



## Safety Symposium

Wednesday 24 May 2006

Marriott Houston Hobby Houston, Texas

- 7:30 AM – 8:15 AM**     **Registration**
- 8:15 AM – 8:30 AM**     **Rodney Jones/Ed Marzsal**  
**WELCOME/OPENING REMARKS**
- 8:30 AM – 9:30 AM**     **Keynote Address – Gary Vischer**  
**Chemical Safety Board Member**  
Gary has served in government service for over 20 years included legislative staff work and as Deputy Assistant Secretary of OSHA.
- 9:30 AM – 10:00 AM**     **Coffee Break/Exhibits**
- 10:00 AM – 11:00 AM**     **Standards Update**  
**ISA S84 Committee – Angela Summers**  
**ISA S18 Committee -**  
**ISA S99 Committee -**
- 11:00 AM – 12:30 PM**     **Exhibits/Lunch**
- 12:30 PM – 2:30 PM**     **Session ONE**  
**Two Technical Tracks**  
**1A-Safety Instrumented Systems**  
**1B-Alarm Management**
- 1A-Safety Instrumented Systems**
- 12:30 PM – 1:00 PM**     **Iwan van Beurden – EXIDA**  
**Integration of Safety Lifecycle and Plc Programming**  
**Abstract**

With the recent adoption of the new international functional safety standard IEC 61511, and the US version, ANSI/ISA 84.00.01-2004, many process plant operations are being challenged with determining if they are in compliance. These new international and national standards have two basic purposes. First,

to define the Safety Lifecycle which is a practical methodology that defines the steps necessary to ensure overall plant safety for process plants. Second, to define how to determine the required level of risk reduction, necessary to reduce plant hazards, and the achieved level of risk reduction of the safety instrumented equipment. These levels of risk reduction are expressed in the Safety Integrity Level (SIL) parameter.

Compliance with the functional safety standards can be challenging, however several tools are available on the market to ease the steps to achieve compliance. One method that can significantly help users comply with many phases of the lifecycle is a methodology known as cause and effects matrix which is also known as a Safe Chart as defined in API 14C. Traditionally this documentation tool was used to provide easy to understand documentation of the safety requirements for a process. However, some suppliers of programmable electronic safety systems have now implemented cause and effect matrices as a language in their programming tools to provide complete automation of this method.

Users who create a conceptual design and subsequently perform reliability calculations to determine the achieved level or risk reduction will want to port this conceptual design into such a cause and effect programming tool to efficiently build their Safety Instrumented System. This article will describe a cause and effect programming tool from Siemens, a reliability calculation tool from exida, and the integration of the reliability calculations into the cause and effect matrix. It will show how the two tools help users comply with the specific sections of IEC 61511 and describes the benefits to the user in terms of engineering and commissioning hours saved. An HIPPS example application will be followed throughout the paper.

**1:00 PM – 1:30 PM    Bart Winters – Honeywell  
A Holistic Approach to Plant Safety**

**Abstract**

The number one and foremost objective of an industrial processing Plant Manager is Safety. This includes the safety of the enterprise's people, the safety of plant assets, the safety of the environment, and of the surrounding community. All other objectives are secondary and contingent upon safety. For example, the least productive plant is one that is shutdown or out of commission due to a safety incident.

From the perspective of the Plant Manager the ever vigilant intent is to mitigate the risk of serious incidents that can cause injury to personnel and the environment. Thus the questions they must ask themselves are “Are we safe enough?”, and; “are we employing all of the tools at our disposal to reduce risk and improve safety?”.

Risk reduction is contingent on a strategy of independent yet interrelated Layers of Protection (LOP). One commonly employed LOP is the use of a fail-safe Safety Instrumented System (SIS) – but plant safety is more than just the SIS and the control and automation equipment (e.g. logic solver) deployed to implement it. Plant safety today also includes Layers of Protection such as operator training, advanced alarm management, constant monitoring of distress indicators, operational effectiveness, personnel tracking, ongoing asset monitoring and maintenance, and plant security (physical and cyber security).

*If it's not Secure, it's not Safe.*

From our perspective, safety means reducing risk— reducing the risk of incidents, and faults, and failures that cost money. This goes far beyond simply installing fail-safe controllers or a safety instrumented system. In fact, to mitigate the risk of serious incidents that can cause injury to personnel and the environment, it is important to consider safety from all aspects of a plant's operation. This goes right to the heart of the question that the plant managers of the world must ask themselves every day: - “Are we safe enough?”

**1:30 PM – 2:00 PM Yasuhiko Yamashiro-Yokogawa  
New VMR Architecture of Safety System and Markov Model**

**Abstract**

The conventional architectures of various safety systems have a common problem of “degrade mode” or “clipped mode” when a failure occurs in the system. In the “Degrade mode”, safety performance is “degraded” until repair is completed. Therefore, “degrade mode” is defined as “a safety system is still running but vulnerable to next failure”. In conventional safety systems, this mode is usually found as a system status of “loosing one leg from the input module through CPU module to output module”. The vendors of such systems are claiming the original safety integrity of their safety system is still available within some period even in “degrade mode” from a safety point of view. However, one leg fault means the loss of system availability for all safety functions. Consequently, users must be aware of the behavior and limitation of this mode to each system and prepare how and by when they must take action to repair the system for keeping their process safety and process availability. A new VMR, Versatile Modular Redundancy architecture is introduced in the latest technology for SIL3 safety system. This VMR architecture based on field-proven redundant technology does not belong to any conventional architecture which is called TMR, QMR or 1oo2D. The VMR has been developed for allowing users to make a free choice of appropriate system availability while securing SIL3 safety level.

VMR system offers a flexible choice of redundancy by module level so that users can select single/dual redundancy for any of Input module, CPU module and Output module, independent from other modules. Users can also select single input/output module next to the redundant input/output module even in a same rack. In any cases, the system is SIL3 because this VMR system is SIL3 certified in a single system, and the redundant configuration is purely for system availability. VMR system does not have any “degrade mode” when a failure occurs in a redundant system. It assures that even a failure occurs, VMR system continues to run in SIL3 without any action taken by users from the safety point of view. However, repair must be made in terms of system availability.

The behavior on how VMR system can survive in SIL3 even with multiple failures is explained with some examples. VMR architecture is also analyzed by the technique of Markov for modeling from normal state to fail-safe/fail-danger states. The Markov model at start is very confusing, but it can be cleared up to a very simple model. The process of simplifying the Markov model brings clarity to understand the VMR architecture.

**2:00 PM – 2:30 PM Mike Scott – AE Solutions**  
**Case Study: Safety Instrumented Burner Management System (SI-BMS)**

**Abstract**

This case study will discuss the application of the Safety Lifecycle as defined by ANSI / ISA 84.00.01-2004 (IEC 61511 mod) to two (2) single burner multiple fuel boilers. Each boiler is capable of firing natural gas, oil and / or waste gas in order to supply the plant header with 1365 psig steam at a maximum capacity of 310,000 lb/hr. The project team included the end client task force at the manufacturing facility, the engineering firm with design / build responsibility, the boiler OEM, the Burner / Gas Train OEM, and the safety instrumented system consultant. This paper will include the following:

- How compliance with the Safety Lifecycle was achieved
- Project cost savings realized attributed to following the Safety Lifecycle
- Challenges encountered during the design process associated with implementation of the Safety Lifecycle with the diverse project team
- Lessons Learned

**2A-Alarm Management**

**12:30 PM – 1:00 PM John Huot – Conoco-Phillips**  
**Managing the Process, Not the Alarms At ConocoPhillips**

**Abstract**

ConocoPhillips Borger, Texas has an initiative to better manage the process. One way to execute this initiative is to reduce the number of alarms. ConocoPhillips went through the process of Alarm Rationalization and after a few years realized that Alarm Rationalization is a continuous process. ConocoPhillips determined that tools required for continuous assessment and analysis were necessary. ConocoPhillips has used Matrikon's Technology Solution to help manage and put in place a Management of Change (MOC) process for managing alarms. The key to managing the process and not the alarms is "Alarm Management".

**1:00 PM – 1:30 PM Bill Hollifield -PAS**  
**A New Method for Alarm Rationalization**

**Abstract**

Alarm Documentation and Rationalization (D&R) is a powerful, logical, best-practice alarm improvement method that achieves high quality results. However, it is also an expensive and disruptive process, in industries that have downsized and do not have people readily available to implement all of the best practices that exist. As a result, too many systems needing a D&R never get one, much like a grown man's excuse to avoid a certain medical

procedure...

PAS recognized the challenges around Alarm Rationalization and has come up with a much more economical alternative. This paper presents a new method called Focused D&R, developed from the analysis of terabytes of real-world industrial alarm system data. The paper highlights important and unexpected findings and presents a new methodology – one that takes out over 50% of the cost of a typical D&R effort, without sacrificing quality of results or operational safety.

**1:30 PM – 2:00 PM Mike Stafford- Shawnee Engineers/Process Safety Center  
TAMU  
Set Alarm Priorities Apriori during Project Design Using  
Hazop**

**Abstract**

Most alarm rationalization studies are based upon review of process operational history long after the initial design team has moved on. When the alarm rationalization procedure is addressed is important, since the earlier the rules of alarming are specified, the more likely the rules are to be obeyed.

At the project front end engineering design (FEED) stage, engineering of alarms is typically carried out at the vendor level, in a wholesale way, without individual alarm signal evaluation. In the case of a recent FEED project for a refinery, an emphasis was put on apriori alarm management (by the client) that has led to new engineering alarm management procedures, and ensures that alarm management becomes a defined deliverable and then becomes an important document for the whole life cycle of the project, then later during plant operations.

The overall concept was to use the results of the HAZOP study to assign alarm priorities plus document the rationale for the assignment (classifications) for all alarms. This was intended to reflect the EEMUA guidelines, so that the number of the highest priority alarms was not overwhelming, and that alarms have been handled and engineered in a consistent way.

This paper details how the HAZOP study was used to obtain the initial alarm rationalization.

**2:00 PM – 2:30 PM Alan Armour-Gladstone Power  
Managing the Alarm Manager-a Case History**

**Abstract**

At Gladstone Power Station, alarm management began when the station started up in 1976, and is recognised by management as an important part of operating a large plant. The plant started with a computer based Data Acquisition System which generated most of the alarms, supported by Annunciator panels (light boxes). In 1994, the analog control system was replaced with a Foxboro I/A DCS .As is usual with implementation of a DCS, alarm traffic became a major

issue. The presentation tells how we reduced the alarm traffic from 2500 alarms per day per boiler turbine unit to an average of 25 alarms per day per unit. The company has attributed annual savings of about \$2.4m to effective alarm management.

**2:30 PM – 3:15 PM      Coffee Break/Exhibits**

**3:15 PM – 5:00 PM      Session TWO**  
**Two Technical Tracks**  
**2A-Pressure Relief and HIPS**  
**2B-Control System Security**

## **2A-Pressure Relief and HIPS**

**3:15 PM – 3:45 PM      Angela Summers – SIS-Tech**  
**HIPS-the good, the bad and the ugly**

### **Abstract**

High integrity protective systems (HIPS) are safety instrumented systems that are installed when overpressure cannot be mitigated using a pressure relief valve:

- Flare system is not sized for full worst case loading
- Inlet of the pressure relief valve can be partially or completely plugged by the deposition.
- Reactive processes where pressure can be generated at such a rate that a pressure relief valve is ineffective.
- Reactive processes where temperature can be generated that is sufficient to cause vessel failure at a lower pressure.

HIPS are not systems installed to prevent secondary consequence events, such as excessive flaring, overwhelming air treatment systems, or unacceptable atmospheric releases. These are simply safety instrumented systems (SIS) and should not be designated as HIPS. This distinction should be given only to those systems installed to mitigate vessel rupture.

HIPS definitely have a place within the process industry. However, their use requires careful consideration of many factors. This paper will discuss the importance of the HIPS design case, the process safety time, the potential for propagating hazards, the required process reliability, and the increased operation and maintenance cost.

**3:45 PM – 4:15 PM      HC Steinz - Yokogawa**  
**The Total Solution for a HIPPS requirement**

## **Abstract**

Following items will be briefly presented to convince the user that the total solution is the best solution for a HIPPS requirement.

- HIPPS, a loop requirement
- Manifolds
- Transmitters
- Logic Solver
- Solenoids
- ESD Valves
- Partial stroke testing
- Communication and sequence of event registration

Of course it is obvious that solving the HIPPS requirement is now a matter of observing the total loop from process variable to process actuators. It is, since a long time now, not a matter anymore of individual components or suppliers. Solving the HIPPS requirements calls for a one supplier, that is one responsibility, with one approach, covering the overall requirements.

Special attention has to be paid on the specifications and functionality of the manifolds to use. Starting with measures against clogging such as size of the process connection, mounting instructions and temperature monitoring and heating, to double block and bleed on (most of the time) three transmitters with mechanical interlocking on the transmitter selection.

Transmitters have to be reliable and without calibration for a long period. They also have to be able to withstand high pressure and hostile process conditions.

Minimum requirement for the safety level of the HIPPS is often SIL 3. This implies that, with the figures known for especially the actuator side of the HIPPS, a logic solver that will take less than 10% of the total Pfd seems to be appropriate. This actually means a SIL 4 certified system. And since HIPPS solutions tend to be out in the open, as close as possible to the source (the well, even subsea) power consumption and environmental specifications are important parameters when choosing a logic solver.

Solenoids and especially the valves are dictated by the safety requirement and the process safety time. Most of the times a large valve is needed with a very fast closing time. Furthermore a single component will not satisfy the safety requirements and there will be a need for configurations in series and parallel for safety but also for availability.

Partial stroke testing is a topic of high interest. Is there a need for partial stroke testing or do we need 'full' stroke testing. Or does partial stroke testing add nothing to the safety performance of the total loop. Is it possible to test fast moving valves and if yes how is this done.

HIPPS solutions are always part of total instrumentation jobs. Need for communication, especially information to the operator is essential in modern plant control. The total HIPPS solution will have to support this need. Sequence of event registration at the source, that is within the HIPPS logic solver, is one way to determine whether the HIPPS operated as intended and might take away the need for special testing.

**4:15 PM – 4:45 PM Ed Marszal - KENEXIS**  
**Reconsidering the Need for Overpressure Protection via I&C  
in the Petroleum Refining Industry**

**Abstract**

As petroleum refineries aggressively plan for future expansion, the capability of existing pressure relief systems to safely dispose of higher capacities is often a significant constraint. Current codes and standards now allow for the use of instrumented pressure protection in lieu of increasing the capacity of emergency relief systems. There is a significant body of knowledge on how to design a High Integrity Pressure Protection System (HIPPS) once the requirement for one has been established; but there remains a lack of clear understanding of when a HIPPS should be required, and confusion about the controlling requirements within codes & standards that affect not only the design of the instrumentation / control system, but also the pressure relief system, and mechanical pressure vessel design. This paper presents practical guidance learned through the author's experience with HIPPS analysis, and how industry is reconsidering the need for additional overpressure protection in light of recent incidents. The paper illustrates an example of HIPPS application in an integrated petroleum refinery.

**2B-Control System Security**

**3:15 PM – 3:45 PM Dennis Holstein – OPUS Publishing**  
**Wi-Fi Protected access for Protection & Automation**

**Abstract**

CIGRE Study Committee B5 commissioned a study to explore the current use of Wi-Fi (Wireless Fidelity) technology and schemes in high voltage electric transmission protection and automation systems. The scope is limited to protected access applications such as retrieving settings, and does not address the execution of underlying protection and automation functions.

If Wi-Fi can be secured, the economic advantages for operations are significant. For example:

- Technical support to diagnose a problem and take corrective action can be available anytime from anywhere when a trouble call is received.
- A field technician can access the remote site local area network and maintenance ports of intelligent electronic devices without the need or authority to enter the substation fence or house.
- A field technician can access locations that are physically difficult to reach or isolated because of inclement weather.

Wi-Fi is the industry standard for IEEE 802.11 compliant products and we know that Wired Equivalent Privacy (WEP) and Wireless Protected Access (WPA) systems are not secure. IEEE 802.11i defines how Wi-Fi systems work

and it defines a new type of wireless network called a Robust Security Network (RSN) and Transitional Security Network (TSN) – RSN and WEP systems can operate in parallel. WPA and RSN share a common architecture and approach. This paper summarizes the work-in-progress of CIGRE B5.22 by describing both the survey of applications using Wi-Fi in protection and automation schemes, and the mitigation of security vulnerabilities offered by IEEE 802.11i on system reliability and performance. Design requirements and security levels needed for Wi-Fi protected access are prioritized in terms of their mitigation of risk related to critical mission protection and automation functions. Specific mechanisms needed to adequately implement Wi-Fi are identified and relate to existing or emerging standards.

It is our belief that Wi-Fi, as defined by IEEE 802.11i, is the underlying technology needed for the business case to ensure with high confidence that access is adequately protected, and for this reason its deployment is justified.

**3:45 PM – 4:15 PM Jon Stitzel – Burns & McDonnell  
Applying Traditional IT Security Principles to Control  
System Environments**

**Abstract**

As control systems migrate toward open networking protocols such as TCP/IP, they are inheriting a multitude of risks that must be accounted for and countered. Network-based risks such as Internet worms, malicious insiders, corporate espionage, and the more recent focus on technological terrorism are an ongoing challenge of traditional IT security; however, these threats may be less well-known in control system environments.

Implementing the same type of network security in control system environments provides a unique and wide-ranging set of challenges. Traditional IT security supports applying every system patch to ward off known threats, but production control systems typically do not have that luxury. Individual authentication is an IT security standard, but a production control system cannot simply be logged off every time an operator walks away. While these and other challenges do exist, with diligent planning, coordination, and cooperation, IT security can be a welcome addition to control system environments.

**4:15 PM – 4:45 PM *Not Confirmed***

**4:45 PM – 5:00 PM Closing Remarks**