SIS Design Basis Revalidation

White Paper

KENEXIS

>> INTRODUCTION

It has been more than eight years since the initial release of the ANSI/ISA 84.00.01-1996 Standard – *Application of Safety Instrumented Systems for the Process Industries*. In fact, the standard has actually been updated to be in conformance with international standard IEC 61511 and has been re-released as ANSI/ISA 84.00.01-2004 – *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*. Since the time of the original standard's release, a lot of process industry users have made great strides at updating and improving their safety instrumented system (SIS) design, implementation, maintenance and operation practices to be in conformance with the standards. Furthermore, a lot of SIS equipment has had ISA 84 compliant design basis documentation developed, along with the associated hardware and management system modifications that these documents specify.

Some control system practitioners and loss prevention specialists are beginning to question the validity of both the design basis documentation that has been developed and the ability of the installed equipment and management systems to meet those targets.

Even before many process plants have completed the effort of getting all of their systems into compliance in the first place, some control system practitioners and loss prevention specialists are beginning to question the validity of both the design basis documentation that has been developed and the ability of the installed equipment and management systems to meet those targets. There are several reasons for their doubts, including the following.

- Process changes have increased levels of risk
- SIS equipment changes have been made
- Process and equipment modifications have removed or invalidated non-SIS independent protection layers
- Testing programs have been modified or ignored
- Demands on the SIS are occurring significantly more frequency than assumed during the design phase
- SIS equipment is not performing as well as assumed during the design phase

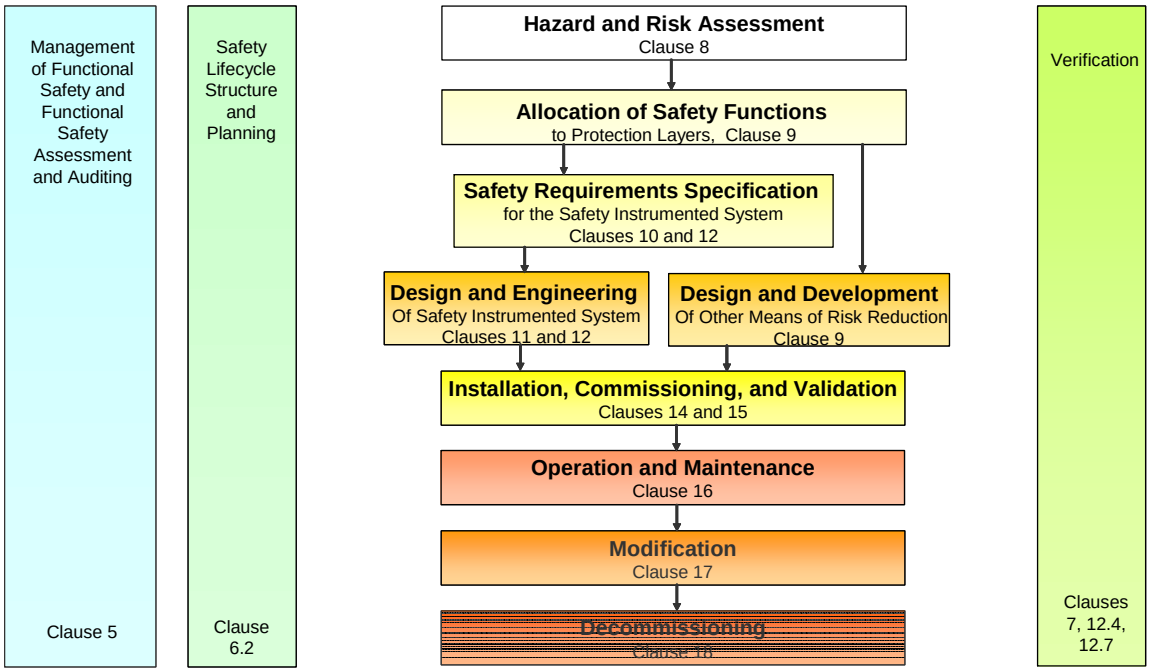
In theory, since the implementation of the SIS design basis was verified and validated, no errors should have existed when the SIS was first put into service. The management of change process should have identified any modifications that might have impacted the SIS design, and evaluated the suitability of proposed changes to SIS design. Of course theory and practice do not always match in the real world. Because procedures are not always follows and mistakes occur, the regulators and the standards writers have included provisions in their respective guidance documents to periodically go back and review prior hazard analysis studies and design basis documents to ensure that they are still valid.

2.0 WHAT IS AN SIS DESIGN BASIS?

Prior to describing the need for SIS design basis revalidation, it is important to start with a description of what a standards-compliant design basis entails.

Figure 1 – ANSI / ISA 84.00.01 Safety Life Cycle

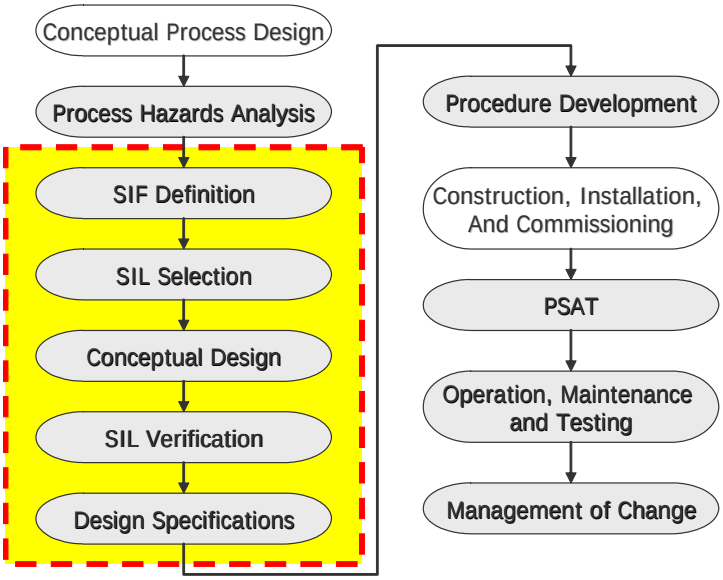
Courtesy of ISA – Used with Permission



The ANSI/ISA 84.00.01 standard defines a safety lifecycle. This safety lifecycle is essentially a set of steps, or required tasks, each of which, if completed satisfactorily, will result in a functionally safe SIS. The safety lifecycle as presented in the ISA standard is shown in *Figure 1*. A more streamlined version of the key design steps in the safety lifecycle, which can be used as a flowchart for project work, is shown in *Figure 2*. This highlights tasks that are required to establish the SIS design basis. Each of the safety lifecycle steps has inputs and outputs, most of which are documented, that carries the design from one task to the next. Some of the important steps, and resulting documents generated during the lifecycle are shown below.

Figure 2 – Project Safety Life Cycle Highlighting Design Basis Tasks

Courtesy of Kenexis Consulting Corporation – Used with Permission



- ***SIF List Development*** – The Safety Instrumented Function (SIF) forms the "inventory" or "scope" of an SIS project. This list contains the "safety loops" that are to be analyzed, defined, and implemented. This step results in a list of SIF called a "SIF List" (or an Instrumented Protective Function List ["IPF List"] to be inclusive of non-safety protective functions).

- ***SIL Selection*** – For each SIF identified for the project, a performance target for that function must be defined. As per the ANSI/ISA 84.00.01 standard, this target is the Safety Integrity Level (SIL) and correlates to bands of the average probability of failure on demand (PFD_{AVG}) of the function. SIL are selected by performing a risk analysis that considers potential accident causes and their frequencies, the consequences of accidents, and the non-SIS independent protection layers that can prevent a cause from turning into an accident. The result of SIL selection is a report that defines the SIL of each SIF and documents the risk analysis that generated the performance target.

- ***Conceptual Design Review / SIL Verification*** – Once the performance target, i.e., SIL, has been selected for all of the SIF, a conceptual design of each SIF is prepared and the proposed equipment, architectures, and maintenance and testing programs are analyzed using quantitative analysis to determine if the target has been met. If the target is met, the SIF moves to the specification phase, and if not the conceptual design is modified until it meets the performance target. The result of SIL verification is a report that presents the calculations that verify that the SIL targets have been achieved.

- ***Safety Requirements Specifications (SRS) Development*** – After the conceptual designs of all of the SIF have been verified as achieving the target SIL, the final conceptual design is documented in a way that

specifies the functional and integrity requirements of all of the SIF contained in a SIS. These specifications then serve as the basis for all subsequent detailed engineering activities and the verification and validation of the final design.

After the safety requirements specifications (SRS) task of the safety lifecycle is complete, the "Design Basis" for the SIS has been established. At this point, the design can be handed off for detailed engineering, construction, installation, and commissioning. As a result, the safety requirements specifications, and the documentation preceding it, form important foundation for the requirements of the SIS. Any future modifications to either the SIS or the process under control that are not "like in kind" replacements need to be reviewed against this "design basis" to ensure the integrity of the process safeguarding is maintained.

3.0 BASIS FOR REQUIRING REVALIDATION

Both the ANSI/ISA 84.00.01 standard and process sector regulations, such as the Process Safety Management (PSM) standard from the Occupational Safety and Health Administration (OSHA) – 29 CFR 1910.119 and "Accidental Release Prevention" rule from the Environmental Protection Agency (EPA) – 40 CFR 68, require that the hazard analyses used to make decisions about the suitability of process plant safeguards are reviewed on a periodic basis to ensure their validity.

PSM requires that process hazards analyses be performed to identify and asses the risks of process plants. OSHA describes a Process Hazards Analysis (PHA) as follows:

> *The process hazards analysis is a thorough, orderly, systematic approach for identifying, evaluating, and controlling the hazards of processes involving highly hazardous chemicals.*

While the PHA is most often considered to be the one formal study that was initially used to holistically address the safety concerns of the entire plant (such as a Hazards and Operability Study – HAZOP), one can argue that all other studies that analyze specific risks – such as pressure relief surveys, chemical reactivity matrices, alarm rationalization, and layer of protection analysis studies used for SIS design basis development – should also be revalidated to the same degree of rigor. OSHA's requirements for revalidation are as follows:

> *All process hazards analyses must be updated and revalidated, based on their completion date, at least every five (5) years.*

Moreover, the ANSI/ISA 84.00.01-2004 standard itself contains numerous requirements for reviewing SIS performance to ensure ongoing integrity of the SIS. Section 5.2.5.3 of the ISA standard states:

> *Procedures shall be implemented to evaluate the performance of the safety instrumented system against its safety requirements including procedures for … assessing whether dangerous failure rates of the safety instrumented system are in accordance with those assumed during the design; assessing the demand rate on the safety instrumented functions during actual operation to verify the assumptions made during risk assessment when the integrity level requirements were determined.*".

The standard also contains requirements for auditing and revision of the SIS design basis and equipment. Clause 5.2.6.1 states:

> *Procedures shall be defined and executed for auditing compliance with requirements …. (i.e., safety lifecycle procedures and safety requirements specifications)*

Furthermore, the standard contains "operation phase" requirements as stated in clause 16.2.6 as shown below.

> *Discrepancies between the expected behavior and actual behavior of the SIS shall be analyzed and, where necessary, modifications made such that the required safety is maintained. This shall include monitoring the following.*
>
> - *The actions taken following a demand on the system;*
> - *The failures of equipment forming part of the SIS established during routine testing or actual demand;*
> - *The cause of the demands;*
> - *The cause of false trips;*

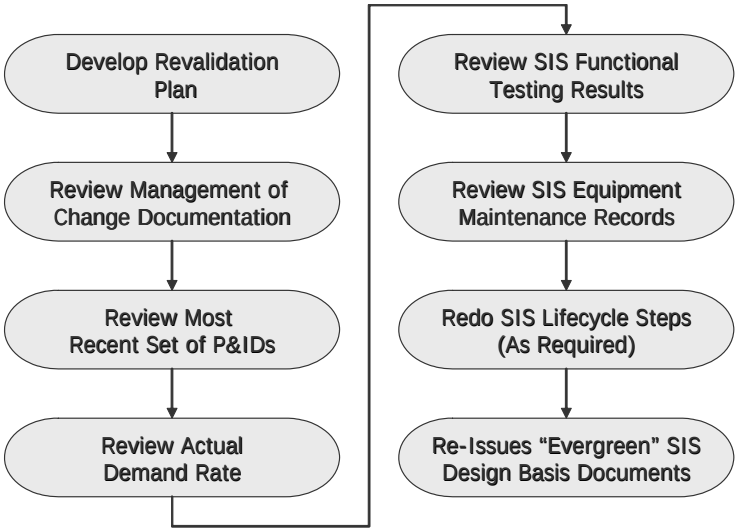
While it is clear that the ANSI/ISA 84.00.01-2004 standard requires ongoing revalidation of the SIS design basis, the standard does not specify any requirements for how frequently these activities should take place, other than that they should be "planned". Since both the PSM standard and the ISA standard require revalidation activities it is appropriate that SIS revalidation should occur at the same frequency as required for PHA revalidation, which is once every five years. At any time for cause (i.e., an accident or near-miss related to the action/inaction of the SIS) the design basis may require review, update, or revalidation.

4.0 THE REVALIDATI0N PROCESS

There currently exists no industry accepted process for SIS design basis revalidation. The guidelines proposed by the authors are intended to fill this gap. The process for revalidation is fairly straightforward, and is analogous to the PHA revalidation process. It is important to remember that the process, in the case of SIS, is extended from a PHA revalidation due to the quantitative properties of SIL verification, which must be confirmed are correct based on actual system SIS performance history.

The steps shown in *Figure 3* should be considered for an SIS design basis revalidation process.

Figure 3 – SIS Design Basis Revalidation
Courtesy of Kenexis Consulting Corporation – Used with Permission



Develop a Revalidation Plan

The first step in any undertaking is to prepare a plan. When preparing a plan for a PHA revalidation it is important to consider not only the activities that need to be undertaken, but also the personnel that will be required. Implementation of a safety instrumented system is a multi-disciplinary activity. There are a number of stakeholders in the SIS, each of which has valid concerns about the operation of the system and valuable input into its current level of performance. The following sections will expand upon not only the tasks that should be undertaken, but also the personnel who will be in possession of key data that will make the revalidation successful.

Review Management of Change Documentation

When any significant change is to be made to a process plant (i.e., other than a like-in-kind replacement), management of change procedures are

required to be executed. The management of change process ensures that the following issues will be addressed prior to any change.

1. The technical basis for the proposed change
2. The impact of the change on safety and health
3. The required modifications to operating procedures
4. The necessary time period for the change
5. The authorization requirements for the proposed change

Management of change results in a package of information about each modification. This information typically includes a detailed explanation of the modifications that are required, along with some degree of process hazards analysis (often checklist based).

The SIS design basis revalidation procedures should require that each management of change documentation be reviewed to assess the impact, if any, on the safety instrumented system. For each modification, the following issues should be considered in relation to the SIS.

1. Did the modification include changing any SIS equipment?
2. Did the modification significantly increase magnitude of the risks posed by the hazards that the SIS protects against?
3. Did the modification change, remove, or invalidate any non-SIS protection layers?

If any of the issues listed above are identified during the review process, the impacted safety instrumented functions should be noted for inclusion in the "re-do" step.

Review Most Recent P&IDs

While the management of change process clearly document all significant process changes and ensure that they are appropriately analyzed and authorized, some changes can still occur without the appropriate protocol being followed. As a result, it is important the review the most recent version of the piping and instrumentation diagrams to determine if any changes for which no management of change documentation has been prepared have been implemented. The most recent P&IDs should be reviewed against the set of P&IDs that were used to prepare the original SIS design basis. All of the drawings that were used in development of the SIS design basis documentation, including the specific revision levels used, should have been incorporated into the SIS design basis report. Any differences between the "recent" set and the "design basis" set should be identified and correlated to a management of change document package. If a change to the P&IDs is noted for which a management of change document package is not available, the modification should be noted and reviewed against the same three criteria is each management of change document package, specifically:

4. Did the modification include changing any SIS equipment?

5. Did the modification significantly increase magnitude of the risks posed by the hazards that the SIS protects against?

6. Did the modification change, remove, or invalidate any non-SIS protection layers?

If any of the issues listed above are identified during the review process, the impacted safety instrumented functions should be noted for inclusion in the “re-do” step.

Review Actual Demand Rate

The SIS design basis, and specifically the selected safety integrity levels, is a function of the amount of risk reduction required from each SIF. The determination of required risk reduction is based upon a risk analysis, a key component of which is the frequency of initiating events that might result in an accident if the SIS or other non-SIS protection layers fail to prevent the hazard. The frequency of initiating events is typically represented as a category, such as infrequent – 5-10 years, and is typically selected through the qualitative judgment of the SIL selection team.

Reviewing demand occurrences provides an opportunity to ensure the following.

7. Causes of demands were appropriately identified in the original SIS design basis.

8. Assumed non-SIS independent protection layers were effective in preventing hazards/demands.

9. Non-SIS independent protection layers were properly identified in the original SIS design basis.

In some cases, the judgment of the SIL selection team may have been flawed, or the actual processing conditions may have become more or less severe since the time of the SIL selection. These issues may have resulted in an initiating event rate that is significantly different than the one assumed to generate the SIS design basis. If the initiating event rate is significantly different than assumed, then there is a chance, that the selected SIL in not appropriate and should be changed to match the actual operating conditions. In turn, this may require a change in SIS equipment or testing procedures.

During the SIS revalidation, the actual demand rate of the SIS should be compared against the one that was assumed during the SIL selection. There are two important sources of information that should be assessed during the revalidation process. First, any available electronic records should be analyzed and reviewed with process operators. In some cases, SIS activations are logged in basic process control system history modules and databases. It is also possible to view historical charts of key process parameters to determine when a plant was shutdown (e.g., the sudden drop in the discharge flow of a compressor is a good indication that the compressor’s shutdown system might have taken action). If key process variables are used to determine when shutdowns occurred, it is important to review the information with operators who will be able to explain the exact cause for the operating profile disturbances. In every case, the operators of the process under control should be interviewed to give their

assessment of the performance of the SIS. The operations personnel should be able to accurately convey the number of shutdowns that occurred during the revalidation period and whether those shutdowns were manually initiated, were caused by a process demand, or were a nuisance shutdown caused by instrumentation and control failures.

Review SIS Functional Testing Results

The SIS functional testing results are a critical source of information on the safety performance of the SIS. Any dangerous (or covert) failures of the SIS that are not identified by on-line diagnostics will only be evidenced during a functional test of the SIS or by a demand being placed on the SIS and it failing to respond. Each SIF is required to be functionally tested on a defined interval. These tests are required to be documented, including the "as-found" and "as-left" information for each component. The functional test records for each SIF, component, and component type should be reviewed in order to ensure that the performance of the SIF components is consistent with the data that was used for the SIF verification calculations.

Several issues can be identified by a review of functional test results. First and foremost, one can confirm that the functional tests are being performed, and also that they are being performed within the specified time interval. The actual safety performance of SIS components can also be assessed. While complete recalculation of all SIF performance criteria using actual "in use" data is possible, it is not required and not recommended. It is recommended that effort during the revalidation process be focused on potential problem areas, specifically SIS component failures. For each SIS component that failed, an analysis of the failure and the performance of all SIF that utilize that type of component should be undertaken. For the failure under study, an assessment should be made of whether the failure is a "random hardware failure" or whether there was a systematic flaw in its application, such as use in an inappropriate application. If the failure was the result of systematic flaw, all other instances of use of that component should be reviewed to ensure that same flaw does not exist elsewhere. If the failure was a random hardware failure then the statistical performance in terms of actual failure rate should be calculated. The actual failure rate achieved should then be compared against the failure rate used in the SIL verification calculations. If the actual failure rate is significantly outside the confidence limits of the failure rate that was used for the SIL verification calculations, the failure rate used in the calculations should be modified to account for actual component performance.

Review SIS Equipment Maintenance Records

In addition to SIS functional test records, the equipment maintenance records are also a valuable source of information on SIS performance. While the dangerous (or covert) failures are typically identified in functional test records, safe (or spurious or overt) failures are typically identified by reviewing SIS equipment maintenance records. Overt failures are quickly identified and repaired, often while the process plant is still in service. When these failures occur, work orders are generated for equipment repair. A review of work orders related to SIS equipment can identify components that may be nuisance failure issues affecting SIS performance. As with identified dangerous failures, these nuisance failures need to be reviewed to determine if they are random hardware failures or

systematic application errors. Depending on the type of error, the appropriate corrective actions and performance recalculations will subsequently be performed. Data collected for diagnostic testing of SIS equipment, including transmitters and valves should be reviewed to ensure that assumed diagnostic testing is in fact occurring and has been effective in detecting fault conditions.

In addition to maintenance records, interviews of instrumentation and electrical technicians that services SIS equipment are an invaluable source of information. In many cases, SIS component failures can be performed very quickly with a very low cost. As such, it is possible that some of these repairs are occurring without the benefit of formal documentation. The only way to ensure that the nuisance failures of SIS components are being addressed correctly is to supplement document review with maintenance personnel interviews. In the event that equipment repairs have not been occurring within the repair time interval assumed in developing the original SIS design basis, the SIL verification calculations should be flagged for "re-do" in order to incorporate a more appropriate mean time to repair.

Re-Do SIS Lifecycle Steps As Required

The previous steps revolved around identifying instances of deviations between actual implementation of a SIS and the design basis that was used to specify the SIS. For each deviation that was identified, some degree of re-design of the function will be required. Based on the type of deviation from the design basis, the safety lifecycle steps will need to be re-done starting at the first lifecycle step that was impacted by the change. For instance, if the initiating event rate was much higher than the design basis assumption, then all of the steps starting with SIL selection would need to be redone, including: SIL selection, Conceptual Design/SIL Verification, SRS, etc.

Re-Issue "Evergreen" SIS Design Basis Documents

Although not strictly required by standards or regulations, the author recommends keeping the SIS design basis documents "evergreen", meaning that as changes to the SIS occur the design basis documents are updated and re-issued so that the documents reflect the as-built condition of the equipment. This approach is preferred to one where changes are compiled in addenda to the report and not incorporated into the report body.

5.0 CONCLUSION

Through an effective SIS design basis revalidation, industry can ensure that non-"like-in-kind" changes are scrutinized and design basis documents are updated to ensure the integrity of the Safety Instrumented System is maintained

The process industries have been implementing SIS in accordance with the ISA 84 standard for several years now. Since implementation, process and equipment modifications may have invalidated the original design basis of some of the safety instrumented functions. The ANSI/ISA 84.00.01 standard and other process safety regulations, require that process hazards analyses and SIS design basis documentation be periodically reviewed to ensure their continuing validity. The author recommends an SIS design basis revalidation process that is performed specifically within five years, in conformance with the revalidation cycle of process hazards analyses, or at any time for cause. The SIS design basis revalidation should include: planning, MOC review, P&ID review, demand rate assessment, SIS functional rest review, SIS equipment performance review, re-do of required SIS lifecycle steps, and maintenance of "evergreen SIS design basis documents. Through an effective SIS design basis revalidation, industry can ensure that non-"like-in-kind" changes are scrutinized and design basis documents are updated to ensure the integrity of the Safety Instrumented System is maintained throughout the life of the process.

6.0 REFERENCES

The Occupational Safety and Health Administration (OSHA), Process Safety Management, 29 CFR 1910.119, 1992

The Environmental Protection Agency (EPA), Accidental Release Prevention Programs, 40 CFR 68, 1996.

Frank, Walter L. and Whittle, David K, *Revalidating Process Hazards Analyses*, Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, NY, 2001.

Marszal, Edward and Scharpf, Eric, *Safety Integrity Level Selection with Layer of Protection Analysis*, Instrumentation Systems and Automation Society, Research Triangle Park, NC, 2002.

About the Authors

Ed Marszal, PE, CFSE
Kenexis
edward.marszal@kenexis.com
2929 Kenny Road, Suite 225
Columbus, OH 43221
+1 (614) 451-7031

Ed Marszal has over ten years of experience in instrumentation, safety systems design and risk analysis. Mr. Marszal has worked with UOP, a developer and supplier of process units to the petroleum and petrochemical industries, where he performed field verification of control and safety instrumented systems at customer sites world-wide. At UOP, he also designed and managed development of custom control and safety system projects. After leaving UOP, he joined a risk management consulting firm specializing in financial risk analysis and process safety management. In this position he performed and managed risk assessment projects that included quantitative consequence and likelihood analysis, including development of EPA Risk Management Programs with off site consequence analysis. He has solid experience in numerous projects involving evaluation of the integrity of safety systems, financial risk analysis and system design. Mr. Marszal has a BSChE from Ohio State University. He is a registered professional engineer in the States of Ohio and Illinois, USA, and the certified functional safety expert (CFSE). Mr. Marszal is a senior member of the Instrumentation, Systems, and Automation Society (ISA) and has held numerous positions of responsibility in that organization, and also a member of the National Fire Protection Association (NFPA), and the American Institute of Chemical Engineers (AIChE).

Kevin Mitchell, PE, CFSE
Kenexis
kevin.mitchell@kenexis.com
2929 Kenny Road, Suite 225
Columbus, OH 43221
+1 (614) 451-7031

Kevin Mitchell has over ten years of experience in chemical process safety and risk management. During much of this time he worked as a consulting engineer for DNV and ERM-Risk, helping companies in the petroleum and chemical industries implement process safety technology and management systems. Mr. Mitchell specializes in state-of-the-art assessment of the risk of toxic, flammable, and explosive materials on people, property, the environment, and, ultimately, the business. He uses risk assessment and cost-benefit analysis to assist in making engineering and business decisions. Mr. Mitchell has defined safety integrity requirements for clients using the principals of risk assessment in over 100 project assignments covering such diverse operations as oil & gas production, refining, petrochemical, specialty chemical, plastic resin, transportation, and general manufacturing. He also has extensive experience in investigating major chemical accidents to identify causes and develop lessons-learned. Mr. Mitchell has a BS in Chemical Engineering from The University of Minnesota and is a Registered Professional Engineer in the state of Ohio. He is also a member of the American Institute of Chemical Engineers and the Instrumentation, Systems, and Automation Society. He has numerous technical publications and is a Certified Functional Safety Expert (CFSE).