B

Risk Management

This appendix deals with another application area of computational decision analysis methods, the area of risk management. The content of the appendix is joint work with Love Ekenberg, IIASA, and Anders Elgemyr, ROA. The text is partly derived from [ED95] and [DEE96].

The risk analysis method DEEP (Damage Evaluation and Effective Prevention) substantially extends the evaluative phases compared with earlier approaches. The concept of risk analysis is used in a little wider sense than usual. Often, only identification and valuation of damage risks are included in the concept, but here selection of risk treatment, risk financing, and analysis of the measures taken are also included. The presentation is focused on the identification and analysis of threats and on the evaluation of the suggested actions since those are the steps where the DEEP method differs the most from other methods. The other steps are fairly well covered in other texts.[1] The idea behind DEEP is to offer an analytical framework for enhancement of the chain identification–valuation–action in risk management without aiming at replacing it.

[1] Risk analysis is less general in its first steps. In different industries, the values to be protected and the threats are fairly industry specific. It is therefore not surprising that, for example, the chemical industries in Sweden publish a text applicable specifically to their own needs [K96]. But also the later evaluation steps are treated as if they were industry specific. This might be due to the lack of general methods that seem to fit in different industries, see for example [EM92].

To acquire a satisfactory understanding of the risk situation, management often desires some kind of structured approach to the analysis. Thus a risk analyst, conducting a risk analysis, frequently has access to standard procedures for identifying and assessing threats and for identifying and valuating assets. A tentative list of basic steps in risk management could be the following:

- Identify the assets/objects that should be protected.
- Identify the threats that should be protected against.
- Estimate the probabilities for the threats to materialise.
- Estimate the values lost if the threats materialise.
- Assess the current protection.
- Decide which threats to rectify and which to leave unmanaged.
- Evaluate which protective measures are reasonable to take.
- Find financing for a reasonable part of the remaining risk.
- Execute the decided plans.
- Follow up on the effectiveness and efficiency of the plans.

In the analysis, different threats are compared to each other, and those not found to be serious are filtered out. The others are ranked in order of treatments necessary. Below, some risk models are criticised for not being able to rank the seriousness of different threats. In the evaluation step, the possible courses of action are specified. Although in real life such analyses are often carried out, this step is left out in most existing risk analysis models. This is a clear deficiency that may substantially reduce the applicability of analysis results.

For insurance management problems, for example, different problems are encountered depending on the type of insurance. For high-volume, high-frequency incidents, insurance companies have a well-developed set of mathematical and statistical tools at their disposal when calculating the cost of insurance. The risk management issue is to keep such insurances or not, balancing the decision against the profit margin for the insurance companies and assuming a reasonably well-working insurance market with at least rudimentary competition

mechanisms. For low-frequency risks, the situation quite is different. Insurance statistics is not as good a tool, but the need for risk analysts to have tools at their disposal is perhaps even greater. This poses some hard challenges to risk staff in general and to risk managers in particular.

To make it easier to grasp the ideas behind the DEEP method, to compare it with traditional approaches, and to indicate some of their disadvantages, a brief survey of some approaches to risk analysis is included. Ensuing this, an informal overview of the method is given, followed by a description of its evaluation step incorporating DELTA.

Risk Evaluation Approaches

Different decision methods are used for assessment in risk analysis. They are typically involved in several steps to identify and evaluate assets, such as properties and information, and to identify and evaluate threats, such as fire, burglary, and industrial espionage. Such analyses are also carried out to verify the current protection, and to evaluate the effects of modifying it.

Often, when evaluating the cost of an incident, the model requires numerically precise data. A main problem is that in real-life analysis it is often impossible for an analyst to explain the difference between closely proximate probabilities, for example 23% and 25%. The problem is emphasised by the inability to express varying reliabilities for different pieces of information. Which data are based on long experience, and which are mere guesses? In models using numerically precise information, this kind of expressibility is severely limited.[2] The following three sub-sections focus on two common techniques used in risk evaluations and a more powerful approach, the expected cost.

[2] Methods for estimating the monetary cost of a simple incident by using numerically precise data in an expected cost model can be found in, e.g., [D90, pp.86 ff.].

Point Scale Models

One attempt to overcome the unrealistic and time-wasting assumption of numerically precise information is to be more imprecise, even in making the estimates. Broder writes: "*[…] it is neither necessary nor desirable to make precise statements of impact and probability. The time needed for the analysis will be considerably reduced and its usefulness will not be decreased if impact (i) and frequency (f) correlations are given in factors of 10*." [B84, p.22]. Then he proposes the following scale:[3]

Loss valuation of an incident		**Estimated frequency to occur**	
$10	i = 1	Once in 300 years	f = 1
$100	i = 2	Once in 30 years	f = 2
$1,000	i = 3	Once in 3 years	f = 3
$10,000	i = 4	Once in 100 days	f = 4
$100,000	i = 5	Once in 10 days	f = 5
$1,000,000	i = 6	Once per day	f = 6
$10,000,000	i = 7	10 times per day	f = 7
$100,000,000	i = 8	100 times per day	f = 8

Table B.1 Broder's point scale

The annualised loss expectancy is then approximated by $\frac{10}{3}^{(f+i-3)}$.

A problem with this approach is that the possible values and frequencies are spaced too far apart. This can be solved by using decimal numbers for *i* and *f*, but then the reasoning is back where it began. Furthermore, an important feature of a method allowing imprecise data should be enabling the detection of critical variables and the study of what effects modifications to the given data will have. This is not least important when the possible values are spaced far apart. Also, a risk analyst using point scales is still unable to express varying degrees of reliability for the different pieces of information.

[3] The method was originally suggested in [C77] and is recommended to prospective U.S. government suppliers by NIST.

Risk Level Models

One way to partially overcome the problems with point scale models is to allow the analyst to express the different values in non-monetary terms. In Sweden, for instance, a relative three-level model has been used for example by [H88, SAF86, W91b]. The probabilities and values involved (somewhat misleadingly called consequences in this approach) are expressed as shown in Figure B.1. Variants of the three-level model are also frequently used. For example, [S89–91] uses a four-level model, as does the Swedish SBA method [W84]. Not infrequently, even more rudimentary models are proposed.[4]

	Probability	Value	Risk level
1	**Low/Small** Seldom occurs	**Small** Low cost, little damage or loss	**Acceptable** Can be allowed Should be remedied
2	**Medium** Occurs neither often nor seldom	**Medium** Greater cost Greater damage or loss	**Unacceptable** Not allowed Must be remedied
3	**Great/High** Often occuring	**Great** Cost cannot be borne Total loss	**Catastrophic** Must be remedied immediately Unforgivable

Figure B.1 From [H88, p.76].

The *risk level* is a function of the sum (not product) PV = *probability* + *value*. If PV ∈ {2}, the risk level is 1, if PV ∈ {3,4}, the risk level is 2, and if PV ∈ {5,6}, the risk level is 3. A major problem with this approach is that the categories are too wide, with no discrimination within them. Therefore, most risks evaluate to risk level 2 with no indication of

[4] Many practitioners have abandoned the concept of probability altogether. For instance, insurance advisors often find it too hard to make estimates of the frequencies of accidents because of low levels of repetition, and they sometimes erroneously draw the conclusion that all kinds of probability based reasoning should be avoided. For example, in [G92b] a five-level model without probabilities is suggested and in [ESF91] probabilities are also ignored.

how to order the risks within that level. A competent risk analyst is capable of differentiating between disastrous, unacceptable, and acceptable risks without the aid of decision tools. The problem is to decide the order and the extent of the reduction needs of different unacceptable risks. Hence, when the risk situation is obvious, there is little need for a model, and when it is not, the models offer little help.

Expected Cost Models

The choice of the formula above for evaluation seems peculiar, and it is obvious that what results from it differs from evaluations using the expected value, which can be formulated in risk analysis terms as follows. The first definition covers the costs of actions, and below costs of incidents are defined as well. They differ conceptually as in the former the probabilities refer to possible incidents following actions, while in the latter the probabilities refer to possible effects of an incident. Example B.2 below uses expected cost in the first sense.

> **Definition B.1**: An *action* A_i may result in a number of possible incidents $\{H_{i1},\ldots,H_{in}\}$. The *expected cost of an action* A_i can be expressed as $p_{i1}\cdot c_{i1} +\ldots+ p_{in}\cdot c_{in}$, where c_{ik} denotes the cost of the incident H_{ik}, and p_{ik} denotes the probability of H_{ik} occurring given that action A_i is taken.

In a corresponding way, the definitions can be expressed in terms of incident costs instead and the expected cost should be minimised. When analysing the consequences of an incident, not only monetary costs are of interest. Thus, the concept of cost will be used in a more general sense, including both quantitative and qualitative values. Utilities could have been used instead, but in this context, cost is a more natural concept than utility. Note that monetary cost is a special case of cost.

The first pure risk concept to be considered is *simple incidents* (resulting in only direct consequences), which then will be extended to *incidents* (resulting in both direct consequences and new incidents).

Definition B.2: A *simple incident* H_i has a number of possible consequences $\{C_{i1},\ldots,C_{in}\}$. The *expected cost of a simple incident* H_i can be expressed as $p_{i1}\cdot c_{i1} +\ldots+ p_{in}\cdot c_{in}$, where c_{ik} denotes the cost of the consequence C_{ik}, and p_{ik} denotes the probability of C_{ik} occurring given that the incident H_i occurs.

It is possible to generalise the description of a simple incident resulting in a set of consequences. The new description allows an incident to generate both new incidents *and* consequences, which in turn can generate even more incidents and consequences, see Figure B.2. The H's in the figure denote incidents, and the C's different consequences. The P's denote the probabilities involved.

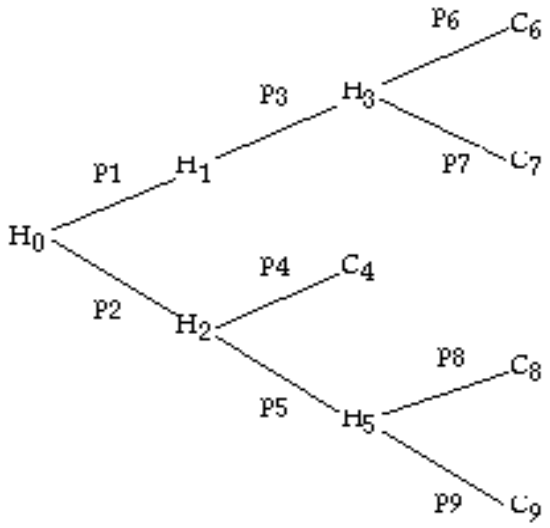

Figure B.2 An extended consequence analysis

Now, the definition of expected cost is extended. Note that in the following definitions, an incident is formally a set of consequences and incidents.

Definition B.3: A set of incidents and simple incidents $\{H_1,\ldots,H_r\}$ is an *incident*. The *expected cost of an incident* $\{H_1,\ldots,H_r\}$ is expressed by the formula $E_i = p_{i1}\cdot E_1 +\ldots+ p_{ir}\cdot E_r$, where E_k denotes the expected cost of the incident (or simple incident) H_k, and p_{ik} denotes the probability of the incident H_k given H_i.

Example B.1: Consider Figure B.2.[5] The incident H_5 can result in C_8 and C_9, and only these. Hence, H_5 is a simple incident, and the expected cost of it is equal to $p_8 \cdot E_8 + p_9 \cdot E_9$. The incident H_2 generates a new incident H_5 and can also result in C_4. The expected cost of the incident H_2 is therefore equal to $p_4 \cdot E_4 + p_5 \cdot E_5$. E_4 is the cost of the simple incident consisting of the single consequence C_4, and E_5 (= $p_8 \cdot E_8 + p_9 \cdot E_9$) is the expected cost of the simple incident H_5. ■

The discussion about evaluation below is based on a one-level description, i.e., an incident does not generate new incidents. This does not cause any real restriction, because as mentioned in Chapter 1, a multi-level tree problem (where an incident generates new incidents) can always be transformed into a one-level problem. Before the evaluation, the next section presents the method in general.

The DEEP Method

This section describes the DEEP method and how it may be used to evaluate the effects of different actions to prevent possible incidents. By using the method, it is easier to realise which threats are the most important to handle and what effects will follow from the treatments. It is also important that the method can be adjusted to the risk policies of the specific companies using it.

Nine Risk Analysis Steps

The DEEP method is a systematic model for risk analysis using sophisticated methods for calculating in which order different threats should be handled as well as comparing different actions to each other. The analysis method is divided into nine steps.

An overview of the process is pictured in Figure B.3. The numbers in the figure relate to the steps in DEEP.

[5] For clarity, the indices have been simplified in the example.

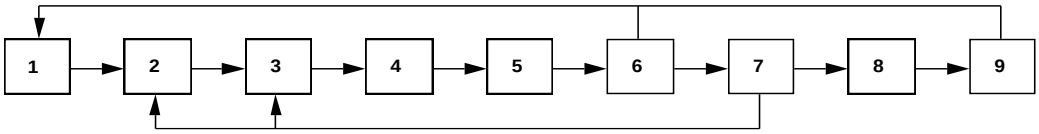

Figure B.3 The DEEP steps

The nine steps follow naturally after each other and comprise everything from investigating possible incidents to sensitivity analysis of the risk analysis. In every step, the results are documented in order to be able to easily return for a renewed analysis should the preconditions for the original analysis have been partially changed. Steps 1–3 and 8–9 are discussed only superficially, as this part of the thesis deals with applications of computational decision analysis and not risk analysis per se. The first three steps aim at providing a picture of the current risk exposure of the organisation under analysis.

1. Scope Analysis

When a risk analysis is planned, it is important to state clear goals for the analysis and delimit its scope. Seldom an entire corporation is to be analysed at the same time, and *Step 1* includes dividing the analysis into suitable parts and risk areas. A decision is often made only to handle pure losses, incidents that only generate costs since then it is easier to apply rational decision processes.[6]

2. Possible Damage

The *second step* in DEEP is to closer examine those parts of the company or organisation that are included in the analysis. Which incidents may occur? Which other incidents may follow as a result of primary damage? To what extent will the production process be interrupted? It is important to systematically identify all potential objects in danger of being damaged and all events that lead to damage to property,

[6] The other option would be to include risks that could result in incomes as well, so called business risks.

personnel, process interruption, liabilities, etc – not only the results of an incident.

3. Current Protection

Ensuing that, it is natural to closely study the current protection. It consists of both direct protection and indirect protection in the form of insurance. Typical questions in *Step 3* include: Is the protection level sufficient? What happens if the protection devices do not work as expected? Which is the appropriate balance between direct protection and insurance? The third step is concluded by investigating possible treatments. For every possible incident that has been identified, some alternative protections are listed. They should be at least two – keeping the current protection and improving it in some way. Often, there is more than one way of reducing the risk, and those alternatives differ with respect to costs and effects. For example, spreading the risk can be done in several ways, physically by changing the flow of work and goods or monetarily by increasing the level of insurance. Another example is reducing the risk, either by pre-incident actions (which decrease the probability of an incident occurring) or by post-incident actions (which decrease the cost of an incident that has already occurred).

4. Probabilities

The next two steps contain statements of probabilities and costs. For all alternative actions, the probabilities for the possible incident and the cost (or value) for the damage given that action are stated. This is done relative to the list of possible actions from the previous step. *Step 4* contains estimates of probability. To perform a reasonable risk analysis, it is necessary to estimate the frequencies of possible incidents. Sometimes, the frequency data available is sufficient, but in many cases the analyst must rely on more or less well-founded estimates.

5. Costs

In the same manner, *Step 5* contains the estimation of costs. This includes protection costs as well as costs incurred from damages. The costs can be expressed directly in monetary values or in some other appropriate scale. In those two steps, it is not unusual to find that the information available is insufficient and a supplementary investigation has to be made in order to achieve reasonable results. In these steps, it may even turn out that the problem has been structured in an unsuitable way, and that the terms of reference for the analysis have to be revised.

6. Evaluation

When all incidents have been identified and valued, it is time in *Step 6* to evaluate the alternative actions. Such an evaluation can be made with respect to different principles, for example minimising the expected loss. An important feature of the evaluation step is the ability to exclude acceptable risks from further evaluation with the aid of threshold levels.[7] If the potential cost for a specific risk is below the policy level of top management, it may be classified as acceptable and no more resources need to be used for further analysis of the accompanying threats.

7. Sensitivity Analysis

Even a thorough analysis may have much to gain from being subject to a sensitivity analysis, which is the purpose of *Step 7*. In this step, the probabilities and costs are altered in order to study the stability of the results. When the numbers are altered, the evaluation result will possibly change as well. Exactly where this occurs is interesting, because it indicates which input data is critical to the conclusions drawn. Those should be studied more closely since they help indicate the better use of the resources for analysis.

[7] Security levels through thresholds are described in Chapter 5 and Appendix A. Here, good alternatives are removed, but the reasoning involved is the same.

8. Implementation

When the evaluation process is concluded, the chosen actions are implemented in *Step 8*. This step is specific to the particular organisation and it also includes the financing of risks remaining after the actions have been taken. This financing could be done by using insurances.

9. Follow-up

After some time has elapsed, it is important to verify the results of the actions. Otherwise, the actions may have resulted in the problems being transferred to other problem areas, and *Step 9* is supposed to discover such problems.

As was explained above, during the analysis it may turn out to be necessary to collect further information or renew discussions made earlier. This feedback is illustrated by backward pointing arrows in the process in Figure B.3.

Evaluation in DEEP

When evaluating information from a consequence analysis, risk analysts using DEEP may use a formula expressing the expected cost of an incident, and this section demonstrates how the DELTA method can be modified to evaluate the expected cost in the same manner as the expected value is handled in Chapters 4–6.

A set of simple incidents is treated simultaneously since much can be gained from studying several interrelated incidents at the same time. The representation of *probabilities* is not considered here, since it is the same as in the original DELTA method of Chapter 4. The representation of *costs* is considered instead, the interpretations of admissible statements are formalised, and this is described for four types of possible cost statements.

1. The cost of the incident H_{ij} equals *m*, is at least *m*.

   Example: The cost of H_{ij} is greater than m.

Translation: $c_{ij} \in [m+\eta_1, m+\lambda_1]$

2. The cost of the incident H_{ij} is between some real numbers.

   Example: The cost of H_{ij} is between k_1 and k_2.
   Translation: $c_{ij} \in [k_1-\varepsilon_1, k_2+\varepsilon_1]$

3. The incident H_{ij} is as expensive as incident H_{ik}, more expensive than incident H_{ik}, the cost of incident H_{ij} is approximately equal to the cost of incident H_{ik}.

   Example: The incident H_{ij} is as expensive as incident H_{ik}.
   Translation: $c_{ij} - c_{ik} \in [-\varepsilon_2, +\varepsilon_2]$

4. The difference in cost between H_{ij} and H_{ik} is not less than the difference in cost between H_{im} and H_{in}.[8]
   Translation: $(c_{ij} - c_{ik}) - (c_{im} - c_{in}) \in [m+\eta_1, m+\lambda_1]$

The important point is that statements as above are translated into a system of linear inequalities that make them easy to handle in the DELTA method. If a risk analyst still is averse to the use of qualitative statements, he may use only interval statements instead.

The conjunction of expressions of the four types above is called the *cost base* K. The probability base and the cost base are linear systems and together constitute the *risk frame* ⟨C,P,K⟩. Evaluating a risk frame is mathematically equivalent to the evaluation of decision frames in Chapters 5–6. Hence, this appendix will not discuss those procedures but rather conclude with an example to illustrate the method.

Evaluation Example

The following example is supposed to show how the DEEP method works in steps 4–7. The much simplified numerical example concerns one burglary event during a given period and the estimates are imprecise. The purpose is to illustrate that the method can facilitate an

[8] For simplicity, assume that the cost of H_{ij} is greater than the cost of H_{ik} and that the cost of H_{im} is greater than the cost of H_{in}.

assessment as to which protective measures are reasonable even though only imprecise information is available.

Example B.2: A company desires to decrease its exposure to risk by installing more protective equipment and mechanisms at a certain production facility. The tax deduction period for such equipment is five years, and thus the analysis below is based on estimates of probability for a five year period.

First, the possible damages for the period are assessed. The assessment results in the following possible incident list.

H_1 No burglary attempts
H_2 All burglary attempts fail
H_3 A burglary succeeds

Table B.2 Incident list

The existing protective equipment is assessed and possible actions are listed. This list contains three possible alternative acts.

A_1 Keep the current protection
A_2 Add the improvements recommended by the insurance company
A_3 Additionally install more functionality as recommended by an independent security consultant

Table B.3 Action list

After that, an analysis commences which gives the following coarse estimates for the probabilities and costs for possible damages with respect to the different available courses of action. The costs listed include purchase costs for the equipment and costs for events that occurred.

Probabilities	No attempts	All attempts fail	Burglary
A_1 – Current protection	20–50%	10–20 %	30–60 %
A_2 – Insurance company	30–50%	20–50 %	15–30 %
A_3 – Ins.comp. + consultant	35–55%	30–60 %	10–20 %
Costs ($ million)	No attempts	All attempts fail	Burglary
A_1 – Current protection	0	0.1–0.3	2.5–6.5
A_2 – Insurance company	0.6–0.8	0.8–1.2	3.3–7.5
A_3 – Ins.comp. + consultant	2.2–2.6	2.4–3.1	5.2–9.1

Other statements

- The probability of 'No attempts' increases the more powerful protection is installed.
- The difference in costs between 'No attempts' and 'All attempts fail' is small if A_2 is chosen. It is estimated to be about \$0.2 to 0.4 million and is due to equipment only.
- Also the difference in costs between 'No attempts' and 'All attempts fail' is small if A_3 is chosen. It is estimated to be about \$0.2 to 0.5 million.

Table B.4 Estimated probabilities and costs

In this example, there are three incidents (H_1–H_3) to each of the three courses of action – the two additional protections plus keeping the current protection level during the period.

$p_{11} \in [20\%,50\%]$	$c_{11} \in [0.00,0.00]$	$p_{11} < p_{21} < p_{31}$
$p_{12} \in [10\%,20\%]$	$c_{12} \in [0.01,0.03]$	$p_{12} < p_{22} < p_{32}$
$p_{13} \in [30\%,60\%]$	$c_{13} \in [0.25,0.65]$	$c_{22} - c_{21} \in [0.02,0.04]$
$p_{21} \in [30\%,50\%]$	$c_{21} \in [0.06,0.08]$	$c_{32} - c_{31} \in [0.02,0.05]$
$p_{22} \in [20\%,50\%]$	$c_{22} \in [0.08,0.12]$	
$p_{23} \in [15\%,30\%]$	$c_{23} \in [0.33,0.75]$	
$p_{31} \in [35\%,55\%]$	$c_{31} \in [0.22,0.26]$	
$p_{32} \in [30\%,60\%]$	$c_{32} \in [0.24,0.31]$	
$p_{33} \in [10\%,20\%]$	$c_{33} \in [0.52,0.91]$	

Table B.5 Translated probabilities and costs

The costs have been transformed into the interval [0,1] by choosing the cost scale to be \$0–10 million. Now the evaluations can be carried out, using the machinery of Chapters 5–6. It is done by calculating the expected cost and expressing it as an interval. The upper bound of the interval is the maximum expected cost, and the lower bound of the interval is the minimum expected cost.

Probability hull	Symmetry hull
P1.1 = [0.200,0.500]	[0.243,0.500]
P1.2 = [0.100,0.200]	[0.114,0.200]
P1.3 = [0.300,0.600]	[0.343,0.600]
P2.1 = [0.300,0.500]	[0.315,0.500]
P2.2 = [0.200,0.500]	[0.223,0.500]
P2.3 = [0.150,0.300]	[0.162,0.300]
P3.1 = [0.350,0.550]	[0.350,0.532]
P3.2 = [0.300,0.550]	[0.300,0.527]
P3.3 = [0.100,0.200]	[0.100,0.191]

```
Value hull
V1.1 = [0.000,0.000]
V1.2 = [0.010,0.030]
V1.3 = [0.250,0.650]
V2.1 = [0.060,0.080]
V2.2 = [0.080,0.120]
V2.3 = [0.330,0.750]
V3.1 = [0.220,0.260]
V3.2 = [0.240,0.310]
V3.3 = [0.520,0.910]

Focal point
Cons.    P      V
C1.1:  0.371  0.000
C1.2:  0.157  0.020
C1.3:  0.471  0.450
C2.1:  0.408  0.070
C2.2:  0.362  0.100
C2.3:  0.231  0.540
C3.1:  0.441  0.240
C3.2:  0.414  0.275
C3.3:  0.145  0.715
```

For the actions A_1, A_2 and A_3 above expressions for the expected costs are obtained. These are denoted E_1, E_2, and E_3 respectively. For each action, both minimal and maximal expected costs have been calculated.

```
min E1 = 0.087
min E2 = 0.110
min E3 = 0.257

max E1 = 0.395
max E2 = 0.296
max E3 = 0.407
```

Table B.6 Expected costs

This means that the expected cost if action A_1 is chosen is in the interval \$870,000 to \$3,950,000. In the same way, the expected costs if actions A_2 or A_3 are chosen are in the intervals from \$1,100,000 to \$2,960,000 and \$2,570,000 to \$4,070,000 respectively. Note that these intervals are overlapping, and it seems hard to determine which action to choose based on those numbers only. Further analysis is required.

By contracting the estimates, the relationships among the three courses of action can be studied. One way is to study how the maximal and minimal expected costs behave under contraction. For a specific course of action to be better, it should have lower costs in the columns of Table B.7. Therefore, from the table it can be seen that action A_3, adding extra equipment as suggested by the security consultant, is more and more becoming the worst action the more the intervals are contracted. The overlap between A_1 and A_2 remains, however, and further analysis is necessary.

	0%	20%	40%	60%	80%
min E_1	0.087	0.109	0.132	0.158	0.186
min E_2	0.110	0.124	0.139	0.154	0.171
min E_3	0.257	0.269	0.282	0.295	0.309
max E_1	0.395	0.355	0.317	0.281	0.247
max E_2	0.296	0.273	0.250	0.229	0.208
max E_3	0.407	0.389	0.372	0.355	0.339

Table B.7 Minimal and maximal expected costs

Figures B.4–B.6 are graphic representations of the table.

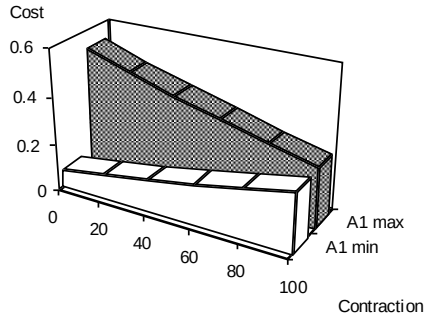

Figure B.4 Action A_1

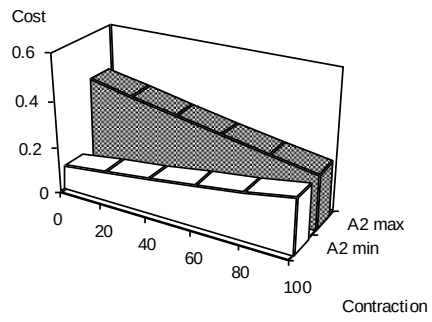

Figure B.5 Action A_2

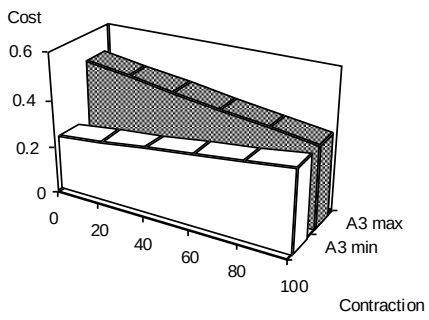

Figure B.6 Action A_3

The first evaluation was based on independent evaluation of the alternatives. The main evaluation using Δ-dominance is the next step in the DEEP evaluation. To be able to study the differences more clearly, pairwise comparisons are carried out. The results for string and weak dominance are presented in Table B.8 and illustrated in the three comparative graphs in Figures B.7–B.9. The table shows the smallest and largest difference between the courses of action. It can now more clearly be seen that action A_3 is inferior in that it is strongly NE-dominated because fairly early in the contraction process it receives positive differences, meaning it is more expensive than the others.

	0%	20%	40%	60%	80%
min $(E_1\text{-}E_2)$	-0.201	-0.160	-0.115	-0.069	-0.023
min $(E_1\text{-}E_3)$	-0.314	-0.276	-0.237	-0.197	-0.153
min $(E_2\text{-}E_3)$	-0.274	-0.246	-0.220	-0.196	-0.168
max $(E_1\text{-}E_2)$	0.284	0.231	0.178	0.127	0.076
max $(E_1\text{-}E_3)$	0.137	0.085	0.035	-0.014	-0.062
max $(E_2\text{-}E_3)$	0.038	0.002	-0.033	-0.067	-0.101

Table B.8 Pairwise comparisons between the alternatives

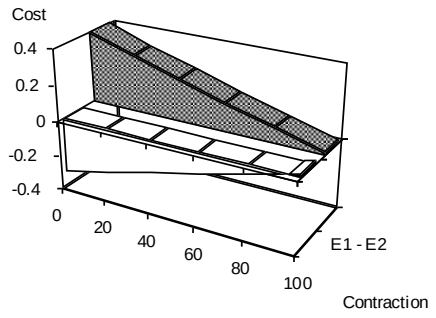

Figure B.7 Actions A_1 and A_2

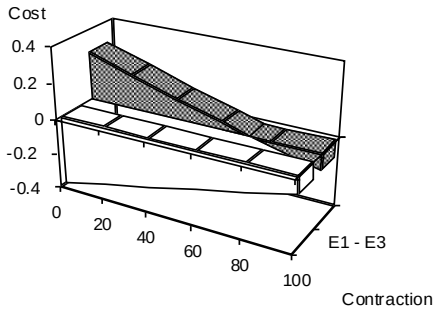

Figure B.8 Actions A_1 and A_3

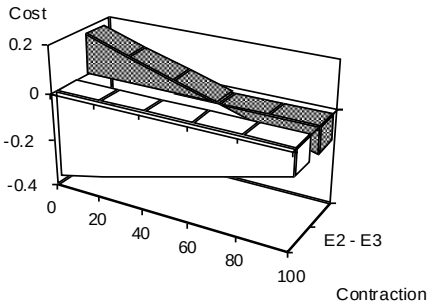

Figure B.9 Actions A_2 and A_3

To be able to discriminate between actions A_1 and A_2, further sensitivity analysis is recommended, for example by contracting subsets of intervals, not all at the same time. This will not be carried out here, since the purpose of the example is to give an impression of how DEEP can evaluate risk information. Possibly, more information is needed about the two courses of action that remain. Especially the estimates of the probabilities when burglary attempts fail are critical. If, after further analysis, it is not possible to obtain more conclusive indications, then it is an indication that the actions are indeed very similar relative to the model data. Then other activities, like contacting more equipment vendors or other insurance companies might help.

This concludes the evaluation example and the description of the DEEP method as well. A longer description can be found in [DEE96].

Every year is getting shorter
Never seem to find the time
Plans that either come to naught
Or half a page of scribbled lines

Far away across the field
The tolling of the iron bell
Calls the faithful to their knees
To hear the softly spoken magic spells

– R. Waters