ELSEVIER

Journal of Hazardous Materials 142 (2007) 685–688

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

Innovative safety valve selection techniques and data

Curt Miller [a,*], Lindsey Bredemyer [b]

[a] *Exida LLC, Pasadena, TX, United States*
[b] *Exida LLC, Bryan, TX, United States*

Available online 27 June 2006

Abstract

The new valve data resources and modeling tools that are available today are instrumental in verifying that that safety levels are being met in both current installations and project designs. If the new ISA 84 functional safety practices are followed closely, good industry validated data used, and a user's maintenance integrity program strictly enforced, plants should feel confident that their design has been quantitatively reinforced.

After 2 years of exhaustive reliability studies, there are now techniques and data available to support this safety system component deficiency. Everyone who has gone through the process of safety integrity level (SIL) verification (i.e. reliability math) will appreciate the progress made in this area. The benefits of these advancements are improved safety with lower lifecycle costs such as lower capital investment and/or longer testing intervals.

This discussion will start with a review of the different valve, actuator, and solenoid/positioner combinations that can be used and their associated application restraints. Failure rate reliability studies (i.e. FMEDA) and data associated with the final combinations will then discussed. Finally, the impact of the selections on each safety system's SIL verification will be reviewed.

Keywords: Safety valve; Safety integrity level (SIL); Functional safety; Safety instrumented safety (SIS); Shutdown valve; SIL verification; Trip valve

1. Introduction—why such a focus on safety valves?

With the evolution of safety rated controllers and transmitters, the lagging component in safety instrumented safety (SIS) design is currently the final element. Normally, a remote operated "trip" valve serves in the capacity. If you consider the valve's probability of failure upon demand (PFD_{avg}) and its mean time to fail spurious (MTTFS) in a SIS pie chart that shows each components contribution, it is easily visualized (see Fig. 1) why you need to improve its design.

Above, the valve contribution to the SIS' availability (PFD_{avg}) and reliability (MTTFS) is 88% and 82%, respectively. If its failure characteristics are better known and modeling that accounts for testing are used, the complete SIS availability and reliability can be optimized.

2. Current ISA 84.00.01 requirements

The September 2004 updated ISA 84 (S84-2004, Ref. [2]) standard has several additions that affect the design and selection of the final element. They include the requirement for "prior use" or IEC61508 (Ref. [3]) certification, system verification, and minimal fault tolerance. Each of these will be discussed in the following subtopics.

2.1. Prior use or IEC61508 certification

"Prior use" is vague statement of historical, safe operation of a safety system product that leaves the owner/operator some discretionary freedom. It is felt, though, that this also requires the proof of a well-established maintenance integrity program that logs important failure rates and modes (discussed in detail in the following section). If this is not the case, then the user must look for certified or assessed devices (Fig. 1).

IEC61508 certified devices are items that have been submitted to outside agencies for detail assessment. They will look at both random and systematic failures areas of the devices as shown in Table 1.

In Table 1, several of the systematic failure areas do not apply to valves since they are associated with software programming. So, the key assessment areas for final elements are the detailed analysis of hardware failure modes and diagnostic capability (through a FMEDA—Failure Modes, Effects, and Diagnostics

* Corresponding author.
E-mail addresses: cmiller@exida.com (C. Miller), lbredemeyer@exida.com (L. Bredemyer).

0304-3894/$ – see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2006.06.072

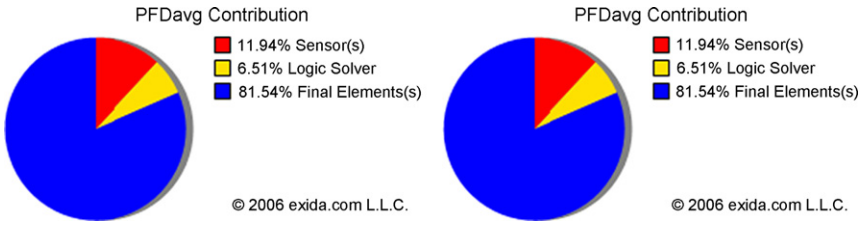


Fig. 1. The valve's contribution to safety and reliability (reprinted with permission, Exida, Ref. [1]).

Analysis), history, hardware design and modification process, and quality manufacturing methods.

If the user feels like they have a good history with a device, they can also take a "middle ground" position and personally contract the FMEDA to supplement their "prior use".

2.2. System verification—new modeling techniques

The complete system, including sensors, safety PLC, and the final valve apparatus, must now be reviewed with a probability model. The two most popular are Fault Trees and Markov Models. (For more information, see Ref. [6], Appendices C and D.) This requires "fail dangerous" data that, for the most part, has not been recorded well. (Note that this reliability data is required for all the remote actuated valve components to complete the calculation.)

The model also includes specifying a testing period. This could include a partial stroke test and its expected diagnostic "coverage" of the failure rates. We will discuss this in more detail in Section 6 and provide an example in Section 7.

2.3. Required fault tolerance (or architectural constraints)

After a safety integrity level (SIL) level is defined, there is a dictated "fault tolerance level" required for all the safety system components. For sensors and valves, Table 2 is shown.

If "prior use" can be demonstrated, you receive one credit towards your mandated level. Also, you can use the Type A table in the IEC 61508 standard, but using this table requires a detailed calculation of the Safe Failure Fraction (SFF). (See Ref. [5] for more detail.)

Table 1
Safety components assessment details (reprinted with permission, Exida, Ref. [4])

Random fault analysis	
Detail analysis of hardware failure modes	Analysis of hardware useful life
Detailed analysis of hardware diagnostic capacity	Analysis of proof test effectiveness
Assessment of operational hours based on manufactured units	
Systematic fault analysis—hardware	
Assessment of field failure return system	Field failures corrected Notification to users of safety issues
Assessment of hardware testing techniques	Assessment of hardware design process
Verification of product safety manual per IEC 61508	Assessment of manufacturing techniques
Assessment of design revision history—few revisions based upon design faults	Assessment of product testing techniques including environmental testing
Assessment of software requirements	Assessment of software criticality
Assessment of software design techniques	Assessment of software testing techniques
Assessment of configuration management per requirements of IEC 61508	

3. Review of current remote operated valve components

To complete a reliability assessment, all the components of the assembly must be accounted for. This includes the pneumatic/hydraulic assembly, actuator, and the valve itself. Each has its own failure characteristics that will affect the safety availability.

Concerning the control assembly, it can be a three way valve, smart positioner, or a complex mix of solenoids, test switches, pneumatic booster relays, quick exhaust valves, etc. Some of these devices will aid in diagnostics, some with response, but all must be accounted for in the failure rate calculation.

There are a whole host of linear and rotary acting, pneumatic, hydraulic, and electric actuators. The specific style chosen is based normally on the valve type. For safety applications, most will use a spring return for "safe state".

The main safety system valve types are:

- ball valves,
- butterfly (+offset version),
- gate valve,
- globe valve.

Ball valves would be the most commonly used in severe service. All have different performance characteristics, failure rates, and failure modes.

It should also be noted that there will be a mechanical linkage between the actuator and valve that affects its safety performance. Mechanisms include rack and pinion, Scotch yoke, and direct driven types. Jammed operation and loss of spring return would be classified as dangerous.

Table 2
Minimum fault tolerance/sensor and end elements (Ref. [2])

SIL	Minimum hardware fault tolerance
1	0
2	1
3	2
4	Special requirements apply (see IEC 61508)

Table 3
Common safety valves and primary dangerous failures

Valve type	Primary failure modes
Trunion mount ball valve	Ball surface damage—leakage Seat seal damage—leakage Trunion binding
Resilient butterfly valve	Seat deal damage—leakage Disk surface damage—leakage Stem breakage/binding
Globe valve	Disk surface damage—leakage Gland packing failure—binding Body seat leakage Stem shaft breakage/binding
Gate valve	Gate leakage Stem shaft breakage/binding Gland packing failure—binding

4. Investigation of common safety valves and their primary failure modes

Table 3 provides a good summary of the most popular valves used with safety solutions and their primary failure modes that must be reviewed.

These failure modes, some based upon severe service conditions, must be considered for each application and overcome if possible through selection of different construction materials and testing (i.e. diagnostics) to match the intended safety integrity level (SIL) required.

5. A sampling of current reliability data

As mentioned earlier, FMEDA (failure mode effects and diagnostic analysis) reliability studies are done to assess how safely a valve can work in service. It can also detect how well a partial valve stoke test (PVST) will support the installation's safety availability. Please review Table 4.

As shown, completing a partial valve stroke test will diagnose a range of the failures attributed to the specific valve combination. These may have been "felt" in past qualitative assumptions—now they are also substantiated by detailed scientific methods.

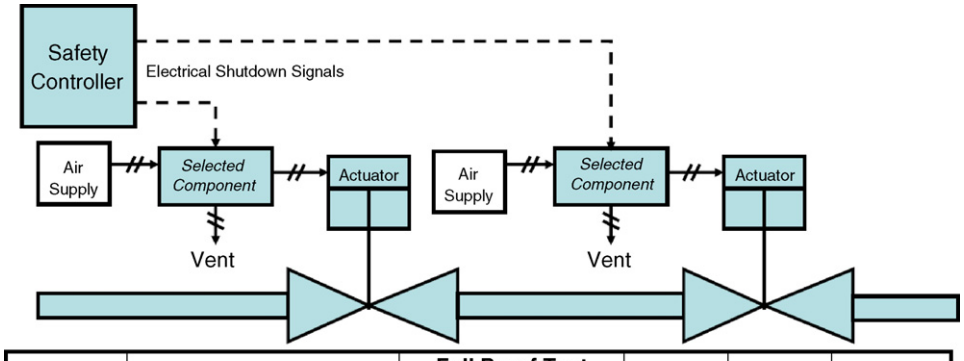
Table 4
Partial valve stroke capability obtained by FMEDA (reprint permission, ISA, Ref. [6])

Valve component	Application	PVST coverage (%)
Solenoid	De-energize to trip	99.0
Pneumatic piston actuator, clean service	De-energize to trip	99.3
Pneumatic piston actuator, severe service	De-energize to trip	99.6
Pneumatic rack and pinion actuator, clean service	De-energize to trip	81.9
Pneumatic rack and pinion actuator, severe service	De-energize to trip	88.0
Scotch yoke actuator, clean service	De-energize to trip	92.6
Scotch yoke actuator, severe service	De-energize to trip	94.0
Gate valve, clean service	Close to trip	84.0
Gate valve, severe service	Close to trip	84.9
Ball valve, severe service, full stroke only	Close to trip	58.2
Ball valve, severe service, tight shut-off	Close to trip	22.2
Resilient Butterfly Valve, clean service	Open to trip	63.6
Resilient butterfly valve, clean service	Close to trip	53.8

6. SIL verification—an example comparing partial stroke testing

One significant challenge that control designers face is supporting the extension of run times between shutdowns. If the shutdown valve was the original weak link in a SIS design, then partial valve stoke testing (PVST) may be the best option (as opposed to adding another valve).

In the following example (Ref. [5]), a solenoid is replaced with a SIL2 rated position controller (Fig. 2).



Method	Component Selected	Full Proof Test Interval	PVST?	PFDavg	SIL Achieved
A	Solenoid	1 yr	no	7.1E-04	2
B	Position Controller	3 yrs	yes	9.4E-04	2

Fig. 2. Example analysis of using partial stroke analysis (reprint permission, Exida, Ref. [1]).

Since the designer has better data and commercially available software (Ref. [7]) to run his calculations, the longer run time is easily verified. The net result is that users can now make good, scientifically supported choices on their SIS designs and testing periods.

7. Conclusion

The new valve data and modeling tools available today are instrumental in verifying that that safety levels are being met in both current installations and project designs. If the new S84 practices are followed closely, good industry validated data used, and a user's maintenance integrity program strictly enforced, plants should feel confident that their design has been quantitatively reinforced.

References

[1] Exida, On-Line Training Series, Introduction to Partial Valve Stroke Testing (PVST), 2005.
[2] ISA 84.00.01–2004, Functional Safety Instrumented Systems for the Process Industries, Parts 1–3, 2004.
[3] IEC61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems—Parts 1–7, 1998.
[4] W. Goble, Exida, Selecting Instrumentation Equipment for Safety Applications, 2002.
[5] I. van Beurden, R. Amkreutz, ISA, What does Proven In Use Imply, 2004.
[6] W. Goble, H. Cheddie, ISA, Safety Instrumented Systems Verifications, 2005.
[7] Exida, exSILentia Modeling Software.

Glossary

Assessment: The design of a trip system should be assessed to ensure it will meet its design requirements. Assessment should be thorough and should cover design specification, operation, testing, maintenance, and system management.

FMEDA (failure mode, effects, and diagnostic analysis): A technique for identifying potential modes of failure, the undesirable effects which would result and whether they can be diagnosed once they occur.

Hardware fault tolerance: The ability of a component or subsystem to continue to be able to undertake the required safety instrumented function in the presence of one or more dangerous faults in hardware.

IEC61508: An international standard that provides a structure for the quantitative and qualitative assessment of "risk" encountered in applications of Electrical, Electronic and Programmable Electronic (E/E/PE) equipment in industry. It also provides measures to be taken to reduce those risks "as low as reasonably practical" (ALARP).

Probability of failure on demand average (PFD_{avg}): The average probability of a protective system being in a fail dangerous state. It is based on the relationship between the number of demands and the number of hazardous events and is used to describe the total time during which a component, equipment or system is incapable of providing protection.

Safe failure fraction (SFF): The ratio of safe and diagnosed dangerous failures to the total failures.

Safety availability: The probability that a system will be able to perform its designated safety function when required for use.

Safety instrumented function (SIF): A function of an E/E/PE system which is necessary to achieve functional safety. A safety instrumented function can be either a safety instrumented protection function or a safety instrumented control function.

Safety instrumented system (SIS): A combination of one or more safety instrumented functions. A SIS is composed of sensor(s), logic solver(s), and final elements(s). It can include either safety instrumented control functions or safety instrumented protection functions, or both.

Safety integrity level (SIL): Safety functions are assigned one of four safety integrity levels. Safety Integrity Level 4 has the highest level of safety integrity and provides the greatest risk reduction, while Safety Integrity Level 1 has the lowest (IEC61508 3.5.6). These levels are defined in terms of the required probability of failure on demand average (PFD_{avg}) (i.e. the average probability that the system will be in a failed state when a demand occurs).

Verification: The activity of demonstrating for each phase of the safety lifecycle by analysis and/or tests, that, for specific inputs, the outputs meet in all respects the objectives and requirements set for the specific phase. For a system design, this step involves probabilistic calculations such as Markov models or fault tree analysis.

Curt Miller, CFSE, PE, Partner/Sr. Engineer with Exida, has more than 17 years of professional experience with safety systems. Before he joined Exida as a Partner/Sr. Engineer, he most recently spent 6 years supporting Gulf Coast safety control markets as senior engineer for an automation supplier. Curt is a BSChE graduate of Texas A&M. You can reach him at cmiller@exida.com.

Lindsey Bredemeyer, PE, Principal Engineer with Exida, has 12 years experience in valve engineering and failure analysis. This includes activities with process, oilfield and fire protection valves and prior experience in aviation/aerospace. Lindsey is a BSME graduate from the University of Houston. You can reach him at lbredemeyer@exida.com.