THE USE OF RISK ANALYSIS IN CONTINGENCY PLANNING

Jan F. Wright and K. Harald Drager
A/S Quasar Consultants
Harbitzalleen 12, 0275
Oslo, Norway

Abstract

The main functionalities of the Public Protection System (PPS) and Chemical and Radioactive Information System (CARIS) which are being developed in the European Eureka project MEMbrain will be described. PPS is a management decision support system that will serve several objectives, related to planning, training and real emergencies. Reliability theory and risk analysis should, in principle, be extremely important disciplines for emergency management to use and learn from, although they will never replace experiences from real life accident handling. However, the exchange of ideas between the theoretical field of reliability and risk analysis and practical emergency management is rather limited, and far from what it could be for the benefit of both sides. Some of the reasons why it is so are described, and remedies discussed. Finally, one way risk analysis could be done, and presented, for emergency management in a MEMbrain/PPS context is outlined.

1. Introduction

The European Eureka project MEMbrain /1/ are in the process of developing a computer based emergency management decision support system. The MEMbrain project includes different participating countries which shall develop national applications, all based on a common MEMbrain technological platform. The common platform shall contain modules that may be tailored to a given application in a much more cost efficient way compared to the case if each country should develop their own applications from 'scratch'. In general, the functionalities of the MEMbrain platform shall be able to:

- monitor hazards during nominal situations
- support contingency planning
- train emergency management and personnel
- display accident exposed areas on computerised maps
- support emergency management's decision making
- provide communication facilities to those involved in an emergency

The national applications range from man-made to natural disasters; from nuclear and chemical accidents to flooding and earth quakes.

2. The PPS and CARIS modules of MEMbrain

QUASAR's responsibility in the MEMbrain project is concerned with two work packages, the PPS (Public Protection System) and the CARIS (Chemical And Radioactive Information System). The PPS shall give advice on how best to protect people (public and rescue personnel) from the effects of an accident, e.g. how to avoid or reduce hazard exposure, or how to effectively evacuate an area. CARIS shall provide rapid access to information on hazardous materials (chemicals, radioactivity) and their properties related to flammability, solubility, dispersability, toxicity, etc. and the associated needs for protection and health consequences of different degrees of exposure. CARIS shall also provide source term information, which through dispersion calculations (another MEMbrain work package), will provide input to PPS. CARIS (together with other MEMbrain modules) will also be used on a daily basis in the surveillance and monitoring of hazard sources in an area. In this way, the operators will enhance and maintain their skills by applying the MEMbrain system for normal working day tasks. This will alleviate, but not eliminate, the need for training and emergency exercises.

In a real emergency situation, or in a simulated case for training purposes, accident information shall be presented on a digitised (computerised) map, based on a Geographical Information System (GIS) technology. Different GIS layers may then be used to represent information that are essential to emergency management, such as:

- The area of a toxic or flammable gas dispersed cloud, radiation levels, explosion impact zones, etc. - as reported, as monitored by remote sensing devices, or as simulated to predict a future status.
- The location of people to be assisted or rescued, in particular those with movement disabilities or other needs which require special assistance.
- The location of rescue means and protective equipment, as well as their availability and response times.
- Finally, storage tanks for chemicals, pipelines and other sources of hazard may also be displayed, information that are essential in the evaluation of possible, further accident development and in the selection of escape routes and evacuee destinations.

Information that are not GIS based, like databases over hazardous materials (chemicals, radioactivity, etc.) and their effects on life and environment, as well as knowledge concerning protection against these hazards will also be available from the PPS/CARIS system, either in a separate window or on another screen.

The PPS and CARIS modules will thus give emergency management and rescue personnel an immediate overview of the situation, as it is - and as it is likely to develop, and what the potential hazardous consequences might be.

3. Risk analysis - possibilities and limitations

Information related to the reliability and risk levels associated with systems is of high importance to emergency management. A 'system' may be a single chemical plant or a defined geographical region containing several sources of hazard. Reliability and risk analysis are dedicated to provide risk related information and are gaining in strength and acceptance by the scientific community as well as by (the high risk) industry. Such analyses are often called Probabilistic Risk Analysis (PRA) to emphasise the probabilistic or stochastic nature of the phenomena studied. PRA as a discipline is only a few decades old /2/ and is said to be the fastest growing profession beside the computer and environmental technologies. It started with the aim to improve the reliability of weapon systems during World War II. During the fifties and sixties, the type of consequences studied have been extended to also include safety and health (e.g. fatalities, casualties, injuries), and the term risk analysis was coined. The application areas of PRA's have gradually increased in number, and such studies are now used to:

- verify compliance to reliability, availability and safety criteria both during design and operations
- drive the design process
- provide input to preventive safety work
- assist in contingency planning
- provide information and support decisions during emergency operations

The order in which the list above is presented also reflects the extent to which PRA's have actually been adopted and used by society. An established practise in the Norwegian offshore oil sector is that the authorities require risk analyses to be conducted at different stages in the development of an oil field as part of the verification and approval process. PRA's have also increasingly been used by industry to improve design safety during the engineering phase. In recent years, PRA's conducted during the operational phase of an oil field have been used to improve the ongoing safety work. However, the use of methodologies and results of PRA in the preparation of emergency plans, or to support emergency management decisions, are the exception rather than the rule. One of the exceptions are related to the offshore safety regulations for the Norwegian Continental Shelf where findings from risk analyses may trigger specific contingency related actions required by the Norwegian Petroleum Directorate.

In principle, PRA methodology should be of great benefit to contingency planning, training and operations: Identification of hazardous conditions, how they may get out of control, as well as the effects upon people involved, are all elements which are treated in a PRA. So why are PRA's not used more frequently in contingency preparedness planning?

An answer may be that a PRA is conducted in a rather sophisticated way, and uses mathematics which many are unfamiliar with. In the modelling, Fault Tree Analysis (FTA) and Reliability block diagrams are often used. An FTA is used to analyse the causes of a hazardous event in such a way that a probabilistic calculation can be correctly performed. An outside observer would probably state that it was the concern of probability theory and mathematical convenience that have driven the development of FTA; the needs of those engaged in practical safety and emergency preparedness work were of less concern.

However, it is not the quantitative nature of PRA that is most important, although knowing the importance of accident causes is useful when mitigative actions are to be selected. Potential hazardous conditions and events that may trigger an accident - and what may make the situation better or worse - are of much more interest than the quantitative results as such.

Another reason for the lack of use of PRA's is related to the way accident causes and propagation of undesirable events are identified. The FTA model does not represent the dynamic nature of an accident development. FTA is a purely logical representation of the causes that may lead to a dangerous situation, developed from a global to a detailed view, or in a top-down approach. An FTA is thus a suitable instrument to detail causes until a level is reached where failure rates and repair times (quantitative data) may be identified and assigned to (basic) events. The procedure is such that one has to backtrace, starting from the effect (a dangerous event like e.g. gas leakage or tank rupture), and then identify possible causes. The starting point of the FTA, the dangerous situation (also called the top event) is then the starting point for the other main tool of PRA: the consequence or event tree analysis. The event tree is generated in the opposite fashion in comparison to the fault tree: by working in a forward time direction.

The consequence analysis is normally represented by a binary tree, where the edges are related to events significant for the accident to develop. An example may be useful at this point: if the top event is a Propane tank rupture, the first node may be represented by the question "immediately ignition?". From this point forward, two scenarios emerge. Then, for the 'unignited branch', the next significant event may be related to the possibility of a delayed ignition, and another two scenarios are created. This continues until all branching possibilities are exhausted. The event tree analysis can represent the dynamic aspect in that the sequence of events is essential to describe the accident tree scenarios, but it lags behind on the logical aspects compared to the FTA. For this reason, 'small' fault tree models are sometimes used to determine the branching probabilities of a consequence tree. However, this difference in how FTA and event trees are generated, and the fact that they must be interpreted differently, is confusing for outsiders. This leads to difficulties in understanding and using PRA results.

One rather serious deficiency of PRA is the lack of representation of problems related to operations, repair and maintenance tasks. Human Reliability, although considered as an area of high importance, is rarely given adequate treatment. Failure events related to such issues are often not considered at all, a fact that is rather peculiar as statistics show that a large majority of accidents are (partially) caused by human errors. And if human reliability is considered in a PRA, it is often treated in a rather superfluous way. A prominent example of this is when reliability engineers use the same approach in the modelling of man-machine redundancy as they use to model hardware redundancy /3/.

Finally, the (proper) identification of risk reducing measures, and the implementation of such measures will in general require a degree of experience beyond what the risk analysts are likely to posess. Unfortunately, risk analysts normally do not have experience in neither engineering design nor in operations and maintenance, as they usually are highly specialised statisticians or reliability engineers. If the practical 'touch' is lacking, it is understandable that result oriented safety and contingency personnel are sceptical to PRA's. Consequently, PRA's are not used to the extent that they could, or rather should be.

4. Improvements needed

Although there are a lot of aspects that should be improved, as indicated in the overview presented above, the focus here will be put on how traditional PRA methods should be simplified. One primary area of improvement is rather obvious: The propagation of events leading to an accident should be described in such a way that it can easily be understood by people from other professions. In other words, the fault tree - event tree approach should be abandoned in favour of a more direct, cause-consequence way of describing the events leading to an accident.

It is interesting to note that the analytical method preferred by most designers is FMEA (Failure Modes and Effects Analysis). In FMEA, the ways each component of a system may fail are identified, and the system consequences of the different failure modes evaluated. FMEA is directly related to the hardware parts of a system, i.e. to the very same components the design engineers are familiar with. An FMEA is thus a straight forward, cause-consequence based description, representing the sequence of failure events in an intuitive way. While fault tree analysis is conducted in a top down fashion, FMEA is a bottom up approach, where one starts from each possible way the component can fail, and then follows the consequences until the system is effected - or not affected. FMEA thus lends itself to a natural way of describing the propagation of events leading to an accident, but it is not very well suited to identify undesirable events which need two or more simultaneous causes to occur.

An FTA is, however, much better suited to represent combinations of causes than the FMEA approach. And as everyone knows, it is the unexpected combination of events that leads to the most serious accidents.

An initiative undertaken by the European Space Agency (ESA) to investigate the use of hazard and risk analysis in the design process, came up with an alternative that may combine the strengths of the FMEA and the FTA. The following 'Hazard Analysis Logic' /4/ may illustrate this:

The presence of	**Hazards**
in the	**system design, operation and environment**
is manifested in	**Hazardous Conditions**
which, dependent upon	**Initiator Events**
can cause	**Undesirable Events**
that combined with the	**Exposure Situation**
result in the	**Hazardous Consequence**

The ESA approach has been tested out on design reviews where safety engineers used this method to communicate safety problems to design engineers with considerable success. The main reason for the favourable reception of the method is probably related to its intuitive nature: it manages to combine a logical approach with the dynamic characteristics of accident propagation in a way that is both easy to understand and easy to apply.

5. Risk Analysis and MEMbrain

In MEMbrain, Risk Analysis will be used for at least three different purposes:

1. Evaluate a region to see if there is a need for a MEMbrain system
2. Generate scenario libraries to be used for contingency planning and training
3. Forecast probable scenario developments during an accident - partly based on scenarios from the library

For the first purpose, traditional PRA will be sufficient. But for the latter two cases, there is a definite need for an improved PRA along the lines discussed above.

The ESA Hazard Analysis Logics seems to be a suitable approach to structure the scenario descriptions to be used in the PPS module of MEMbrain. Several steps may be needed to form a complete description of the undesirable event path before an exposure situation occurs. Each step will then be the point where the scenario splits into two (or more) branches, like in the event tree descriptions. And one or more events or conditions may determine the probability of the alternative directions. In this way, the description will combine the sequential and the (Boolean) logical approach without separating the two as in the Fault Tree/Event Tree dichotomy.

To be of any use to emergency management, for planning purposes or in actual operations, the scenarios must be derived from a common starting condition. A set of scenarios, or a hazard tree, starts from the same hazardous condition, but results in different consequences depending on other events or conditions that happen along the accident path. In the MEMbrain/PPS context, the common starting condition compares to the onset of an accident, e.g. a rupture of a Propane tank. Now, if this situation has been analysed and translated to a hazard tree, the emergency management can display the tree and replay the future events of importance to investigate what may happen next, and what the probabilities are for the different alternatives. The information related to the events and conditions that may alter the direction of the accident path is of high importance to the accident fighting itself. Some of these events may be influenced by actions initiated by the emergency management, and the decision module in PPS will then be able to advice on action priorities, and what the effects on future options are. When a critical event proves true or false, meaning that it either happens or it does not happen, the hazard tree is simply updated.

This benefits of risk analysis, or rather hazard analysis, as described above, are evident when the time period from accident onset to the final consequences occur is sufficiently long. The approach may not be that suitable for rapidly developing accidents, although other MEMbrain properties related to e.g. availability and response times for rescue equipment may prove useful.

But for those accidents which develop more gradually and which can be influenced, a better use of risk analysis methods will be benficial. To achieve this, it is necessary to identify and analyse the hazardous conditions, using e.g. the scenario based approach described above, and to store the hazard trees in a database so that they can be immediately available to emergency management should an accident occur.

References

/1/ Yaron Shavit.
"Decision-Support Integration-Platform for Major Emergency Management (MEM)". SCS, Washington 1993

/2/ Henley, J.H and Kumamoto, H.
Probabilistic Risk Assessment. IEEE Press. N.Y. 1992. 568 p.

/3/ Aarset, M. & Wright, J.
"On modelling Human Reliability in Space Flights - Redundancy and Recovery Operations." 43rd Congress of the IAF. Washington 1992.

/4/ Preyssl, C. and Wright, K.
"Spaceflight Hazard Analysis - The Devil Hides In The Details." 44th Congress of the IAF. Graz. 1993.