WSRC-MS-95-0358

CONF-951135--31

Accident Management & Risk-Based Compliance With 40 CFR 68 for Chemical Process Facilities (U)

by

K. R. O'Kula

Westinghouse Savannah River Company
Savannah River Site
Aiken, South Carolina 29808

R. P. Taylor Jr.

S. G. Ashbaugh
Innovative Technology Solutions
NM

A document prepared for PROCEEDINGS OF THE 1995 AMERICAN SOCIETY OF MECHANICAL ENGINEERING (ASME) INTERNATINAL MECHANICAL ENGINEERING CONGRESS AND EXHIBITION (IMECE95), RISK & SAFETY ASSESSMENTS: BUILDING VIABLE SOLUTIONS at Livermore from 11/12/95 - 11/17/95.

DOE Contract No. **DE-AC09-89SR18035**

Accident Management & Risk-Based Compliance With 40 CFR 68 For Chemical Process Facilities (U)

K. R. O'Kula and R. P. Taylor, Jr.
Westinghouse Savannah River Company
1991 South Centennial Avenue
Aiken, South Carolina 29803-7657

S. G. Ashbaugh
Innovative Technology Solutions
8015 Mountain Road Place, NE, Suite 210
Albuquerque, NM 87110

ABSTRACT

A risk-based logic model is suggested as an appropriate basis for better predicting accident progression and ensuing source terms to the environment from process upset conditions in complex chemical process facilities. Under emergency conditions, decision-makers may use the Accident Progression Event Tree approach to identify the best countermeasure for minimizing deleterious consequences to receptor groups before the atmospheric release has initiated. It is concluded that the chemical process industry may use this methodology as a supplemental information provider to better comply with the Environmental Protection Agency's proposed 40 CFR 68 Risk Management Program rule. An illustration using a benzene-nitric acid potential interaction demonstrates the value of the logic process. The identification of worst-case releases and planning for emergency response are improved through these methods, at minimum. It also provides a systematic basis for prioritizing facility modifications to correct vulnerabilities.

I. REGULATORY ENVIRONMENT

In late 1993, the Environmental Protection Agency (EPA) published intent of rulemaking in proposed 40 CFR 68, "Risk Management Program for Chemical Accidental Release Prevention" [EPA, 1993]. The final rule will be published in March of 1996 and is referred to as Part 68 , or the Risk Management Program rule. Under this program, chemical process industries that possess chemical inventories above specified threshold quantities must develop Risk Management Program (RMP) plans that contain hazard assessment, prevention program, and emergency response program elements. Table 1 summarizes the significant provisions of the accidental release prevention program. Table 2 lists the documentation requirements for the hazard assessment and the analysis of offsite consequences.

The hazard assessment phase of the proposed chemical process facility RMP has prompted the development of a spectrum of compliance plans. In each one, nevertheless, consequence analysis meeting Part 68 requirements must be undertaken. These analyses may demand rethinking the basis for characterizing a worst-case and the associated response planning and accident management phases, and are likely to extend beyond current industry practices. For example, RMP consequence analyses under 40 CFR 68 must include both "probable" scenario and a worst-case scenario according to the regulated substances in each process under consideration. For each scenario, release quantities, likely effects, and exposure estimates to downwind populations are required.

Probable and worst-case releases are reasonably straightforward to quantify for low hazard, relatively simple processing or storage tank conditions. Despite recent supplemental guidance from the EPA [EPA, 1995] relieving some facilities from compliance with the full Risk Management Program however, intermediate and complex chemical processes present release conditions that potentially are difficult to define and present considerable

Table 1.
Provisions for Accidental Release Prevention Under Proposed Part 68

Topic	Action/Analysis
Purpose of Hazard Assessment	Evaluate impact of significant accidental releases on the public health & environment, & to develop a history of such releases
Scope of Hazard Assessment	For each regulated substance present at the stationary source above threshold quantity - determine worst-case scenario - identify other more likely significant accidental releases for each process . . ., including processes where substance is manuf., processed, or used, and where the regulated substance is stored, loaded, or unloaded - analyze offsite consequences of worst-case release scenario and other more likely significant accidental release scenarios
Required Consequence Analysis	For each regulated substance, offsite consequences of worst-case or more likely significant accidental release scenarios shall be determined: - estimate rate and quantity of substance lost to air and duration of event - evaluate distance in all directions, at which exposure to substance or damage to offsite property or environment from release could occur using both worst-case and meteorological conditions most often occurring at stationary source

difficulty during emergency response. In particular, accident progression in the latter facilities is dependent on the interaction of design, passive and engineered safety features, and the operator/process interface. Sufficiently complex chemical processes may

Table 2.
Hazard Assessment and Consequence Analysis Documentation Required From Part 68

Topic	Action/Analysis
Description	(1) Worst-case Scenario (2) Other, More Likely Scenarios (Include assumptions, analyses/worksheets used to derive accident scenarios, and rationale for selection of specific scenarios;
Scope of Documentation for Offsite Consequences for Each Scenario	(i) Estimated Quantity of Substance Released; Rate of Release; Duration of Release (ii) Meteorological Data Bases for Typical Conditions at Source (iii) The concentration used to determine the level of exposure and the data used for that concentration

possess several barriers and protective system redundancy to achieve safety margins. Environmental effects such as terrain and population density patterns surrounding the facility present yet another layer of complexity in assessing a "worst case" scenario. Development of planning indicating the best options to take to mitigate downwind effects is therefore problematic. For the complex multi-barrier systems, risk-based methodology using logic models is the recommended approach.

The balance of this paper discusses this methodology. It is suggested that implementation will improve the identification of accident conditions, including those that may be defined as worst case, and will better predict imminent release conditions from chemical process facilities. Emergency management is then improved since identification of the best countermeasure strategies is facilitated. An overall approach is outlined, consisting of five phases. Accident progression logic models developed for nuclear reactor and waste processing safety are then discussed as the core basis for estimating probable accident phenomenology and integrating likely releases to a source term predictor. An illustration of the methodology with an example follows. Next, the steps required to yield a unique source term predictor model are identified. A discussion of the additional areas to be treated before the integrated methodology can support emergency management goals under the RMP concludes the paper.

II. ACCIDENT PROGRESSION METHODS

Determining the timing, quantity and composition of a chemical or radiological release (i.e., the source term) is the most difficult aspect of determining potential offsite consequences of an accident at a processing facility where combinations of multiple engineering barriers must be taken into account. The number and magnitude of technical uncertainties associated with basic phenomena that govern chemical release and transport from these facilities are sufficiently large to limit the usefulness of direct mechanistic calculations for cases beyond simple, one-step failure scenarios. As a result, it is essential that any realistic accident analysis not simply acknowledge, but quantitatively address the influence of these uncertainties on source term prediction.

At the Savannah River Site (SRS), both reactor and waste processing facilities have augmented their existing safety basis for operation by performing probabilistic accident analyses. These analyses apply probabilistic logic models, supplemented by mechanistic calculations, to track credible accident sequences from postulated initiating events. A principal goal of these analyses is to evaluate the performance of the confinement systems in mitigating the release of hazardous materials to the environment.

Overview of Integrated Methodology

A linked set of modules can facilitate the identification of plant status and enable prediction of the environmental source term that may result from postulated or real upset conditions in a chemical facility. The method for source term prediction can be applied to any facility that generates or stores hazardous materials. In a fully implemented system, plant system, accident progression, and hazardous material release models are linked by a computer interface, to allow the user to interpret facility status information as it becomes available. The linked methodology then uses a self-consistent logic model to predict the likelihood of hazardous material release based on the user supplied information. If a release is expected, the magnitude and timing of that release is estimated.

The overall source term predictor methodology is composed of five phases of work. These are:

1. Accident Class Development,
2. Source Term Algorithm Development,
3. Accident Progression Logic Model Design and Testing,
4. Observable Accident Characteristics to Accident Classes Mapping, and
5. User Interface Development and Component Integration.

A general description of each of the five phases listed is outlined below.

Accident Class Development

Accident classes are defined by grouping postulated accident scenarios that exhibit similar characteristics with regard to initiating events and the availability or failure of facility systems and engineered safeguards. That is, accident scenarios that present similar initial and boundary conditions to the evolution of a chemical species release and transport define an accident class. Such a grouping allows a finite number of accident progressions to be analyzed without severely compromising the accuracy of the source term estimation.

Source Term Algorithm Development

To correctly estimate the source term for a given accident sequence, relationships must be developed between the accident phenomena and the source term parameters. The objective of this module is to establish relationships that describe how the accident progression influences hazardous material release and transport. For example, an explosion in a tank containing hazardous waste may release a certain amount of hazardous material. Depending on the location of the release, the hazardous material may be confined or transported to other locations or the environment. The development of such quantitative relationships usually requires supporting calculations, such as confinement failure and chemical transport characterization.

Accident Progression Logic Development

The magnitude of an environmental release of hazardous material resulting from an accident are determined using the source term algorithm. However, systematic tracking of the state of the facility and a means for evaluating possible future accident progressions are necessary inputs to the algorithm. Probabilistic accident progression analysis involves the application of a logic model, supplemented by mechanistic calculations, to track possible accident progressions. An Accident Progression Event Tree (APET) logic model provides the framework for the probabilistic representation of potential accident sequences.

Correlation of Observable Accident Characteristics with Accident Classes

As stated above, the accident class definitions represent the initial and boundary conditions for the evaluation of the accident progressions. To define an accident class, the accident initiator and the state of facility systems that may mitigate accident progression or consequences must be known. The objective of this module is to develop a rule set that will characterize each accident class in terms of known and measurable facility parameters. This allows the emergency response team to obtain an estimate of the source term based on information that should be available at the time of the accident.

The work required to complete this task should involve personnel associated with the operation of the facility. Once a complete data base of available information is compiled, a rule set that correlates this information to each accident class should be developed. This rule set should uniquely define each class in terms of the parameters that can be observed, measured or easily inferred by the facility operations personnel. It would be beneficial to provide the preliminary rule set to facility operations personnel and emergency response personnel for feedback and suggestions before the final rule set is incorporated into the model.

User Interface Development and Component Integration

This task consists of developing the computer interface and combining all of the components discussed above into an integral source term prediction tool.

Information regarding potential accident scenarios, plant or facility response, damage states, and potential environmental source terms typically is generated for facilities as part of the authorization basis for operation. Examples include, but are not limited to Safety Analysis Reports (SARs) or Health and Safety Plans (HASPs). The information generated in support of a SAR or HASP would be an ideal departure point for development of a source term prediction tool. Other, non-DOE Complex facilities may utilize other safety reports developed for purposes of meeting the EPA RMP, including but not limited to, fault tree models, what-if checklists, or other system/component based analyses.

III. IMPLEMENTATION FOR PROCESS FACILITY ANALYSIS

Analysis software for accident progression to ultimately assessing the risk posed by complex commercial and production nuclear facilities has evolved over the last twenty years since the early WASH-1400 reactor risk study [USNRC 1975]. While the computer applications have improved, the primary methodology used by SRS and other nuclear facilities for probabilistic accident analysis has remained accident progression event trees. Logic models of this nature have been employed to evaluate the risk of operation for K Reactor, and to supplement safety analysis for operation of the Defense Waste Processing Facility at SRS (Massey and Taylor, 1995, and Brandyberry et al., 1994). While the risk of operation may be quantified through application of the logic model, the additional benefits of identifying vulnerabilities and cost-effective prioritization of any facility modifications are also realized.

Assuming a mixed source term (both radiological and chemical hazardous materials), the risk of operation using the event tree methodology is linked fundamentally to the breach of confinement barriers. The primary barriers to the release of the hazardous material is the vessel or piping containing the nuclear/chemical inventory being processed. A second barrier in most cases is the confinement system which includes the buildings housing the process and auxiliary filter/ventilation systems. The potential consequences of an accident in the facility under consideration is determined by the systematic tracking of the progression of the accident in terms of the extent of damage to the confinement barriers. Accident progression analysis integrates event tree logic models with mechanistic evaluations to define possible accident sequences from a postulated initiating event, through damage to the primary confinement barrier and to the final state of the confinement system. The goals through the application of the accident progression methodology in addition to those discussed earlier are to:

- Evaluate the success of the confinement system in mitigating the release of hazardous material to the environment; and
- Provide sufficient information such that the magnitude of any release to the environment can be estimated as well as the timing and energy associated with that source term.

An APET is the core methodology supporting this analysis approach based on EVNTRE computer code [Griesmeyer, 1989]. The APET for a given facility safety analysis provides a probabilistic representation of potential sequences along which an accident may progress. A key objective of the APET-based analysis is the evaluation of the success of the confinement system in mitigating releases. The APET consists of "questions" phenomenologically tied to the performance of the safety barriers identified previously. A question is analogous to a top event in a classical event tree. Each question identifies important aspects of accident progression as well as questions that establish integrity status and performance of the confinement system. The possible answers to the questions are specified in terms of two or more discrete outcomes represented as branches. The probability that a particular branch is taken is evaluated based on the answers to previous questions (i.e. accident progression is sequence dependent) and on mechanistic analysis of accident progression and confinement response.

Waste Processing Facility Chemical Illustration

Representative of the APET-based analysis is an illustration drawn from recent safety analysis enhancement work supporting startup of a waste processing facility at SRS. *The example is altered significantly from the current and planned operating conditions for the facility.* It is provided only to show how this approach helps uncover facets of accident analyses that may otherwise be missed using alternative methodologies.

The analysis uses the APET to model a hypothetical chemical process facility with two processing vessels, one containing benzene and the other containing a 50 wt.% nitric acid solution. The facility schematic is shown in Figure 1. The two tanks containing material of interest are located inside the processing cell. Tank 1 contains a process generating benzene as a waste product. A purge system utilizing compressed air provides air flow through the vapor space of Tank 1 to prevent the lower flammability limit (LFL) of benzene from being reached. The purge stream from the tank ties into the building exhaust header which provides sufficient air dilution to prevent explosive mixture from occurring in the exhaust system. Tank 2 is located next to Tank 1 but is separated by a shield barrier wall. Tank 2 contains 50 wt.% nitric acid which is hazardous but not explosive. While not shown on the drawing, the processing cell is roofed by 10,000 lb steel cell covers to provide proper exhaust flow balancing. Above the processing cell is a large area that provides space for an overhead crane used to remove the cell covers when maintenance is required. The processing cell and crane operating area are both exhausted through a filter system and stack by the building exhaust system. The Tank 1 purge compressors and building exhaust system are both powered from normal

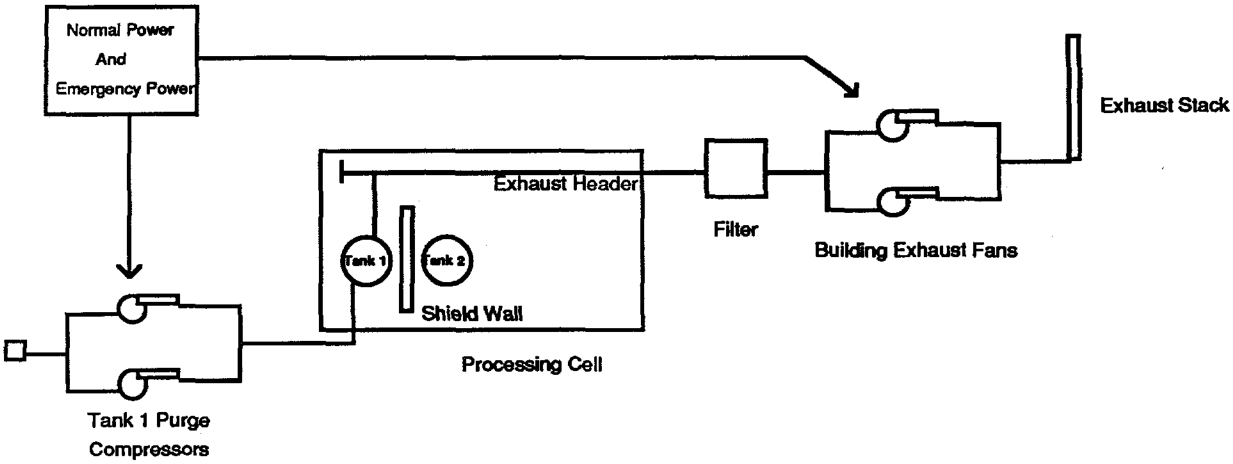

Figure 1: Schematic of Hypothetical Chemical Facility

power with emergency diesel backup, therefore both power sources must fail before either of these systems fail due to a loss of power.

Many accident progressions can be developed from the system described here. Each particular sequence may be quantified in terms of the source term expected and the frequency, or likelihood of occurrence. The magnitude and content of the source term will depend on the course of the accident and performance of the confinement system. Table 3 lists major interactions that are captured by the APET logic model.

Ultimately, thousands of source terms could result with complete quantification of the APET. This number typically is not treated in terms of analysis of consequences. Rather, accident sequences that have similar characteristics in terms of the chemical source terms to the environment are grouped or binned. Different characteristics (called dimensions) are used to bin source terms and characterize the accidents in terms of damage to the various vessels within the hypothetical chemical facility and the status of release and mitigation system barriers. Quantification software ensures that every accident progression sequence having "significance", viz., above a specified cutoff criterion, is assigned to a bin. It is the frequency of these bins that is reported as the result of the analysis at this stage.

These source term bins may be used to quantify the overall risk posed by operation of the chemical/nuclear facility. However, in support of the methodology outlined in this paper, the chief end product use is input to the source term predictor for emergency management.

Table 3.
APET Phenomenological Interactions: Illustrative Case - Nuclear/Chemical Facility

Initiator	Potential Outcome
Normal/Emergency Power Failure	-Tank 1 Purge System Failure -Building Exhaust System Failure
Random Failure of Components	-Tank 1 Purge System Failure -Building Exhaust System Failure
Ignition Source	-Tank 1 Explosion upon Tank 1 Purge System Failure
Tank 1 Explosion Failure	-Shield Wall Between Tank 1 and Tank 2 Failure - Cell Covers Above Processing Room to Dislodge & Fall
Damage from Tank 1 Explosion Collateral Events	Tank 2 Spill Unto Processing Cell Floor
Tank 1 Explosion	Vessel damage causing contents (benzene) to be Spilled unto Processing Cell Floor
Benzene Vapor Generation	Processing Cell Deflagration/Fire
Processing Cell Deflagration Not Followed By Fire	Crane Operating Area Deflagration and Potential Severe Building Damage

Quantification of the APET containing ~fifteen accident progression questions for the Tank 1/Tank 2 system shown in Figure 1 is illustrative. Four damage states are derived from the logic model showing various combinations of Tank 2 compromise with concurrent phenomena. Table 4 presents the facility damage description with an associated relative frequency index. The relative frequency is the frequency for the damage state in question relative to the frequency of Tank 2 failure without fire and deflagration. In this analysis, damage state 3 is the reference damage state, and is approximately the result obtained if one considered the Tank 2 situation using Table 1 definitions and the Part 68 prescription for "worst-case" scenario.

Several points may be made from the results of Table 4. First, additional states are possible with additional phenomenological features that may significantly change the manner of release to the environment. Energetic events such as tank fire and deflagration may lead to appreciable atmospheric releases within short times. Secondly, if it is assumed that the logic within the APET is self-consistent, then two of the three damage states (facility damage states 1 and 2) are not only more difficult to manage in an emergency environment, but are *more likely*. Finally, the APET methodology is observed to provide a basis from which facility operators and emergency management staff may *anticipate* classes of deleterious effects and introduce steps to protect both nearby workers at nearby facilities as well as the general public. If adequate monitoring capability is in place, the APET tool will allow interpretation of current and predicted facility status, thus providing a unique proactive accident management opportunity.

IV. REMAINING ELEMENTS TO ACHIEVE FULL MODEL

The two distinct benefits from applying risk-based logic models to assist chemical processing facilities in meeting consequence and emergency *response compliance objectives of Part 68 are:*

- Demonstration that worst-case and more probable sequences and associated phenomenology are identified more credibly than would be the case through the application of other known safety methods. It is shown that the binned facility damage classes can be tagged with a relative frequency from the logic model. This information can be used to prioritize plant modifications and/or procedure revision, as well as serve as a basis for the source term prediction.

- Illustration of an overall methodology as a basis for predicting and proactively responding to imminent chemical release conditions.

Table 4.
Damage State from Quantification of Tank 1 - Tank 2 System APET

Damage State	Damage Description	Relative Frequency
1	Tank 2 Splashed; Deflagration & Fire	5.9
2	Tank 2 Splashed; Deflagration, But No Fire	1.2
3*	Tank 2 Splashed; No Deflagration & No Fire	1.0*
4	Tank 2 Splashed; Fire, But No Deflagration	0.1
* Reference damage state		

The first benefit of the risk-based approach was illustrated through the Tank 1/Tank 2 analysis. The second one is heavily dependent on the integration of chemical process, facility, siting, and emergency response plan characteristics. In this section, the other elements that would demand attention before a real-time source term predictor is achieved are summarized.

Integration of a user-friendly PC interface with the other system components is required. For optimum flexibility, a Windows^{TM}-based platform using a knowledge-based decision analysis framework to model facility systems and accident progression is desirable. The development team for this model would address accident class definitions, chemical source term algorithm and link to the accident progression logic model. Output from the APET driver would be transferred into the source term predictor module. Binning and model development for the source term module are significant in themselves, and this discussion cannot adequately describe the full process in its entirety. Finally, one would need to perform a sanity check of the overall model by seeking to correlate or map postulated and potentially observable accident characteristics with the APET's accident classes. A more complete process description is provided elsewhere (McClure et al., 1995).

V. LIMITATIONS

The APET-based methodology is a supplemental tool rather than a standalone replacement for current emergency planning and response. The approach is applicable for facilities where

- processing operations are at a medium- to high-complexity level,
- several barriers or layers of defense exist between the hazard and potentially impacted populations such as facility workers and the public, thus leading to various combinations of success and/or failure regarding release of chemicals, and,
- environmental dispersion and ultimate consequences are difficult to assess because of topography, meteorological complexity, or population distributions.

The approach is dependent on the adequacy of existing safety analyses. If the licensing and operational bases are not robust, then the model too will yield few insights. It can also be time-intensive to develop even a simple prototype system. Thus single-barrier processes, such as isolated storage tank situations, do not warrant application of this methodology.

VI. CONCLUSIONS

A risk-based logic model can augment chemical process industry's compliance effort for meeting Part 68. Identification of worst-case release conditions and other more likely environmental source terms can be demonstrated with the methodology. The fully implemented model can be used as a prognostic tool available as a basis for invoking action levels before release actually begins. Application of the methodology is justified for complex chemical facilities in which several barriers exist or where emergency response options are difficult to select.

ACKNOWLEDGMENT

This abstract was prepared in connection with work done under Contract No. DE-AC09-89SR18035 with the U. S. Department of Energy. By acceptance of this paper, the publisher and/or recipient acknowledges the U.S. Government's right to retain a nonexclusive, royalty-free license in and to any copyright covering this paper, along with the right to reproduce and to authorize others to reproduce all or part of the copyrighted paper.

REFERENCES

Brandyberry, M.D., et al., *Application of Accident Progression Event Tree Technology to the Savannah River Site Defense Waste Processing Facility SAR Analysis*, Proceedings of PSAM-II, San Diego, CA (March 1994).

Griesmeyer, J.M., *A Reference Manual for the Event Progression Analysis Code (EVNTRE)*, NUREG/CR-5174, SAND88-1607, Sandia National Laboratories (September 1989).

Massey, W.M. and R.P. Taylor, *APET Methodology for Defense Waste Processing Facility Mode C Operation*, WSRC-TR-95-0113, Westinghouse Savannah River Company, Aiken, SC (April 1995).

McClure, P.R. et al., *A Decision-Oriented Source Term Estimator for Emergency Preparedness*, pp. 108-113, Proc. Fifth Topical Meeting on Emergency Preparedness and Response, (April 1995).

U. S. Environmental Protection Agency (EPA) Proposed Rule 40 CFR 68, *Risk Management Programs for Chemical Accidental Release Prevention*, Federal Register (FR Vol. 58, No. 201, pp. 54190-54219), (October 20, 1993).

U. S. Environmental Protection Agency (EPA) Supplemental Notice of Proposed Rulemaking (SNPR), (March 13, 1995).

U. S. Nuclear Regulatory Commission (USNRC), *Reactor Safety Study - An Assessment of Accient Risks in U.S. Commercial Nuclear Power Plants,* WASH-1400 (NUREG/75-014), (October, 1975).