Meeting the SIS Standard's Challenge – Users and Manufacturers Working Together

Harold W Thomas (Hal)
Air Products and Chemicals, Inc.

Prepared For
Valve Manufacturer's Association
Technical Seminar

Houston, TX
March 3 & 4, 2005

ã Air Products and Chemicals, Inc
January 2005
Unpublished

Abstract:

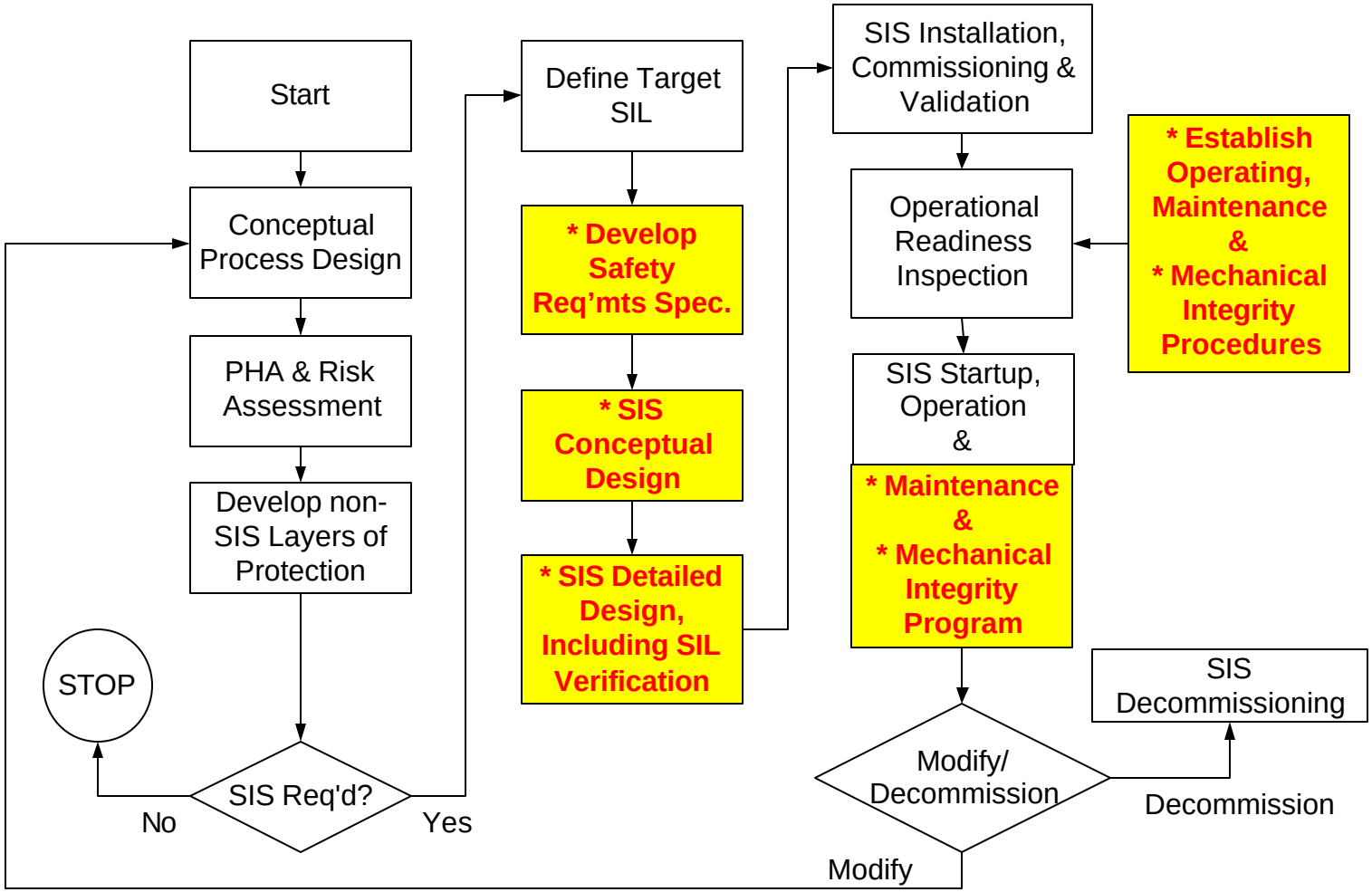
With the recently approved IEC 61511 and ANSI/ISA-84.00.01 standards, process industry companies are being challenged to determine what level of performance is required from their safety instrumented functions (SIF) and to then verify that the design, installation, operation and maintenance employed is sufficient to ensure that the required performance can be sustained until the SIF is decommissioned. These companies have turned to equipment manufacturers for assistance, sometimes expecting the full answer, which is beyond the control of the equipment manufacturers whose equipment is exposed to a variety of process conditions. This paper seeks to provide some insight as to what can be reasonably expected of equipment manufacturers regards compliance to these standards and how process industry users and equipment manufacturers can work together so that the whole is greater than the individual sum of the parts.

Introduction

In today's world, IEC 61508[1] and IEC 61511[2] have become the expected reality, irrespective of whether they are well understood. At their core, they are performance based standards that apply to the entire life cycle of safety instrumented systems illustrated in Figure 1. When this approach is viewed from an academic perspective, it makes perfect sense. However, when it comes time to implement, reality sets in as it becomes obvious that it is a formidable task. It requires the coordination and cooperation of a great many entities, both internal and external to a user organization. Manufacturers need to provide equipment capable of performing to a defined Safety Integrity Level, SIL, and to provide documentation that demonstrates that claim. They also need to have management systems in place that deal with changes and upgrades to that equipment over time so that spare parts can be considered to be "Replacement in Kind." User's need to combine equipment from several manufacturers and demonstrate that together they are capable of performing to some defined SIL in their specific process application. In addition, the user needs to develop systems that manage change and a program to ensure the mechanical integrity of the safety instrumented system and associated protection functions over its entire installed life.

This paper first provides a cursory look at the scope of the standard and some of the issues faced by users and equipment manufacturers as they try to cope with compliance. It then attempts to capture user expectations, not all of which are realistic, but none the less expected. It further seeks to differentiate those expectations that are realistic and those that are not. This sets the stage to recommend an approach of mutual cooperation between equipment manufacturers and users via an industry initiative under the auspices of the Center for Chemical Process Safety, CCPS, as a vehicle.

Figure 1


Start
Conceptual Process Design
PHA & Risk Assessment
Develop non-SIS Layers of Protection
STOP
SIS Req'd?
No
Yes
Define Target SIL
* Develop Safety Req'mts Spec.
* SIS Conceptual Design
* SIS Detailed Design, Including SIL Verification
SIS Installation, Commissioning & Validation
Operational Readiness Inspection
* Establish Operating, Maintenance & * Mechanical Integrity Procedures
SIS Startup, Operation &
* Maintenance & * Mechanical Integrity Program
Modify/ Decommission
SIS Decommissioning
Decommission
Modify

Applicability of Standard to Actuated Valves

The title of IEC 61508[1] is "Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related-Systems." Its focus is clearly on electrical, electronic and programmable electronic equipment. However, when the standard is examined in more depth, it is clear that the standard applies to the total instrument loop, i.e. sensor, logic solver, and final elements such as actuated valves when the loop is applied to a safety instrumented function, SIF, as part of a safety instrumented system, SIS. Once it is accepted that process sensors and final elements are included in the scope, suddenly the process wetted and mechanical parts must also be considered, even though they were never the main focus of the standard or initial 3rd party equipment certifications. Inclusion of the process environment and mechanical aspects of the equipment in a safety instrumented function significantly increases the degrees of freedom that must be addressed when assessing performance. These issues have been a point of confusion among both users and manufacturers, many of which are not expert in the interpretation of the standard. To further the conundrum, the standard is generally performance based rather than prescriptive. As such, there are potentially many different means of compliance.

The standard is also applicable to the entire life cycle of safety instrumented functions and their associated equipment. Effective compliance requires greater cooperation between not only various user functional disciplines, but also between users and equipment manufacturers of equipment intended for use in safety instrumented systems.

User Expectations

General - When required by regulatory/customer expectations, or even the user company's internal standards, it is the user's responsibility to ensure an appropriate design, operation and maintenance program throughout the safety instrumented system lifecycle as shown in figure 1. Different users may approach this responsibility in a variety of ways. For convenience, I have divided users into three broad categories. These are:

- The Unknowing
- The Unknowledgeable
- The Knowledgeable

The unknowing are those that are not aware of the standard or who have chosen to ignore it. Typically this group will simply continue to approach engineering as they always have with no changes. This group would have no expectations and as such is of little relevance to the remainder of the paper. Although the user has no expectations due to ignorance, the equipment manufacture may have some industry product stewardship responsibilities when dealing with this user group.

The unknowledgeable group is aware of the standard, but is largely ignorant of the true requirements. This group typically may believe that all they have to do is buy certified equipment with the appropriate SIL rating and then perform design as they always have in the

past. When dealing with this group, just as with the unknowing, the equipment manufacture may have some industry product stewardship responsibilities to educate the end user.

Between the unknowledgeable and the knowledgeable, there is an infinite continuum of increasing understanding, unfortunately with the potential for a number of interpretations. This paper assumes the knowledgeable user, or at least the user who is attempting that path. For these users, Figure 1 shows the areas (shaded boxes with bold text and asterisk) where the user expects the equipment manufacturer to provide assistance meeting regulatory and customer requirements. The knowledgeable user would expect this help and documentation from the equipment manufacturer irrespective of whether the equipment is certified to IEC 61508.

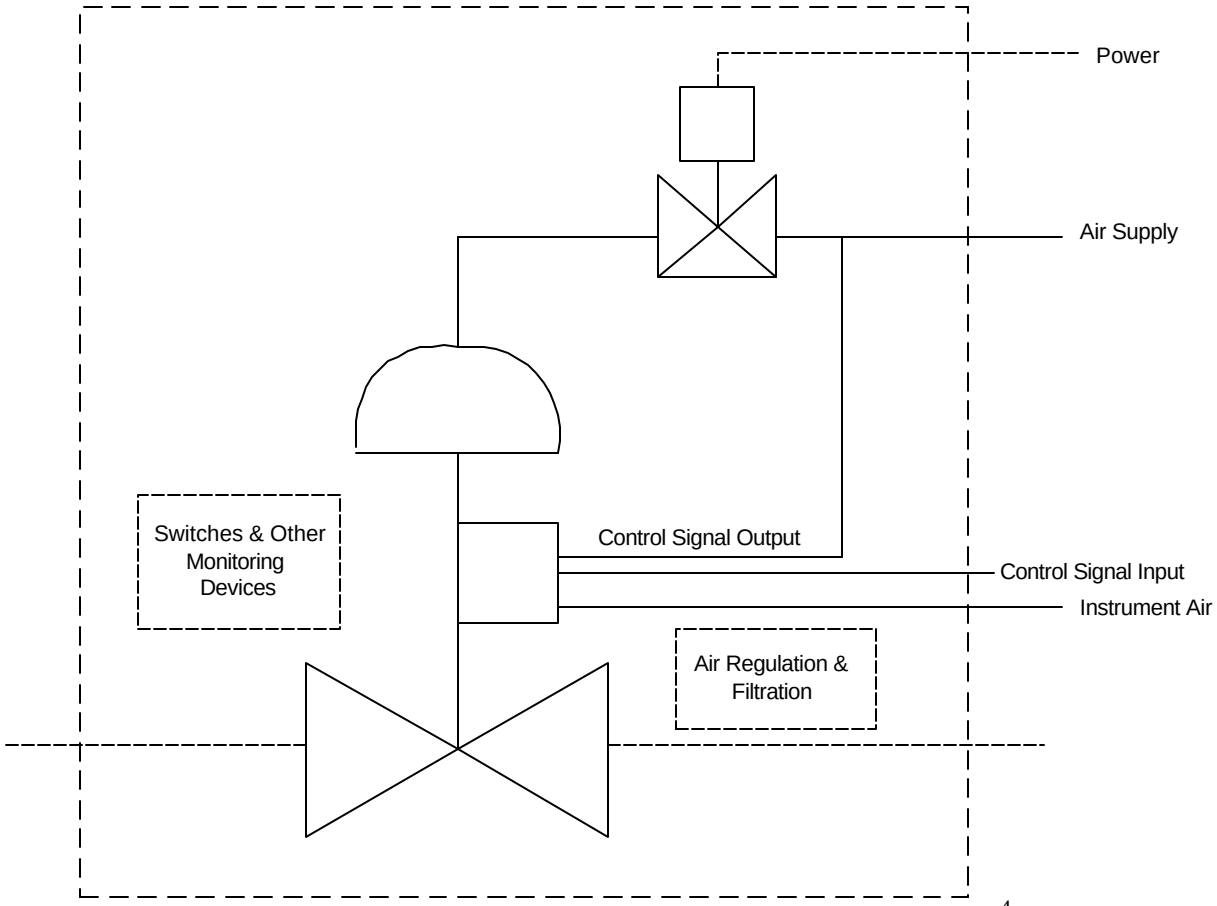
The Specifics – The user needs adequate information to design a safety instrumented system so that its probability of failing to function is less than or equal to some acceptable probability that is a function of varying proof test intervals and required repair times for detected dangerous failures. They also need data to determine the frequency of spurious shutdowns due to the manufacturer's equipment to predict plant reliability. This requires data for failure modes that go beyond the classifications of dangerous and safe as referenced in the industry standards. Table 1 documents the remote actuated valve failure modes as determined by the Center for Chemical Process Safety (CCPS) Process Equipment Reliability Database[3] (PERD) initiative as part of their taxonomy development procedure. The failure modes are applicable to the boundary diagram of a remote actuated valve as depicted in Figure 2.

Table 1
Remote Actuated Valve Failure Mode Table

Failure Modes	Failure Classification
Complete Failures	
Spuriously fail to closed position	Depends on application
Spuriously fail to open position	Depends on application
Fail to close on demand	Dangerous
Fail to open on demand	Dangerous
Frozen Position (Modulating Service)	Dangerous
Valve Rupture	Dangerous
Seal/Packing Blowout	Dangerous
Partial Failures	
Reduced Capacity	Depends on application
Seat leakage	Depends on application
External Leak	Depends on application
External Leak - Body/Bonnet	Depends on application
External Leak - Packing/Seal	Depends on application
Fugitive Emission	
Controlled variable high	Depends on application
Controlled variable low	Depends on application
Fail to hold position	Depends on application
Unstable control (hunting)	Depends on application
Responds too Quickly	Depends on application
Responds too Slowly	Depends on application
Excessive Noise	Depends on application

(Excerpted from CCPS PERD Remote Actuated Valve Draft Taxonomy)[4]

FIGURE 2 – Example Boundary Diagram – Remote Actuated Valve



(Excerpted from CCPS PERD Remote Actuated Valve Draft Taxonomy [4])

After reviewing and reflecting upon the failure modes, one should readily be able to see that the particular application has a significant impact upon whether a particular failure mode will result in a dangerous loss of protection failure or a spurious shutdown. Moreover, this data needs to be trusted and of a high quality. To illustrate these points, let's look at the following examples:

a. Single isolation valve on fuel gas feed to furnace – In this case, both 'Fail to Close' and 'Seat Leakage' would be considered dangerous failure modes. Experience tells us that 'Seat Leakage' occurs much more frequently than a complete failure like 'Fail to Close.' That is why double block and bleed isolation valve arrangements are often employed.

b. Double block and bleed isolation valves on fuel gas feed to furnace – In this installation, 'Seat Leakage' is still a dangerous failure, but fault tolerance has been used to lessen its likelihood of having a significant negative impact. Let's look at the bleed valve however. If it were to 'Fail to Open' during a shutdown, the significance of primary valve 'Seat Leakage' would increase significantly. As such, the failure mode of 'Fail to Open' for the bleed valve would be considered dangerous, while it would not be for the primary isolation valves.

Depending upon the risks being considered, the bleed valve 'Spuriously Opening' during normal operation may or may not be dangerous, depending on the vent system design.

c. Cryogenic liquid isolation valve on feed to vaporizer – In the event that the feed flow through the vaporizer exceeded its capacity, there would be the potential for embrittlement and rupture of warm end downstream piping. Therefore, the failure mode 'Fail to Close,' is clearly a dangerous failure in this case. Assuming the valve closes however, 'Seat Leakage' would not be considered a dangerous failure as the vaporizer would perform its function in an inherently safe manner by significantly reducing the flow.

To complicate matters, data for the various failure modes are not a constant for specific equipment as the multitude of process applications and operating modes have a distinct impact on the performance of field equipment. To address this, the knowledgeable user would expect that when data is supplied, any limitations and the basis be clearly documented. When the equipment is certified, the data and limitations/manufacturer requirements are documented in a mandatory safety manual. Whether the equipment is or is not certified, Table 2 documents the typical information that the knowledgeable user would seek.

From Table 2, it becomes obvious that field equipment is more problematic when it comes to meaningful certification than it does for electronic equipment in controlled environments. Even when field equipment is certified today, it is highly doubtful that the failure rates reported can be used without serious review as to applicability for a specific application. Using certified equipment is still quite valuable for the user because it helps ensure that the manufacturer's quality assurance and management of change processes are sound, a definite plus when seeking to comply with the overall safety lifecycle approach. In addition, some data is better than none, especially when the basis of that data is documented in a manner that can be understood by the user.

Recognizing that there are additional problems when addressing the process wetted portion of field equipment, the standards offer an alternative called "Proven in Use." During the on going development of the ISA technical report, ISA-TR84.00.04, *Guideline on the Implementation of ANSI/ISA 84.00.01-2004 (IEC 61511)*, Proven in Use (PIU) and Certification were addressed. Highlighted below are some key points that I gleaned from the discussions:

"Proven in Use" Key Points

1. Certification alone is not enough to determine adequacy of safety instrumented functions.
    - Certifying agencies make assumptions as to installation, performance of supplied utilities, response to diagnostics, and maintenance performance to perform their review.
    - Certifying agencies do not consider likelihood of human error.
    - Certifying agencies have in the past not considered failures outside the electrical/electronic boundary, i.e. they have in the past ignored process wetted parts.
    - Therefore, as a practical matter, all installed, operated, and maintained, safety instrumented functions and systems are user certified.

Table 2
Safety Manual Expectations

Information Description	Comments
• Failure rates for each failure mode of interest	
• Diagnostic coverage percentage for each failure mode	
• Operating mode that data applies to	i.e. • Continuous Operation • Standby Operation • Cyclical Operation • Batch Operation
• Environmental limits	i.e. range of ambient conditions that the data applies (indoors, outdoors, temperature, humidity, Alaska, Sahara Desert, Gulf Coast, etc.
• Process Limits	i.e. range of process applications that the data applies (process temperatures, pressures, corrosiveness, fluid phases, etc.)
• Configuration **requirements** for programmable software	Limits on configuration freedom so as to ensure stated performance
• Special performance capabilities	i.e. seat tightness, time to close, time to open, etc.
• Documented test procedures to be accomplished during turnarounds for each failure mode that can contribute to dangerous fail to function	See Table 1 for failure modes that are potentially dangerous
• Documented on line test procedures	When applicable
• Expected lifetime of equipment system/key components with applicable environmental, operating mode and process conditions	i.e. beginning of wear out stage of life. This is necessary so that PFDavg calculations based upon exponential distribution are not misused/abused in the determination of mechanical integrity programs.

"Proven in Use" Key Points (Continued)

2. Certification with some level of PIU is necessary for programmable electronic equipment.
    - Complexity of programmable components makes full user certification of component impractical.
    - As the lead time for new and improved programmable equipment is so short, it is impractical to apply the same level of classical proven in use concepts that one would consider for field wetted components.

- PIU for programmable devices would typically consist of 1) Third party certification 2) Benchmarking of equipment in actual operation. This may mean discussions with other users and/or actual beta and pilot testing of equipment by users prior to widespread use.

3. Certification provides marginal value for field wetted devices relative to failure rates.
    - The myriad of process applications and severity make third party certification impractical for the most important aspect of field device failure rates.
    - PIU for field devices comes from appropriate field data and a statistically sound analysis of equipment in similar services. To begin to be statistically sound from a failure frequency perspective, the operating years of experience should be an order of magnitude greater than the anticipated mean time to failure (i.e. for a failure rate of 0.1/year, need 100 operating years). From a probability of failure perspective, the number of demands should be an order of magnitude greater than the reciprocal of the PFD, AND, the operating years experience should not be less than the product of the desired proof test interval and the number of demands. Proof test and process demand event forms developed by one user, designed to be compatible with the CCPS Process Equipment Reliability Database initiative have been provided as examples in figures 7, 8, 9, and 10. Data recorded on forms such as these can supply the needed information for fail to function to support PIU.
4. Certification of components may be independent 3rd party or self-certification by user.
    - It may be inappropriate to use data from existing installations unless it is verified that the installed sample is of the same design as the new device being evaluated. Manufactures may make subtle revisions to design tolerances or materials to which the user is not aware. This illustrates the value of 3rd party certification, even for field devices as it addresses the quality assurance and management of change issues.

Manufacturer Limitations

Now that the user needs and expectations of the manufacturer have been defined, can the manufacturer deliver? For many of the items the answer is yes. Clearly a manufacturer should be able to list the potential failure modes, provide documentation of performance capability across a wide range of ambient and process conditions as well as to provide documented test procedures targeted at specific failure modes. If a manufacturer makes claims about having fault tolerant hardware, they better be able to provide and defend their basis of diagnostic coverage.

Generally this requires the performance of an FMEDA to rigorously consider part failure modes and their effect on the system, i.e. system failure modes. For system failure modes considered dangerous, the question can be asked whether diagnostics exist to detect the failure and take action (alarm or initiation of instrumented protection function), thus allowing recovery from a failure mode that may render the protection useless, or at a minimum, reduce its performance capability when fault tolerant systems are employed. Diagnostic coverage can be thought of somewhat simplistically as the fraction of dangerous failures that are designed to be detected.

The manufacturer will however have a difficult time providing the level of failure rate data truly needed by their customers, as this data is a function of:

- Equipment Service
- Operating Mode
- Maintenance Employed

These are things that the manufacturer does not control. Any information provided by the manufacturer as a result has to be wrapped in a number of caveats.

Meeting the Challenge

To fully achieve the expectations, the knowledgeable user requires a cooperative approach that yields high quality trusted data. The goal would be to have User/Manufacturer Management Information Systems capable of tracking inventory populations that use/address:

- Consistent Terminology
- Equipment Descriptions
- Equipment Service
- Operating Mode

In addition the User/Manufacturer Management Information Systems must also have the capability and work processes in place to record event data in a consistent manner that allows inference of failure modes and quality/type of maintenance.

Co-operative Approach/Opportunities

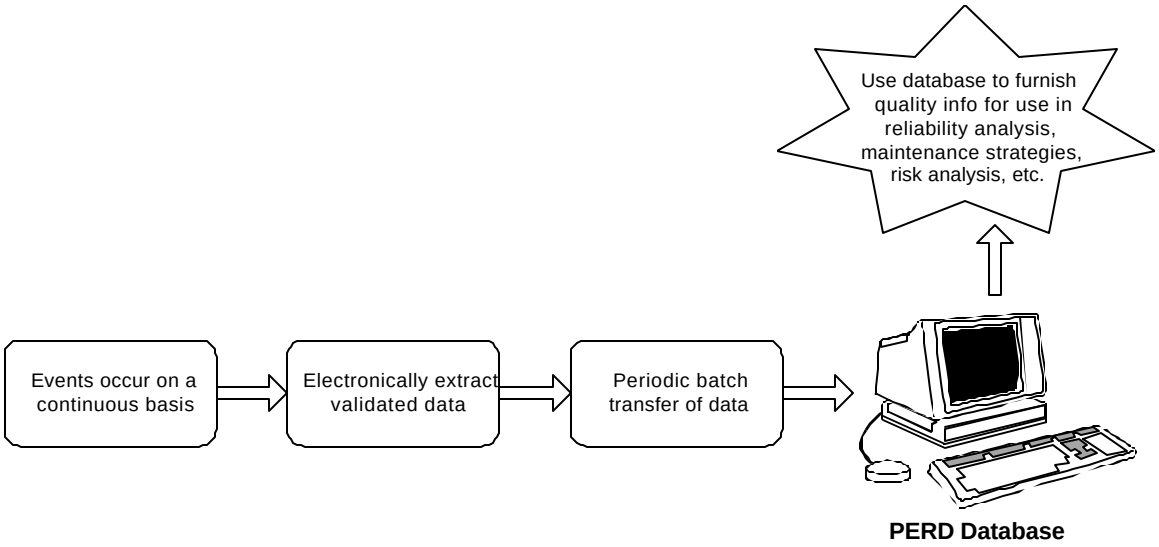
Although the challenge is formidable, the technology exists to make it happen if the stakeholders can find a mechanism to work together for the common good. The Center for Chemical Process Safety (CCPS), part of an AIChE industry technology alliance has accepted that challenge and is leading an effort through its Process Equipment Reliability Database (PERD) initiative[3]. Its stated mission ultimately is to:

> Operate an equipment reliability database making available high quality, valid, and useful data to the HPI and CPI; enabling analyses to support availability, reliability, and equipment design improvements, maintenance strategies, support life cycle cost determinations; and provide better, more credible information for risk analyses.

Multiple companies from the oil, chemical, and industrial gas industries, as well as equipment manufacturers, consultants, and insurance companies, have banded together to achieve this aim. These participants have come together under the aegis of CCPS, a non profit organization dedicated to technical advancement and knowledge. CCPS is providing a forum to facilitate the necessary technical development and sharing of information to achieve the stated mission. This effort has built upon the ground breaking work published as part of prior industry initiatives such as IEEE-500[5], OREDA[7], and ISO standard 14224[6].

The Process Equipment Reliability Database (PERD) initiative seeks to improve the quality and lower the long term cost of data utilization by automating the process to the extent possible. They prefer to think in terms of harvesting data as if operating a data farm[10]. Figure 3 illustrates the concept. Success means that a fundamentally sound quality infrastructure is in place to support reliability analyses, maintenance strategies, risk analyses, and equipment improvement which in turn allows the expectation of continuous improvement and reliability growth[8]. To achieve these goals the PERD initiative has applied a three pronged development plan consisting of equipment taxonomy development, software development, and upgraded infrastructures to facilitate data acquisition that can support determination of reliability/failure rate parameters for equipment failure modes, etc. Success in all of these areas allows recorded data to be aggregated, enabling analysis and ultimately the fulfillment of the mission.

Figure 3
Supporting "Proven in Use"



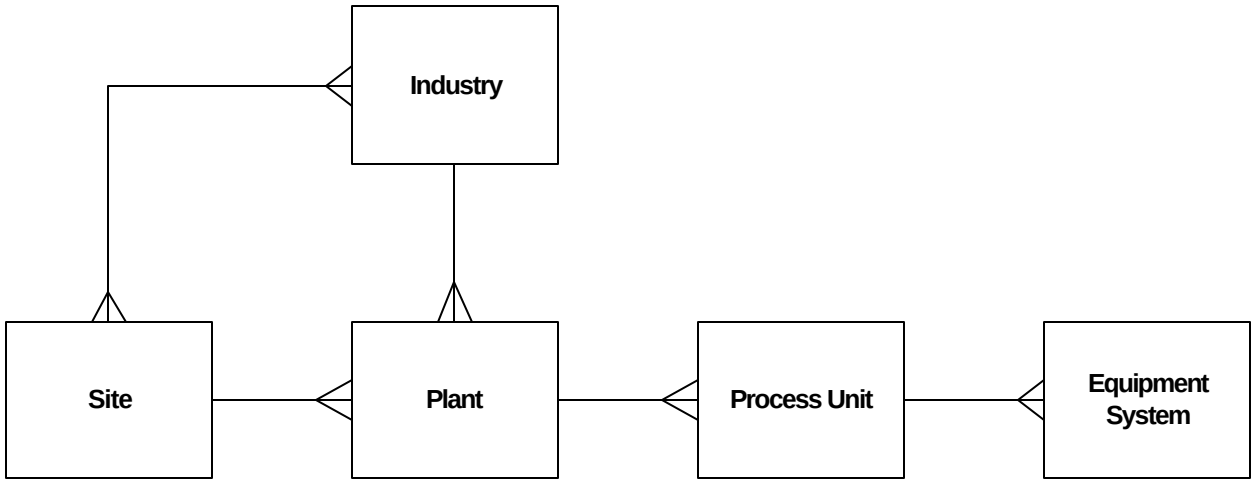
Taxonomy Development – Taxonomies are nothing more than the data relationships that exist within the overall plant/equipment hierarchy. Figure 4 shows the CCPS PERD relationships at a high level and Figure 5 shows the generic relationships for any specific equipment item. To develop taxonomies in a consistent manner requires standard definitions and a methodical development work process so that fundamental technical information is available for software and infrastructure development.

Of particular importance to this work process is the functional analysis as described by Rausand and Oin[9] that takes place as part of the taxonomy development. It is this methodology that rigorously identifies and defines plant and equipment failure modes. Table 1 included failure modes for remote actuated valves using this work process and methodology. In turn, the failure

mode definitions can help determine what data allows the inference of specific failure modes from recorded event data.

Software Development – The intent of the CCPS PERD software is to create and operate an off line database that when populated, allows immediate statistical analysis. It is the wish of CCPS to provide the foundation that allows industry to establish a standard. This is important as it allows the data from different systems to become more compatible, increasing the value of industry data. Benefits accrue from being able to aggregate data without degrading its quality. Using the work documented from the detailed taxonomy development work process, it provides a practical means to define the data inventory and event data fields and formats as well as any mandatory validation of entered data with input field pick lists. As there is one defined home for the data intended for analysis, it allows multiple companies the ability to aggregate data as long as they can map data from any applicable information system that they may have. The aggregation concept is shown in Figure 6.

Figure 4
CCPS PERD Overall Taxonomy Data Structure



Relationship Legend

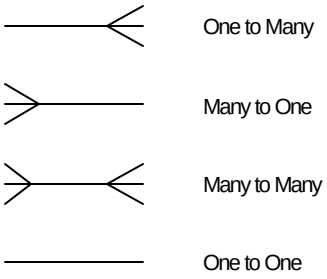


Figure 5
System Level Taxonomy Relationships

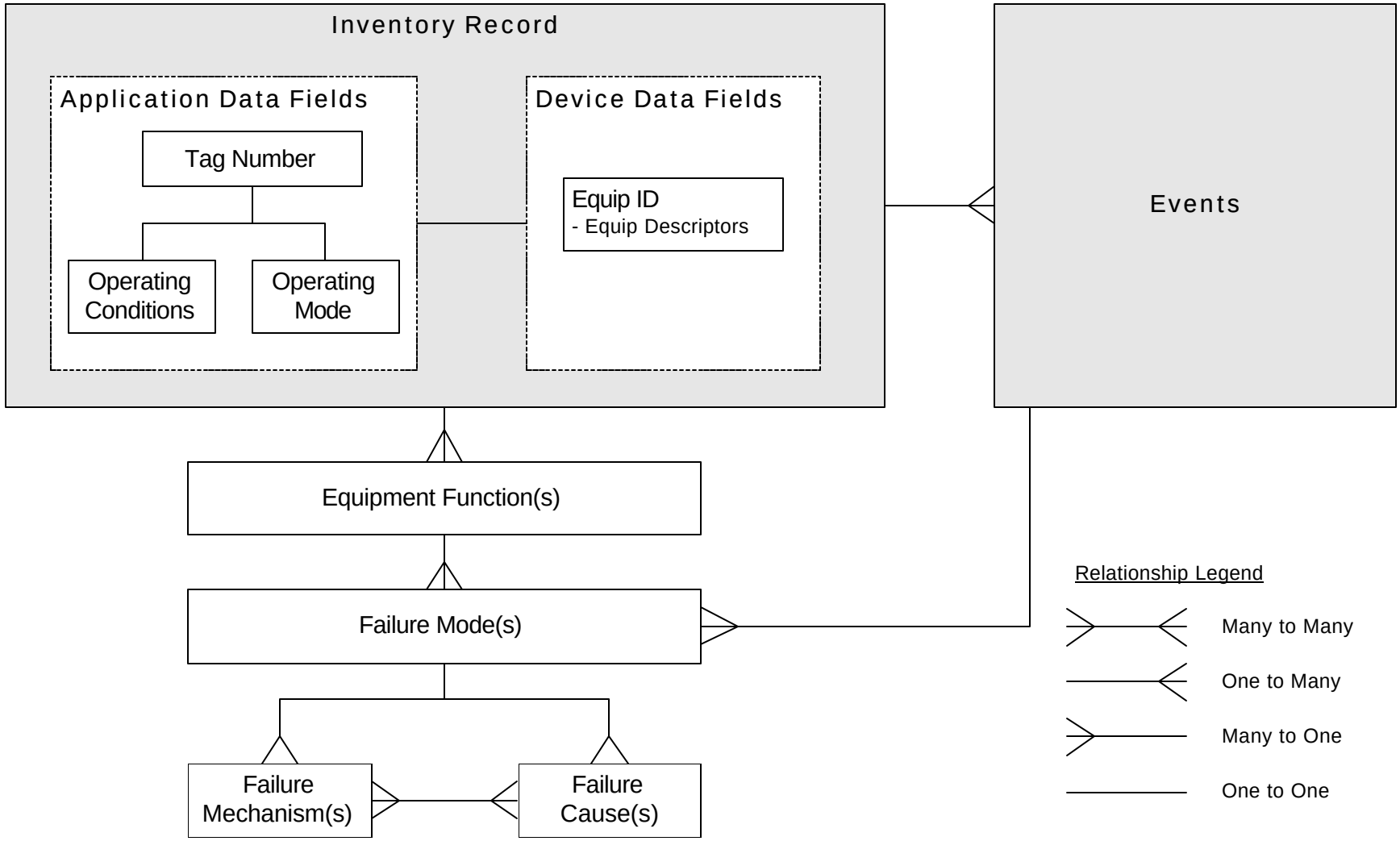
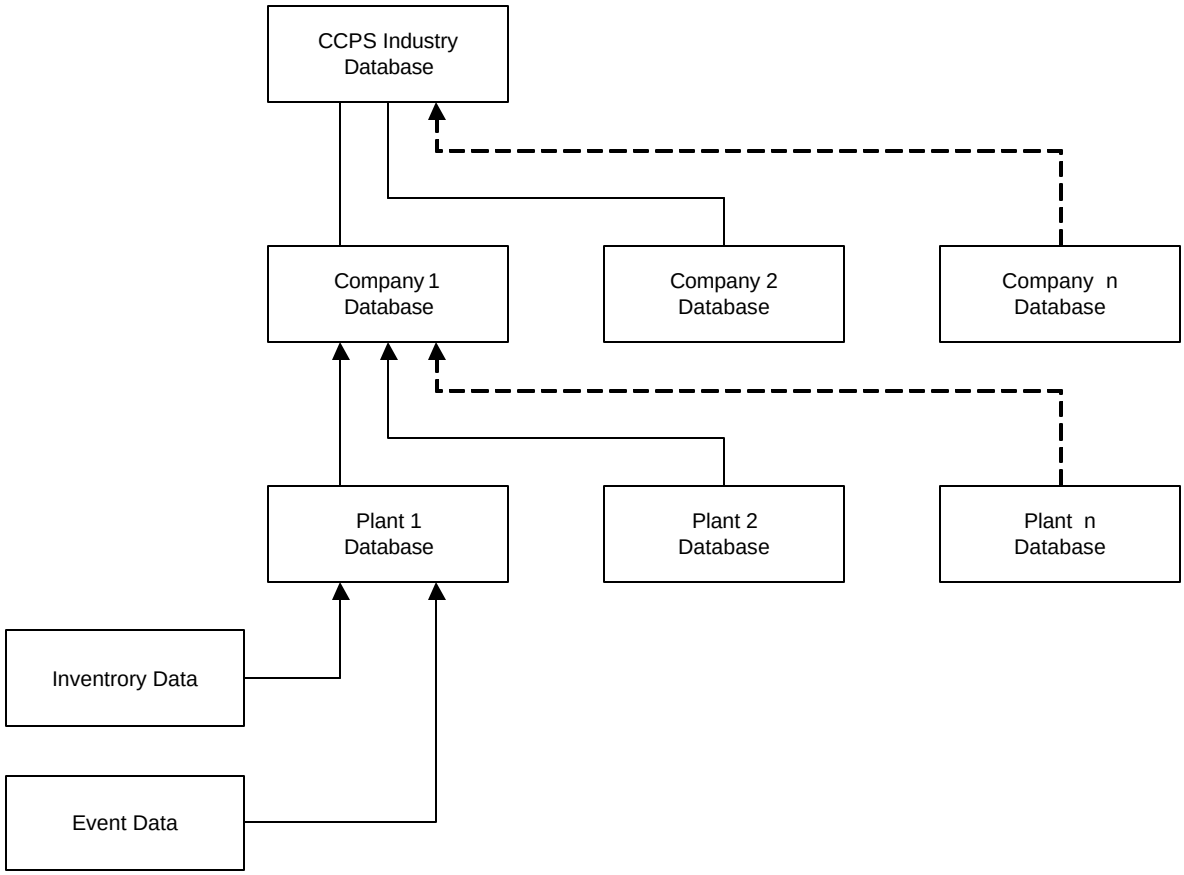


Figure 6
Data Aggregation Concept



Upgraded Infrastructure – The event data input forms created in the software use the equipment taxonomy information including failure mode rule sets documented during the development process. A well documented taxonomy allows these input forms to be 'Engineered' so that only the data necessary to infer failure modes of interest and to perform analysis are included. This has significant ramifications for an individual company's work process. This same thought pattern can be used to document hard copy forms or electronic forms that may be used as part of a company's information system. Figures 7, 8, 9, and 10 show examples of engineered event input forms, with figures 9 and 10 being working drafts from the current remote actuated valve taxonomy development work process. When the development process is complete, the data contained in these forms can be input into the CCPS PERD software allowing inference of numerous failure modes and providing a database capable of supporting "Proven in Use" vis statistical analysis.

Figures 7 and 8 are examples of input forms developed as part of a mechanical integrity program for safety instrumented systems. Figure 7 for field sensors allows the determination of the two failure modes, "output high" and "output low". Figure 8 applies to the total instrumented protection loop or

safety instrumented function. In this case, the recorded information allows the determination of alarm fail to function or interlock fails to function.

Figure 7
Field Sensor Verification Form

Date of test: _____

Calibration performed by: _____

Facility Code Number: _____

Plant Code Number: _____

Loop Sheet/Documentation accurate: (Y/N) _____

PARENT LOOP ID	TAG NUMBER	RELATED TAG NUMBERS	RANGE REQUIRED	% SIGNAL VARIANCE	CALIBRATION REQUIRED?	
					YES*	NO

*In the event that calibration is required, the as found, as left results shall be documented via a calibration form.

In addition, depending upon the cause of failure, additional information could be recorded. For example, suppose the cause of the interlock failing to function was the automated isolation valve. Figure 9 shows a more in depth proof test event input form focused on the valve. This form is a working draft based upon the CCPS PERD taxonomy being developed. In this form, one can determine a number of failure modes such as the valve "failed to close,"/"fail to open," or "spuriously closed"/"spuriously opened." The cause can also be documented in a consistent manner, allowing more in depth analysis.

Data can also be recorded as a result of demands on a protection system during normal operation. Figure 10 shows a fairly simple demand report for a single safety instrumented function, SIF. From this simple form, four distinct failure modes can be inferred; seat leakage, external leakage to atmosphere, SIF failed to function, and SIF spuriously functioned. The data on these forms, if captured electronically, record factual information that are immediately available for analysis with essentially no need for interpretation.

With event input forms being engineered to allow inference of failure modes and to support more rigorous analysis, future reliability growth is enabled. The next challenge is to automate the data collection process to the greatest extent possible. Automaton of data recording is the key to cost effectiveness as well as to improved data validation and consistency. Equipment manufacturers with today's smart technology have the opportunity to leverage this technical foundation and provide at least some of that automation.

A prime example of using this approach would be in the recording of partial stroke test data using a format compatible with the CCPS PERD software. This would allow the data to periodically be electronically batch transferred, aggregated with other data sets and analyzed. Figure 11 shows the concept, including potential data fields and formats. Implementing this concept would allow data to populate the off line database in a continuous batch manner. The fact that the data is factual and engineered to yield valuable information when combined with data from other valve tests, would provide an extremely high quality data set that would grow in statistical significance over time, providing the means to address failure distributions for each failure mode as a function of time. The hypothesized exponential distribution function assumed in certification document reported numbers could be tested as well as the ability to determine some day, the useful life of a valve and its components in specific services.

Figure 8
Proof Test Form (Applicable to Validation and Revalidation)

Date of test: _____

Test performed by: _____

Facility Code Number: _____

Plant Code Number: _____

Safety Instrumented Function (SIF) identification number: _____

Protective System Type (Circle applicable type)

- Alarm
- Shutdown interlock
- Permissive interlock
- Auto-Start interlock

Protective Circuit Description: (Reference applicable interlock table or master alarm summary as appropriate)
_____

Alarm Info

Required Set point: _____ Unit of measure: _____

Initiates on (Circle one)

- Increasing signal
- Decreasing signal

Did alarm function? Yes No (Circle one)

If Yes, functioned at (insert actual number) (insert actual unit of measure)

If No, list loop components that failed: _____

Shutdown interlock Info

Required Set point: _____ Unit of measure: _____

Initiates on (Circle one)

- Increasing signal
- Decreasing signal

Did SD interlock function? Yes No (Circle one)

If Yes, functioned at (insert actual number) (insert actual unit of measure)

If No, list loop components that failed: _____

Permissive interlock Info

Function Correctly? Yes No (Circle one)

If No, list loop components that failed: _____

Auto-start interlock Info

Did system start on first attempt? Yes No (Circle one)

Did system start within defined criteria? Yes No (Circle one)

If either question No, list loop components that failed: _____

Figure 9

Remote Actuated Valve Proof Test Record (Draft)

TAG NO. _____
VALVE SERIAL NO. _____

REQUIRED ACTION WHEN SIF INITIATED Open Close (Circle one)

EVENT DATA
PROOF TEST DATE/TIME: _____

VALVE PERFORMED REQ'D ACTION? Yes No (Circle one if valve tested)

If No, List causes from pick list:
_____

VALVE RESPONSE TIME: _____ seconds (Record Time)

SEAT LEAKAGE? Yes No (Circle one if valve tested)
If Yes, LEAKED AT _____ PSIG

DISPOSITION OF ORIGINAL VALVE FOLLOWING INITIAL INSPECTION/TEST:

Returned to Service Repair/maintain Send to Inventory Scrapped Valve (Circle one)

COMMENTS

NAME: _____ DATE: _____

Figure 10
SIF Valve Demand Report (Draft)

Demand Start Date: _____ Report By: _____
Demand Start Time: _____

Tag Number: _____
Serial Number: _____
Valve Function to: Open Close (Circle one)

DEVICE OPERATION

	(Circle One)	
Type of Demand	Isolation required	
	Additional capacity required	
	Venting required	
	Valve Spuriously Opens	
	Valve Spuriously Closes	

If Type of Demand = Isolation required, circle appropriate valve response

Valve Response	Valve Closed
	Fail to close on demand
	Frozen Position
	Seat leakage

If Type of Demand = Additional capacity required, circle appropriate valve response

Valve Response	Valve Opened
	Fail to open on demand
	Frozen Position
	Controlled variable high
	Controlled variable low

If Type of Demand = Venting required, circle appropriate valve response

Valve Response	Valve Opened
	Fail to open on demand
	Frozen Position
	Reduced Capacity
	Controlled variable high
	Controlled variable low

Protected Equip Damaged? Yes No (Circle one)

Demand End Date: _____
Demand End Time: _____

DISPOSITION OF ORIGINAL VALVE FOLLOWING EVENT:

Returned to Service Repair/maintain Scrapped Valve (Circle one)

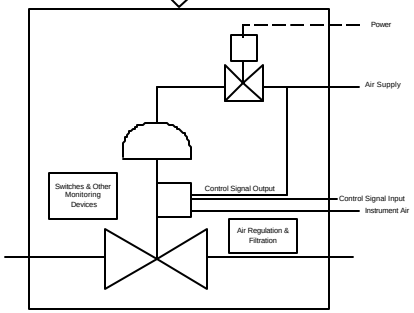
DESCRIPTION OF EVENT/REMARKS (Include on reverse side)

Notes:

1. This report must be completed anytime a safety instrumented function operates or is supposed to operate.
2. If work request is generated, please attach copy of this demand report.

Figure 11
Automated Partial Stroke Test Data Collection Concept

Partial Stroke Test Events Occur on a Periodic Basis



Identification Information

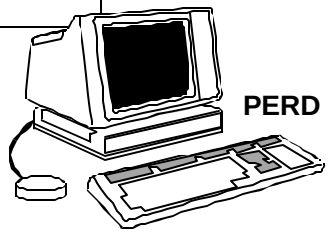
Field Name	Field Format	Value
Site ID	Text	User Configured
Plant ID	Text	User Configured
Unit ID	Text	User Configured
System ID	Text	User Configured
Equipment Tag	Text	User Configured
Applicable Event	Text	Proof Test
Required Percent Travel	Number	User Configured
Max Allowable Response Time (seconds)	Number	User Configured

Potential Partial Stroke Test Data

Field Name	Field Format
Proof Test Date	date
Proof Test Time	time
Stroke Test	
Percent Travel Achieved	Number
Actual Response Time (seconds)	Number
Solenoid Valve Test	
Pressure Vented	Yes/No
Time to Vent (seconds)	Number
Other Data	
Increased Torque	Yes/No
Increased Break Out Torque	Yes/No
Stem Shear?	Yes/No
Broken Springs	Yes/No
Gearbox Problem	Yes/No

Use database to furnish quality info for use in reliability analysis, maintenance strategies, risk analysis, etc.

Periodic batch transfer of data



PERD Database

Conclusion

This paper has looked at what users expect from manufacturers in their efforts to comply with industry standards, but more importantly, what information can reasonably be supplied by equipment manufacturers. The importance of the information that should be contained in a safety manual was shown, as well as the importance of proven in use to process wetted equipment.

A means for users and manufacturers to work together under the aegis of CCPS PERD was presented that would greatly enhance the type of data available for proven in use analyses. Using the technology and concepts being developed under this initiative allows data to be easily aggregated for analysis. Once the process is automated, statistically significant populations of data can rapidly accrue. The essence of what can be achieved is the extension of well designed experiments during initial product development into the field on a continuing basis. This would allow the principles of reliability growth[8] to be extended throughout the life cycle of the product, providing benefits to both users and manufacturers alike.

Literature Cited

1. IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, 1998.
2. ANSI/ISA 84.00.01-2004 (IEC 61511), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*.
3. CCPS *Guidelines for Improving Plant Reliability Through Data Collection and Analysis*, 1998.
4. CCPS PERD Remote Actuated Valve Taxonomy (Draft December 2004).
5. IEEE Std 500-1984, *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and mechanical Equipment Reliability Data for Nuclear-Power Generating Stations*.
6. ISO 14224, International Standard, *Petroleum and natural gas industries – Collection and exchange of reliability and maintenance data for equipment*, First Edition, 1999.
7. OREDA-1992, *Offshore Reliability Data*, DNV Technica, Høvik, Norway, 1992
8. Criscimagna, Ned H. and Zsak, Michael G., *Reliability Growth*, The Journal of the RAC Reliability Analysis Center, Third Quarter 1998, pp. 1-5.
9. Rausand M. & Øien, K., *The basic concepts of failure analysis, In Reliability Engineering and System Safety*, 53 (1996), pp. 73-83.
10. Moosemiller, M. and Thomas, H.W, *Establishing a Data Farm to Harvest Quality Information*, AIChE 2001 Spring National Meeting, April 2001.