Oxidation Reaction Safeguarding with SIS

Edward M. Marszal, PE, CFSE (Edward.Marszal@kenexis.com)
Kevin J. Mitchell, PE, CFSE (Kevin.Mitchell@kenexis.com)
Kenexis
3366 Riverside Dr, Suite 200
Columbus, OH 43221
(614) 451-7031

1.0 ABSTRACT

A variety of useful chemical compounds are economically produced using catalyzed oxidation reactions. These products include many common organic acids and anhydrides, industrial alcohols, and organic peroxides. Safely conducting catalyzed oxidation reactions on an industrial scale is a core competency of many chemical companies. However, there is a history of numerous incidents involving fire and explosion in oxidation reactors, and these accidents are compelling reminders of the hazards of oxidation reactions.

The primary hazard that is common to these technologies is the use of oxygen – either in air, enriched air, or pure form – as a reactant in contact with a combustible hydrocarbon, which is used either as a reactant or a solvent. Oxidation reactor design typically involves ensuring that residual oxygen levels in equipment are sufficiently low that they do not support combustion. This strategy safeguards against ignition of a flammable gas mixture within the reactor or downstream separation equipment. Normally, the basic process control system regulates the process chemistry and avoids potentially dangerous excursions involving high oxygen concentration. However, upset conditions often occur, and one of the commonly-employed safeguards to prevent an explosion is a Safety Instrumented System (SIS).

This paper explores some of the common risks that are encountered in oxidation process reactor sections. The paper also describes the instrumented safeguards that are typically used to prevent these risks from being realized and addresses some of the important details that should be considered during their design.

1.0 INTRODUCTION

Catalyzed oxidation reactions allow for a variety of useful chemical compounds to be economically produced. These products[1] include many common organic acids and anhydrides, industrial alcohols, and organic peroxides, as shown below.

- Terephthalic Acid (PTA)
- Isophthalic Acid (PIA)
- Phthalic Anhydride
- Adipic Acid
- Maleic Anhydride
- Phenol / Cumene Hydroperoxide (CHP)
- Butandiol, 1,4-
- Acrylonitrile
- Ethylene Oxide

Safely conducting catalyzed oxidation reactions on an industrial scale is a core competency of many chemical companies. However, there is a history of numerous incidents involving fire and explosion in oxidation reactors, and these accidents are compelling reminders of the hazards of oxidation reactions. Loss of control of an oxidation reaction can result a reactor explosion, with the potential for worker injury, significant environmental and property damage.

The primary hazard that is common to these technologies is the use of oxygen – either in air, enriched air, or pure form – as a reactant in contact with a combustible hydrocarbon, which is either as a reactant or a solvent. Oxidation reactor design typically involves ensuring that residual oxygen levels in equipment are sufficiently low that they do not support combustion. This strategy safeguards against ignition of a flammable gas mixture within the reactor or downstream separation equipment. Normally, the basic process control system regulates the process chemistry and avoids potentially dangerous excursions involving high oxygen concentration. However, upset conditions often occur, and one of the commonly-employed safeguards to prevent an explosion is a Safety Instrumented System (SIS).

The purpose of the SIS is to automatically return the process to a safe state when pre-determined safety conditions have been violated. They are often referred to as emergency shutdown systems, or safety interlock systems. ISA 84 defines a SIS as “a system composed of sensors, logic solvers, and final control

[1] This abbreviated list of substances was generated using catalyzed oxidation reactions was generated by reviewing the licensed processes shown in the Petrochemical Processes Special Report section of the March 2003 Edition of *Hydrocarbon Processing* Magazine. The list presented here is only intended to give a small example of the numerous catalyzed oxidation reactions utilized the in the chemical processing industries.

elements for the purpose of taking a process to a safe state when predetermined conditions are violated".

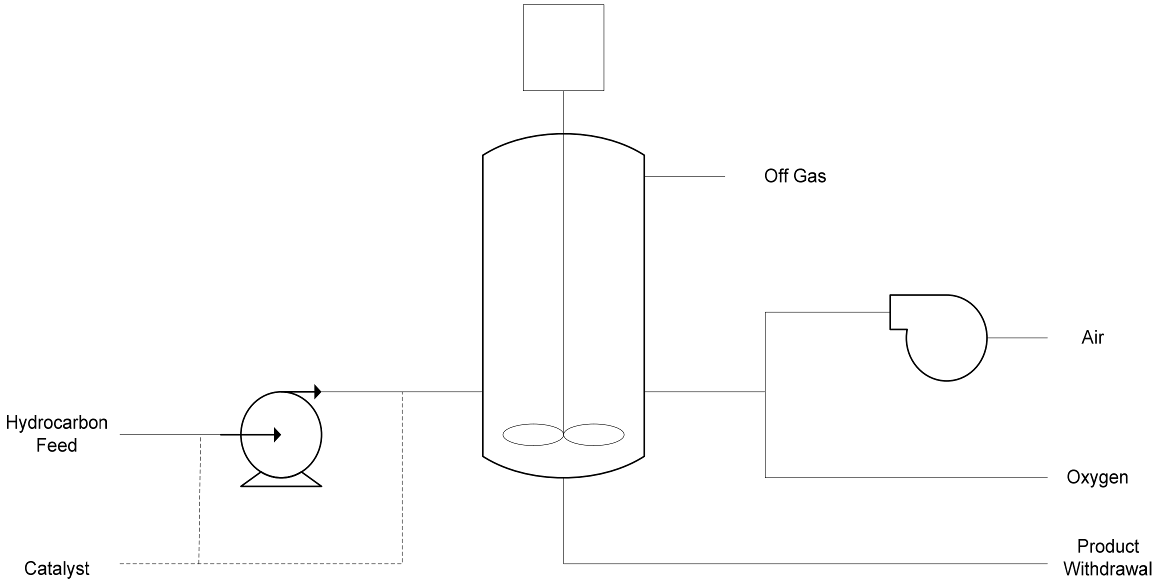
Design of SIS for oxidation reactor safety is governed, in part, by recent industry consensus standards from ISA and IEC.[2] These standards employ a performance-oriented approach in that they allow each individual company to define performance goals based on achieving a required amount of risk reduction rather than prescribing the hardware design of the SIS. Exida has performed numerous conceptual design projects involving SIS for oxidation reactors. This paper will illustrate some of the common Safety Instrumented Functions (SIF) used in oxidation reactor technology and illustrates practical application of the ISA and IEC standards.

2.0 GENERAL PROCESS DESCRIPTION

Commercial catalyzed oxidation reactions can take a number of forms. The primary difference between reaction types is the phase of the hydrocarbon reactant and the phase and type of catalyst used in the reaction. This white paper will focus on reactions where the hydrocarbon reactant (and reaction products) is in the liquid phase, and the catalyst for the reaction is also a liquid.

Figure 1 presents a typical process flow for the reaction section of a plant that employs a catalyzed oxidation reaction. The process mainly consists of a reactor vessel with an agitator. In some cases, the reactor may be jacketed to maintain the temperature of the reaction mixture.

Figure 1 – Typical Configuration of Process Section of Oxidation Process



[2] Instrumentation, Systems, and Automation Society (ISA), ANSI/ISA S84.01, *Application of Safety Instrumented Systems for the Process Industry*, 1996. International Electrotechnical Commission (IEC), IEC 61508, *Functional Safety of electrical/electronic/programmable electronic safety-related systems*, First Edition, 1998. IEC 61511, *Functional Safety: Safety Instrumented Systems for the Process Sector*, FDIS, 2001.

The reactor is typically fed with two streams, the oxygen containing stream and the hydrocarbon stream. The oxygen containing stream varies, depending on process, from pure air to pure oxygen. When air is used, the air is typically compressed and fed into the reactor under pressure. In some cases, air is “spiked” with pure oxygen to make the reaction conditions more favorable. In other cases, the reaction is run using pure (chemical grade) oxygen.

The hydrocarbon feed is typically pumped into the reactor from a feed surge drum or feed mix tank. The liquid catalyst is either added directly to the feed mix in the feed mix tank, or continuously metered into the reaction vessel, sometimes through a separate process connection.

The reaction off gas is a combination of unreacted hydrocarbon feed, inert materials in the hydrocarbon feed, nitrogen (from the air feed), and a small amount of unreacted oxygen. The product is typically withdrawn in the liquid phase along with excess hydrocarbon feed materials and catalyst.

The reaction occurs in the liquid phase. The air and oxygen feed is injected into the liquid full portion of the reactor, which is agitated. The combination of agitation injection of gases acts to partially fluidize the reaction bed. The reaction is conducted using excess hydrocarbon feed in order to limit the amount of unreacted oxygen leaving with the off gas. The reaction can occur in either a continuous process or a batch operation.

3.0 PROCESS HAZARDS

The primary hazard involved in the reaction section (and downstream separation equipment) is the potential for the occurrence of flammable mixtures of hydrocarbon and oxygen occurring in the process equipment. If a source of ignition is put in contact with any flammable mixture that might be generated in the process, the result could be a fire or explosion.

The desired reaction in virtually all of the commercial oxidation processes are catalyzed to allow the creation of a valuable and desired product. In addition to use of the proper catalyst, the desired reaction path may also depend on appropriate temperature, pressure, and bed fluidization (mixing) in the reaction vessel. If all of these conditions are not present in the reactor system there is a potential for the desired reaction to fail to occur. This will then result in unreacted oxygen and hydrocarbon accumulating in a potentially flammable mixture in the reactor vapor space, and downstream equipment.

If a flammable mixture develops outside of the liquid reaction mixture inside the reaction vessel, ignition will lead to the uncatalyzed and undesired side reaction where oxygen and the hydrocarbon combust to form carbon dioxide, carbon monoxide, water, and various other reaction products. This undesired side reaction proceeds very rapidly and very exothermically given that a flammable mixture is present. The reaction will likely result in an explosion in the vessel where the reaction occurs, or loss of containment and a potential fireball if a fire occurs in the vessel instead of a sudden explosion.

4.0 INCIDENT CASE HISTORIES

1969 explosion in a Reactor Producing an Organic Acid

This operation involved a batch oxidation reaction. After the reactor was charged, air was introduced to begin the reaction. Because a grossly insufficient amount of hydrocarbon reactant was charged to the reactor, the reaction terminated unexpectedly after only 10 minutes, at a time when air flow had been ramped up to a maximum rate. As the reaction died off, oxygen concentration in the vent system began to rise rapidly. At the same time the temperature of the batch decreased because the reaction had stopped producing heat. Both conditions resulted in the vapors in the reactor vent entering the flammable operating region. The explosion caused extensive damage to the reactor and associated equipment.

1973 explosion in a Cumene Oxidation Reactor

Enriched air was being used to oxidize cumene to produce phenol. The plant had experienced plugging in the air distribution header to the oxidation reactor. These deposits were removed by flushing liquid back from the reactor through the header. During this procedure air flow had to be positively isolated. On the day of the incident two valves were left partially open in the air header. Enriched air entered the pipe and reacted with the hydrocarbon liquid. The pipe ruptured and ignited immediately, creating a massive fire that destroyed the entire plant.

1974 explosion in a Reactor Producing an Organic Acid

This oxidation reactor system involved continuous feed of catalyst to control the reaction. On the day of the incident, the reaction was proceeding normally, when it was discovered that the catalyst flow had been interrupted. An operator was sent to investigate and found that a manual block valve had been closed on the catalyst addition system. By the time the problem was corrected, the reaction had died off and oxygen levels were rapidly climbing in the reactor overhead system. The explosion blew off the vapor outlet line from the reactor and damaged associated piping.

1982 explosion in a Reactor Producing an Organic Acid

This batch oxidation reactor system used the concentration of oxygen in the overhead as read by analyzers as a key parameter in determining when a reaction had terminated. Increasing oxygen concentration in the overhead system indicated that the hydrocarbon reactant had been completely oxidized. On the day of the incident, operators were having problems with the oxygen analyzers causing them to periodically give a false high oxygen spike and subsequently cause the reactor to suddenly shutdown. During an attempt to re-start the reaction, operators disabled the oxygen analyzers. Operators were being taxed with other operational problems in downstream separation equipment at the time the explosion occurred. It turned out that because the oxygen analyzers had been disabled, the control system did not terminate air flow to the reactor when the reaction had been completed. Minor damage to reactor equipment resulted from this explosion.

1983 explosion in a Reactor Producing an Organic Acid

During the day prior to the explosion, an operational problem resulted in the reactor being put in a hot hold condition. Air was isolated from the reactor and its contents were kept hot in anticipation of a reactor restart. Over many hours, air slowly leaked into the reactor past the air isolation valve, which was either leaking or left slightly open. Oxygen concentration built up in the reactor’s vapor space, but this remained undetected. An explosion occurred, which was relieved through the reactor’s emergency pressure relief device.

1987 explosion in a Reactor Producing an Organic Acid

During the initiation of the batch reaction, operating conditions (temperature and pressure) drifted into the flammable operating region. Operators activated an inert gas dilution system in an attempt to re-establish the reaction. They also disabled the oxygen analyzers which would have shutdown the reactor on high oxygen concentration. However, operators were unable to re-establish temperature and pressure control within normal operating limits. Less than 10 minutes after the start of the reaction, an explosion occurred, resulting in major damage to the reactor vessel, and its associated instrumentation.

1995 explosion in a Reactor Producing an Organic Acid

A leak in an air line internal to the oxidation reactor occurred. This allowed air to directly enter the reactor’s vapor space and bypassed the air sparging system at the bottom of the reactor. A fire in the vapor space broke out immediately, and this actually depleted the concentration of oxygen in the overhead system. Reactor temperature measurements shot up rapidly. Within minutes overhead piping on the reactor failed due to overtemperature. The reactor contents were ejected under pressure and extensive fire damage resulted from this incident.

1999 explosion in an Air Line to an Oxidation Reactor

An operational upset occurred in a reactor producing an organic acid. Solvent from the reactor back-flowed into an air feed line due to problems maintaining the required differential pressure between the air line (normally higher pressure) and the reactor (normally lower pressure). On subsequent re-start of the reactor, enriched air was introduced into the feed line which started oxidation and combustion reactions with the solvent contained in the line. Field operators noticed the air feed line was glowing “cherry red”. Within seconds, the line failed and a large fireball erupted.

2000 explosion in an Ethylene Oxide Manufacturing Plant

An explosion and fire occurred in the ethylene oxide manufacturing unit. Problems with an oxygen analyzer resulted in a decision to disable the device.

This key safeguard normally monitored residual oxygen concentration in the process. Over a period of time oxygen concentrations increased above safe operating limits. Subsequently a detonation occurred resulting in extensive damage to the plant.

Lessons Learned

These case histories emphasize several key lessons which have been learned from oxidation reactor accidents, including:

- Ensure that residual oxygen concentrations are – at all times – well outside the flammable operating region.

- Ensure that the oxidation reactor is shutdown and air isolated upon detection of high residual oxygen concentration.

- Use pressure and temperature measurements to predict an approach to a flammable operating condition and initiate a reactor shutdown.

- Ensure operating pressures are maintained that do not allow flammable or combustible materials to backflow into air feed lines to the reactor.

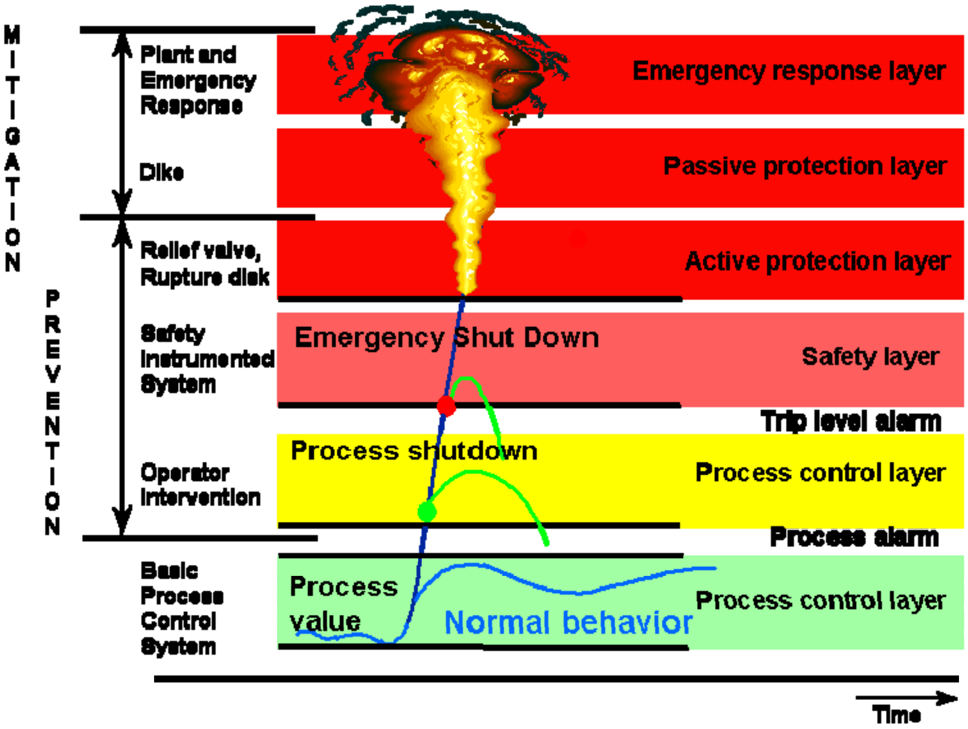
These lessons bring the topic of Safety Instrumented Systems to the forefront of the discussion on how to design and operate oxidation reactors safely.

5.0 SAFETY FUNCTIONS

Safe operation of oxidation reactors is primarily achieved through careful control of the reactor operating conditions. The temperature and pressure of the reaction, along with the oxygen concentration in the vent system will determine whether the system is within the flammable operating region or outside (i.e., either fuel rich or fuel lean). At any given time, the operator must ensure that the process is not entering in the flammable region or even approaching it. This is often accomplished by either monitoring oxygen concentration in the process directly, through oxygen analyzers, or predicting a potentially flammable condition by using a combination of pressure and temperature measurements.

The basic process control system (BPCS) regulates normal process behavior. The normal operating conditions are set such that they are well outside the flammable region and they typically use a robust safety factor to ensure a wide margin of safety (See Figure 1). Safety critical alarms are set such that when process conditions deviate from normal operating ranges, operators have ample opportunity to intervene and correct the abnormal situation. Exida's experience in oxidation reaction technology shows that in most cases, operator intervention is successful in terminating a reaction before dangerous operating conditions develop.

Figure 1 – Layers of Protection



However, many companies who conduct oxidation reactions have adopted a philosophy that operator intervention alone is not a sufficient safeguard. This best-practice philosophy dictates that when certain pre-defined safety conditions are violated, control is taken away from the operator by the SIS, and the process is immediately brought to a safe state in an orderly manner. A logic solver, such as an industrial safety-rated Programmable Logic Controller (PLC), is used to continuously monitor process variables and initiate a safe shutdown. This logic solver is usually separate from the BPCS.

An oxidation reaction system will typically have between 5 and 15 Safety instrumented Functions. A safety instrumented function (SIF) is a set of specific actions to be taken when specific safety limits have been violated, and thereby will move the process from a potentially unsafe state to a safe state. On the other hand, a Safety Instrumented System (SIS) is the collection of equipment (sensors, logic solver, and final control elements) used to perform the SIF. Multiple SIF are often implemented in a single, complex SIS. Using the perspective of a Safety PLC, there can be many individual SIF that are executed in that single Safety PLC.

Some of the typical SIF found in oxidation reactors are shown in Table 1:

Table 1 – Safety Instrumented Functions

Item	Description	Inputs	Outputs
SIF-01	High oxygen concentration in oxidation reactor overhead causes reactor shutdown	O2 Analyzers	Air Isolation Valves Closed (Double Block and Seal)
SIF-02	Oxidation reactor low temperature or high pressure indicates approach to flammability limit and initiates a reactor shutdown	Reactor Temp. Reactor Press.	Air Isolation Valves Closed (Double Block and Seal)
SIF-03	Oxidation reactor fire (as indicated by high reactor temperature) initiates a reactor shutdown	Reactor Temp.	Air Isolation Valves Closed (Double Block and Seal)
SIF-04	Low differential pressure between air header and oxidation reactor initiates a reactor shutdown	Differential Press. Transmitter	Air Isolation Valves Closed (Double Block and Seal)

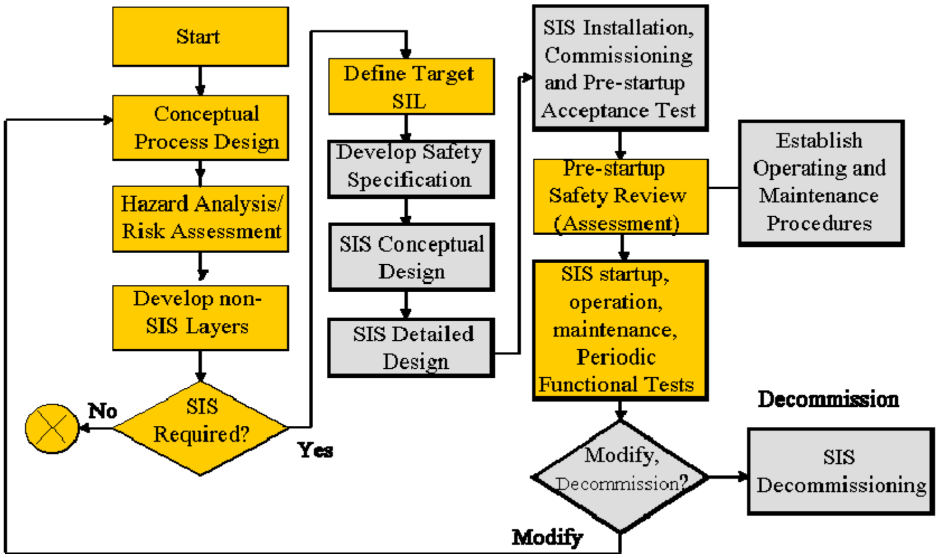
Additional SIF are typically used when enriched air is used in the reaction. The objective of these additional SIF is to ensure that oxygen concentration in the enriched air header does not exceed a certain pre-defined safe operating limit.

6.0 SIS IMPLEMENTATION

The ISA and IEC consensus standards guide the user in ensuring that high-availability safety systems are designed, installed, operated, and maintained in a manner that will promote ongoing integrity of plant operations. The performance-oriented nature of the standards allows for flexibility in implementing an approach that fits within a company's overall risk management framework, but it also requires a fundamental understanding of what SIS are required to do, and how well they need to perform to adequately manage risk.

An effective SIS design only begins with defining the Safety Instrumented Functions for the oxidation process. Establishing the key performance measurement for a SIF is the next step in the safety lifecycle shown in Figure 2. This is known as the Safety Integrity Level (SIL).

Figure 2 – Safety Lifecycle


Start
Conceptual Process Design
Hazard Analysis/ Risk Assessment
Develop non-SIS Layers
SIS Required?
No
Yes
Define Target SIL
Develop Safety Specification
SIS Conceptual Design
SIS Detailed Design
SIS Installation, Commissioning and Pre-startup Acceptance Test
Pre-startup Safety Review (Assessment)
SIS startup, operation, maintenance, Periodic Functional Tests
Establish Operating and Maintenance Procedures
Decommission
Modify, Decommission?
SIS Decommissioning
Modify

Companies are now specifying Safety Integrity Levels (SIL) based on the amount of risk reduction that is required to achieve a tolerable risk level. The SIS is then designed to meet or exceed this level of performance. The SIL represents the amount of risk reduction that is required from a Safety Instrumented Function (SIF), and it is categorized based on the average Probability of Failure on Demand (PFD_{avg}) as shown in Table 2.

Table 2 – Safety Integrity Levels

Safety Integrity Level	Probability of failure on demand (Demand mode of operation)	Risk Reduction Factor
SIL 4	0.001% to 0.01%	100,000 to 10,000
SIL 3	0.01% to 0.1%	10,000 to 1,000
SIL 2	0.1% to 1%	1,000 to 100
SIL 1	1% to 10%	100 to 10

The actual Safety Integrity Level that is selected for each SIF has an enormous impact on the design and testing requirements. Some of the most significant impacts are exhibited in the following areas:

- *Architecture* – A SIL1 design can usually be achieved using a single input / single output. However, if a SIL 2 or higher is required, a fault tolerant design may need to be employed, such as 1-out-of-2 (1oo2) voting on redundant oxygen analyzers. While this fault tolerance can result in significant improvements in Probability of Failure on Demand (and thus the achieved SIL level), it also can also significantly increase the frequency on nuisance trips due to instrumentation failures. A robust design must meet the required SIL as well as minimize the likelihood of a nuisance trip. Requiring a Safety Function to meet a SIL 3 requirement is possible, but often cost prohibitive.

- *Testing* – Air isolation valves in a SIS normally remain energized for very long periods of time before a demand is placed upon them, when they are required to quickly de-energize and to isolate the process. This results in an situation where an effective test of the SIS is the only way to ensure that a component has not failed in such a way that will defeat the entire system. More frequent testing decreases the probability that the system will fail when a demand is placed upon it. A higher Safety Integrity Level will often result in a requirement to test the system more often. Scheduling and completing this testing can be problematic for plants that have large on-stream times.

In addition to the quantitative requirements of ISA 84.01, the standard also lists a number of design criteria that must be considered and specified. These items include such considerations as:

- Tightness of shutoff

- Failure characteristics upon loss of utility (e.g., fail-open or fail-closed valves)

- Response time

- Required diagnostics, etc.

7.0 CONCLUSION

The historical record of accidents involving oxidation reactions is compelling evidence that process safety should not be taken lightly in such systems. Most of these accidents have occurred as the result of undesired high levels of oxygen in areas where oxygen is not desired, resulting in flammable atmospheres. In many cases, the risk posed by these hazards is reduced through the use of Safety Instrumented Systems. Some typical safety instrumented functions of oxidation reactors might include:

- Isolation of air upon detection of high reactor vapor space oxygen concentration

- Isolation of air upon detection of potential reverse flow of reactant into the air system

- Isolation upon detection of a fire in the air system

- Isolation upon detection of unfavorable reaction conditions (e.g., low temperature and high pressure)

If you use Safety Instrumented Systems, you should ask if they have been designed, operated, and tested as per the requirements of ISA 84.01. If not, you should begin to carefully scrutinize your systems. They key questions you need to have answered are:

- How much risk reduction does our current SIS technology provide? Have we calculated a Probability of Failure on Demand for the system

- How much risk reduction do we need? Has this requirement been documented so we can justify our decisions?

- Does the existing design have sufficient amount of redundancy and fault tolerance to meet our risk reduction requirements?

- How often should our SIS be tested in order to ensure we meet our risk reduction requirements?

- Have all design requirements for the SIS been appropriately specified, including tightness of shutoff and process safety time?

If you don’t have answers to these questions, or haven’t started any of the steps in the safety lifecycle, you may need to take action.