APPLYING SIS STANDARDS TO COKER PROCESSES

Unique Coke Drum Switching Hazards Are Addressed By ISA 84.01/Iec 61511 Standard

Bryan Zachary, Director, Product & Application Engineering, SIS-TECH Solutions, LP

Presented at the:
10th Annual Universal Delayed Coking Seminar, www.cokingcokers.com, Long Beach, CA, August 1-3, 2005
IV Congresso Rio Automacao, Centro de Convencoes – FIRJAN, Rio de Janeiro, Brazil, May 9-10, 2007

According to a United States Occupational Safety & Health Administration (US OSHA) chemical safety alert, *Hazards of Delayed Coker Unit (DCU) Operations*, "The batch portion of DCU drum switching and coke cutting operations creates unique hazards, resulting in relatively frequent and serious accidents." The report goes on to explain the need to understand the hazards, which are listed as Coke drum switching, Coke drum head removal, and Coke cutting (hydroblasting operations).

On the *Delayed Coker & Communications* (www.Coking.com) website, users and suppliers post questions and answers, as well as contribute articles and suggest ways to improve DCU operation and safety. One topic that has received significant discussion concerns the pros and cons of installing limit switches on valve actuators. The limit switches are used in an interlock matrix to prevent operators and/or automated sequences from inadvertently opening an in-service drum, thereby releasing hydrocarbons to the atmosphere and/or allowing hydrocarbons to enter an open drum.

Experienced users often reply on www.coking.com that reliability is a difficult problem to overcome when adding limit switches to existing valve actuators. Several replies even went so far as to suggest foregoing the attempt to install external limit switches and simply replace existing valve actuators with ones providing integral limit switches – a very costly solution.

An alternative solution was developed by SIS-TECH Solutions (Houston, TX, USA) working in cooperation with three international companies. This solution relied on the installation of multiple independent protection layers (IPLs) including a safety instrumented system (SIS) to ensure safe DCU operation.

Impact of International Standards

Years of process operation provide valuable insight into probable hazards and risk associated with DCU operation. Historically, owner/operators have implemented prescriptive risk reduction strategies based on experience and good engineering practice. Risk criteria were not used to define the risk reduction requirements. Instead, internal practices detailed the required architecture, including redundancy, voting, diagnostics, and installation details, and prescribed a maximum proof test interval.

As early as 1993, the Center for Chemical Process Safety (AIChE/CCPS) published Guidelines for Safe Automation of Chemical Processes, which addressed the importance of designing safety systems to meet performance expectations established by a hazard and risk analysis. It also introduced the concept of safety integrity level (SIL) to benchmark performance of safety instrumented systems (SIS), implemented to reduce the risk of hazardous events resulting in catastrophic consequences.

SISs are covered by the international standard, IEC 61511, which has been adopted in many countries, including the United States, where it is known as ANSI/ISA 84.00.01-2004 (IEC 61511 mod). ISA 84.01/IEC 61511 uses the SIL concept established by Safe Automation as a platform for various requirements affecting all aspects of the SIS lifecycle. ISA TR84.00.04, Guidelines on the implementation of ANSI/ISA 84.00.01-2004 (IEC 61511 mod), provides guidance related to specific topics and requirements of ISA 84.01/IEC 61511.

While performance-oriented standards provide flexibility in SIS design and management, they do not eliminate the need for internal practices. A new CCPS book, Guidelines for Safe and Reliable Instrumented Protective Systems (IPSs), discusses this issue and offers work processes to support the development and continuous improvement of owner/operator practices. The IPS lifecycle (Figure 1) addresses the instrumentation and controls responsible for preventing process safety incidents, such as SIS. Prescriptive internal practices ensure consistency in the SIS design and implementation across a process facility and allow standard solutions to be developed using the ISA 84.01/IEC 61511 lifecycle.

Figure 1. Risk Assessment and the IPS Lifecycle

Understanding the Problem

Over the course of a year, hazard and risk analyses were performed at three international companies, each with more than 10 refining sites per company. The hazard and risk analysis teams included Coker process and operations experts. Each DCU involves at least two coke drums, whose operation is controlled by a field operator who manually lines-up the coke drum. Each drum has a set of valves with little to distinguish between one valve set and another. Valve line-up places the operator within close proximity of the coke drums and potentially within harm's way should release occur.

Human factors analysis had previously been applied at the worksite, resulting in improved equipment labeling, color coding, and high visible signage. Operator procedures and training emphasize the importance of correct line-up and the hazards associated with deviating from the approved procedure. However, even with labeling, the frequency of the line-up activity is so high that it is likely that incorrect line-up will occur. Failure to open or close the valves in the correct sequence can result in the release of hot

hydrocarbons as well as H2S. In fact, improper line-up of coke drums has led to serious safety incidents, including fatalities, within the refinery industry.

To reduce valve line-up error, most companies use a verification step in the line-up procedure where the board operator confirms the valve indication at critical points during the switching operation and gives verbal approval for the field operator to proceed. At some sites, the board operator is required to initiate a permissive at critical points during the switching operation to allow operation of the valve by the field operator.

The team was given the task of evaluating the hazards associated with coke drum switching and to determine whether the existing safeguards were sufficient. Following a seven step process (Figure 2), the team identified events that result in the release of hydrocarbons and H2S from an in-service or open drum during drum switching and de-heading. The release presented a significant personnel exposure hazard and the hydrocarbons presented a fire hazard.

Figure 2
Evaluation process

1. Hazard identification
2. Initiating event identification
3. Initiating event frequency estimation
4. Consequence severity evaluation
5. Risk gap analysis
6. IPL identification
7. Risk reduction allocation

The following initiating events were identified for each operating mode:

Operating Mode	Initiating Events
In-Service	• Vent valve opening • Blowdown valve opening (system not rated for high temp >800F) • Drain valve opening • Top head opening • Bottom head opening
Open drum	• Overhead to Fractionator valve opening • Inlet feed valve opening

Since the valve line-up is manually executed, the initiating cause is operator error; either operating the wrong valve on the right drum or operating the right valve on the wrong drum. The valve line-up is made more complex by the implementation of multiple drum sets. Improvements in DCU operation have shortened DCU cycle times increasing the likelihood for error. The initiating event frequency was estimated based on team experience.

Operator error was assumed to be 1 in 10 years under the following conditions:

- Unique labeling is used on each coke drum and its associated valves;
- Operators are trained and tested prior to being assigned responsibility;
- Operator action is considered a normal part of the operator's duties.
- Operator actions are periodically audited to determine whether procedures are being followed; and
- Operators are provided easy access to job aids (procedures).

The consequence severity of the identified hazards was assessed. The team determined that the release of hot hydrocarbon and H2S could result in possible fire with personnel exposure and potentially a fatality. A tolerable event frequency of 1/10,000 years was used for a single fatality event. With an initiating event frequency of 1/10 years, the team identified a risk gap of 1,000, which clearly indicated the need for IPLs.

Identifying Protection Layers

A protection layer (Figure 3) is a physical entity supported by a management system, which is capable of preventing a hazardous event from propagating into an undesired consequence. Many process units including DCUs rely on the following protection layers:

- Control--standard operating procedures, basic process control systems, and process alarms--this layer is generally focused on maintaining the process within the normal operating limits;
- Supervisory--protective alarms, operator monitoring and supervision, and process actions--this layer is designed to achieve or maintain a safe state of the process to reduce the frequency of the hazardous event; and
- Preventive--protective instrumented systems, such as safety instrumented systems, environmental protective systems and asset protective systems--this layer is designed to achieve or maintain a safe state of the process to reduce the frequency of the hazardous event.

Protection layers can be considered independent protection layers (IPLs), when they are designed and managed to the rigor necessary to achieve the core attributes:

- Independence--the performance of a protection layer is not affected by the initiating cause of a hazardous event or by the failure of other protection layers;
- Functionality--the required operation of the protection layer in response to a hazardous event;
- Integrity--related to the risk reduction that can reasonably be expected given the protection layer's design and management;
- Reliability--the probability that a protection layer will operate as intended under stated conditions for a specified time period;
- Auditability--ability to inspect information, documents and procedures, which demonstrate the adequacy of and adherence to the design, inspection, maintenance, testing, and operation practices used to achieve the other core attributes;
- Access Security--use of administrative controls and physical means to reduce the potential for unintentional or unauthorized changes; and
- Management of Change--formal process used to review, document, and approve modifications to equipment, procedures, raw materials, processing conditions, etc., other than "replacement in kind," prior to implementation.

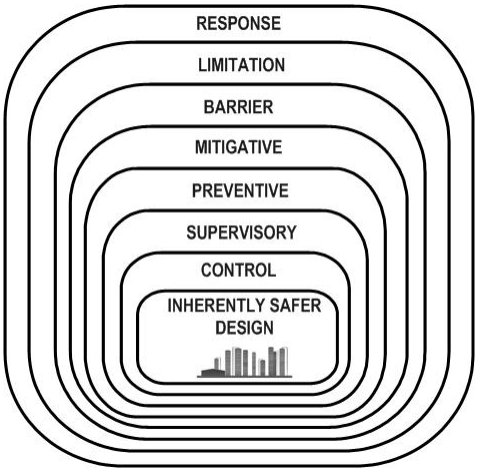

Figure 3. Protection Layers.

The team identified the following IPL:

1. A supervisory function.

   Board operator verifies the drum operational mode and valve position on the operator interface and communicates approval to the field operator to proceed with the next step in the switching and de-heading operation. This verification is included in the operator procedure and all DCU operators are trained on the importance of following the procedure to ensure safe operation.

   Function provided a risk reduction factor (RRF) of 10.

Figure 4 provides the risk gap evaluation considering the existing IPLs. Insufficient risk reduction is provided by the current equipment, resulting in a risk gap of 100. The team considered a number of options for reducing the risk reduction gap and each option was evaluated in terms of cost, complexity, and risk reduction benefits.

Figure 4
Gap Evaluation

Operator Error = 1/10 years
Independent verification = 1/10
Event Frequency = 1/100 yrs
Tolerable Frequency = 1/10,000 yrs
Gap = 100
Gap = 100

Valve permissives can easily be installed to prevent specific valve combinations. As shown in Figure 5, this left a risk gap of 10.

2. A control function.

   A valve permissive system monitors valve position and prohibits specified valve combinations (opening/closing of valves) if specified criteria are not met.

   This function provides an RRF of 10.

Figure 5
Gap Evaluation
Operator Error = 1/10 years
Independent verification = 1/10
Valve permissive system = 1/10
Event Frequency = 1/1,000 yrs
Tolerable Frequency = 1/10,000 yrs
Gap = 10

The DCU hazard analysis often focuses on the improper sequencing of the valves, since this is the initiating cause for the event. However, the act of opening or closing a valve is not hazardous; rather it is the opening of a valve on a drum that is in operation or is open to the atmosphere. The drum status can be detected using three process variables: overhead pressure, overhead temperature and inlet temperature. Each variable clearly and unambiguously indicates a process condition that presents a hazard if the incorrect valve is opened.

A preventive function can be implemented using an SIS that monitors the process variables and prevents certain valves from being opened unless the process conditions indicate that it is safe to do so. The SIS can be designed to provide a RRF of 10. The risk gap is eliminated by the identified IPLs and associated risk reduction. The SIS was assigned a RRF of 10, which establishes an SIL 1 (safety integrity level) requirement. As shown in Figure 6, the risk gap is reduced to 0.

3. A preventive function.

   An SIS monitors three process variables and prevents operation of valves that would result in a hazardous event.

   The function provides an RRF of 10.

Figure 6
Final Gap Evaluation
Operator Error = 1/10 years
Independent verification = 1/10
Valve Permissive System = 1/10
SIF = 1/10
Event Frequency = 1/10,000 yrs
Tolerable Frequency = 1/10,000 yrs
Gap = 0

Designing the SIS

The SIS monitors three inputs - overhead pressure, overhead temperature, and inlet temperature – and provides dry contact outputs wired in series with the control signals of the motor operated and hydraulic valves. The logic solver evaluation included a variety of safety PLCs (programmable logic controllers) and relays. When applied to individual drums, none of the safety PLCs were cost effective due to the low I/O point count. A relay-based SIS could be implemented for each Coke drum for less than the hardware cost of a single safety PLC capable of protecting all of the Coke drums.

The use of relays eliminates the need for software and special training. Installation, testing and maintenance can be performed by a qualified electrician following relay drawings and test procedures. Common cause errors are minimized due to simplified inspection, testing, and maintenance. Each drum is provided with its own SIS to yield maximum operability and maintainability, since each drum SIS can be inspected, tested and maintained independently. The individual SISs also improve process equipment availability by minimizing the potential for common cause failure to impact multiple drums.

Summary

Coker drum switching is a complex activity with multiple opportunities for misaligning valves. In such a complex environment, end users have struggled with evaluating the ways and means to identify the required SIF's; a struggle significantly simplified by the use of the ISA 84.01/IEC 61511.

Following the risk assessment process of the SIS lifecycle, a team of Coker and process experts were able to identify the process variables that presented significant hazards; develop a risk reduction strategy employing multiple IPLs and define the SIS requirements. The valve permissive was implemented as a control function with the BPCS layer. The result is that each Coker drum switching operation is monitored and protected by a stand-alone SIS (relay system) that minimizes the affect of common cause on the operation of other Coker drums.

References

United States Environmental Protection, *Hazards of Delayed Coker Unit (DCU) Operations*, Chemical Emergency Preparedness and Prevention Office, Agency (2003).

CCPS/AIChE*, Guidelines for Safe Automation of Chemical Processes*, New York (1993).

CCPS/AIChE, *Guidelines for Safe and Reliable Instrumented Protective Systems*, New York (expected 2007).

IEC, *IEC 61511, Functional Safety: Safety Instrumented Systems for the Process Sector*, Geneva, Switzerland (2003).

ISA, ANSI/ISA 84.00.01-2004 (IEC 61511 modified), *Functional Safety: Safety Instrumented Systems for the Process Sector*, Research Triangle Park, NC (2004).

ISA, ISA TR84.00.04, *Guidelines on the Implementation of ANSI/ISA 84.00.01-2004 (ISA 61511 Modified)*, Research Triangle Park, NC (2006).

About The Author

Bryan Zachary is Director, SIS-TECH Solutions, LP. He has over twenty five years of experience with industrial instrumentation, control and protective systems. His work has included design, installation, training instructor and maintenance supervisor. He has worked in control systems for various major company facilities, including refineries and chemical plants. Since 1992 Mr. Zachary has worked specifically in the area of safety instrumented systems performing risk analysis, specification, design, and implementation.