CHEMICAL ENGINEERING TRANSACTIONS
VOL. 48, 2016
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.aidic.it/cet
Guest Editors: Eddy de Rademaeker, Peter Schmelzer

ISBN 978-88-95608-39-6; **ISSN** 2283-9216
DOI: 10.3303/CET1648031

Process Risk Assessment using Dynamic Simulation of Scenarios

Frank Markert*, Igor Kozine, Nijs Jan Duijm

Technical University of Denmark, Produktionstorvet 424, 2800 Kongens Lyngby, Denmark
fram@dtu.dk

Process plants may be very complex and may combine various processes in close proximity. Hence, the response to accidents may easily grow complex. Traditionally, after gathering and getting acquainted with the plant's technical information, risk is analysed in prescribed steps starting with hazard identification, description of accident scenarios and using the conventional approach to develop static event trees for events following a loss of containment. Modelling the impacts and consequences needs models to describe the release, dispersion and effect of the hazardous material, as well as models for predicting the egress time of people, response times of detectors and other safety equipment. A common assumption is the independence of these models and their sequential treatment, but often the consequences and effects are mutually dependent. The prediction of the consequences and effects are deterministic assignments applying simplified engineering models with averaged/expected values as input to account for the characteristics of the system, e.g. describing the physical and environmental phenomena and workers responses. The size of the release and dispersion depends on technical and environmental parameters. Ignition sources may be permanent or temporarily present at various locations near the release. The response times of detectors may be dependent on the velocity of cloud spread. The available save egression time depends on these parameters. Such dynamics are easily modelled using Discrete Event Simulation (DES) of the scenarios, which is a Monte Carlo type method.
The paper describes the application of DES to conduct the analysis part of a risk assessment that enables better time resolution in the modelling of the specific scenarios, simulate the interactions between concurrent chains of events under the hazardous scenarios, and produce probabilistic risk measures. The outcome provides possibilities to structure the results in a comprehensive way. Scenarios with severe consequences can be 'played back' to learn from them and can be animated, which apart from the learning effect provides a new way of validation.

1. Introduction

Process industries are a corner stone of our society producing the products we need in daily life. Hereunder, the processes may require handling and storage of various chemicals regulated under the Seveso directive. To ensure proper safety management including the fulfilment of regulatory requirements risk assessment is a common accepted method to predict the safety level of processes. Hereunder, application of event and fault trees are common and widely accepted tools. The basic purpose of risk analysis is the prediction of all the adverse states of the plant processes (e.g. Figure 1) to prevent or mitigate accidents. The risk analyst records and evaluates the events' probability, their consequences and final impacts. By nature, the occurrences of concurrent events that may be mutually dependent are defining a dynamic system, which may be better evaluated using a dynamic risk assessment approach. There is though some ambiguity using the term "dynamic risk assessment", as Hakobyan, Aldemir et al. (2008) found three different interpretations in the literature. These are:

1. Methods for periodic updates of an Probabilistic Risk Analysis (PRA) to address any changes in a plant configuration (see e.g. the review by Villa, Paltrinieri et al. (2015));
2. Updates to account for the aging of equipment; and

Please cite this article as: Markert F., Kozine I., Duijm N., 2016, Process risk assessment using dynamic simulation of scenarios, Chemical Engineering Transactions, 48, 181-186 DOI:10.3303/CET1648031

3. Approaches that include explicit deterministic modelling of dynamic processes combined with stochastic modelling to describe a systems evolution.

The third usage introduces time-dependent variables to describe the plants states when establishing the event trees. It is the last definition we refer to in the paper.
The objective of a Quantified Risk Assessment (QRA) is to evaluate on the installation's safety level, e.g. that people are not exposed to intolerable risk levels. This is achieved by identifying the most important events that contribute to risk and to ensure that the overall risk is effectively and efficiently reduced, which an accepted risk indicator measures. The widely accepted state-of-the-art risk assessment techniques use static methods to analyze the systems, as e.g. (static) fault trees and event trees. Time dependent input parameters are applied as averages over a period, as e.g. average failure rates over the installation's lifetime, average ignition probabilities, average numbers of workers and average escape route distances. This includes also weather data and the process conditions, e.g. using initial release data. These simplifications are not sufficient to avoid very complex event trees as an outcome. Moreover, they do not capture the dynamic nature of the system in a fully convenient manner, leading to conservative assumptions to avoid underestimation of the risks.

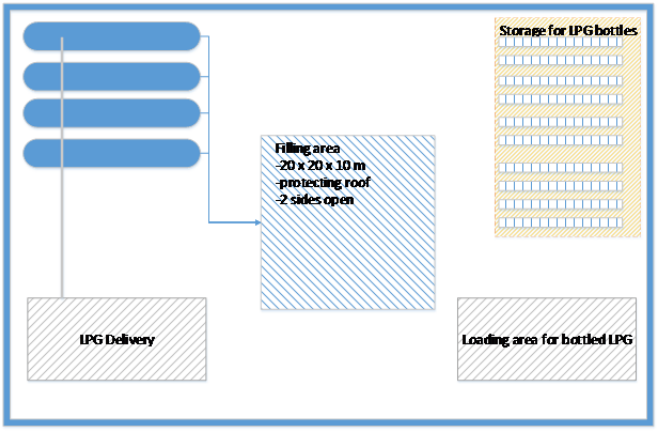

Figure 1: Layout of LPG filling facility

Therefore, concerns have been raised on the potential limitations of using static event and fault trees in the probabilistic risk assessments reviewed by Bucci, Kirschenbaum et al. 2008. The authors established a list of the major concerns which are cited in the following:
"1) Lack of time element in the ET/FT methodology to represent fault propagation through logic loops or possible dependence of the system failure modes on the exact timing of the component failures with respect to the changing magnitudes of the plant process variables.
2) Treatment of the coupling between the plant physical processes and triggered or stochastic events (e.g. valve openings, pump startups) which could lead to statistical dependence between failure events.
3) Semi-quantitatively modeling of the propagation of system disturbances through a classification of changes in the process variables […] which may lead to omission of some failure mechanisms due to inconsistencies in the definition of the allowed ranges for the process variables or due to possible significant changes in the system behavior arising from very small changes in the system parameters.
4) Possible sensitivity of the Top Event frequencies to stochastic changes in the system settings or process dynamics."
Decision making in risk management is often done within complex environments and it depends on validated computational simulation models. The developed easy-to-use modelling tools and the nowadays-powerful personal computers promote the use of such complex modelling and simulation as a standard tool for the reliability and risk engineer. Discrete Event Simulation (DES) models as described in this paper are a complementary alternative to the conventional static techniques described above (Kozine, Markert et al. 2009, Markert, Kozine 2012, Duijm, Kozine et al. 2013). DES models may capture the systems dynamics, i.e. the time dependence of occurring events and the development of the consequences. Static event trees that need to capture the fact that due to delays of e.g. ignition, there may be a range of alternative outcomes, become complex, and only a finite number of alternatives can be treated. By explicitly modelling the dynamic behavior, the event trees become simpler, because the time dependency is taken out of the event tree logic. The dynamic simulation will capture the fact that e.g. a later ignition causes a more severe explosion because the explosive cloud is explicitly simulated to have grown to a bigger size. Because the event trees are simpler, there plausibility is easier to be demonstrated, which also helps to produce verifiable risk assessments.

In the following, this is shown for a process unit. The model construction is explained and an example is given using an arbitrary process plant. The possibilities to analyze the individual results more detailed using statistical approaches and to establish a comprehensive transparent reporting are shown and discussed.

2. DES Simulation Model for Risk Assessment

Conducting a QRA for complex accident scenarios some simplifications are made as to regard events as classes of scenarios that can be treated in a homogeneous way. To calculate the total risk the combined outputs for these representative scenarios (the consequences and likelihood) may be mapped to a single parameter, the risk indicator. An example is the F-N curve describing the multifaceted aspect of "consequence" to a number of fatalities or financial damage in form of a cumulative probability distribution. Alternative ways of reporting the QRA output can be by using the concept of Individual Risk, the Location Based Risk or Fatal Accident Rate. Thus, a QRA applies a set of linked models describing possible events and their outcomes. The outcome of the QRA is determined through the models and the way they are linked.
The following approach is based on simulation of the dynamic interactions (see Figure 2 and 4) between concurrent phenomena following loss of containment using the example of an arbitrary LPG filling plant (Figure 1), specifically:

- The physical processes (outflow, dispersion, ignition, heat radiation, explosion)
- Detection, alarming and emergency shutdown
- Escape and evacuation
- Impact on persons, escalation and impairment of safety functions

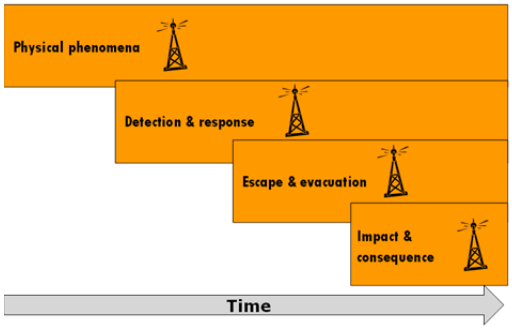

Figure 2: Time dependence

The simulation model as shown in Figure 3 runs repeatedly loss of containment scenarios to evaluate the associated stochastic events in time with random delays, durations, instances of occurrences and others. The output data sets are collected over all the simulated scenarios and are further processed to predict risk indicators as the Individual Fatality Risk (IR), the Potential Loss of Life (PLL), the Fatal Accident Rate (FAR, at workplace level), and the group risk (distribution of number of simultaneous fatalities).

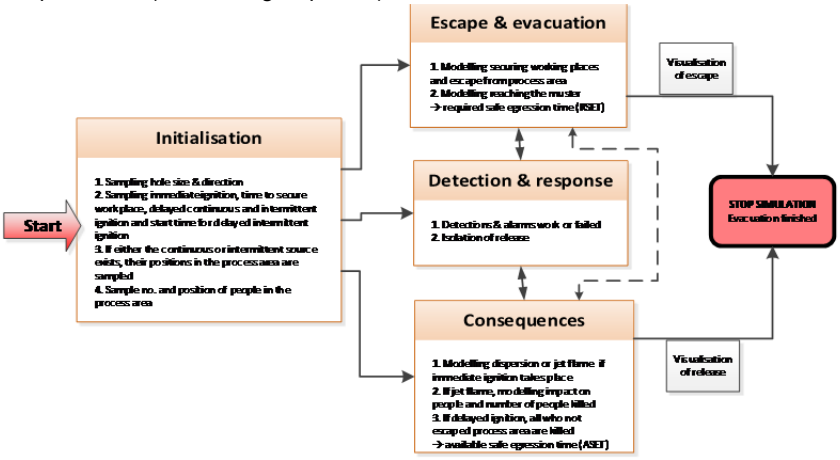

Figure 3: DES model logic

This way of tackling the problem allows capturing a great deal of specific characteristics of different workplaces, dynamic change of people's responses and other characteristics. Scenarios with severe consequences can be 'played back' to learn from them and can be animated, which except for the learning effect provides a new way of validation. This also makes the simulation models a good communication tool between system analysts and domain experts.

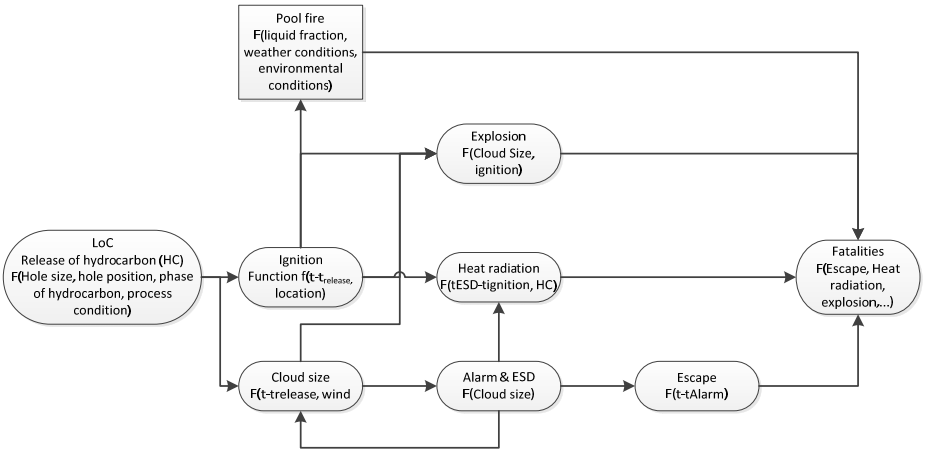

Figure 4: Indication of interdependencies used in the model.. The one's in the squared box are not yet implemented

3. Application of the DES modelling approach

An LPG filling facility is imagined, as shown in Figure 1. A LoC starts in the filling area that leads to a release of gaseous and flammable LPG, which is eventually ignited at a certain position due to permanent and/or temporary ignition sources located at chosen or random positions. The difference between the start of LoC and the ignition time is used to calculate the available safe egress time (ASET). After a short delay, a gas sensor located at a certain position may detect the gaseous release and an alarm is activated, if the gas sensor has no defect. The alarm triggers the start of the worker's evacuation procedure that includes time to secure the workplace and different distances to the muster area. This is calculated as the required safe egress time (RSET). The alarm could also trigger mitigation measures to minimize the consequences of the release, as e.g. shut down procedures, which is not implemented presently. In figure 4 some of these interdependencies are shown.

Table 1: Example output from the LPG simulation

No.	*Wind speed [m/s]*)	*Ventilation speed [m/s]*	*Hole diameter [m]*)	Mass flow [kg/s]	Ignition time [s]	ASET [s]	RSET [s]
22	5.0	0.8	0.049	9.3	0.6	0.5	250
45	*5.0*	*0.4*	*0.034*	*4.4*	*4.7*	*4.6*	*259*
172	16.7	2.5	0.001	0.005	>600	600	216
315	5.0	0.3	0.086	28.3	0.7	0.6	223
507	10.8	1.6	0.025	2.5	20.3	20	268
724	11.7	1.7	0.008	0.27	>600	600	251

The model is simulated 15000 times and a subset of the results are presented in Tabel 1. The simulation allows to record all the results and by that to make further detailed evaluation of the results. By setting minimum and maximum values of the parameters as in Table 2, no prior assumption has to be made on the worst case situation. All both minor, medium and large accidents are assessed and by using all the results the "worst case scenarious" can be re-found and reviewed. This is indicated for the related flammable volume development following a release in Figure 5 and the ratio of the ASET / RSET indicating safe or unsafe egression conditions in Figure 6. Also further general statistics can be elaborated as it is shown in Table 2.

Table 2: Statistics from LPG simulation. No of gas release simulations 15000. At any time, there are 1 to 5 workers present.

	Average	Std.dev.	Min.	Max.	Fractions as no of occurrences per all events				
Hole diameter [m]	0.012	0.027	0.001	0.20	0.66	0.18	0.13	0.02	0.01
					<5mm	5 - 10mm	10–100 mm	100 - 150mm	>150mm
Mass flow [kg/s]	3.432	15.6	0.004	154.7	0.67	0.19	0.10	0.04	0.01
					<0.1	0.1-1 kg/s	1-10 kg/s	10-100 kg/s	>100 kg/s
Ignition Time [s]	172.41	2.5481	0	600[2)]					
ASET [s]	482	6.321	0	600[2)]					
RSET [s]	235	25	0	304					
ASET/RSET	2.0	1.1	0	3.6	0.8	0.2			
					>1	<1			
Jet flame length [m]	9.8		1.3	88					
Fatalities [1)]	0.25		0	5					
Workers rescued [1)]	3.29		0	5					
workers in total [1)]	3.54		0	5					

[1)] per accident based on 53123 workers over all simulations [2)] The max. duration of the simulation is 600 s

The output is the accumulated number of fatalities and escaped people following each simulated accident. Based on these data the average number of fatalities per accident is assessed as the ratio in equation 1

$$E\left(N^{fatalities}\right) = \left(\sum_{i=1}^{N^{runs}} N_i^{fatalities}\right) / N^{runs} \quad (1)$$

Here N^{runs} is the number of simulated accidents (model runs) and $N_i^{fatalities}$ is the number of fatalities in each accident. $E\left(N^{fatalities}\right)$ may be interpreted as the average number of fatalities, if the number of simulated releases N^{runs} is large. $E\left(N^{fatalities}\right)$ multiplied by the frequency of a gas release gives the risk measure Individual Risk per Annum.

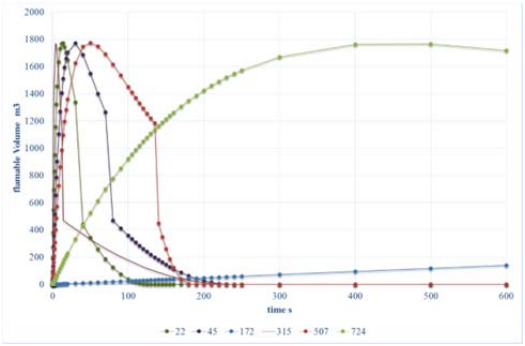

Figure 5: Time dependence of the flammable volume for different size releases

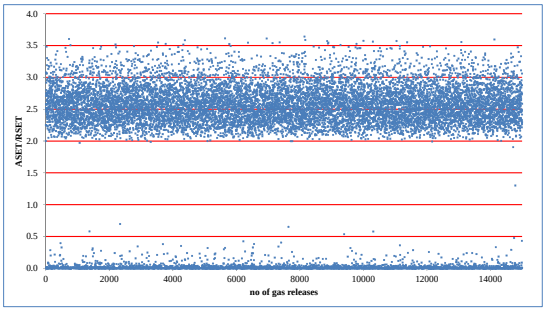

Figure 6: Ratio of ASET and RSET. Values above 1 indicate safe egress conditions.

The possible evaluation of all accident scenarios is assumed to help validating risk assessments. The calculation of high frequent, low consequence accidents may be compared to the plants accident statistics and the effect of additional safety barriers may be addressed. The possibility of animation of the scenarios provides a validation by field experts and improved communication to lay people.

4. Conclusions

One of the objectives of the paper is to describe a framework, which supports validation of risk assessments using a framework that describes subsequent and simultaneous processes during a loss-of-containment (LoC) event. The possibilities of Discrete Event Simulation are exploited by defining the framework as a few separate “event diagrams”. Each event diagram describes the sequence of events that are directly linked by causality as a function of time, while the events in separate event diagrams may occur in parallel. By that the diagrams form a set of dynamic event trees, allowing for interaction. Such a set of parallel event diagrams,

while each diagram is rather simple on its own, allows for a much larger variety of scenarios, than what can be obtained by building one static event tree that should capture all possible combinations (in time) of events.
The dynamic approach enables to combine several FT and ET within one analysis and to preserve the time delays between the sequences. Such variables are easily integrated into the modelling using a dynamic approach and by that many more scenarios are being modelled providing a better picture on the outcome of the overall scenario. These FT and ET are less complex and easier to overlook compared to the one's established in the static approach of risk assessment.
The discrete event simulation “simulates” release scenarios. This allows a demonstration of the correctness of the implementation and the trustworthiness of the logic diagrams. Single scenarios can be analyzed step by step, demonstrating the sequence of events in time. This will provide some evidence that the framework provides realistic and traceable outcomes. That is, we can find back to certain scenarios and study the values of all parameters, accidental events and their combination that have resulted in the observed consequences. Validation of the implementation of the framework can be performed by investigating the response of the software with special input sets and models, for which the output can be predicted analytically.
Each event diagram consists of a number of events that are linked by causal or probabilistic relations. More complex events (such as “jet dispersion”) require a separate (deterministic) model to describe the outcome of those events. The structure of the event diagrams with embedded events means that models can be developed individually for those events without too much concern about interactions between the events in the diagram. The framework of diagrams describes the relations between these models, and what requirements these models should fulfil in terms of input and output. These models can be selected and “plugged in” individually, according to the required level of detail or simplification.
Another advantage is the possible animation of the simulations that allows for validation of the models by field experts that may not be fully familiar with abstract disciplines as Boolean algebra, probability theory and consequence modelling. In that way field experts who very well understand the technological processes can interact in the development of the specific models, which improves validity and raises confidence about the outcome. This also makes the simulation models a good communication tool between system analysts and domain experts. This method leads to a transparent framework for modelling, which helps to demonstrate the correctness and appropriateness of models and assumptions.

Acknowledgments

The partial support of the work by DONG ENERGY A/S is gratefully acknowledged.

Reference

Bucci, P., Kirschenbaum, J., Mangan, L.A., Aldemir, T., Smith, C. and Wood, T., 2008. Construction of event-tree/fault-tree models from a Markov approach to dynamic system reliability. Reliability Engineering & System Safety, 93(11), pp. 1616-1627.

DUIJM, N.J., KOZINE, I.O. and MARKERT, F., Assessing risks on offshore platforms by dynamic simulation of accident scenarios, , 17 - 19/06/2013, Society for Risk Analysis - Europe (SRA-E).

Hakobyan, A., Aldemir, T., Denning, R., Dunagan, S., Kunsman, D., Rutt, B. and Catalyurek, U., 2008. Dynamic generation of accident progression event trees. Nuclear Engineering and Design, 238(12), pp. 3457-3467.

Kozine, I., Markert, F. and Alapetite, A., 2009. Discrete event simulation in support to hydrogen supply reliability. CEA.

Markert, F. and Kozine, I., 2012. Computer simulation for risk management: Hydrogen refueling stations and water supply of a large region. Curran Associates.

Villa, V., Paltrinieri, N. and Cozzani, V., 2015. Overview on Dynamic Approaches to Risk Management in Process Facilities. Chemical Engineering Transactions, 43, pp. 2497.