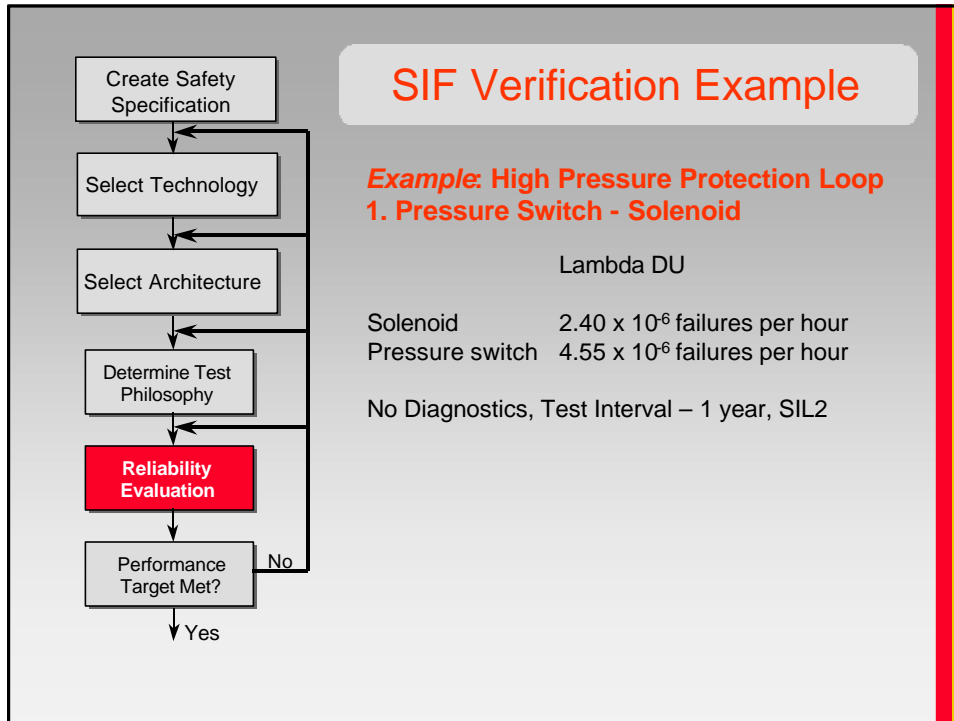
SAFE DETECTED

SAFE UNDETECTED

$$\lambda^S = \lambda^{SD} + \lambda^{SU}$$

$$\lambda^D = \lambda^{DD} + \lambda^{DU}$$





SIF Verification Example

Example: High Pressure Protection Loop
1. Pressure Switch - Solenoid

Lambda DU

Solenoid	2.40 x 10 ⁻⁶ failures per hour
Pressure switch	4.55 x 10 ⁻⁶ failures per hour

No Diagnostics, Test Interval – 1 year, SIL2

$$PFD_{avg} = \lambda^{DU} TI / 2$$

$$PFD_{avg} = (0.00000695 * 8760) / 2$$

$$PFD_{avg} = 0.03$$

$$RRF = 1/PFD_{avg} = 33$$

Safety Integrity Levels

Safety Integrity Level	Probability of failure on demand (Demand mode of operation)	Risk Reduction Factor
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	100000 to 10000
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	10000 to 1000
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	1000 to 100
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	100 to 10

exida SILver Tool

Tools are often used to do these calculations.

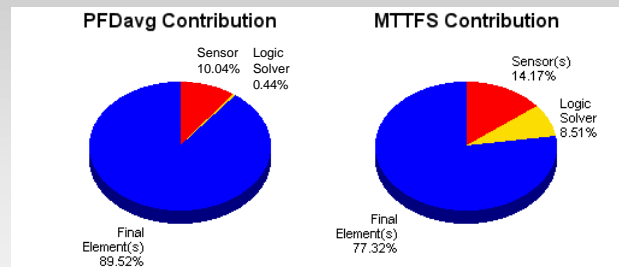
Sensor Part Information	
Source Group(s)	CE#
(1) Pressure	Details
IPIDavg Sensor Part	3.24E-03
MTTF Sensor Part (years)	125.28
Maximum SIL allowed (Architectural Constraints)	1

Logic Solver Part Information	
Logic Solver	CE#
(1) Logic Solver	Details
IPIDavg Logic Solver Part	1.41E-04
MTTF Logic Solver Part (years)	202.26
Maximum SIL allowed (Architectural Constraints)	0

Final Element Part Information	
Final Element Group(s)	CE#
(1) Valve	Details
IPIDavg Final Element Part	2.09E-02
MTTF Final Element Part (years)	22.39
Maximum SIL allowed (Architectural Constraints)	1

SIP Performance Metrics	
Safety Instrumented Function	Details
Average Probability of Failure on Demand (IPIDavg)	3.21E-03
Safety Integrity Level	1
Safety Integrity Level (Architectural Constraints)	1
Risk Reduction Factor	21
MTTF (years)	17.31

Often the results show that the final element contributes the majority of the probability of failure. This is primarily due to the relatively high failure rate data found in industry databases combined with conservative estimates of failure modes.



Scenario ID = 1532
Logged in as: William Coble

Home : Applications : SILver : Final Element Part Information : Component Details

Final Element Group 1: Valve

Final Element / Interface Data						
Component	Failure Rate (1/hr)	MTTF (years)	% Safe Failures	Safe Coverage Factor (%)	Dangerous Coverage Factor (%)	Architectural Constraint Type
Generic 3-way solenoid	6.00E-06	19.03	60	0	0	A

Valve Data						
Component	Failure Rate (1/hr)	MTTF (years)	% Safe Failures	Safe Coverage Factor (%)	Dangerous Coverage Factor (%)	Architectural Constraint Type
Generic air operated ball valve	3.00E-06	98.05	55	0	0	A

SIF Verification Task

Safety Requirements Specification - Safety Function Requirements including target SIL

Where does the data come from?

Manufacturer's Failure Data

Failure Data Database

7d. Reliability and Safety Evaluation

PFDavg, RRF
MTTFS,
SIL achieved

Failure Rate Data Models

1. Industry Databases – NOT Application Specific,
NOT Product Specific
2. Manufacturer FMEDA, Field Failure Study –
Product Specific
NOT Application Specific
3. Detail Field Failure Study – Application model.
Product Specific
Application Specific

Solenoid Failure Data Industry Database

exida.com estimate	Generic 2-way solenoid (DTT)	5.00E-06	75%	0%	0%	mean
dTR84.02	Solenoid (DTT)	7.75E-06	77%	0%	0%	mean
SINTEF	Pilot valve	4.20E-06	59.5%	30%	20%	mean
Smith	Valve - Solenoid (DTT)	1.00E-06	-	-	-	low
	Valve - Solenoid (DTT)	8.00E-06	-	-	-	high
CCPS-89	Valves-Operated-Solenoid	6.79E-07	-	-	-	low
	Valves-Operated-Solenoid	4.87E-05	-	-	-	mean
	Valves-Operated-Solenoid	1.89E-04	-	-	-	high
CCPS-89	Combination spurious and demand failure rate	7.32E-07	56.00%	-	-	mean
CCPS-89	Combination spurious and demand failure rate	1.06E-06	38.76%	-	-	mean
CCPS-89	Combination spurious and demand failure rate	5.71E-07	71.69%	-	-	mean
Ility Engineering	Solenoid Valves	2.97E-05	-	-	-	mean
Ility Engineering	Solenoid Valves	4.79E-05	-	-	-	mean
Ility Engineering	Solenoid Valves	3.00E-05	-	-	-	mean
Ility Engineering	Solenoid Valves	3.40E-05	-	-	-	mean
NPRD-95	Valve - Solenoid	6.15E-06	-	-	-	mean
NPRD-95	Valve, Pneumatic Solenoid	1.67E-05	-	-	-	mean
NPRD-95	Valve, Solenoid Operator	1.11E-05	-	-	-	mean
IEEE Std. 500-1984	Solenoid Valve	1.32E-06	-	-	-	mean

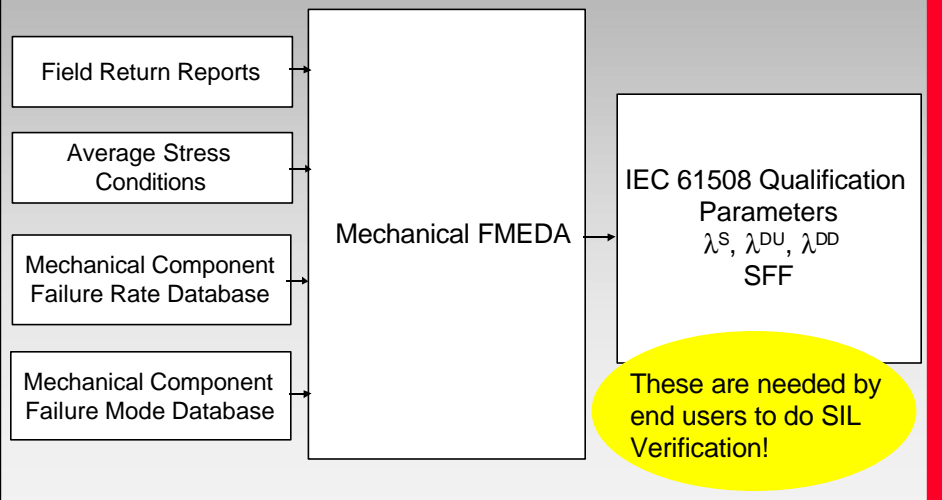
Ball Valve Failure Data Industry Database

- Ball valve example

Source	Description	Failure rate
ISA - DTR84.02 Draft (average)	Air operated ball valve	5.23E-06
Smith	Valves - Ball	2.00E-07 (low) 3.00E-06 (mean) 1.00E-05 (high)
RAC-Non electronic parts 1995 [x]	Valve, Pneumatic, Ball	7.14E-05
OREDA	Valves, Ball, Pneumatic	1.51E-06 (low) 2.92E-06 (mean) 5.64E-06 (high)

Source	Component	Total Failure Rate	% safe	Safe coverage	Dangerous coverage	Range	Notes
exida.com estimate	Generic air operated ball valve	3.00E-06	55.00%	0.00%	0.00%	mean	

Manufacturer's FMEDA Mechanical Components



FMEDA Procedure

- Extension of FMEA Technique
- Add diagnostic capability column
- When component / failure mode is detectable, indicate detection mechanism (and error code).
- Fault Injection results documented in chart

Four categories of failure rates

$$\lambda^{SD} = C^S * \lambda^S$$

$$\lambda^{SU} = (1 - C^S) * \lambda^S$$

$$\lambda^{DD} = C^D * \lambda^D$$

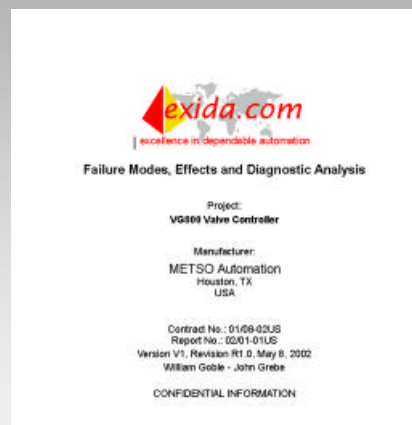
$$\lambda^{DU} = (1 - C^D) * \lambda^D$$

C^S – Coverage factor for safe failures

C^D – Coverage factor for dangerous failures

- ✓ FMEDA Reports – many manufacturer's are supplying such reports, primarily for electronic and electro-mechanical equipment.

- ✓ Metso Automation
- ✓ Fisher Controls
- ✓ Bettis
- ✓ Rosemount
- ✓ ...



FMEDA Analysis to date

Manufacturer	Product	Description	FMEDA Report	61508 Certification
Del-tronics	Pointwatch Eclipse IR	Hydrocarbon Gas detector	exida	None
	X3301 multi-spectrum IR	Flame Detector (fire detection)	exida	None
ABB	600T	Pressure Transmitter	TUV	TUV
Honeywell	ST3000	Pressure Transmitter	exida	None
	STT250	Temperature Transmitter	exida	None
Moore Industries	TRY	Temperature Transmitter	exida	None
	SPA	Site Programmable Alarm	exida	None
Rosemount	3051C	Pressure Transmitter	FM	None
	3051T	Pressure Transmitter	exida	None
	3144P	Temperature Transmitter	exida	None
	3051S	Pressure Transmitter	exida	None
	8800C	Vortex Flowmeter	exida	None
Yokogawa	EJA	Pressure Transmitter	exida	None
	YTA	Temperature Transmitter	exida	None
WIKA	T32	Temperature Transmitter	exida	None
Elcon	HD 2026 (SK)	Smart isolator	exida	None
	HD 2030 (SK)	Smart isolator	exida	None
	HD 2842	Switch/Proximity Detector	exida	None
Pepperl+Fuchs	ED2-STC***	Smart isolator	exida	None
	KFA*-S***-Ex*	Isolated Barrier	exida	None
	MUX 2700	HART Gateway	exida	None
MTL	MTL 5042	Repeating Power Supply	BASEFFA	BASEFFA
Magnetrol	Eclipse Model 705	Guided Wave Radar Level Transmitter	exida	None
	Eclipse Model 708	Guided Wave Radar Level Transmitter	exida	None
Endress & Houser	Fieldgate FXA 520	HART Gateway	exida	None
Fisher Controls	DVC6000	Valve controller	exida	TUV
Metso Automation	VG800	Valve controller	exida	TUV
Bettis Corporation	G series	Pneumatic Valve actuator	exida	None
	CB series	Pneumatic Valve actuator	exida	None
Mokveld	RXD series	Valve	AEA	TUV

Mechanical FMEDA

Item	Part Description	Failure Mode	Effect	Mode	Qty.	Lambda	% distr.
1-10	Housing	Fracture	Torque transmission failure	D	1	5.00E-09	95%
		Deflection	No effect	#	1	5.00E-09	5%
1-20	Housing cover	Fracture	Valve will not move	D	1	5.00E-09	95%
		Deflection	No effect	#	1	5.00E-09	5%
1-30	Guide block assembly	Fracture - piston side power sw	Springforce will cause shut down	S	1	3.00E-08	32%
		Fracture - spring side power sw	Valve will not move	D	1	3.00E-08	32%
		Fracture - middle	Valve will not move	D	1	3.00E-08	32%
		Deflection	No effect	#	1	3.00E-08	5%
1-50	Extension rod assembly	Fracture	Springforce will cause shut down	S	1	5.00E-08	95%
		Deflection	No effect	#	1	5.00E-08	5%
1-60	Extension retainer nut assembly	Loss of Thread	Springforce will cause shut down	S	1	5.00E-08	20%
		Loosen	Springforce will cause shut down	S	1	5.00E-08	80%
1-70	Yoke	Fracture	Valve will not move	D	1	1.00E-07	75%
		Deflection	Valve not fully seated	D	1	1.00E-07	20%
		Wear	Valve not fully seated	D	1	1.00E-07	5%
1-80	Yoke pin	Fracture	Valve will not move	D	1	6.00E-08	95%
		Deflection	Valve not fully seated	D	1	6.00E-08	5%
2-20	Guide bar bearing	Excessive friction	No effect	#	1	3.00E-08	40%
		Excessive play	No effect	#	1	3.00E-08	10%
		Seized	Valve will not move	D	1	3.00E-08	50%
2-25	Yoke pin bearing	Excessive friction	No effect	#	1	3.00E-08	40%
		Excessive play	No effect	#	1	3.00E-08	10%
		Seized	No effect	#	1	3.00E-08	50%
2-30	Yoke/Guide block bushing	Tear	No effect	#	2	3.00E-08	100%
2-40	Yoke bearing	Excessive friction	No effect	#	2	3.00E-08	40%
		Excessive play	No effect	#	2	3.00E-08	10%
		Seized	No effect	#	2	3.00E-08	50%
2-50	O-ring seal	Leak	N/A	#	2		99%
		Complete failure	N/A	#	2		1%
2-80	Rod wiper	N/A	N/A	#	1		100%
2-90	O-ring seal	Leak	N/A	#	2		99%
		Complete failure	N/A	#	2		1%
3-10	Inner end cap	Fracture	Air leak	S	1	2.50E-08	95%
		Deflection	Air leak	S	1	2.50E-08	5%
3-20	Tie bar	Fracture	Valve will not move	D	2	2.50E-08	5%
		Fracture	Release of pressure	S	2	2.50E-08	90%
		Deflection	Valve will not move	D	2	2.50E-08	1%
		Deflection	Release of pressure	S	2	2.50E-08	4%
3-30	Piston	Fracture	Springforce will cause shut down	S	1	2.50E-08	95%
		Deflection	Valve not fully seated	D	1	2.50E-08	5%

Mechanical FMEA Results for air operated actuator

Total failure rate	1.38E-06		
Safe failure rate	9.19E-07	% safe failure	66.64%
Dangerous failure rate	4.60E-07		
NoEffect failure rate	4.26E-07		
PVST - dangerous detected	4.26E-07	SFF no PVST	74.51%
PVST - dangerous undetected	3.40E-08	SFF with PVS	98.12%

Mechanical FMEA Problems

1. Component data sources still limited:
further correlation with field failure data
2. Stress - Strength Analysis needed for
more accuracy: tools available
3. Application Stress levels needed for
further accuracy: tools available

Mechanical FMEDA Problems

1. Component data sources still limited:
further correlation with field failure data
in progress now
2. Stress - Strength Analysis needed for
more accuracy: tools available
3. Application Stress levels needed for
further accuracy: tools available

Future

Debate on probabilistic methods – design value will be even more recognized and methods will become more widespread.

Failure Data – manufacturer's are responding to their customers are supplying data, this will continue.

Mechanical Equipment – IEC61508 probabilistic methods will show their value even for mechanical equipment used in functional safety applications and data available for that purpose will become more accurate.

