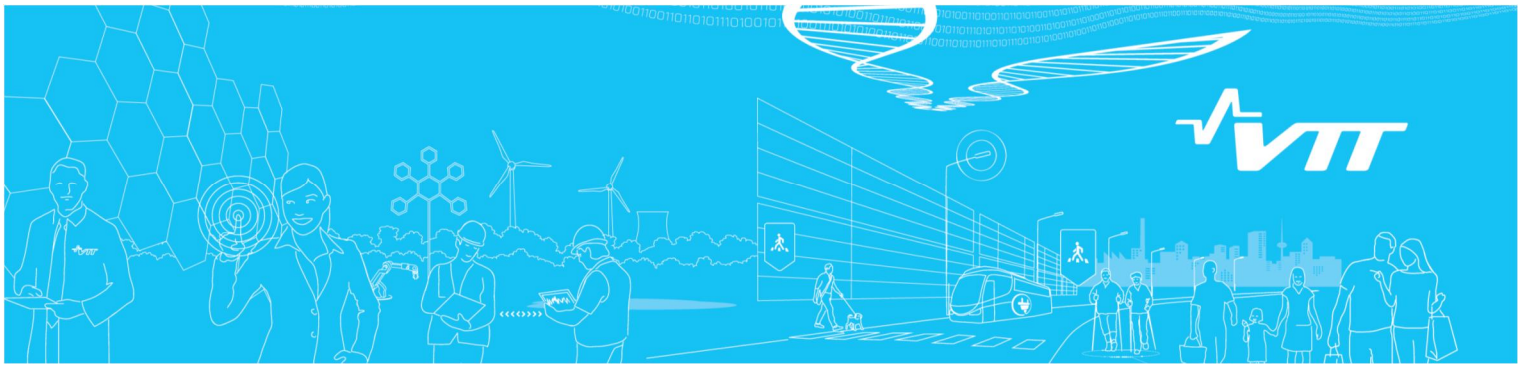


RESEARCH REPORT

VTT-R-01743-14

Modelling of prevention and emergency operations for probabilistic risk analysis

Authors: Ilkka Karanta

Confidentiality: Public

Report's title Modelling of prevention and emergency operations for probabilistic risk analysis	
Customer, contact person, address VYR	**Order reference** 28/2013SAF
Project name PRA developments and applications	**Project number/Short name** 77378 PRADA
Author(s) Ilkka Karanta	**Pages** 33
Keywords emergency operations, nuclear power plants, project management, activity networks	**Report identification code** VTT-R-01743-14

Summary

Prevention and emergency (P&E) operations are fast-response operations to prevent damage, mitigate its consequences, or recover from it. This report presents an approach to such activities based on methods presented in the project management literature, more particularly on activity networks.

There are many operations relevant to nuclear safety that may be considered as P&E operations, e.g. recovery from a loss of coolant accident (LOCA), construction of flood dams to prevent rising sea water from entering NPP facilities, and fire extinguishing. It is tedious to model such operations as a part of a probabilistic risk analysis (PRA) model, such as an event tree, and many simplifications may be needed. Modelling P&E operations separately allows their more explicit treatment. The results, such as success probability of the operation, may be integrated into the main PRA model in the manner that the results of human reliability analysis (HRA) are currently integrated.

Within project management research, many methods and formalisms have been developed to model and analyse schedule risks, and traditional PRA methods, coupled with project management models, can be used to analyse performance (quality of end product) risks. These are the main risks associated with P&E operations in the nuclear safety setting.

An illustrative example, the installation of booms to prevent oil spillage from entering NPP feedwater system, is presented.

Future research is needed e.g. on the modelling of plan changes, and on the modelling of schedule risks when resources available for the P&E operation are constrained. Practical experience in the risk analysis of P&E operations is also needed.

Confidentiality	Public

Espoo 15.8.2014

Written by	**Reviewed by**	**Accepted by**
Ilkka Karanta Senior scientist	Markus Porthin Senior scientist	Eila Lehmus Head of research area

VTT's contact address
Box 1000, 02044 VTT, Finland

Distribution (customer and VTT)
SAFIR2014 support group 8

Preface

This report is an initial attempt to improve the modelling and analysis of prevention and emergency activities for the purposes of probabilistic risk analysis (PRA). It was written in the PRADA project, which is a part of the SAFIR2014 research programme. The author thanks Ilkka Niemelä (STUK) for proposing many interesting targets of application (section 2.2.1), and Tommi Purho (Fortum) for supplying the case study (section 4).

Espoo 15.8.2014

Ilkka Karanta

Contents

1. Introduction

Prevention and emergency (P&E) operations, as considered in this report, are fast response operations for preventing adverse events from disturbing a system's operations or damaging its equipment or structures, for responding to and mitigating the consequences of adverse events, and for recovering from such events. Their time range varies from a few minutes to a few weeks. They are operations that involve more than one actor, more than one task to be completed, precedence relations between tasks, usually limited resources and a finite amount of time for completion. Such operations are almost ubiquitous in any developed society. Some examples are construction projects, product development in industry, fire extinguishing by a fire brigade and surgery in a hospital.

Prevention and emergency operations are common also in the normal operations and emergencies at any industry where safety is a concern, such as the nuclear, chemical and transportation industries. Some safety-relevant examples are fire extinquishing and its epilogue, complex repair and maintenance operations, and emergency and rescue operations.

This report's focus is in prevention and emergency operations relevant to the safety of nuclear power plants. Within it, the goals of prevention and emergency operations are to prevent production breaks and damage to utility, minimize damage, protect personnel and prevent a release of radioactive substances.

Prevention and emergency operations consists of work phases called activities. They interconnect with each other via precedence relations: e.g. the needed emergency personnel have to be first called onsite, and they have to equip themselves and arrive before they may take action. It is evident that the failure to complete the activity in time, or with sufficient quality, may be a major risk factor.

In probabilistic risk analysis (PRA), P&E activities are normally handled in event trees; however, an event tree is not a natural way of expressing a set of interdependent activities with uncertainties, and may grow too large if all alternative paths of action are taken into account. Thus, it would benefit PRA if a set of activities for achieving a certain goal (e.g. preventing rising sea level from causing damage) could be modelled and analyzed separately, and the result of this analysis – the probability that the goal is achieved – could be used in the PRA model. Then the event trees of the PRA model would be smaller and simpler, and the P&E operation could still be analysed in sufficient detail.

An assembly that consists of interlinked activities to achieve a given goal (from here on, called the end product) is called a project. It is therefore natural to think of prevention and emergency operations in terms of project management. Project management and the analysis of project risks is a respectable field where substantial developments have taken place during the last decades, with much vigorous research ongoing.

This report shows how to model and analyse P&E activities with the formalisms and methods of project management. P&E operations are represented by activity networks, with nodes representing activities and edges representing precedence constraints between activities. The report also contains the results of a literature survey on project risks.

2. Prevention and emergency operations and risk analysis

We consider the relation between P&E operations from two viewpoints. First we review the risk analysis of projects, with a view of applying the methods, formalisms and concepts of project management literature to P&E operations. Then, we consider the relation of P&E operations to probabilistic risk analysis, and consider what role models of P&E operations could play in PRA.

2.1 Risk analysis of projects

The analysis of risks in projects is quite well-established and widespread. In this section, we will consider the types of risks that are commonly analysed in projects, the sources that these risks might stem from, and methods used to analyse risks in projects.

In practical applications, the project risk analysis methods used are usually quite simple [3] – the most used qualitative techniques are personal and corporate experience, and engineering judgment, and the most used quantitative techniques are scenario analysis, estimation of expected monetary value, estimation of expected net present value, and break-even analysis. It seems also that simple risk analysis methods, based on decision analysis and simple Monte Carlo simulation, also have their place in project risk management [49]. However, here we consider somewhat more sophisticated methods, with a view of applicability in probabilistic risk analysis (PRA).

2.1.1 Types of risks

In project management literature, the following types of risks have been identified [55]:

- schedule risks. The main schedule risk is that the project will not be completed in time. In P&E operations, even provisional results might be crucial – for example, in the case of a fire, it is essential to both rescue humans and to extinguish the fire, and delays in either might yield serious results – and therefore the completion times of even individual activities might have great significance.

- quality risks (sometimes called performance risks). The risk here is that the end product of the project does not meet its specifications. For example, a constructed sandbag dam might leak, and thus water could enter critical parts of a site.

- cost risks. The risk here is that the costs of the operation are higher than expected, or exceed a given limit. In project management, this is a central risk, but it may have less significance in safety-critical P&E operations at nuclear power plants.

In addition, some sources [49] list also scope risks as a major risk category. The risk here is that the specifications of the end product are changed while the project is in progress. For example, it might be found out during an evacuation operation that some people cannot be safely evacuated at the moment, and so they would only be asked to move to a sufficiently safe location in the evacuated area. Another example is that the emergency situation is initially diagnosed wrongly, and therefore misguided actions are undertaken. It seems that scope risks are more typical of long-running projects, and are related to the decision making of executives and stake-holders, and therefore they have relatively little relevance to probabilistic risk analysis. They will not be elaborated more here.

From a planning point of view – and also to some extent, from an analysis point of view – these risks are interconnected. Striving for quality may easily lead to failing schedules and cost overrun; similarly, striving for tight schedules may lead to compromises in

quality and high costs, and minimizing costs may lead to tardiness in schedules and lowered quality.

2.1.2 Sources of risks

Risks to P&E operations stem from many sources, such as

- resources. Some resources might become unusable during the project, due to e.g. equipment failure, humans falling sick, accidents etc. It is also sometimes uncertain whether the resources at hand are sufficient to accomplish the stated objectives within the given timeframe.

- human errors.The analysis of human errors, and more generally, human reliability analysis [51], is a prominent field within risk analysis, and its methods and results may be used also in the analysis of risks in P&E operations.

- management decisions. The management may make e.g. decisions that allocate the available resources non-optimally, or lead to the neglect of a crucial part of the system. In a broad sense, wrong decisions are human errors, but they differ both in the nature of decisions and in the scope of consequences.

- external events. These include bad weather, other natural phenomena, traffic accidents that e.g. prevent the fire squad from arriving by blocking a road, and so on. The typology of external events given in [32] may be used as a basis, but there seems to be a need for extending that typology to cover all significant types of external events that cause risk to P&E operations. It is to be noted that many initiating events leading to P&E operations are external events, and then adverse external conditions are to be expected during the P&E operation.

- mischief, sabotage and terrorism. These could obviously cause serious risks to P&E operations, even jeopardizing their completion. However, they will not be further elaborated here, because they are generally not included in the risk analyses of nuclear power plants.

- contracts. This is a major source of risk in ordinary projects (e.g. construction or product development). In the kinds of P&E operations considered in this paper, contracts do not generally play a central role. However, when there are several parties that participate in an operation – perhaps a local fire squad and plant personnel – an unclear and ambiguous contract between the parties might lead each to believe that some important task in the operation is the other party's responsibility.

2.1.3 Analysis of schedule risks

The most well-known methods of analyzing schedules, and also schedule risk, in projects are program evaluation and review technique (PERT) and critical path method (CPM), which are often used together. Indeed, these methods have made their way to undergraduate textbooks [29][30] and practical guidebooks [40] in the field. PERT is based on constructing an activity network model of the project, and then analyzing the earliest start times and end times of activities, from which slacks (differences between minimal and maximal start times and end times, so that the project will still meet its schedule) can be computed. CPM is an algorithm for computing the critical path, or path in the activity network in which delays in activities cause delay of project completion. The details of PERT and CPM are covered in most project management textbooks, and in many operations research textbooks, and will not be covered here.

From project schedule risk point of view, the main drawback of PERT and CPM is that they don't cover all the paths from project start to project completion in the activity network. However, in the general case any such path may in principle become a critical path (delaying the completion of the project), or at least we cannot a priori neglect that possibility. Therefore PERT and CPM cannot be used in assessing project schedule risk in the general case.

The analysis of project completion times has received some attention in the literature. [24] presents an analytic algorithm for the exact computation of the probability distribution of the project completion time in stochastic networks, where the activity durations are mutually independent and continuously distributed random variables. It seems that no assumptions need be made about the probability distribution of an activity's completion time. The computational efficiency of the algorithm is unknown, and needs further analysis. [7] presents an approach based on computing all the paths from the activity network's start node to its end node, and then determining the longest path either by computing it by scenario or by formulating the maximal path finding as a mixed integer programming model and solving it. A drawback of the method is that it assumes discrete probability distributions, which are not a natural presentation for time distributions. [58] presents an approach that may assume any probability distribution on activity durations, and computes the probability distribution by Monte Carlo simulation. The computational load of the simulation is reduced by replacing the calculation of the maximum of the paths in the activity network by an approximation, and reducing the error caused by the approximation by a simple heuristic rule. The computational load is still rather big for large activity networks. Also [50] presents an approach based on simulation, using importance sampling techniques. [48] presents an approach for computing the exact overall duration of a project, when task durations have independent distributions; the method seems to be efficient, but the probability density functions of activities are limited to a special form, and the approach is based on the activity-on-arc network approach which has its own limitations. Other approaches to finding the probability distribution of project completion time include e.g. [11] and [45].

There is some research on the derivation of exact bounds on project completion times, usually based on analytic methods. One would naturally assume that such methods are not needed because methods for the calculation of completion time distribution exist, and this distribution contains also all the information that the bounds do. However, the matter is not quite as simple: methods for computing the probability distributions of completion time are either limited to special cases or require heavy computational resources especially with large projects. Therefore methods that derive exact bounds are valuable especially if risk analysis is to be done interactively, or if the project (operation) to be analysed is very complex. Some examples of methods for computing exact bounds on project completion time include [15][25][37].

An alternative to trying to figure out a probability distribution (or bounds) for project completion tardiness is to predict the probability that the project does not meet its completion time limit. This approach is taken by [38] and [43], who both use a Bayesian belief network for estimating this probability. Their approach is as follows: identify risks with the help of experts (and literature), construct the network, obtain the probabilities needed from experts, and test the model ([43] using sensitivity analysis, [38] by two case studies). The main drawback of this approach is materialized when the focus of analysis is not on the probability that a currently set deadline is not met – the deadline is often arbitrary anyway – but rather more generally on the probability distribution of the completion time; in this quite ordinary situation, the approach cannot be used.

All the methods described above are for activity networks with no resource constraints. It seems that there is little work done on the practically relevant case when there are resource constraints. The existing approaches seem to be based on simulation ([56] p. 99, [52]), with the exception of [36], who develop a Markovian model for the project assuming independent and exponentially distributed activity durations. However, there are difficulties in modelling the completion time distribution of resource-constrained activity networks, even on the

conceptual level. For example, it is not clear what resource allocation should be used in analysing the project completion time distribution; one choice would be to use the optimal resource allocations, but then 1) the optimal resource allocations would have to be computed for each combination of activity duration times considered, 2) there would still be no method of accounting for resource risks, and 3) it is not at all clear that an optimal resource allocation would be followed or even known in a practical situation. Therefore, more research on the schedule risks of resource-constrained projects is needed.

2.1.4 Analysis of performance risks

Although project success (from various viewpoints) has been subject to extensive research [27], there is relatively little literature on performance risk modelling and analysis [55]. This is remarkable, because Morris [41] claims (with a literature list to back up his point) that "research has shown time and again, projects fail because the technical content of the program is not controlled strictly enough or early enough." The few references found don't seem to be particularly suited for modelling P&E operations: [8] uses a complex matrix method to derive the probability distribution function of cost and the probability of achieving goals; however, the modelling of goal achievement is left largely to the reader's responsibility. [22] propose, in the context of evaluating research and development projects, a model that combines the probability density functions of "technological advancement", time and cost; here, too, the modelling of technological advancement is left largely to the reader. [34] use failure modes, effects and criticality analysis (FMECA) to assess the reliability of a disaster relief supply chain in trying to efficiently and effectlively reach the intended victims; however, the analysis is only qualitative.

Since the literature on this topic is so scarce, a method for modelling and analysing performance risks of P&E operations is outlined in the following. The method is based on established methods of probabilistic risk analysis, and therefore it should be easily implementable as a part of PRA.

Performance risks can be modelled and analysed in an activity network in the following way. First, a reliability model – for example, a block diagram – of the end product is constructed. The purpose of this reliability model is to represent the quality specifications that the end product must meet. Time-related aspects of the specifications – e.g. that some people must be evacuated within 3 hours from alarm – may be handled as schedule risks, and may thus be excluded from the analysis of performance risk. Then, the activities are identified that contribute to the probabilities in this reliability model. This may be done by, for example, constructing a fault tree for each specification, where the basic events of the fault tree are quality-related failures of activities in the activity network. Quality-related failure probabilities are estimated for these activities, and these are used in the reliability model to calculate the probability that the end product does not meet its specifications. The estimation of the individual quality failure probabilities in the individual activities is not simple, because several factors – for example, the resources available, schedule constraints, contextual factors (e.g. night time, poor weather, stress) might affect them.

The procedure outlined above for identifying and estimating performance risks is just a conceptual sketch created for this document, and has not been tested.

2.1.5 Analysis of cost and economic risks

The computation of the total cost as a probabilistic sum of cost-elements is well-established. Indeed, the calculation of this sum is often termed 'risk analysis' in the financial field. Assessment of cost risks is much easier than assessment of schedule risks or performance risks, because the cost-elements are additive: the total cost is always the sum of partial costs.

In the financial sector, risk analysis is usually conducted by running Monte Carlo on a spreadsheet [12][53]. The starting point in the context of project risks is usually the work breakdown structure, whose elements are assigned probability distributions regarding costs; often, a cost breakdown structure, separate but close to the work breakdown structure, is developed. Dependences between cost elements are often handled by simple correlation structures.

Sometimes there is also considerable uncertainty about the benefits of the project. Then, the analysis should incorporate also the future profits brought about by the project. Instead of a probability distribution of costs, a probability distribution of e.g. the net present value of the project is sought [19].

Also more sophisticated methods have been developed for analysing cost risks in projects (see [56] for references).

2.2 Models of prevention and emergency operations as a part of probabilistic risk analysis

It is evident that the analysis of P&E operations has relevance to practical applications in and of itself. However, within the nuclear industry a major source of interest in the modelling and analysis of P&E operations is in the role they can have within PRA. Another connection of interest is the role that traditional PRA models can play in the analysis of P&E operations, and the requirements that the PRA context sets to P&E models.

It seems that modelling and analysis of P&E operations has not received much attention within PRA. Of the major textbooks, only [4] handles project risks, and these too in a context more fit for analysing e.g. construction projects than the kinds of activities that are related to risk prevention, accident management and consequence mitigation. In the context of fire research, Hostikka, Kling and others [23][31] have developed a Monte Carlo simulation model for predicting the probability that a fire produces damage before it is extinguished. The model is a simulation model consisting of two timelines, one for the fire and one for the fire brigade trying to extinguish the fire after it has been detected. The activities of the fire brigade are represented as a flow diagram that might be seen as an activity network (though Hostikka et al. don't present it as such). Each activity of the fire brigade has a time delay associated with it; the delay consists of the time it takes to perform the activity, and another delay that is added to the first delay if the activity doesn't go as planned. The model has some resemblance to the schedule risk models proposed in this report on the conceptual level: activities cause time delays, and the delays are propagated in a network; however, the model of Hostikka et al is not a project model, and they do not consider performance risks.

However, models of P&E operations do have a natural role and function in probabilistic risk analysis. In this section, we will consider some examples of PRA-relevant operations that could be modelled as P&E operations, how to integrate the models and analyses of P&E operations as a part of PRA, and some special requirements that PRA-relevant operations pose to such models (as opposed to ordinary projects such as construction projects).

2.2.1 The role and use of prevention and emergency operations models in PRA

In a broad sense, all activities to prevent, mitigate or recover from initiating events, or manage accidents, are P&E operations in the sense described in this report. Also other activities, such as maintenance work, may be modelled as P&E operations, and their risk contribution thus analysed. Therefore, the scope of P&E operations models is quite wide in PRA.

Currently, it seems that P&E operations are modelled either within the main PRA model (event tree or fault tree), or as a part of human reliability assessment (HRA). Modelling P&E operations as a part of the main model is problematic, because the complexity of the

operations cannot be represented accurately in a fault or event tree, and for example complicated timing considerations have to be modelled separately anyway. Modelling P&E operations as part of HRA is also problematic, because P&E operations have many aspects that HRA doesn't address such as systemic schedule risks and resource allocation issues.

A better approach to taking P&E operations into account in PRA is to model the P&E operations separately, and integrate the results back to a PRA model (e.g. a fault or event tree) by providing success probability or timing information from the P&E operation's model. This is similar to the use of HRA analyses in PRA. Modelling activities separately in P&E operations models provides several benefits to PRA:

- activities are modelled in a formalism that has been developed for the analysis of projects. Thus the models provide a natural and easy-to-understand description of the activities and their interconnections.
- methods and algorithms developed in the last 60 years within project management research can be utilized in analysing the models, providing efficient computation.
- the complexity of P&E operations is isolated from the PRA model, simplifying its presentation. This may result in a large reduction to the size of e.g. an event tree.

There are numerous examples of potential applications within the PRA of nuclear power plants:

- accident prevention operations, such as construction of flood dams from sandbags when the sea level is rising
- consequence mitigation operations such as pumping of coolant to a damaged core
- recovery operations such as recovery from a loss of coolant accident (LOCA)
- safety measures such as evacuation of personnel
- emergency operations such as fire extinguishing and its epilogue
- maintenance operations from the point of view of their contribution to safety and availability

Thus it seems that the modelling and analysis methods of project management have many important practical applications within PRA. However, those methods have been developed for purposes different from those of PRA, and therefore project management models seem to lack many central PRA concepts such as importance measures and uncertainty analysis (though some related items such as sensitivity analysis have been developed and used also in project management literature). It seems, though, that measures analogous to PRA importance measures, and analyses analogous to uncertainty analyses, can be developed for activity networks.

2.2.2 The role of PRA in analysing prevention and emergency operations

Methods commonly used in PRA have also been used to analyse project risks. These include fault and event trees [9][10], HAZOP [10] and FMEA [10], and influence diagrams [9]. However, it seems that their use isn't widespread in project management, and the few public applications seem all to use risk analysis methods in a qualitative manner. [14] uses event trees as a part of a systems analysis as a part of a risk analysis model for programs consisting of projects. They also assess the probability of technical failures (the end product of a project fails to perform as expected, i.e. a performance risk).

2.2.3 Special features of prevention and emergency operations from modelling and analysis point of view

P&E operations have many features not present in ordinary projects. They often happen as a response to external events; therefore, although the operation itself may be preplanned, its timing and details are not necessarily. Furthermore, the operations often have high stakes and time pressure – for example, in the case of Fukushima, there was 50-60 hours of time to start pumping cooling water to reactors before core damage.

The following is a list of features that have to be taken into account in many P&E operations:

- they may contain significant amount of improvisation, situation-specific decisions, adaptation to fast-changing situations and change of plans. This is so because they are often responses to surprising external events; even in the case that plans had been made in advance, these plans may turn out to be inadequate in the response to the specific situation. Modelling such decisions may take different routes. E.g., there might be alternative methods of executing an action, from which one is chosen; there might be conditional actions that are executed only if their predonditions apply; and so on.

- their time scales are often short: an operation may have to be carried out in hours or even minutes, whereas in ordinary projects the time scale is weeks, months, or even years.Thus, schedule is a bigger issue in P&E operations than in ordinary projects. In some P&E operations, failing to meet a deadline means that the performance criteria of the operation's end product will not be satisfied; an example of this is pumping coolant to the reactor core in a LOCA.

- resources are limited. Well-trained emergency workers, NPP operators etc. may turn out to be a scarce resource when rapid actions in different parts of a large system are called for. Also special equipment, materials etc. may turn out to be scarce when quick response is needed and there is no time to transport equipment from a distance.

- there are risks in the emergency work itself. These risks, for example accident risks, may contribute not only to deterioration of safety, but also to all major forms of project risks – schedule, cost and performance risks.

- high uncertainty may be associated both with individual activities and with the whole P&E operation. No statistical data exists on many P&E operations, because there has been so far no need to carry them out in practice. Furthermore, there is inherent uncertainty related both to the context (e.g. phenomenological uncertainties in level 2 PSA), and the operation itself (e.g. human factors).

In addition to these special features, P&E operations often have safety aspects that are not present in ordinary projects.

3. Modelling and analysis of prevention and emergency operations

In this section we present some groundwork and requirements for risk analysis models of P&E operations, together with a process description of the modelling process, these constitute a framework for modelling and analysis of P&E operations. The basic assumption underlying the framework is that P&E operations are treated as projects, and presented by activity networks (or suitably extended activity networks).

3.1 Risk analysis using activity networks

As we saw in section 2.1, activity networks are used in analysing schedule risks and may be used in analysing performance and cost risks. Here we will consider how risk analysis fits in the overall modelling and analysis process of P&E operations.

The modelling and analysis process of P&E operations is presented schematically in Figure 1. The central outcomes of the process are the activity network, a schedule consisting of start and end times of activities, resource allocation to activities and as a function of time, and the results of risk and uncertainty analyses.

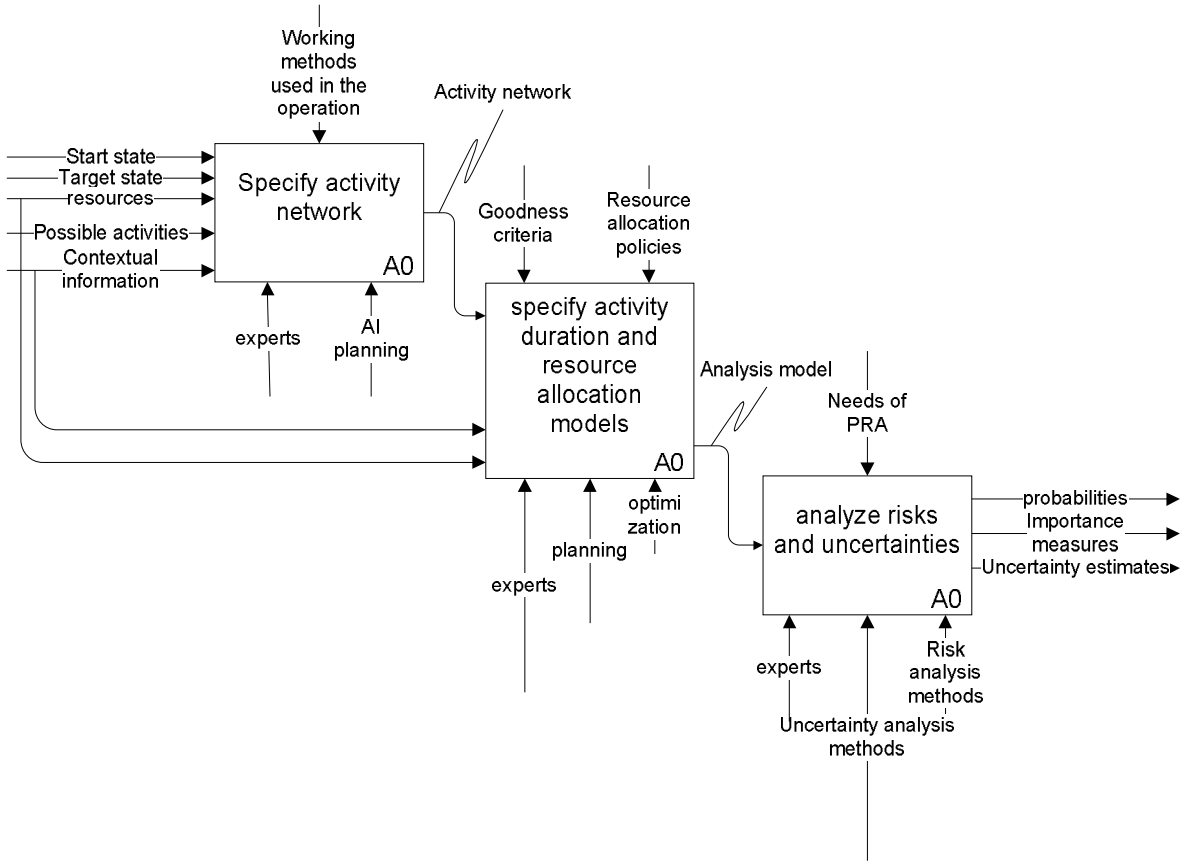


Figure 1. The process of risk analysis with activity networks

The first phase of the process is the specification of an activity network model. This covers the activities to be executed and their interdependences. It takes as inputs a start state (the state of the world at the beginning of the operation), a target state (what things should be true at the completion of the operation), available resources, possible activities (from which the activities to be performed are selected), and contextual information. Here contextual information means any other information relevant in the model, such as weather conditions, distances, performance figures of equipment used etc. Activity network specification is guided by working methods commonly used in the intended operation. The actual specification is usually done by experts, but it may be automatized using e.g. methods of artificial intelligence planning [18].

The second phase is the specification of activity duration and resource allocation models. These must be done together, because resource allocation affects activity durations. Probability distributions of the duration times of different activities have to be specified; possibly, when there are significant dependences between activity durations, the durations must be described as a multivariate distribution. The use of resources may be presented as

fixed resource allocations, rules describing resource allocation in a given situation, or a mathematical model. This phase assumes the activity network as its input, as well as available resources and contextual information. It is guided by goodness criteria of resource allocation, and resource allocation policies (rules or guidelines governing resource allocation, or empirical knowledge about how the resources would be allocated in a given P&E operation). Construction of these models may be done by experts; alternatively, optimization methods or artificial intelligence planning methods may be used in arriving at a resource allocation for the operation. The main outcomes of this phase are a probability model of time durations, and a resource allocation model.

The final phase of the process is risk and uncertainty analysis. It takes the probability and resource allocation models as inputs, and may use some contextual information such as uncertainty associated with weather factors. It is guided by the needs of the risk analysis. It is performed by experts, using risk analysis and uncertainty analysis methods. The outcomes include performance failure probabilities, probability distributions for operation completion time (and perhaps time distributions for some milestones or significant activities as well), importance measures of various activities or resources, and uncertainty analysis results.

The process outlined above is only indicative; in practice, it may turn out that for example activity network construction and resource allocation are so intermingled that they have to be done together.

3.2 Elements of an activity network model for prevention and emergency operations

Activity networks (precedence networks, activity nets) are the most important formalism for representing dependencies between tasks within a project. Not only is it the representation formalism on which both PERT and CPM (see section 2.1.3), the most important project schedule risk analysis methods within project management. It is also described in project management textbooks [30], and even given a separate subchapter in a handbook of discrete mathematics [47]. Activity networks consist of activities (often called tasks) and relations between them.

There are two kinds of activity networks. In activity-on-arc (AOA) networks, the activities are represented by the arcs in the network, and nodes represent events. In activity-on-node (AON) networks, activities are represented by nodes in the network, and the arcs describe precedence relations between tasks. AON networks are easier to explain and are more readily understood by nontechnical users, and most (if not all) project management software programs use the AON formalism. On the downside, the description of AON must include a list of tasks and each of their immediate predecessors. On the other hand, PERT and CPM initially used AOA networks, so there are historical reasons for using the AOA formalism; furthermore, the description of an AOA network consist of the tasks with their respective starting and ending event numbers (one starting and one ending event per task). This report deals with AON networks.

In the following, the central elements of an activity network model are described. The intent here is to describe a general model that can be used in most situations; in special cases, some elements (such as resources) may be left out of the model.

3.2.1 Activities

An activity is a single workphase or task of the P&E operation. It is an element that will not be further divided into smaller parts in the model (although it often could). The scope of an activity depends on the desired granularity of the model. In a detailed study, for example the repair of a machine may be split into several individual tasks, whereas in a more granular model the repair may be considered as a single activity. Granularity may also vary, so that

more critical activities are modelled in more detail, and peripheral tasks on a more granular level. The choice of granularity level is one of the central choices in P&E operations modelling.

Suppose that the P&E operation consists of *n* activities. All the activities in the operation can be listed as $V = \{A_0, A_1, \ldots, A_n, A_{n+1}\}$. The ordinary convention (see, e.g., [1]) is that A_0 is the start activity (the activity marking the start of the operation), and A_{n+1} is the end activity (the activity marking the end of the operation). The start activity and the end activity have neither a time duration nor contents related to activity or resource use; for this reason, they are sometimes called dummy activities. Start and end activities are not necessary in the model, but they simplify certain analyses and make visualization easier. The set of the proper activities of the project are denoted by $\mathrm{A} = \{A_1, \ldots, A_n\}$.

From the modelling point of view, an activity is an entity that will not be split into smaller parts. An activity has a start time S_j and an end time C_j which are central variables in the scheduling of the operation. Additionally, it is handy to denote the duration of an activity with its own variable D_j, and then naturally

$$D_j = C_j - S_j \tag{1}$$

The duration is assigned a probabilistic distribution. Some commonly used distributions are

- the lognormal distribution, often used as a model for repair time distribution [46]. Some distributions alternative to the lognormal distribution are Pearson type 5 distribution, log-logistic distribution, the gamma distribution, Johnson S_B ja Johnson S_v [35]
- the Weibull distribution, or its special case, the exponential distribution
- the normal distribution
- the beta distribution. Also other distributions with bounded support (i.e. all probability mass is concentrated on a finite length of time) may be used [26][28][33].

Failures of technical and other systems may affect the duration of an activity. For example, the transport of materials may be delayed because the allocated truck is broken; in this case, the transport activity is delayed until it is repaired or another truck comes to execute the activity. Typically, these kinds of failures result in a finite mixture distribution [39]: with probability p (the failure probability), the duration obeys a given continuous distribution, and with duration (1-p) (the success probability) the duration obeys another continuous distribution.

Besides duration, also other variables connected to an activity may be uncertain. One is the success probability of the activity. To determine this probability, one must first specify conditions under which the activity may be considered failed – otherwise, the activity might continue forever, and success probability (or failure probability) wouldn't be well-defined. One such condition might be activity duration: when the activity has taken more than a certain preset amount of time, it may be considered failed. More generally, the failure of an activity may be defined as a clause in predicate logic, when the elementary events associated with it have been given probabilities. Also the availabilities of resources needed in the activity may be random variables.

Some activities may be executed in several ways, called modes [6]. The set of modes that are feasible in executing activity A_j is denoted by M_j. For example, the removal of cut stock from a road may be done by men dragging the logs, by using a winch attached to a vehicle,

or by using a lifting apparatus, among other means. Different modes presume different resources (e.g. shovels or an excavator). Furthermore, the consumption of even similar resources may vary between modes: for example, the clearing of a road may be done by a team of 4 persons in some mode, or by 40 persons in another mode. The duration of an activity depends on its mode: e.g. clearing of road probably goes faster with lifting equipment than by hand. The mode of an activity may change during the activity, which should be reflected in its duration time distribution.

Each activity has, associated with it, a list of resources (see section 3.2.2) needed to complete it. The use of resources depends on the mode of the activity. For example, digging of a ditch may be performed in two modes: digging by shovels or digging by an excavator; further modes may result from using e.g. two or four men in digging by shovels etc.

The start time of an activity A_j usually depends on the status of some other activities, which are called its predecessors (see section 3.2.4).

If the spatial dimension of an activity is of importance, the activity may be assigned a location. This location can then be used for example in the calculation of transfer times between activities (e.g. the persons completing activity A_j may need to be transferred to start activity A_k in another location). Some activities, such as transport activities, do not have a location, but they may be assigned start and end locations. The necessary location information consists of the locations of resources, locations of activities, network models representing the road and similar networks, and possibly some auxiliary information (e.g. maximum possible speed in a road segment). This information may be used in calculating transfer times, and is reflected in schedules and resource allocation.

At each time instance, only a certain set of activities is ongoing. This set may be denoted by $\mathrm{A}(t) = \{A_i \in \mathrm{A} \,|\, S_i \le t < C_i\}$.

3.2.1.1 Transfer and preparation activities

There are two types of activities that occur in many P&E operations. Moreover, the completion times – probabilistic or deterministic – depend on the kinds of activities that precede them and succeed them. These activities are related to the transfer of resources from a location to another location, and preparation of the activity in the new location.

If the spatial dimension is important, it may be useful to describe the location of each resource as a function of time. In the beginning of the operation, each resource has a given location (e.g. vehicles at a depot, construction workers in their homes or at a place of assembly). After this, the location changes to the location of the activity it is used in.

When a resource changes from an activity to another activity, it takes a time duration called transfer time. This may result from moving the resource from the previous location to the location required by the new activity, or from configuring the resource for the new activity (e.g. starting a motorboat, pushing the boat to water, dressing protective clothes to crew etc.). Both transfer and preparation times depend both on the previous and the next activity where the resource is used.

Transfer and preparation activities may need their own resources (see section 3.2.2), for example trucks for transfer and tools for preparation. These resources are unavailable to other activities during the transfer or preparation activity. These activities may also consume non-renewable resources such as fuel; this has to be modelled if e.g. the sufficiency of fuel reserves is in question and may cause changes to operation schedule.

3.2.1.2 Use of resources in an activity

An activity needs certain resources in order to be completed. The resource needs of an activity may, in principle, vary with time (e.g. in the beginning, more firemen are needed in

extinguishing a fire than later). In a simple model, however, the resources used by an activity are reserved to it from the activity's beginning to its end, and they cannot be used in other activities.

The use of resources in an activity depends on its mode (see section 3.2.1). The use of resource *k* in activity A_j in mode *m* is assumed to be known and is denoted as $r_{j,k,m}$.

3.2.2 Resources

To execute an activity, work, material and equipment are needed. Collectively these are called resources. A feature common to all resources is limitedness: the use of any resource at any given time instance must be less than or equal to the amount of that resource available at that moment.

In principle, the resource needs of an activity may change with time (e.g. more mechanics might be needed in beginning of the installation of a switchgear than later); in simple models, however, all the resources needed by an activity are attached to it throughout its lifecycle.

Many resources are characterized by exclusivity: if they are used in an activity at a time instance, they cannot be used simultaneously in other activities; some resources, such as supervisors or communications channels, may be shared between several activities simultaneously.

We denote the amount of each resource *k* at time *t* by $x_k(t)$. Naturally, the amount of each resource must be non-negative, i.e. $\forall k,t : x_k(t) \geq 0$.

Each resource may be used in certain activities; this depends on the kind of resource (e.g. kind of equipment or special training of humans).

There are two kinds of resources: non-renewable and renewable [57].

3.2.2.1 Non-renewable resources

Some resources are non-renewable: once they have been used, they cannot be used later; for example, fuel, spare parts, construction materials etc. are non-renewable. If a sufficient amount of some non-renewable resource isn't available for an activity, it must be brought in from some external source, and this may mean delays in the completion of the activity, or in the extreme case, cancellation of the activity and change of plan. Introduction of resources from an external source may be modelled in a preparation activity of the activity (see section 3.2.1.1).

The amount of a non-renewable resource *k* at time *t* may be represented by the inventory equation

$$x_k(t+1) = x_k(t) + s_k(t) - d_k(t), \quad (1)$$

where $s_k(t)$ is the supply of resource *k* from an external source at time *t*, and $d_k(t)$ is the consumption of resource *k* at time *t*. (all currently active activities consuming resource *k* combined). If location of resources is of importance, the inventory equations should be listed not only by resource but also by location, and moving a resource to a different location should show in (1) as demand in the sending location and supply in the receiving location.

3.2.2.2 Renewable resources

Some resources are renewable, i.e. they can be used later in other activities; for example, crew and equipment are such resources.

The availability of a renewable resource may depend on the availability of a non-renewable resource: for example, a truck may be used only if there is enough fuel available. Then, the amount of available resource (trucks) is the minimum of the amount of the resource itself and the amount of the available non-renewable resource in terms of usage (e.g. the amount of available fuel divided into portions needed by trucks).

In detailed modelling, it should be taken into account that a resource may be used at its peak efficiency only for a certain time: an engine might be used at its peak power only for a certain time, and a human will get tired after doing hard work for a while. Furthermore, using a resource at its peak efficiency may increase failure probability of that resource.

Associated with a renewable resource is the risk that it is not available at a given moment due to failure or maintenance; for example, engine failure in a truck or injure of a human may be considered failure, and sleep and dining may be considered maintenance of humans. Then, the amount of resource at a given moment is the amount of that resource available at that moment. Possibly a failed resource will be available at a later moment after the machine has been repaired or the human has healed. Failure of a resource may be represented in the way that its demand $d_k(t) > 0$ in equation (1) ($d_k(t)$ is then the number of resource k that fail at the time instance t).

3.2.3 Activity networks

Activity networks are the most common model used in project management; they are used in, e.g., PERT and CPM. The nodes of an activity network are activities. An arc of an activity network represents a time precedence relation between two activities. These precedence relations will be examined more closely in section 3.2.4.

An activity network is a directed directed graph. It is directed, because the arcs represent time relations between activities. It is acyclic, because an activity cannot precede itself in time. As explained in section 3.2.1, an activity network has two special nodes that don’t have a time duration in themselves. These are the start and end activities.

Figure 2 is a simple activity network representing the construction of a sandbag dam to prevent raising sea from entering nuclear power plant premises. The network contains only activities (represented by circles) and their precedence relations (represented by arrows). The start activity of the network – which might also be called triggering event – is the “Water level rise alarm” activity. The end activity is “Dam in place”.

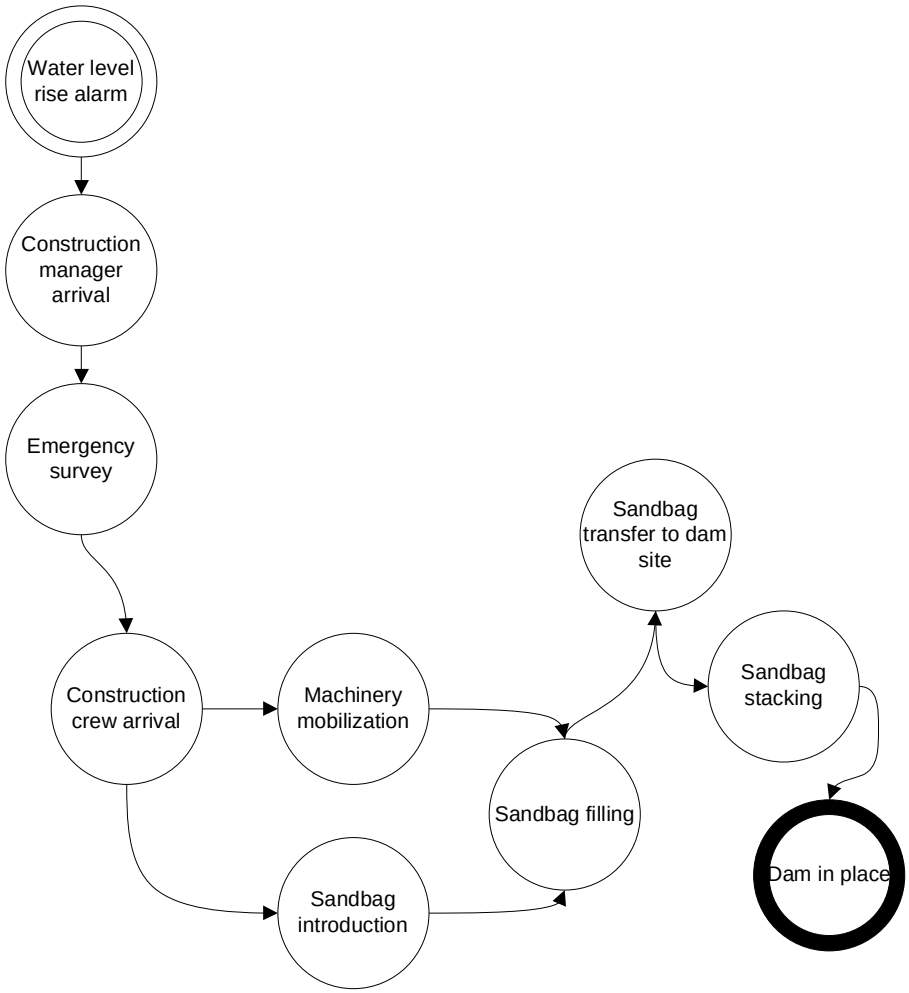


Figure 2. A simple activity network for the construction of a sandbag dam

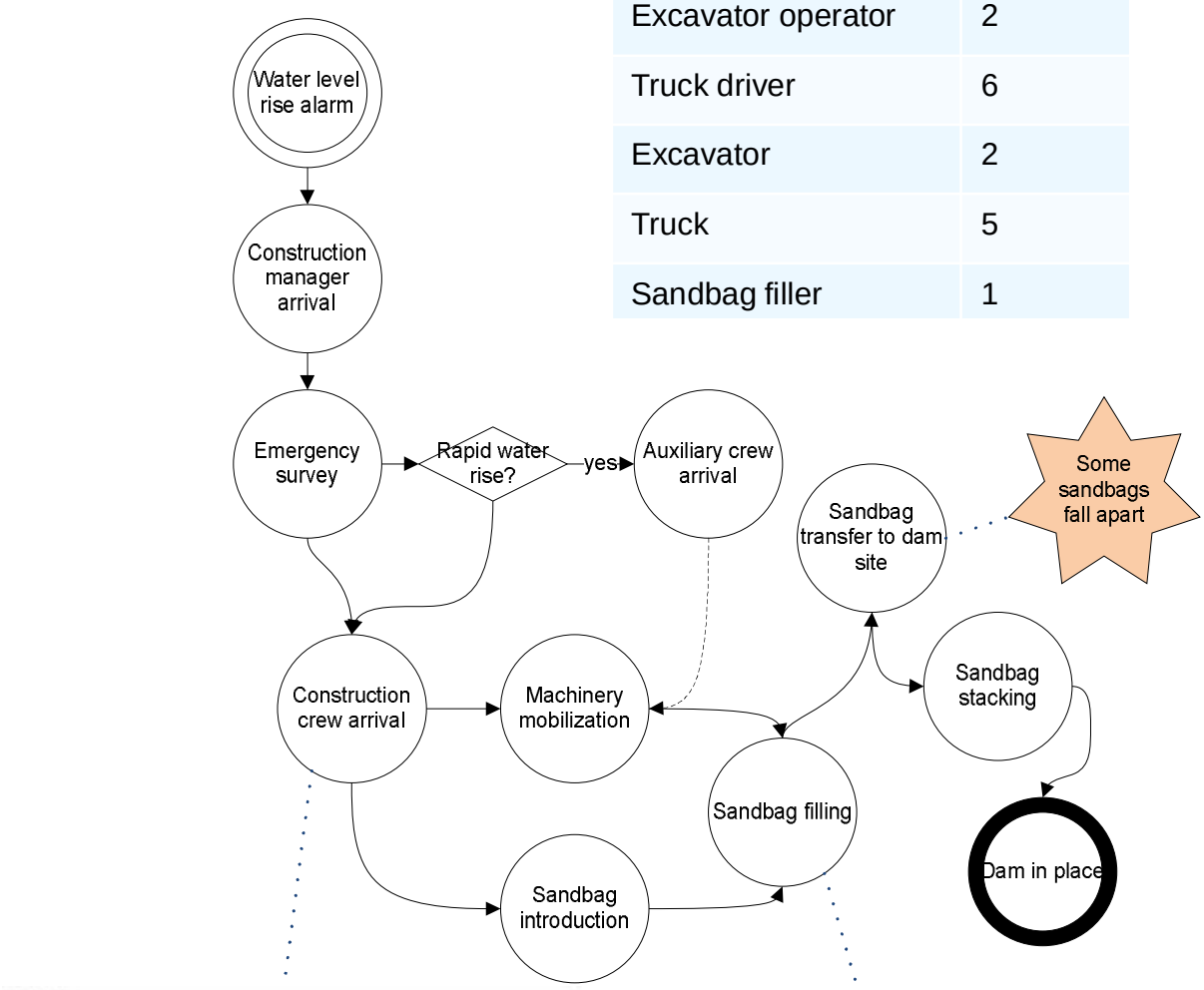
However, a simple diagram doesn't contain all the information that is often utilized such as time distributions of task completion. Furthermore, analysis of P&E operations sets special requirements to the models used, as described in section 2.2.3.

Figure 3 represents these additional features of an activity network needed in modelling P&E operations. The network itself is the network of Figure 2, together with some resource and activity time distribution information for illustration purposes. The additional features are as follows:

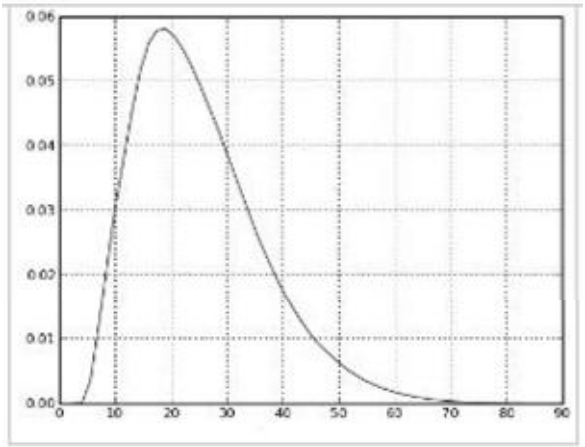
- The total resources available in this illustrative example are listed in the table in the top right corner; the available resources are not connected to any individual activity, but rather the whole network.
- The probability distribution of the duration of the activity "Construction crew arrival" is represented at the bottom left corner.
- The resources required by the activity "Sandbag filling" in some given mode are listed at the bottom right corner.
- a situation-specific aspect – whether water rises slowly or rapidly – and the resulting decision of whether to introduce more crew to the activity is depicted as the diamond-shaped node "rapid water rise?" and the conditional activity "auxiliary crew arrival" that may be executed if the water rises rapidly. There are, of course, other means of modelling situation-specific decisions and adaptation.

- a failure event – “some sandbags fall apart” – is attached to the node “sandbag transfer to dam site”. This represents a chance event contributing to performance risk.

resource	amount
Excavator operator	2
Truck driver	6
Excavator	2
Truck	5
Sandbag filler	1



resource	required
Excavator operator	1
Excavator	1
Sandbag filler	1



Arrival time distribution

Figure 3. A simple activity network and its associate resource and activity time distribution information

3.2.4 Dependences between activities

An activity may depend on the status of some other activities. Usually this means that the start of an activity A_j presumes that some other activities, which are called its predecessors, have been executed first. In an activity network, these dependences are represented by directed arcs.

Consider possible time dependences between two activities A and B. The most important kinds of dependences are

- end-to-start: activity B cannot begin until activity A has been completed. This is the most common kind of dependence, and the only one used in the examples of this report. Example: the transfer of heavy equipment to a site (activity B) cannot start until the road to the site has been repaired (activity A).

- start-start. Activity B cannot start until activity A has started. Example: road repair (activity B) cannot start until removal of fallen trees from the road (activity A) has started; the two activities may be interconnected also in the sense that at any given moment, road repair cannot proceed further than to the point from which the trees have been removed.

- start-end. Activity B cannot end until activity A has started. Example: if sea level by a site has to be continuously monitored in an emergency situation, monitoring by group 1 (activity B) cannot end until monitoring by group 2 (activity A) has started.

- end-end. Activity B cannot end until activity A has ended. Example: connection of spare communications cable to equipment (activity B) cannot end until the cable has been laid (activity A); however, connection may have started at the other end even before laying the cable was started.

- the dependences above may be generalized so that, instead of start or end, for example a constraint might be used where a certain percentage of activity A has to be completed before activity B may start, or that at most a certain percentage of activity A may be completed before activity B must start.

- either-or. The activities A and B cannot go on simultaneously. Example: it might not be possible to simultaneously do welding work in an area (activity A) and transfer flammable liquid through that same area (activity B).

In a general case, there might be for example a condition that activity B cannot start before one of the activities A_1, …, A_n has been completed. An example of such a dependence is a situation where there are several broken pumps, each being repaired by a repair crew, and pumping cannot start until one of the pumps has been repaired.

There might be other dependences between activities, such as that they use some same resources. These dependences are, however, not represented as arcs in the activity network; rather, they are modelled separately in the mathematical model.

3.3 Handling of plan changes in activity networks

An activity network, in the form usually described in project management literature, is a static structure: all the activities and their connections (precedence relations) have been pre-chosen. However, a P&E operation is often conducted as a response to rare adverse events, may contain unforeseen elements, and commonly has to be executed with the resources available at the moment. Therefore there may be considerable uncertainty as to what activities will be executed and in what order.

Reasons for plan changes, and thereby uncertainty about the activity network's structure, include

- adverse events during the complex operation such as equipment failures, accidents, and human errors
- decisions – perhaps on-the-spot and improvised – made in order to adapt to unforeseen features in the present situation
- unforeseen situations or states of the system, perhaps resulting from phenomenological uncertainties

A big difficulty in modelling plan changes is that changes involve human decision making which is hard to predict.

The literature on accounting for such changes in the activity network structure seems to be scarce, and seems mainly concentrated on project management and leadership aspects rather than modelling and analysis [21]. However, there are several directions to which handling of plan changes in project risk analysis models could go:

- the project is modelled within the formalism of stochastic project networks [44]. Also known as GERT (Graphical Evaluation and Review Technique) networks, these are a generalization of the PERT activity-on-arc networks. Their modelling constructs facilitate, in particular, the analysis of research and development projects. They possess more general arc weights (activity completion times), several different node types (containing stochastic elements), and cycles (feedback or doing the same activities again if the first time didn't produce success). Stochastic project networks can provide valuable modelling constructs for modelling plan changes; however, it is unclear whether these modelling constructs truly help in modelling the central aspects of plan changes.
- all foreseen significant plan changes are incorporated in the activity network model by using conditional nodes (for an example, see Figure 3). Drawbacks of this approach are that the activity network may become very large and therefore tedious to construct and hard to handle, and that seemingly the only analysis method of such networks would be simulation.
- all foreseen significant plan changes are incorporated in the activity network by listing them as alternatives and assigning a probability to each alternative. This approach suffers from the same deficiencies as the previous one.
- parts of the activity network are not modelled explicitly, and generated when needed by for example using graph grammars. Then, the model wouldn't consists of a ready-made activity network. Rather, it would consists of activities with preconditions (what has to be true in order to execute the activity) and postconditions (what will be true after the activity has been executed), and construction of the activity network would amount to finding a set of activities whose postconditions would collectively ensure the fulfilment of the operation's goals. An activity network could then be automatically generated on an as-needed basis, perhaps using the methods of artificial intelligence planning [18].
- activity networks may be considered as adaptive rather than static networks. In adaptive networks, the network topology can evolve dynamically in time, and the links may change adaptively with respect to its states [20]. Adaptive networks are a topic under intensive study by a large research community.

The question of modelling plan changes in an activity network will not be further elaborated here. Suffice it to say that it is a difficult but important topic meriting research in the future.

3.4 Conditions for completion of a prevention and emergency operation

We consider the question of when a P&E operation can be considered to be successfully completed. In ordinary activity network models, this is handled in the way that the project is completed when all its activities have been completed. However, this doesn't necessarily apply in the P&E operations context: activities of a P&E operation may change during the execution of the operation, as seen in section 3.3.

Therefore, a need exists for handling the question of completion in a more abstract manner. A suitable way to handle this is to represent the conditions of completion as logical statements (possibly in a formal logic framework such as provided by knowledge representation research [5]). For example, the minimal completion condition of an operation to pump coolant to a damaged reactor is that coolant is being pumped to the reactor. The completion condition can be handled as a logical postcondition that the activities in the activity network must collectively satisfy.

4. A demonstrative example

To illustrate the concepts presented above, we next turn to an example from the Loviisa nuclear power plant: blocking the entry of floating oil to the cooling water system in the case of an oil spill.

We will create an activity network, together with completion time distributions for its individual activities, and analyse the model using Monte Carlo simulation. The simulation tool used is @Risk version 6.2, which is a widely used Monte Carlo risk simulation tool built on top of Microsoft Excel.

It is emphasized that this is not a case study but rather a conceptual demonstration. The model's description of operations contains inaccuracies, and the values of parameters do not necessarily have any connection to the actual figures; therefore the results have no implications to the functioning (or lack thereof) of the emergency arrangements at Loviisa.

4.1.1 Description of the system and operation

To prevent accidental oil slicks from entering the cooling water system of Fortum's Loviisa nuclear power plant, the fire brigade of the plant shall construct a barrier of oil booms to block the bay in front of the plant when needed (Eastern-Uusimaa's Emergency Services Department shall simultaneously construct similar barriers to block certain water inlets, but this is not modelled here). The description of this operation is based on [16].

The booms, and an electric winch, are stored in a container by the bayside. An asphalted ramp leads from the container to waterline. A wire rope connects this entry point to the opposite shore, where a pulley has been anchored. In addition to that, the plant fire brigade has boats. A schematic illustration of the assembly is given in Figure 4.

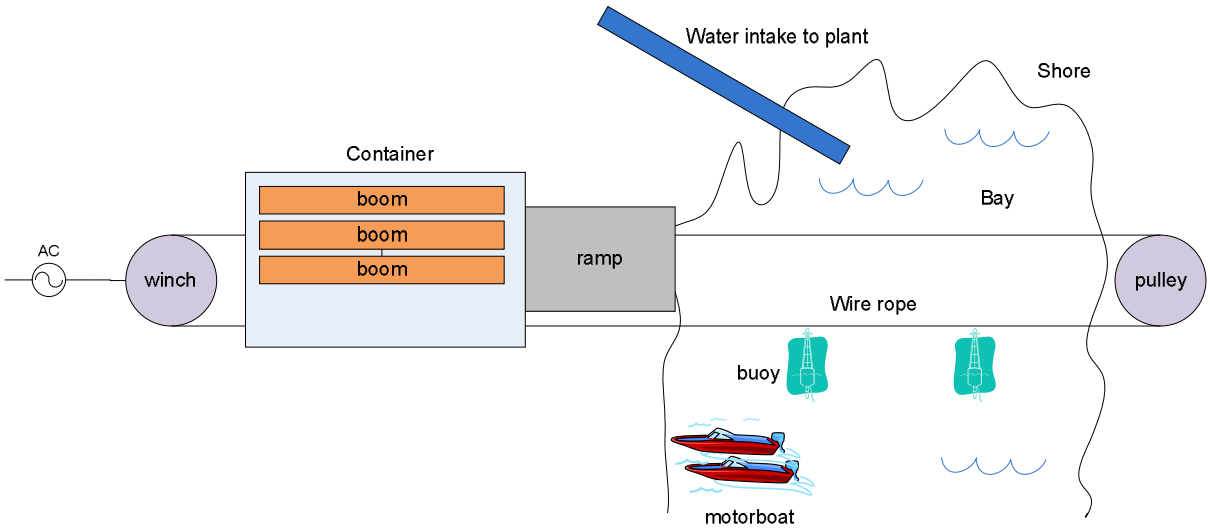


Figure 4. The assembly of equipment and infrastructure for oil slick barrier construction

When the need arises, the current roster of the fire brigade enters the container, secures each boom by its end to the wire rope, and uses the electric winch to pulley the booms in a chain over the bay. Finally, the fire brigade secures the two outermost booms to points of support on the shore, and connects the booms to anchor buoys. The specified maximum completion time is 2 hours from the alarm.

If the situation demands, members of the fire brigade not in the current roster are called to service.

4.2 A model for the schedule risk of the operation

We model only the schedule risk of the oil slick barrier construction operation. It is obvious that the operation also contains quality risks – for example, the booms might be improperly secured to the buoys, thus causing an increased risk of falldown of the barrier in windy conditions, or a boom might be broken during transfer thus allowing the entry of oil to the other side – but these are left out for simplicity.

As stated in section 4.1.1, the schedule risk is realized when the completion of the operation takes more than 2 hours.

We assume the following work breakdown structure for the operation:

1. upon alarm, the current roster of the fire brigade is transported to the container. It is evident that this activity could be split into more detailed phases, such as the alarm phase, crew gathering at the vehicle(s), drive from the fire station to the container, and the unloading of the roster from vehicle(s). However, to keep things simple, we aggregate these activities into a single collective activity.

2. fireman A opens the door of the container. Predecessor: task 1.

3. fireman B commissions the electrical winch, starts operating it. Predecessor: task 1.

4. two firemen secure each boom – one at a time – to the wire rope from the boom's ends, and to the preceding boom (if any). Predecessor: task 2.

5. fireman B operating the electrical winch reels the wire rope so that the currently secured booms move towards water, and the next boom can be secured both to the wire rope and the preceding boom. Predecessors: tasks 3 and 4.

6. the securing and moving of the booms (the two previous steps) is repeated until there are enough booms secured so that the booms form a continuous barrier for the surface water of the bay. For the purposes of illustration, we assume that 10 booms suffice for this. Then the fireman operating the winch moves the barrier to its place. This is a summary activity covering 10 individual boom securing and moving activities.

7. fireman B locks the winch so that the booms will not move. Predecessor: task 6.

8. firemen secure the left outermost boom to support point on the left beach. Predecessor: task 7.

9. firemen secure the right outermost boom to support point on the right beach. Predecessor: task 7.

10. in the meanwhile, two firemen have taken a motorboat to the bay, heading for the first buoy. Predecessor: task 1.

11. The firemen in the motorboat secure ropes to the first anchor buoy and wait for the booms to arrive at their places, with the other ends of the ropes in the motorboat. Predecessor: task 8.

12. when the booms are in their places, the firemen in the motorboat secure the ropes in the first anchor buoy to the respective booms. Predecessors: tasks 7 and 9.

13. the firemen in the motorboat continue to the next buoy, secure ropes to it, move to the respective booms and secure the other ends of the ropes to the booms. This is repeated until all booms have been secured to a buoy with a rope.

14. the barrier is in place. This is the end activity with duration of 0 time units. Predecessors: tasks 8, 9 and 13.

We make the following assumptions:

- 10 booms suffice to contain the bay
- there are 2 anchor buoys, and each buoy is to be connected to 5 booms
- there is one motorboat available close to the container
- all precedence relations are of the end-to-start type: the later activity cannot start until all its preceding activities have completed.

A possible activity network is represented in Figure 5. Besides the activities, also the failure events are marked in the network.

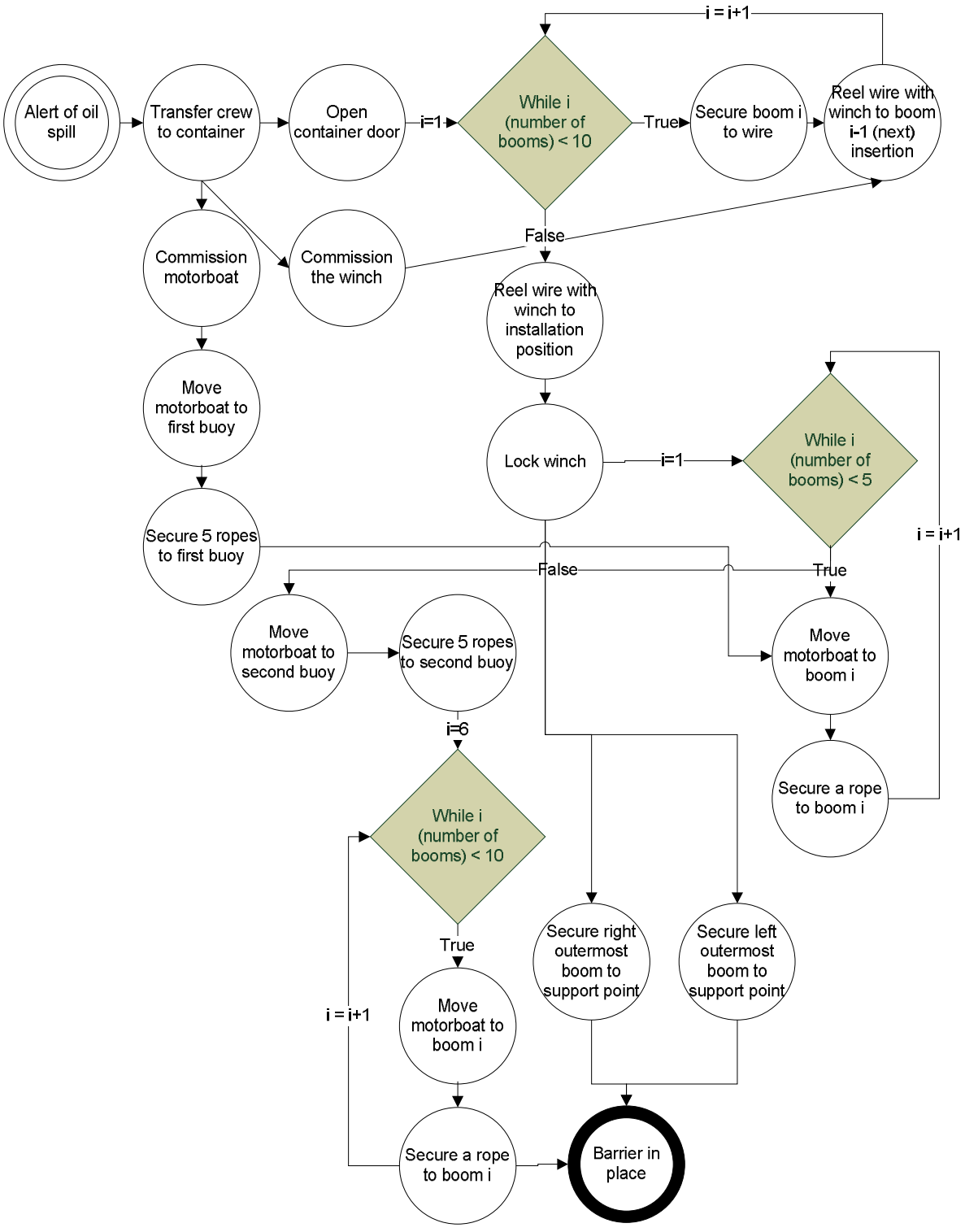


Figure 5. Activity network for oil slick barrier construction

Probability distributions for the time durations of each activity were postulated, and are presented in Table 1. In the model, the start time of an activity is the maximum of the end times of its predecessors; this corresponds to the end-to-start precedence constraint (all predecessor activities must have completed for the current activity to start).

Table 1. Postulated probability distributions of some oil slick barrier construction activities. Parameters expressed in terms of mean and standard deviation of the distribution clarity.

Activity description	Probability distribution
transfer crew to container	Normal μ=10 minutes, σ=2,5 minutes
commission the motorboat	Lognormal μ=5 minutes , σ=3 minutes
commission the winch	Lognormal μ=3 minutes , σ=1 minute
secure boom i to wire (i=1,…,10)	lognormal μ=1 minute, σ=2 minutes
reel wire with winch to next boom	lognormal μ=2 minutes, σ=1 minute
lock winch	lognormal μ=1 minute, σ=1 minute
secure left/right outermost boom to support	lognormal μ=2 minutes, σ=1 minute
move motorboat to 1st buoy from beach	normal μ=5 minutes, σ=3 minutes
secure ropes to 1st/2nd buoy	Lognormal μ=5 minutes , σ=4 minutes
move boat from 1st buoy to boom 1	normal μ=5 minutes, σ=1 minutes
secure rope to boom i, i=1,…,10	lognormal μ=2 minutes, σ=1 minute
move boat from boom i to boom i+1, i=1,…,4, 6,…,10	lognormal μ=1 minute, σ=1 minute
move boat from boom 5 to 2nd buoy/from 2nd buoy to boom 6	normal μ=5 minutes, σ=1 minutes

4.2.1 Modelling risk associated with an activity

For demonstration purposes, we model also the effect of a technical failure to the schedule.

A potential failure, causing a mixed activity completion time distribution for task 10, is assumed. This failure is that the motorboat close to the container is not available (perhaps due to hole in the bottom, or breakdown of the engine). This causes the firemen operating the boat to fetch another boat from further away. This, in turn, introduces extra delay in their work, which is reflected in the schedule risk.

Naturally, there are other potential failures that could also be modelled. For example, the container door cannot be opened immediately (the lock is broke, the fire brigade has not taken the correct key with them, …). In this case, the door has to be broken, which causes an extra delay. Another failure could be that the electrical winch does not work properly (for example, due to electrical or mechanical failure), in which case the booms have to be taken to water using a fire engine. However, one failure suffices to illustrate the handling of failures and their effect on schedule.

Remember that in section 3.2.1, it was mentioned that failure associated with an activity may be modelled as a mixture model. Here we illustrate the concept as follows. Let the failure probability be p, probability distribution $f_1(t)$ the duration time probability density function on the condition that no failure has occurred, and $f_2(t)$ the duration time probability density function when on the condition that the failure has occurred. Then the mixture distribution of the activity's time duration is $p\ f_1(t)+(1-p)\ f_2(t)$.

Let us assume that the motorboat may be unserviceable with probability p. For demonstration purposes, assume that p takes the unrealistically high value of 0.1.

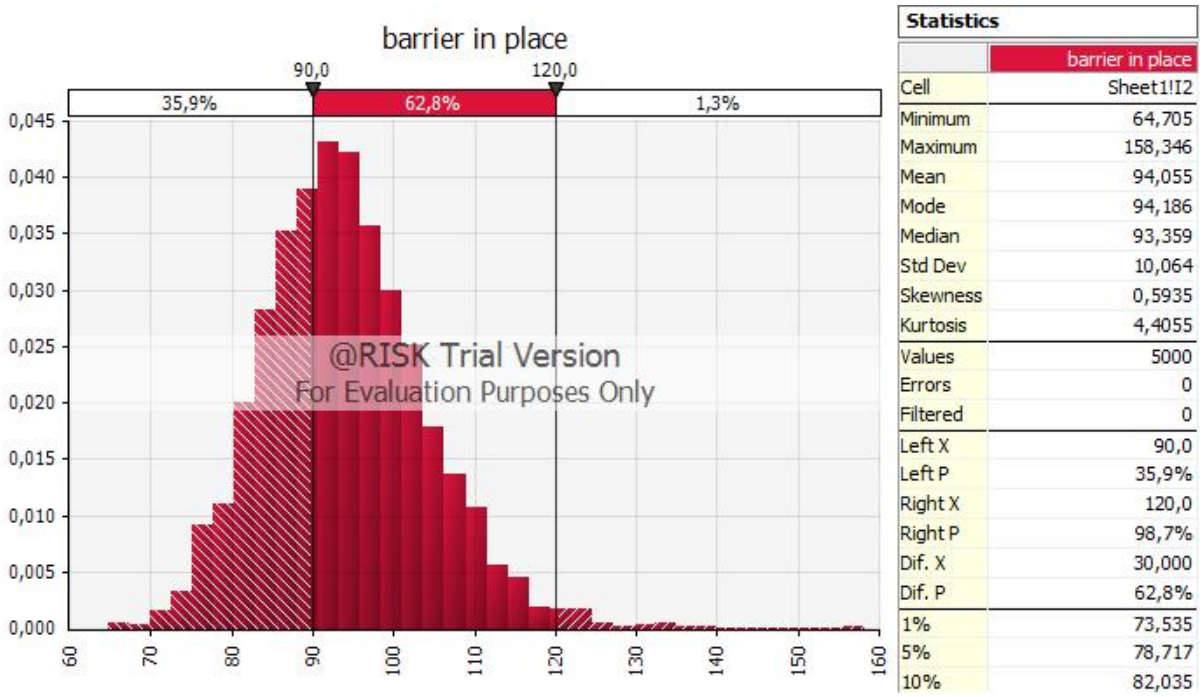
Assume further that when the motorboat is broken, another motorboat is fetched from nearby, and this takes 20 minutes. Assume also that the other motorboat needs some extra work to be taken into use, and commissioning this other boat takes time that is lognormally distributed with mean 7 minutes and standard deviation 4 minutes.

The probability distribution of the time duration of “commission the motorboat” (see Table 1) is the time distribution on the condition that no failure occurs. The probability distribution of the activity’s duration time t, with failure, is 0 when

$$\begin{cases} 0, \text{ when } t < 20 \\ Lognormal(t - 20; 7{,}4), \text{ when } t \geq 20 \end{cases} \quad (2)$$

4.3 Analysis results

The probability distribution of the operation’s completion time was estimated by Monte Carlo simulation. We first take a look at the completion time distribution without the postulated failure, which is presented in Figure 6.



Statistics	barrier in place
Cell	Sheet1!I2
Minimum	64,705
Maximum	158,346
Mean	94,055
Mode	94,186
Median	93,359
Std Dev	10,064
Skewness	0,5935
Kurtosis	4,4055
Values	5000
Errors	0
Filtered	0
Left X	90,0
Left P	35,9%
Right X	120,0
Right P	98,7%
Dif. X	30,000
Dif. P	62,8%
1%	73,535
5%	78,717
10%	82,035

Figure 6. Probability distribution of oil slick barrier construction completion time. Time units are in minutes.

As seen from the figure, the probability of the oil slick barrier construction exceeding two hours (120 minutes) is small, only 1,3 %.

Table 2 shows the results of sensitivity analysis: the 10 variables in which unit change produces the greatest change in the mean of the barrier construction completion time. It is seen, that securing the booms to buoys with the ropes has the greatest effect on completion time; this is natural considering that especially securing buoy 2 to the respective booms can occur only after almost everything else has been done. Also transfer of crew to container is a critical activity in the light of this sensitivity analysis; this is also natural, because it precedes everything else in boom construction, and therefore delays in it directly translate to increased completion time of barrier construction.

Table 2. Sensitivity analysis: the 10 activities affecting the construction completion time mean the most.

Rank	Name of activity	barrier in place Range of Mean
#1	secure ropes to 2nd buoy	12,39

#2	transfer crew to container	10,76
#3	move boat to 2nd buoy	9,22
#4	secure boom 3 to wire and boom 2	6,91
#5	secure boom 5 to wire and boom 4	6,70
#6	secure boom 6 to wire and boom 5	6,60
#7	secure boom 8 to wire and boom 7	6,34
#8	secure boom 7 to wire and boom 6	5,93
#9	secure boom 2 to wire and boom 1	5,91
#10	secure boom 10 to wire and boom 9	5,77

The probability distribution of the operation's completion time assuming failure risk (see section 4.2.1) is depicted in Figure 7.

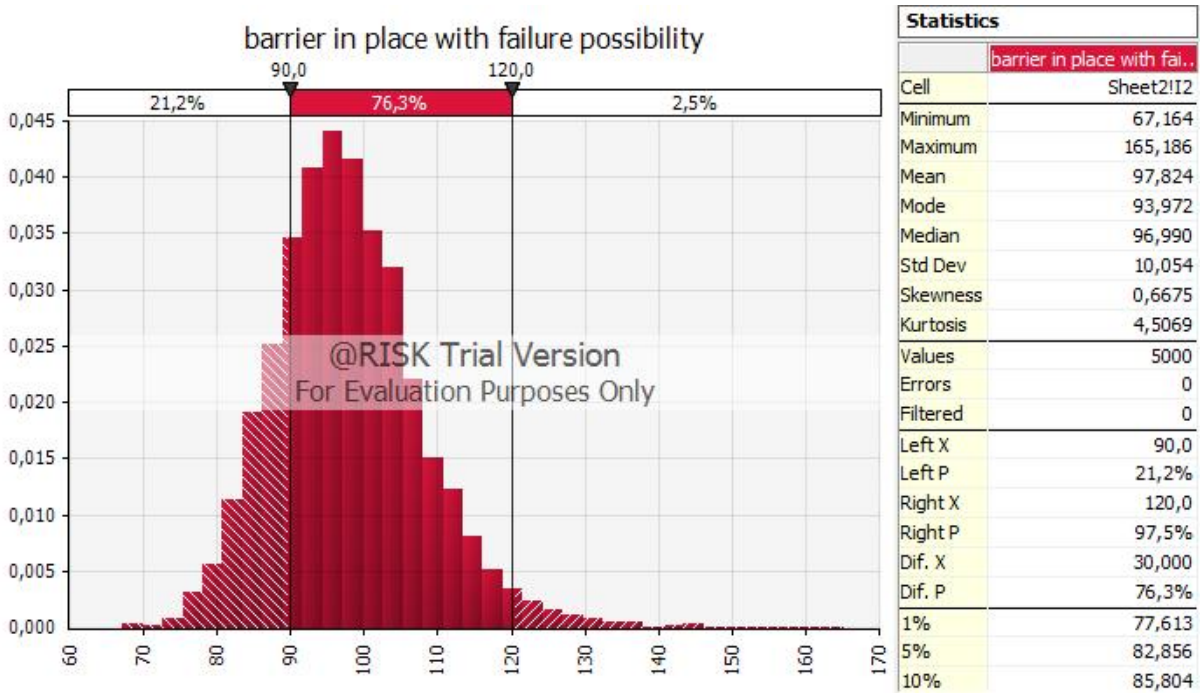


Figure 7. Probability distribution of oil slick barrier construction completion time when we assume that the motorboat might be unavailable with a certain probability, and a reserve motorboat must be used. Time units are in minutes.

The probability of not meeting the target of 2 hours has almost doubled: here it is 2,5 % whereas in the case of no motorboat failure it was 1,3 %.

5. Conclusions

We have considered methods to model and analyse P&E operations – such as rescue operations, repair operations etc. – with methods from project management. Our viewpoint has been that of probabilistic risk analysis, applied to nuclear safety. Such models and analyses have many important applications in the probabilistic safety analysis of nuclear power plants. Most importantly, P&E operations can be modelled in a separate model, which reduces the complexity of the main PRA model (e.g. a fault or event tree). Models and methods of project management may help in constructing more detailed, more natural and clearer models, and produce mathematically justified analysis results for PRA.

It seems that the issue of P&E operations has not received much attention in PRA, and certainly not as much as the importance of the topic would imply.

From the current perspective, the most important issue in need of further theoretical developments, and their testing in practical applications, may be probabilistic risk analysis when there are resource constraints on the P&E operation. The analysis of resource-constrained projects is still very much a research issue, and it seems that attention has not been paid to the risk analysis side. There are still formidable conceptual, mathematical and computational problems to be solved in this topic.

Another outstanding issue is the modelling and analysis of plan changes. This is important because P&E operations occur often in situations that have great uncertainty associated with them, and change of plans is likely as the situation unfolds.

Some important topics of PRA that have not been touched upon in this report, for brevity, are importance measures and common-cause faults. It seems clear that importance measures can be developed for P&E operations, and plausible that existing ones can be applied in a modified form. Then, for example, the impact of the failure of a given activity on the success probability of the whole operation can be analysed. Similarly, it seems likely that concepts and methods developed for common-cause faults within PRA can be applied in the analysis of P&E operations.

Another important PRA topic, uncertainty analysis, received only little attention in the demonstrative example. Many traditional uncertainty analysis methods, such as Monte Carlo simulation, may be used as such in the analysis of P&E operations. More research is needed in, for example, the modelling of high-dimensional dependences between uncertainties.

P&E operations are a highly human activity and will remain so for at least some time. Therefore human reliability assessment plays an important role in the risk analysis of P&E operations, and HRA research for the purposes of P&E operations will be needed. Conversely, some scenarios that have been traditionally been analysed as problems in HRA may be amenable to analysis via methods developed for P&E operations. A case in point is the analysis of human actions under disturbance. However, it needs to be emphasized that HRA and the analysis of P&E operations are distinct fields: there are aspects of P&E operations that are not in the realm of HRA (such as schedule risks due to systemic factors), and aspects of HRA that are not part of P&E operations (such as cases where only one human actor needs to be considered).

A most important task remaining is that of finding out what modelling and analysis concepts are relevant in practice, and which parts of the theory need to be developed for the benefit of practical applications. Case studies that are to be performed in the future will shed light on these issues.

References

[1] C. Artigues. The resource-constrained project scheduling problem. Chapter 1 in [2], 21-48.

[2] C. Artigues, S. Demassey, E. Néron (eds.). Resource-constrained project scheduling - models, algorithms, extensions and applications. Wiley, Hoboken, USA 2008.

[3] Baker, S., Ponniah, D., Smith, S. Techniques for the analysis of risks in major projects. Journal of the Operational Research Society, Vol. 49 (1998), 567-572.

[4] Bedford, T., Cooke, R. Probabilistic risk analysis – foundations and methods. Cambridge University Press, 2003.

[5] R. Brachman, H. Levesque. Knowledge presentation and reasoning. Morgan Kauffman, 2004.

[6] P. Brucker, A. Drexl, R. Möhring, K. Neumann, E. Pesch. Resource-constrained project scheduling: notation, classification, models, and methods. European Journal of Operational Research, Vol. 112 (1999), No. 1, 3-41.

[7] Bruni, M., Guerriero, F., Pinto, E. Evaluating project completion time in project networks with discrete random activity durations. Computers and Operations Research Vol. 36 (2009), pp. 2716-2722.

[8] Bushuyev SD and Sochnev SV. Synergetic intelligence methods for risk management by projects. Proceedings of the INTERNET 12th World Congress on Project Management, Oslo, June 1994, 230–241.

[9] Chapman, C., Ward, S. Project risk management – processes, techniques and insights. 2nd edition, Wiley, 2003.

[10] Cooper, D., Grey, S., Raymond, G., Walker, P. Project risk management guidelines – managing risk in large projects and complex procurements. Wiley, 2005.

[11] Cox, M. Simple normal approximation to the completion time distribution for a PERT network. International Journal of Project Management, Vol. 13 (1995), No. 4, p. 265–270.

[12] Day, A. Mastering risk modelling – a practical guide to modelling uncertainty with Microsoft Excel, 2nd edition. Prentice-Hall, 2009.

[13] Demeulemeester, E., Herroelen, W. Project scheduling – a research handbook. Kluwer, 2002.

[14] Dillon, R, Paté-Cornell, E. APRAM: an advanced programmatic risk analysis method. International Journal of Technology, Policy and Management, Vol. 1 (2001), No. 1, 47-65.

[15] Dodin, B. Bounding the Project Completion Time Distribution in PERT Networks. Vol. 33 (1985), No. 4, p. 862-881.

[16] Forsberg, K. Selvitys Loviisan voimalaitoksen lähialueen öljyntorjunnasta ulkopuolisella merialueella sattuneen öljyvahingon tapauksessa (a briefing of oil destruction activities in the adjacent areas of the Loviisa power plant in the case of oil spill in the outside sea area, in Finnish). Internal document, Fortum Power and Heat Oy, Loviisa power plant, 4.7.2008.

[17] Frame, J.D. The new project management – tools for an age of rapid change, complexity, and other business realities. Jossey-Bass, 2002.

[18] M. Ghallab, D. Nau, P. Traverso. Automated planning – theory and practice. Morgan Kaufmann, San Fransisco 2004.

[19] van Groenendaal, J., Kleijnen, J. On the assessment of economic risk: factorial design versus Monte Carlo methods. Reliability Engineering and System Safety, Vol. 57 (1997), 91-102.

[20] Gross, T., Sayama, H. (eds.) Adaptive networks – theory, models and applications. Springer, 2009.

[21] Harrington, J., Conner, D., Horney, N. Project change management – applying change management to improvement projects. McGraw-Hill, 2000.

[22] Hazelrigg, G.A. and Husband F.L. RADSIM—a methodology for large-scale R&D program assessment. IEEE Transactions of Engineering Management Vol. 32 (1985), 106–115.

[23] Hostikka, S., Kling, T., Paajanen, A. Simulation of fire behaviour and human operations using a new stochastic operation time model. 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012 (PSAM11 ESREL 2012).

[24] Hou Zhen-Ting, Zhang Xuan, Kong Xiang-Xing. A new analytical algorithm for computing probability distribution of project completion time. Journal of Central South University, Vol. 17 (2010), No. 5, pp. 1006-1010.

[25] Janssens, G., Phusavat, K., Anussornnitisarn, P. On the completion time of a project with random activity durations based on a model of stochastic marked graphs. Proceedings of the 2010 European Simulation and Modelling Conference ESP '2010, Hasselt University, Hasselt, Belgium, October 25-27, 2010, p. 247-252.

[26] Johnson, N., Kotz, S., Balakrishnan, N. Continuous univariate distributions, Volume 1, 2nd edition. Wiley, 1994.

[27] Ika, L. Project Success as a Topic in Project Management Journals. Project Management Journall, Vol. 40 (2009), No. 4, 6–19.

[28] Johnson, N., Kotz, S., Balakrishnan, N. Continuous univariate distributions, Volume 2, 2nd edition. Wiley, 1995.

[29] Kerzner, H. Project management – a systems approach to planning, scheduling, and controlling, 10th edition. Wiley, 2009.

[30] Klastorin, T. Project management – tools and tradeoffs. Wiley 2003.

[31] Kling, T., Hostikka, S., Rinne, T., Vaari, J. and Hakkarainen, T. Stochastic operation time modelling of rescue situations. 13th International Conference and Exhibition on Fire Science and Engineering (Interflam 2013), Royal Holloway College, Nr Windsor, UK 24-26 June 2013.

[32] Knochenhauer, M., Louko, P. Guidance for external events analysis. SKI Report 02:27, February 2003.

[33] Kotz, S., van Dorp, J. Beyond Beta – other continuous families of distributions with bounded support and applications. World Scientific, 2004.

[34] Kumar, S. Managing risks in a relief supply chain in the wake of an adverse event. OR Insight, Vol. 24 (2011), 131-157.

[35] Law, A. Simulation modelling and analysis, 4th edition. McGraw-Hill, 2007.

[36] Lee, H., Suh, H.-W. Estimating the duration of stochastic workflow for product development process. International Journal of Production Economics, Vol. 111 (2008), p. 105–117.

[37] Ludwig, A. A Computational Study on Bounding the Makespan Distribution in Stochastic Project Networks. Annals of Operatins Research, Vol. 102 (2001), 49-64.

[38] Luu, V., Kim, S.-Y., Tuan, N., Ogunlana, S. Quantifying schedule risk in construction projects using Bayesian belief networks. International Journal of Project Management, Vol. 27 (2009), 39–50.

[39] McLachlan, G., D. Peel. Finite mixture models. Wiley, 1999.

[40] Milosevic, D.R. Project management ToolBox – tools and techniques for the practicing project manager. Wiley 2003.

[41] Morris, P.W.G. Managing project interfaces – key points for project success. In: Project management handbook, 2nd edition, Cleland D.I. and King W.R. (eds.), Van Nostrand Reinhold, 1988, 16-55.

[42] Möhring, R. Scheduling under uncertainty: bounding the makespan distribution. In Computational Discrete Mathematics – Advanced Lectures, Helmut Alt (ed.), Lecture Notes in Computer Science Volume 2122, 2001, pp 79-97.

[43] Nasir, D., McCabe, B., Hartono, L. Evaluating Risk in Construction–Schedule Model„ERIC–S: Construction Schedule Risk Model. Journal of Construction Engineering and Management, Vol. 129 (2003), 518-527.

[44] Neumann, K. Stochastic project networks – temporal analysis, scheduling and cost minimization. Springer, 1990.

[45] Ord, K. A Simple Approximation to the Completion Time Distribution for a PERT Network. Journal of the Operational Research Society, Vol. 42 (1991), No. 11, p. 1011-1017.

[46] Rausand, M., A. Höyland. System reliability theory – models, statistical methods, and applications, Second edition. Wiley, 2003.

[47] Rosen, K., Michaels, J., Gross, J., Grossman, J., Shier, D. Handbook of discrete and combinatorial mathematics. CRC Press, 1999.

[48] Schmidt, C., Grossmann, I. The exact overall time distribution of a project with uncertain task durations. European Journal of Operational Research, Vol. 126 (2000), 614-636.

[49] Schuyler, J. Risk and decision analysis in projects, 2nd edition. Project Management Institute, 2001.

[50] Shih, N.-H. Estimating completion-time distribution in stochastic activity networks. Journal of the Operational Research Society, Vol. 56 (2005), 744-749.

[51] Spurgin, A. Human reliability assessment – theory and practice. CRC Press, 2009.

[52] Vanhoucke, M. Project management with dynamic scheduling – baseline scheduling, risk analysis and project control. Springer, 2012.

[53] Vose, D. Risk analysis – a quantitative guide, 3rd edition. Wiley, 2008.

[54] Wideman, M. (ed.). Project and program risk management – a guide to managing project risks and opportunities. Project Management Institute, 1992.

[55] Williams, T. A classified bibliography of recent research relating to project risk management. European Journal of Operations Research, Vol. 85 (1995), No. 1, pp. 18-38.

[56] Williams, T. Modelling complex projects. Wiley, 2002.

[57] Williams, T. The contribution of mathematical modelling to the practice of project management. IMA Journal of Management Mathematics Vol. 14 (2003), No. 1, pp. 3-30.

[58] Yao, M.-J., Chu, W.-M. A new approximation algorithm for obtaining the probability distribution function for project completion time. Computers and Mathematics with Applications, Vol. 54 (2007), pp. 282-295.