Where For Art Thou Failure Rate Data

David C. Arner
Engineering Associate – Process Controls
Air Products and Chemicals, Inc.
7201 Hamilton Blvd
Allentown, PA 18195-1501

William C. Angstadt
Asset Management Group
Rohm & Haas Company
PO Box 584
Bristol, Pa. 19007

KEYWORDS

Loop, CCPS PERD, Failure Rate Data, Equipment Taxonomy

ABTRACT

With the advent of Safety Integrity Levels (SIL) representing the relative reliability of instrumented protection systems in a quasi-quantitative manner, there has been a stirring interest by engineers seeking to understand where quality failure rate data can be obtained. This paper addresses that issue in the context of the Center for Chemical Process Safety (CCPS) initiative regarding operation of an industry Process Equipment Reliability Database (PERD). The work performed to date regarding instrument loops will demonstrate the overall project, the importance of failure mode definitions and what it takes to obtain high quality trusted data that can be turned into useful information.

INTRODUCTION

It seems that today, everyone in industry is asking where failure rate data can be found, as process control engineers seek to design and implement safety instrumented systems, SIS, to satisfy some safety integrity level, SIL. The answers are often the OREDA[5] data book, IEEE-500[4], or the CCPS Guidelines for Process Equipment Reliability Data[1]. Additional reliability data for portions of an SIS may be inferred from third party certifications to a SIL level, if the equipment design is integrated into the overall protective loop and maintained in accordance with the dictates of the certification. Invariably, those answering the question indicate that actual plant data is the best, as it would be more applicable to the specific application of interest, and definitively represent the design, operation and maintenance of the system(s) in question. This response sounds good, but it strikes an ironical note. If the best data exists within plants operated by those asking for the data; it begs the question, why is the data not available?

The Center for Chemical Process Safety (CCPS), an AIChE industry technology alliance, has been attempting to answer that question by facilitating an industry effort whose ultimate goal 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, equipment design improvements, maintenance strategies, support life cycle cost determinations, and provide better, more credible information for risk analyses. While contributing to the advancement of knowledge in this area, participants learn what it takes to accomplish this goal and to utilize the knowledge gained and apply it to their management systems in a manner that adds value and lays the foundation for continued improvement.

Multiple companies from the oil, chemical, and industrial gas industries, as well as consultants, insurance companies, and equipment manufacturers have banded together to achieve this aim. These participants have come together under the aegis of CCPS which is a non profit organization dedicated to technical advancement and knowledge. CCPS is providing a forum to facilitate development and sharing of technical information with respect to an industry process equipment reliability database (PERD)[2].

WHO NEEDS DATA ANYWAY

Failure rate and reliability data is useful for many different analyses. The major focus of this paper will discuss what it takes to validate and measure the performance of instrument loops with respect to SIL levels in a true sense. Other activities requiring the use of credible data include; risk analysis, risk based inspection decisions, reliability analyses, improved equipment selection, and protection system proof test interval optimization.

THE KNOWLEDGE ADVANCEMENT PROCESS

In order to take advantage of plant data effectively, a management information system is needed that has addressed the issues of what data fields must be collected, in addition to what format and structure. Experience has shown that companies have not built fundamentally sound information systems that support the analyses that need to be performed using actual plant data. Accessing plant data is too often a costly exercise, often leaving the analyst guessing as to the relative quality of the data, since interpretation is often required.

CCPS PERD has developed a rigorous taxonomy development work process that can be applied to any type of equipment, which defines the following; the failure modes, inventory data (necessary for analysis of different populations), and event data (necessary to infer specific failure modes). This is accomplished in a consistent format and structure that allows industry to aggregate high quality data in a cost effective manner. Figure 1 shows an overview of the work process.

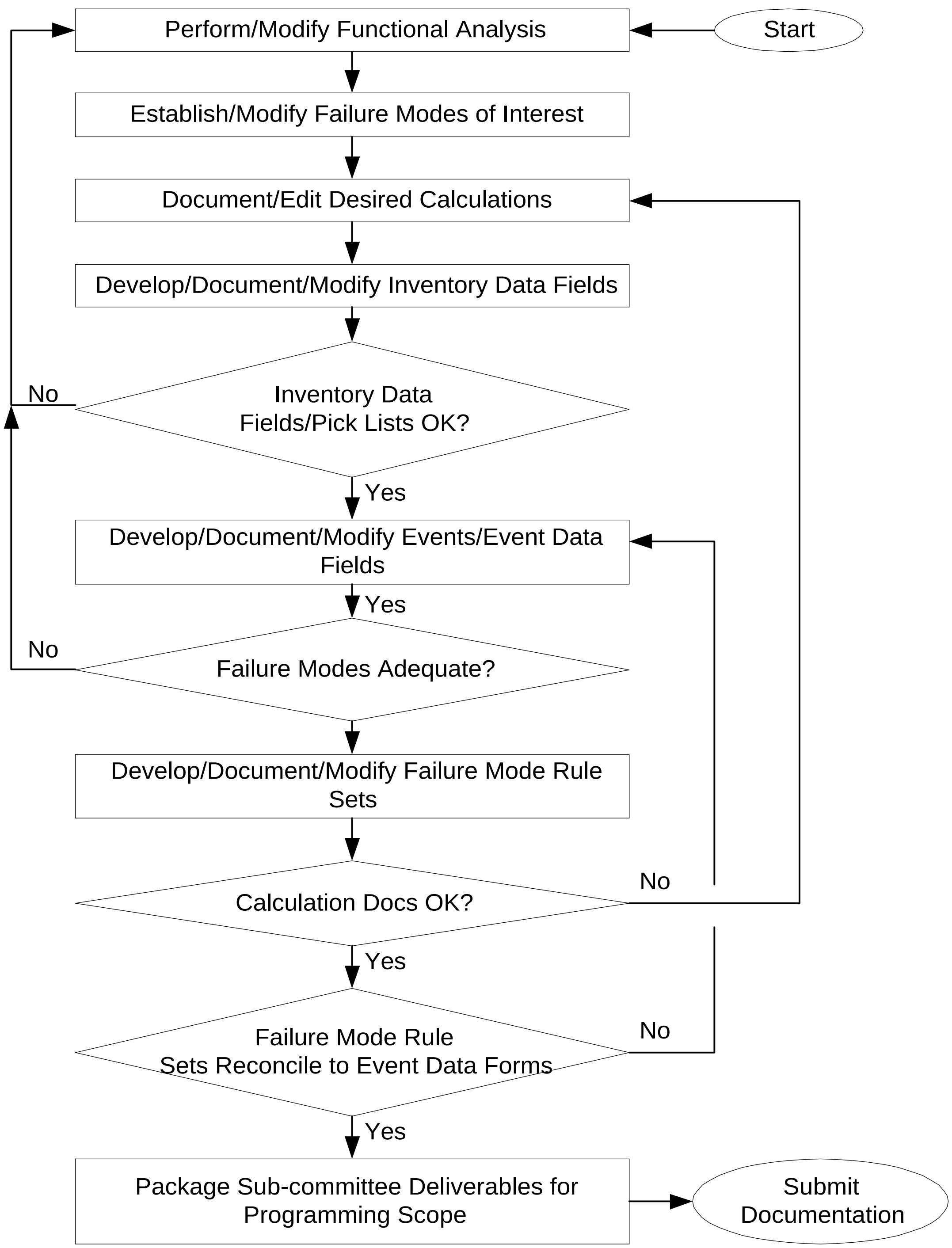

FIGURE 1 – TAXONOMY DEVELOPMENT WORK PROCESS

The taxonomy development work process is at the core of the engineering foundation enabling the development of an industry database. It provides excellent scope documentation in a consistent manner, regardless of equipment type, for the database software programmer. This enables the programmer to add new equipment taxonomies efficiently to the overall software application program. The basic procedure uses a rigorous step-by-step methodology. It provides an understanding of the role of the taxonomy and data field specifications in the database. The procedure takes advantage of basic OREDA[5] concepts and then uses the theoretical thought process expounded by Rausand and Oin[6], into a rigorous and practical methodology for creating equipment taxonomies.

A functional analysis begins the work process. The ultimate purpose of this step is to determine the equipment's finite list of applicable failure modes. Prior to documenting the functions, it is necessary to develop the boundary diagram that explicitly shows what is included and what is excluded from consideration when a failure occurs. Figure 2 shows an example PERD boundary diagram for an instrument loop.

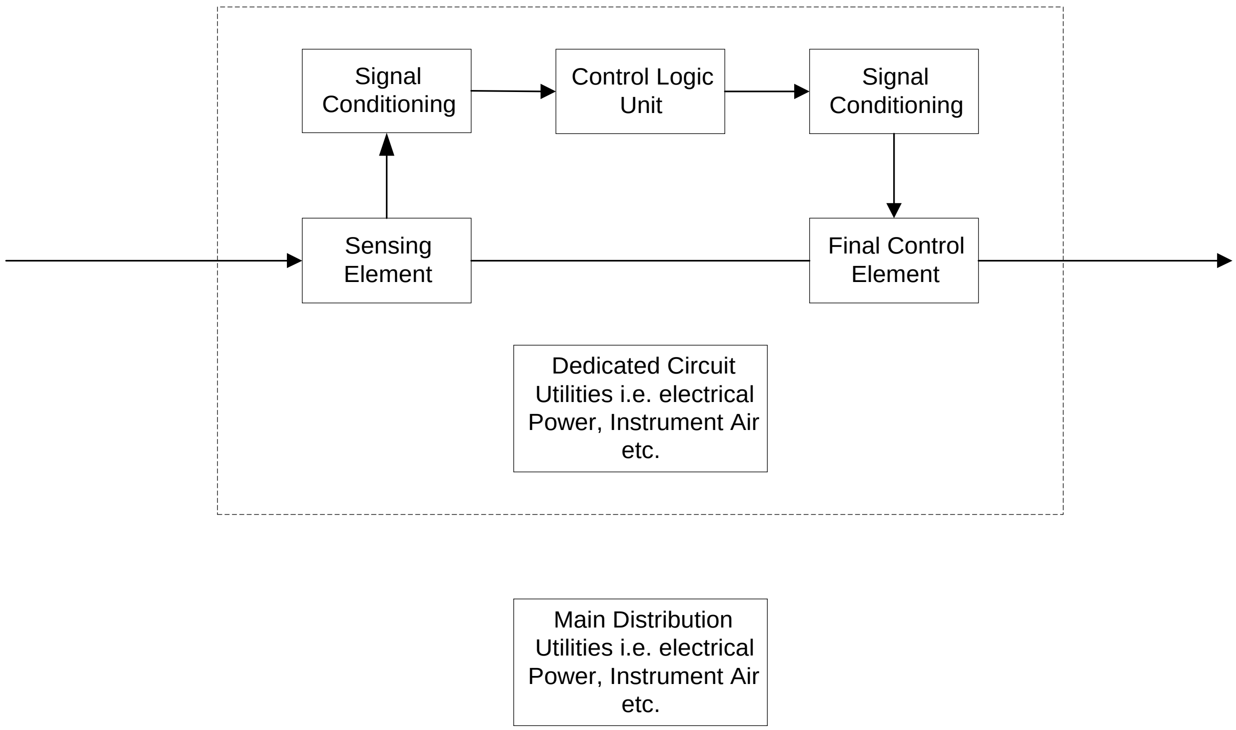

FIGURE 2 – INSTRUMENT LOOP BOUNDARY DIAGRAM

Once the failure modes have been identified, the standard calculations necessary to provide the reliability parameters applying to each failure mode can be documented. Following this, the data inventory fields useful in the analysis of different populations are recorded. Standard industry specifications generally provide the necessary information. To maximize usefulness, field validation rules are established wherever possible. Table 1 represents some of the general inventory data describing loops.

When selecting the type of loop, the choices of primary function are: process control, interlock, indicator, or alarm. Operating modes can be: continuous operation, standby, cyclical operation, or batch. As many systems are multifunctional, secondary loop functions may be specified. For each of the primary functions, additional information may be recorded. Table 2 illustrates a sample of this for interlocks. These tables and associated validation pick list tables provide the documentation a programmer needs to either improve their information management systems or to assist electronic extraction and translation of data from existing systems into a CCPS PERD compatible format.

Field Name	Description/Comments	PickList/Units
Equipment Loop Number (1)	The property or tag number assigned to the system by the subscriber..	
Loop Name		
Systemtype (1)	Represents primary loop function	Final choice of cascading menu
System ID (1)	Same as loop number for instrument loops	
Normal Operating Mode (1)	For the primary loop function	PL_OperatingMode
Secondary Loop Function(s)	Allow selection of all that apply. [Use the choices selected to enable tabs as appropriate]	PL_Loop_Func_2ND Check boxes
Initial Commissioning Date		
Subordinate to other system		Check box
Parent System	Only if subordinate checked yes	

(1) CCPS PERD required data

TABLE 1 – GENERAL LOOP INVENTORY DATA

Interlock Function Input Form **[**Enabled if Primary Loop Function (Systemtype) = Interlock Protection OR Secondary Loop Function = Interlock]

Field Name	Description/Comments	PickList/Units
Variable batch setpoints?		Check box
	MUST ALLOW FOR MULTIPLE ENTRIES OF THE FOLLOWING INFORMATION	
Interlock Name		
Interlock Type		PL_IntlkType
Interlock set point		% of scale
Initiation direction	Radio Buttons	• N/A • Increasing • Decreasing
Interlock Initiation By?	Radio Buttons	• N/A • Deenergize • Energize • Hybrid

TABLE 2 – ADDITIONAL INTERLOCK INVENTORY INFORMATION

The real work comes when developing the event data fields and validation rules that allow the inference of failure modes that have been identified and defined as part of the functional analysis. Examples of some inference rules are shown in Table 3. Figure 3 shows how it is all tied together in a relational structure. The figure shows the basic relationship used for any equipment, and has been annotated to show how it would be used for instrument loops.

Complete Failures	Failure Mode Definition	Input Form	Criteria
Control Output Frozen	1. Final element does not change with change in measured variable (i.e. failure may be due to controller or final element) 2. Control Fails to Respond	Demand - Control Tab	Control Response Successful? = No AND "Control Output Frozen" selected
		Proof Test - Control Tab	Control Response Successful? = No AND "Control Output Frozen" selected
		Maint/Repair	Condition Found = Control Output Frozen
		Auto Control Bypass	Reason for Manual Control = Control Output Frozen
		Tuning	Condition Found = Control Output Frozen
Interlock Spuriously Function	1. Interlock causes actuation of its function without measured variable exceeding its set point OR 2. Startup not allowed to proceed even though safe state exists OR 3. Shutdown occurs even though fault condition does not exists 4. Shutdown occurs even though degraded state within system hardware/software does not exist	Maint/Repair	Condition Found = Interlock Spuriously Function
		Demand - Auto Start Tab	Did process reach/exceed auto start setpoint? Field = No AND Premature Start? = Yes
		Demand - Shutdown Tab	If Process Interlock functioned? Field = Yes AND Did process reach/exceed interlock set point? Field = No, THEN Failure Mode = Interlock Spuriously Function
Partial Failures			
Interlock voting channel fail to function	Individual channel or point unable to accomplish its function if measured variable exceeds set point. Loop as a whole may still be able to accomplish its mission.	Maint/Repair	Condition Found = Interlock voting channel fail to function

TABLE 3 – FAILURE MODE INFERENCE RULE EXCERPTS

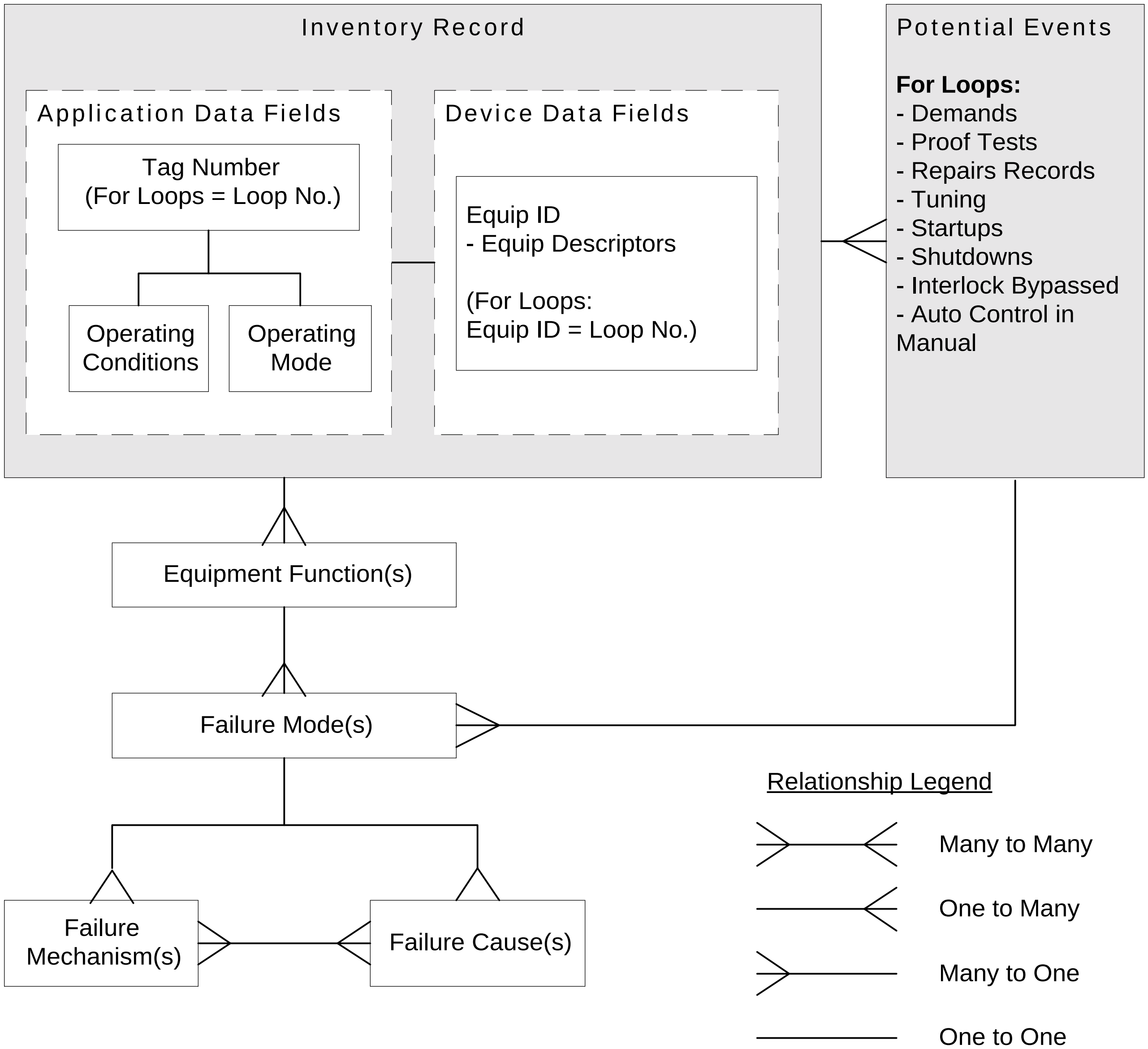

FIGURE 3 - SYSTEM LEVEL TAXONOMY RELATIONSHIPS

TRIPPING OVER FAILURE MODES

Table 4 displays the failure modes that were determined following the functional analysis of instrument loops. Complete failures represent 100% loss of one or more functions, while partial failures represent a degraded or partial loss of one or more functions. The importance of identifying the complete list of fundamental failure modes cannot be understated. Many of the industry standards today are using the terms, fail danger, or fail-safe. These terms are only true when very specific assumptions are made, which apply to a relatively small percentage of total loops within a plant. Whether a failure mode is dangerous or not is generally a function of the process (initiation on increasing or decreasing signal) and its design (on-off versus modulating signal, de-energize versus energize to initiate, etc.). The CCPS PERD work allows for a rigorous accounting of failure modes so that those applicable to a given analysis may be used.

Complete Failures	Partial Failures
• Control Output > 100 % • Control Output Frozen • Control Output < 0 % • Process Variable Indication > 100 % • Process Variable Indication Frozen • Process Variable Indication < 0 % • Control Output Indication > 100 % • Control Output Indication Frozen • Control Output Indication < 0 % • False Discrete Indication • Alarm Fail to Function • Alarm Spuriously Function • Interlock Fail to Function • Interlock Spuriously Function	• Control Output High • Control Output Low • Control Output Slow to Respond • Control Output Too Fast • Control Output Erratic • Auto Controller in Manual Mode • Process Variable Indication High • Process Variable Indication Low • Process Variable Indication Erratic • Control Output Indication High • Control Output Indication Low • Control Output Indication Erratic • Alarm Function Delayed • Interlock Functions Early • Interlock Function Delayed • Interlock voting channel fail to function • Interlock voting channel spuriously functions

TABLE 4 – INSTRUMENT LOOP FAILURE MODES

An example of how this rigorous methodology compares to some of the best references available today can be seen in Table 5, comparing a level transmitter with CCPS PERD failure modes versus two separate editions of OREDA data books. Comparing the failure modes, one can note that some failure modes are not listed in the OREDA tables. As before, the CCPS effort is methodically reducing and eliminating confusion by documenting the outcome of a rigorous approach, that if done in a fundamental way, need only be done once and forever used for the benefit of industry.

OREDA -92 Databook **Level Sensors – Transducer (1)**	**OREDA -97 Databook** **Process Sensor - Level (2)**	**CCPS** **Transmitter - Level (Includes Sensor)**	**CCPS** **Switch - Level (Includes Sensor)**
Critical Failure Modes	**Critical Failure Modes**	**Complete Failure Modes**	**Complete Failure Modes**
	• Fail to Operate on Demand		• Fail to Function on Demand
	• Spurious Operation		• Spuriously Functions
		• Output > 100 %	
• No Change of Output With Change of Input		• Frozen Output	
		• No Output	
• Unknown			
Degraded Failure Modes	**Degraded Failure Modes**	**Degraded Failure Modes**	**Degraded Failure Modes**
		• High Output	• Set Point High
• Low Output		• Low Ouput	• Set Point low
		• Output Slow to Respond	
		• Output Too Fast	
• Erratic Output	• Abnormal Output	• Output Erratic	
• Unknown	• Others		
Incipient	**Incipient**	**Incipient Conditions**	**Incipient Conditions**
• Contaminated • Unknown	• Minor in-service problems		
	Unknown		
	• Unknown		

Table 5 Notes:

1. Taxonomy consists of (OREDA-92 pages 436 &437)

   - Safety Systems
   - Process Alarm Systems
   - Level Sensors
   - Transducers (analog signals out, electric)
   - Application = Level measurement/alarm on process systems
   - Operational mode = Continuous

2. The boundary definition shown in OREDA-97 Figure 15, page 320 comprises the sensing element and the (local) electronics for signal conversion and transmission. The sensing element measures some process parameter (e.g. pressure, level, temperature, flow, etc,) and the electronics connects the measurement to a standard electric signal that is transmitted to a computer. Some sensors may be calibrated by adjusting a screw at the electronic housing. Isolation valves (block valves) and associated pipe work are also included.

TABLE 5 - CCPS VS OREDA FAILURE MODES

CONCLUSION

It can be seen a new day is dawning in the world of failure rate data. A methodical process has been developed to make use of actual plant data from multiple companies. This consistent methodology establishes a foundation of meaningful data that satisfies the needs of many different applications. Participation in this initiative allows companies to achieve immediate financial benefits as information systems can be engineered to performance criteria that adds value.

ACKNOWLEDGEMENTS

The authors would like to acknowledge Hal Thomas, our process safety mentor and PERD Initiative Chairman, Det Norsk Veritas, the PERD phase one contractor and technical consultant, CCPS for its support, and the PERD Instrumentation Subcommittee, consisting of George Bacak, Gary Helman, Dave Arner, Chip Rauth, Hal Thomas and Bill Angstadt, Instrumentation Subcommittee Chairman .

REFERENCES

1. *CCPS Guidelines for Process Equipment Reliability Data*, AICHE, 1989
2. CCPS *Guidelines for Improving Plant Reliability Through Data Collection and Analysis*, 1998.
3. CCPS PERD Instrumentation Sub-committee, *Loop Taxonomy Documentation*, Unpublished.
4. 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*.
5. OREDA-1992, *Offshore Reliability Data*, DNV Technica, Høvik, Norway, 1992
6. Rausand M. & Øien, K., "*The basic concepts of failure analysis, In Reliability Engineering and System Safety*" 53 (1996), pp. 73-83.
7. Weber, Bernard J.; "*Integrating Risk Based Mechanical Integrity and ISA 84.01*", AIChE 35th Annual Loss Prevention Symposium Proceedings, April 2001.

NOMENCLATURE

Failure -	The termination of the ability of an item to perform a required function.
Failure cause -	The circumstances during design, manufacture or use which have led to a failure.
Failure descriptor -	The apparent, observed cause of failure.
Failure mechanism -	The physical, chemical, or other process or combination of processes that has led to a failure.
Taxonomy -	A systematic classification of items into generic groups based on factors possibly common to several of the items, e.g., functional type, medium handled.