	
DECRIS ARBEIDSNOTAT 3	
TITTEL	
DECRIS –Description of InfraRisk (Beskrivelse av verktøy InfraRisk)	
FORFATTERE Jørn Vatn	
SAMMENDRAG	
The tool <i>Infrarisk</i> for risk analysis of critical infrastructure is described	
ISBN	DATO 2007-12-17.
GRADERING ÅPEN	ANTALL SIDER 35
KONTAKT DENNE RAPPORT Jørn Vatn	ADRESSE Jorn.vatn@ntnu.no , tlf 73597109/41473730
NØKKEWORD NORSK Risiko, sårbarhet, kritisk infrastruktur, risikokommunikasjon	NØKKEWORD ENGELSK Risk, vulnerability, critical infrastructure, risk communication

Table of content

Table of content	2
List of tables	3
List of figures	3
1 Introduction.....	4
2 Method description – simplified analysis	5
2.1 Anchoring of the process	5
2.2 Definition of scope.....	5
2.3 Identification of main events for the analysis	5
2.4 Elements of the main events analysis.....	5
2.4.1 Societal critical functions.....	6
2.4.2 Vulnerabilities.....	7
2.4.3 Probability assessment	8
2.4.4 Assessment of consequences	9
2.5 Visualize the result in a risk matrix.....	11
3 Method description – comprehensive analysis.....	12
3.1 Frequency analysis	14
3.2 Consequence analysis.....	17
4 Main events and societal critical functions (SCFs).....	20
5 Using the computerized tool - InfraRisk	27
5.1 Analyzing main events.....	28
5.2 Filtering events.....	30
5.3 Configuration	31
5.4 Analysis.....	31
5.4.1 SCF ranking	31
5.4.2 SCF improvement potential	32
5.4.3 SCF listing.....	32
5.4.4 More analyses... ..	32
5.4.5 Summary of commands and functions.....	32
Index	35

List of tables

Table 1 Type and strength of relation between the SCF and the main event.....	6
Table 2 Vulnerability factors and their values	7
Table 3 Consequence classes for each consequence dimension	9
Table 4 Consequence matrix, quality and delivery of service	10
Table 5 Proposed calibration of the risk matrix	11
Table 6 List of main events	20
Table 7 List of societal critical functions	23

List of figures

Figure 1 Bow tie model.....	12
Figure 2 Bow tie model with fault- and event tree.....	12
Figure 3 Fault tree for the pump station.....	14
Figure 4 LoadSCF statement.....	16
Figure 5 Specification of TOP event frequency.....	16
Figure 6 Result of compilation.....	17
Figure 7 Probability specification of an emptied water storage tank.....	17
Figure 8 Lifeline unavailability.....	18
Figure 9 Event tree with water tank and water trucks as barriers	18
Figure 10 Vulnerability factor.....	18
Figure 11 Statements to complete the event tree analysis.....	19
Figure 12 Main menu of InfraRisk.....	27
Figure 13 Screen for analyzing main events	28
Figure 14 Plot main events in the risk matrix	29
Figure 15 Text editor for specifying the detailed model	30
Figure 16 Calibration of risk matrixes	31

1 Introduction

This document presents a method description for identification and estimation of risk related to critical infrastructure. The method primarily focuses on the identification and estimation of the risk. The subject of identifying risk reducing measures, and a plan for implementation is not a part of this report.

A computerize tool has been developed to assist the risk analysis process. The tool named InfraRisk is described in detail in Chapter 5. The tool supports two analysis levels. On the first level the tool works very much as a so-called preliminary hazard analysis (PHA). Risk is directly assessed by specifying frequencies and consequences. The starting point for this analysis is a predefined list of main events related to critical infrastructure. For each main event it is possible to link societal critical functions (SCFs) that are relevant for main event under consideration. This simplified method for risk analysis is described in Chapter 2. In Chapter 3 we introduce a more comprehensive analysis method. In the comprehensive analysis it is possible to perform a more explicit linking between the SCFs and the main event. Typically such relations are established by fault tree analysis (FTA) and event tree analysis (ETA). The InfraRisk tool does not currently support a graphical FTA or ETA editor. But the user may specify the fault and event trees by a command language. Examples of how these commands are used are given in Chapter 3.

Chapter 2 contains a broader scope for the analysis process compared to Chapter 3, i.e., in Chapter 2 the definition and structuring of the analysis is elaborated, whereas we in Chapter 3 put more focus on the details of risk modelling supported by the InfraRisk tool.

2 Method description – simplified analysis

In the following we highlight main elements of the procedure for risk identification and estimation for urban critical infrastructure. It shall be noted that the method is very general, and may be used also in other areas of concern. A computerized tool, InfraRisk, has been developed to help structuring the process. In this chapter a simplified analysis is describe where the risk is assessed and plotted directly into risk matrixes. In chapter 3 a more comprehensive analysis is described where probabilistic models are introduced to assess frequencies and consequences. Also for the comprehensive analysis, the risk picture could be visualised by risk matrixes, but now the link to the societal critical functions and vulnerabilities are made explicit.

2.1 Anchoring of the process

The method needs anchoring in national ministries or at a European level because decisions on risk reducing measures will be taken on a high national level. For more dedicated analyses, it may also be possible to anchor the process on a municipal level.

Further the method need anchoring in governing documents, and sufficient resources need to be allocated. A separate process organization shall be established to ensure that the method will be executed as planned. A national coordinator will be necessary to ensure comparable approaches between areas.

2.2 Definition of scope

The scope of the analysis must be clearly defined in terms of which areas shall be covered, which level of detailed will be appropriate for the current analysis, what will be the use of the analysis etc.

2.3 Identification of main events for the analysis

Reference is made to the scope definition of the analysis. The main events are the focus for the analysis. Table 6 in Chapter 4 presents a list of main events to be included in the analysis. The list is presented in a hierarchical form, and for a given analysis the aim is to conduct the analysis on the same level. The level of detailing will depend on the available resources and the scope of the analysis

2.4 Elements of the main events analysis

To describe the risk level we basically assess the probability of occurrence of the main events, and the consequences with respect to:

- Life and health
- Environment
- Economy
- Manageability
- Political trust
- Supply failure, both quality and availability of delivery

In order to analyse probability and consequences the analysis is structured by the following assessments:

- Assessment of societal critical functions (SCF) that are relevant for the scenario being covered by the main event, and the importance of each SCF in the scenario
- Assessment of relevant vulnerability factors, and the importance of these in the scenario

Figure 14 on page 28 shows the analysis screen for the main events.

2.4.1 Societal critical functions

Societal critical functions (SCFs) are functions that if they fail to deliver the required output will reduce the quality of life. Table 7 in Chapter 4 present a list of SCFs that could be linked to each main event. One or more SCF could be specified for each main event. The SCFs could be linked to the main events in three manners:

- Loss of, or reduction in the performance of the SCFs could be the *cause* for the main events. In this situation we say that the SCF works “before” the main event.
- The loss of, or reduction in the performance of the SCFs will increase the consequences if the main event occurs. In this situation we say that the SCF works “after” the main event, i.e. it operates as a barrier or a mitigating factor
- The occurrence of the main event will threaten the performance of the SCF

For each SCF linked to the main event we also identify the type of relation to the main event. We also identify the strength of the relation between the main event, and the SCF by specifying one of the codes in Table 1:

Table 1 Type and strength of relation between the SCF and the main event

Code	Text
I100	Loss of SCF is the initiating event in the scenario
B100	SCF acts as a complete barrier
R90	SCF is very important for the scenario
R60	SCF is important for the scenario
R40	SCF is medium important for the scenario
R15	SCF is not very important for the scenario
R05	SCF is hardly important for the scenario
V90	SCF is very vulnerable wrt the main event
V60	SCF is vulnerable wrt the main event
V40	SCF is medium vulnerable wrt the main event
V15	SCF is not very vulnerable wrt the main event
V05	SCF is hardly vulnerable wrt the main event

The numbers in the code field represent the importance of the SCF with respect to the scenario being analysed. When a criticality measure is established, this number is used to give a score of the SCF.

2.4.2 Vulnerabilities

The various main events may be affected by one or more vulnerability factors. Typically, these vulnerability factors are important when assessing the consequence of the main events. A list of vulnerability (risk) factors are listed in Table 2. It is possible to add more than one vulnerability factor to each main event. We also specify the influence of the vulnerability factors according to the suggested influences in Table 2. For some of the main events, the consequences of the event will depend significantly on the type of influence that will occur in a given situation. Since this is not known at the point of time of the analysis, one therefore could add two main events with the same event type code, but with different value of the vulnerability factor influences, and hence also different consequences. In the probability statement we then could include the probability of the corresponding vulnerability factor influences to occur.

Table 2 Vulnerability factors and their values

Vulnerability Factor	Influence	Comment
Area	(1) Minor	Open ground
	(2) Small	Transportation trace
	(3) Medium	Street in town, dens building mass, landslide risk area etc
	(4) Huge	Close to dangerous installation, factors etc
	(5) Very huge	Terminal for person traffic or tunnel
Geographic scope	(1) Local	+ neighbourhood in large city or equivalent
	(2) City	+ Large city, major suburbia
	(3) Region	Limited to regions
	(4) National	+ Capital
	(5) International	If current country is affected
Population density pr 1 km ²	(1) 1 - 4	Isolated village settlement
	(2) 5 - 29	Village settlement
	(3) 30 - 199	Open settlement
	(4) 200 - 499	Suburbia
	(5) 500 - 15200	Cities
Outdoor temperature	(1) +20 °C - +30 °C	No heating or cooling demand
	(2) +5 °C - + 20 °C	Some heating demand
	(3) -5 °C - +5 °C, > +30 °C	Significant heating or cooling demand
	(4) -20 °C - -5 °C	Large heating demand
	(5) < -20 °C	Heating critical for survival
Time of day	(1) Night	Silence
	(2) Evening	Most people are at home
	(3) Working hours	Most people are at work
	(4) Early morning	Early morning
	(5) Rush hours	From and to work, school etc
Duration	(1) < 1 day	Fast normalization

Vulnerability Factor	Influence	Comment
	(2) < 1 week	Normalization within weeks
	(3) > 1 month	Normalization takes more than one months
	(4) > 6 months	Normalization takes up to one year
	(5) Quasi permanent	Years or decades to normalize
Dependency with other social critical functions	(1) Very little	Small dependencies
	(2) Little	Medium asymmetric dependencies
	(3) Medium	Medium symmetric dependencies
	(4) Huge	Strong Medium symmetric dependencies
	(5) Very huge	Strong symmetric dependencies
Substitution opportunities for infrastructure	(1) Very huge	Easy substitution
	(4) Huge	Substitution with some problems
	(3) Medium	Substitution requires significant effort
	(4) Little	Substitution difficult
	(5) Very little	Indispensability
Degree of coupling	(1) Very little	Anarchism
	(2) Little	Simple set of rules sufficient for activity functions
	(3) Medium	Complex set of rules sufficient for activity functions
	(4) Huge	Operative governing functions necessary
	(5) Very huge	Strong centralized governed with small tolerance for deviations
Culture	(1) Very favourable	Frankness, humility, real competence, honesty
	(2) Favourable	Cooperation climate, looks for opportunities, consciousness
	(3) Medium	Caution, delays, naivety
	(4) Unfavourable	Reluctance, anxiety, isolation
	(5) Very unfavourable	Power struggle, closed, dishonesty
Mental preparedness	(1) Very favourable	Frequent targeted training
	(2) Favourable	Significant effective measures
	(3) Medium	Good risk consciousness, some measures
	(4) Unfavourable	Under communicated risk
	(5) Very unfavourable	Lack of potential risk consciousness

2.4.3 Probability assessment

The probability of occurrence of each main event shall be assessed based on the following classes:

1. Very unlikely Less than once pr 1000 year
2. Remote Once pr 100-1000 year
3. Occasional Once pr 10-100 year
4. Probable Once pr 1-10 year

5. Frequent More than once a year

Note that the assessment will depend on the scope of the analysis. If only a small country or a specific city is considered, the probabilities will generally be small. However, if the analysis is conducted on a European level, the most probable classes apply. To be precise we should rather use the word *frequency* rather than *probability* because the event may occur more than once in a time interval

To help assessing the probabilities the following should be considered:

- The vulnerability factors in Table 2
- If any of the safety critical functions relates to the probability of occurrence
- Statistics both on a national level, but also international statistics in case of very rare events
- Use the threat components “intention” and ”capability” to consider malicious events whenever relevant
- Dynamic changes in the threat picture
- The assessment shall be supported by qualitative argumentation

2.4.4 Assessment of consequences

The consequences of each main event should be assessed in terms of consequence classes defined in Table 3. The classes are the same for all consequence dimensions, but the narrative description varies between consequence dimensions.

Table 3 Consequence classes for each consequence dimension

Consequence dim.	Class	Description
Life & Health	(1) Delimited	Up to 5 fatalities, Up to 20 injured
	(2) Some damage	Up to 50 fatalities, Up to 200 injured
	(3) Serious	Up to 300 fatalities, Up to 1200 injured
	(4) Critical	Up to 1000 fatalities, Up to 4000 injured
	(5) Catastrophic	More than 1000 fatalities, More than 4000 injured
Environment	(1) Delimited	Minor environmental changes
	(2) Some damage	Major environmental changes
	(3) Serious	Moderate environmental injurious to health changes
	(4) Critical	Store environmental injurious to health changes
	(5) Catastrophic	Destruction of human habitat
Economy	(1) Delimited	Up to 0.01 % of GNP
	(2) Some damg.	Up to 0.1 % of GNP
	(3) Serious	Up to 1 % of GNP
	(4) Critical	Up to 10 % of GNP
	(5) Catastrophic	More than 10 % of GNP
Manageability	(1) Delimited	No or minor disturbances
	(2) Some damage	Short disturbances
	(3) Serious	Major disturbances

Consequence dim.	Class	Description
	(4) Critical	Serious disturbances
	(5) Catastrophic	Critical disturbances, permanent changes
Political Trust	(1) Delimited	No significant effects
	(2) Some damage	Passively constructive, loyalty, adoption
	(3) Serious	Actively constructive, disturbances, protest, demanding changes
	(4) Critical	Passively destructive, non-participation, substitutional behaviour
	(5) Catastrophic	Actively destructive, political exit, violence, system delegitimizing, system change
Loss Of Infrastructure	(1) Delimited	See Table 4 for definition of consequence classes according to number of persons affected, and duration of outage or loss of quality. Note that the matrix could be configured (calibrated).
	(2) Some damage	
	(3) Serious	
	(4) Critical	
	(5) Catastrophic	

Table 4 Consequence matrix, quality and delivery of service

	0 - 6 hours	6 - 24 hours	1 - 7 days	1 - 4 weeks	One to 6 months	More than 6 months
1 - 10 persons	Delimited	Delimited	Delimited	Some Damages	Some Damages	Serious
10 - 100 persons	Delimited	Delimited	Some Damages	Some Damages	Serious	Serious
100 - 1 000 persons	Delimited	Some Damages	Some Damages	Serious	Serious	Critical
1 000 - 10 000 persons	Some Damages	Some Damages	Serious	Serious	Critical	Critical
10 000 - 100 000 persons	Some Damages	Serious	Serious	Critical	Critical	Catastrophic
More than 100 000 persons	Serious	Serious	Critical	Critical	Catastrophic	Catastrophic

The following shall be taken into account when assessing the consequence classes

- The consequence is assessed conditional on the situation where the main event occurs
- Consequences are assessed for all main events, and all consequence dimensions
- Consider which SCF in addition to the "main SCF" that influence the main event, and how much

- Consider identified vulnerability factors with respect to their impact on the consequence, given the main event has occurred. If measures have been implemented against the vulnerability factors this should be taken into account in the assessment
- Consideration of historical consequences, both domestic events, and international events when information is available
- The assessment shall be supported by qualitative argumentation

2.5 Visualize the result in a risk matrix

A risk matrix is used to visualize the result. The format of the risk matrix is shown in Table 5. Separate matrixes may be established for each consequence dimension, i.e., personal safety, environment, economy etc. It is also possible to plot the worst risk dimension for each main event to get an overall overview of the various events. Each event is given a unique identifier, which is plotted in the cells of the risk matrixes to visualise more than one event at a time. See Figure 14 page 29 for an example.

Table 5 Proposed calibration of the risk matrix

Probability	(5) More than once a year	Low risk	Medium risk	High risk	Very high risk	Very high risk
	(4) Once pr 1-10 year	Low risk	Medium risk	Medium risk	High risk	Very high risk
	(3) Once pr 10-100 year	Very low risk	Low risk	Medium risk	Medium risk	High risk
	(2) Once pr 100-1000 year	Very low risk	Low risk	Low risk	Medium risk	Medium risk
	(1) Less than once pr 1000 year	Very low risk	Very low risk	Very low risk	Low risk	Medium risk
		(1) Delimited	(2) Some damage	(3) Serious	(4) Critical	(5) Catastrophic
		Consequences				

3 Method description – comprehensive analysis

In this chapter we describe a detailed risk analysis procedure where it is possible to explicitly link societal critical functions (SCFs) and vulnerability factors to the risk picture. The starting point for the detail analysis is still the main events as described in chapter 2. As a mental model for the comprehensive analysis we apply the so-called Bow tie model shown in Figure 1.

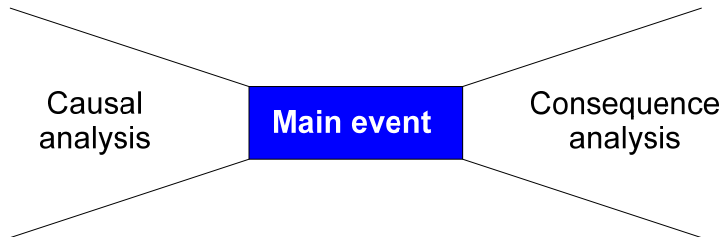


Figure 1 Bow tie model

There exist several methods for the “causal analysis”, but fault tree model analysis seems to be the most common one. Similarly, the most common consequence analysis model is event tree analysis. The bow tie model with fault- and event tree is illustrated in Figure 2. The end consequences to the right correspond to those described in Chapter 2.4.4. Separate analyses are performed for each consequence dimension like personal safety, environment and so on.

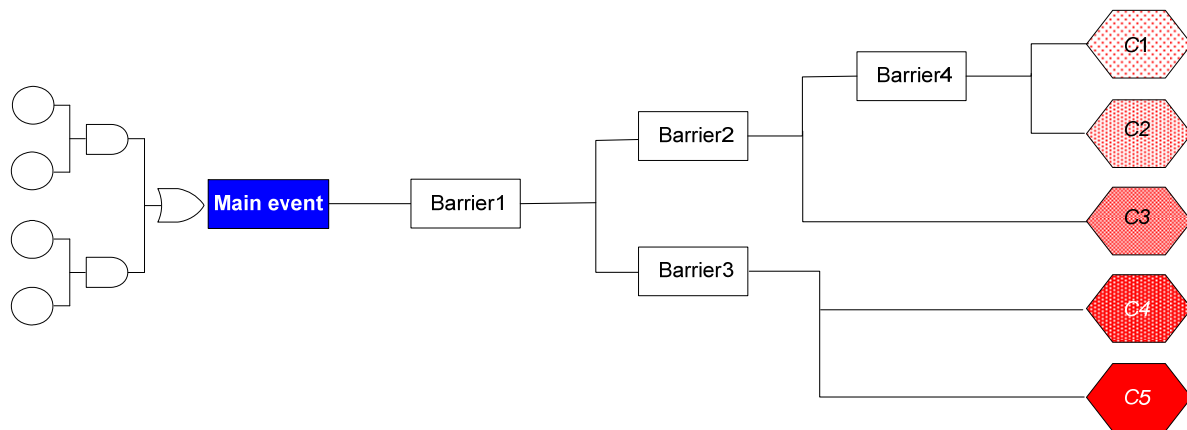


Figure 2 Bow tie model with fault- and event tree

Each main event is analysed separately. The frequency and consequence analysis are conducted by fault tree statements, and event tree statements. Typically the frequency of the main event is assessed by a fault tree analysis (FTA) comprising one or more SCFs. Next, the consequence analysis is conducted by a mixture of event tree, and fault tree analysis. Currently the FTA and ETA (Event Tree Analysis) is not supported by a graphical interface, but the event trees and fault trees are specified by commands.

The detailed model is specified in a text editor. The editor is loaded by pressing the “Edit formula” button from the “Analysis of Main Events” screen, see Figure 13. The required steps for defining the model are as follows:

1. Define attributes for each SCF. An attribute is typically the occurrence frequency of the SCF, the mean downtime (repair time after component failure), and/or a probability of failure on demand (PFD) of the SCF.
2. Define attributes for each vulnerability factor, or risk influencing factor (RIF). Attributes for vulnerability factors or RIFs are typically performance measures, like 1=very good, up to 5=very bad.
3. Define a fault tree to determine the occurrence frequency of the main event. A fault tree comprises a combination of AndGates and OrGates. The arguments (inputs) to these gates are either other gates, numeric values, or expressions containing SCF attributes and/or vulnerability attributes.
4. Define event trees to determine the probability of each consequence class for each dimension life and health, environment, etc. Such an event tree could also contain fault trees determining the failure probability of a barrier. Barrier probabilities are specified by reference to a fault tree, by numeric values, and/or by expressions containing SCF attributes and/or vulnerability attributes.

By this detailed specification of the model we are now able to:

1. Calculate the frequency of each consequence class for all dimensions (safety and health, environment, economy etc.) both for each main event, and totally for a set of main events
2. Calculate an importance measure for each SCF and/or vulnerability factor. The importance measure is a “improvement” potential measure, i.e. what will be the total risk reduction if the SCF is brought to a perfect state.

Note that these measures may also be calculated if one or more main events only are analyzed with the simplified approach. Note, however, that in the simplified approach frequencies represent interval ranges, and the consequences take only one value (and not a probability distribution over the consequence values). Further, the link between SCFs and the risk is rather vague.

To describe the detailed steps required to build the risk model, we will introduce an example where the main event is described by the following four levels (from Table 6 on page 20):

1. Technical catastrophe (T)
2. Failure to deliver (critical infrastructure) (D)
3. Lack of water (1)
4. Waterworks and purification (2)

Only a subset of relevant SCFs and RIFs will be included in the example. The SCFs to be considered are:

1. Critical infrastructure, remaining (C); Water and sewage systems (1); Distribution networks (4); Pumps
2. Critical infrastructure, basic (B); Electrical power (1); Distribution net (3)
3. Critical infrastructure, remaining (C); Water and sewage systems (1); Distribution networks (4); Water tanks

and the vulnerability factors/RIFs considered are:

1. Operational procedures
2. Level of maintenance and renewal

3.1 Frequency analysis

The first step in the frequency analysis is to be explicit about the main events. In fault tree terminology this means to define the so-called TOP event in an unambiguous manner. The TOP event will be identical to the main event found in Table 6. However, a specification of the content of the main events has to be performed. In our example we will consider a pumping station, and we let the TOP event be “failure of the pumping station”. In our example we also have assumed that a water storage tank (height reservoir) is a buffer acting *after* the main event. This means that if the main event occurs (pumping station fails), the consumers will still have water for a period of time depending on the capacity of the water storage tank. Note that it would also be possible to include the water tank in the main event (as part of the frequency analysis). Then the TOP event would have been something like “Unacceptable low pressure downstream of the water tank”.

To model the occurrence of our TOP event we will use fault tree analysis. In the analysis we assume that the pumping station basically comprises three main pumps, each pump having a capacity of 50%. A system comprising of three 50% units are usually modelled by a so-called 2-out-of-3 (2oo3) gate in the fault tree. To model the three pumps with a (binary) fault tree is a simplification, where in fact only two states are considered, the fault state where two or more pumps are in a fault state, and the functioning state where two or more pumps are functioning. In a more advanced model we could also have differentiated between the situation where all pumps have failed (no flow into the water storage tank), and the situation where one pump is still functioning (and a reduced flow into the water storage tank, extending the time period where there still is water left in the tank).

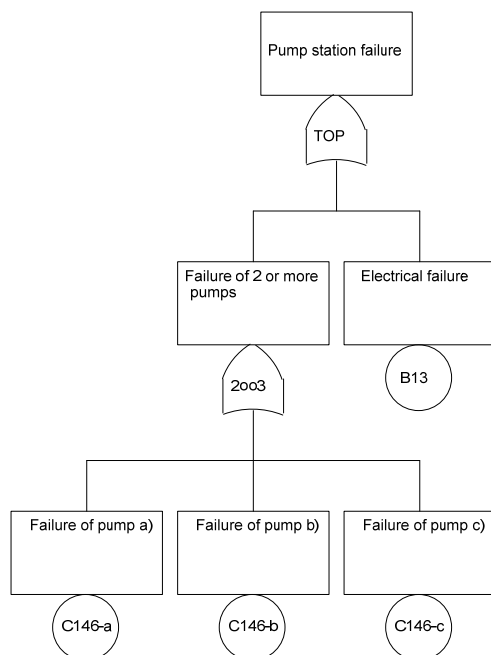


Figure 3 Fault tree for the pump station

There exist a huge number of computerized tools to conduct a fault tree analysis, see <http://www.ntnu.no/ross/info/software.php> for a comprehensive list. In our situation, we would rather want to integrate the fault tree analysis into our analysis tool. To be able to integrate the fault tree into the total analysis we therefore use a simplified fault tree engine provided by the tool. Our fault tree engine comprises a set of available functions. These functions could be invoked by a set of statements specified in a text editor. See @@.

The fault tree statements basically comprise a combination of statements containing:

- AndGate's
- OrGate's
- KooNGate's

The AndGate statement is used when each input to the gate have to occur in order to ensure that the gate occurs. The OrGate statement is used when it is sufficient that one or more of the inputs have to occur in order to ensure the gate to occur. The KooNGate statement is used when the occurrence of K or more out of N inputs ensure the gate to occur.

Before we can use these statements we have to define the parameters describing so-called basic events. The basic events are the leaf nodes in the fault tree. In Figure 3 the basic events are those events with a circle below the descriptive text. The required parameters depend on the modelling situation. We will discriminate between two situations:

- A frequency analysis where the output from the gates is a frequency, i.e. it is an occurrence rate. We will here always assume that the frequency is specified in terms of expected number of occurrences *per year*. Frequency modelling usually applies in the causal analysis part of the bow tie model.
- A probability analysis where the outputs from the gates are probabilities, i.e. a number between 0 and 1. A probability analysis is typically used to model barrier probabilities, typically in the consequence analysis part.

The analysis is easiest to conduct when we only treat probabilities. In this situation it is sufficient to specify only one probability parameter for each basic event. When we conduct a frequency analysis we need to specify both the occurrence frequency, and the duration of the occurrence (repair times).

In the example we will assign reliability parameters to the various SCFs. We then use the LoadSCF statement as shown in Figure 4:

```

LoadSCF C146 AS Pump
Lambda = 2
MTTR = 8/8760
End Load

LoadSCF B13 AS Electricity
Lambda = 0.1
MTTR = 8/8760
End Load

```

Figure 4 LoadSCF statement

For each SCF to load data for, we use a separate LoadSCF statement. The syntax is:

```

LoadSCF <SCF-ID> [AS <Alias>]
<Parameter1> = <expression>
[<Parameter2> = <expression>
:]
End Load

```

The <SCF-ID> must be identical to the SCF code used in the hierarchy of SCFs, see Table 7 page 23. The <Alias> is a more meaningful name for the SCF, e.g. Pump. Alias names cannot include spaces, or special characters. After the LoadSCF statement, reliability parameters are specified. In the example we have used Lambda to indicate the failure rate, and MTTR to indicate the mean time to repair. Note that the time unit is assumed to be *years*, hence the failure rate of the pump is 2 failures in average per year, and the mean time to repair is 8 hours. The LoadSCF statement is terminated by an End Load statement.

Note when we are referring to the parameters, we use the alias as a prefix to differentiate between the parameters for different SCFs. For example, Pump.Lambda.

To define the frequency of the TOP event, we now use the specifications shown in Figure 5:

```

PumpFailures = fKooNGate(2, Pump.Lambda, Pump.MTTR, _
Pump.Lambda, Pump.MTTR, Pump.Lambda, Pump.MTTR)
Frequency = OrGate(Electricity.Lambda, PumpFailures)

```

Figure 5 Specification of TOP event frequency

We have used the “frequency” version of the KooNGate, i.e., the fKooNGate since we are heading for a frequency, and not a probability. The first argument in the fKooNGate is K , meaning the number of failures that will cause the gate to occur. In the example $K = 2$. Then follows in pairs, the failure rate, and the mean time to repair for each input (pumps a , b and c in the example). In our example we have assumed that the three pumps have the same failure rate, and the same mean time to repair. Note that the statement was too long to fit on one line, hence we have used the concatenation characters “_”. Also note the space before “_”. PumpFailures is a new variable we have created. The variable is used to temporarily hold the frequency of pump failures.

The second statement in Figure 5 is an ORGate statement because a pump station failure will occur if either the electricity fails, or two or more of the pumps fail. Since an OR gate just represent a sum of the input frequencies (or probabilities), it is not required to specify the repair times.

The variable `Frequency` is a reserved name. When the statements shown in Figure 4 and Figure 5 are compiled, the frequency of the main event is set to the content of the `Frequency` variable. The result from the compilation is shown in a separate window in `InfraRisk`, e.g., as in Figure 6:

```
Pump.Lambda=2
Pump.MTTR=9.13242E-04
Electricity.Lambda=0.1
Electricity.MTTR=9.13242E-04
PumpFailures=2.191781E-02
Frequency=0.1219178
```

Figure 6 Result of compilation

Also note, that a frequency of 0.12 occurrences per year represents the category *Occasional*, i.e., once per 1-10 year as defined in `InfraRisk`. This means, when the statements are compiled, any frequency statement made explicit, will be replaced with the calculated one.

3.2 Consequence analysis

We will make a very simple consequence model. The critical situation is when the water tank becomes empty. In this situation we might have both a quality problem due to low pressure in the pipes, and lack of water. If we assume exponentially distributed repair times, the expected repair time given an electricity failure, or a failure of the 2003 pump system will be 8 hours. Since the capacity of the water storage tank is assumed to be 24 hours, the probability that the tank becomes empty is $\exp(-24/8)$. Thus we make the following statement:

```
LoadSCF C144 AS WaterTank
Empty = exp(-24/8)
End Load
```

Figure 7 Probability specification of an emptied water storage tank

We will assume that if the water tank is not emptied, there will be only *delimited* consequences with respect to water (lifeline) availability. However, if the tank is emptied, we assume *critical* consequences with respect to water availability. To specify the distribution over the consequence categories for lifeline unavailability we now specify in Figure 8:

```
LifelineUnavailability = Dist(1-WaterTank.Empty, _
0, 0, WaterTank.Empty, 0)
```

Figure 8 Lifeline unavailability

Note that `LifelineUnavailability` also is a reserved variable which will be used when we want to specify the probability distribution over the lifeline unavailability. See 5.4.5 for a reference of all reserved variable names for consequence distributions.

The `Dist()` function is used to assign a probability for each value (category) of the variable `LifelineUnavailability`. It is required to specify exactly 5 arguments in the `Dist()` function. Argument one represents the probability of category 1 (Delimited), argument two represents the probability of category 2 (Some Damages), up to argument five which represents the probability of category 5 (Catastrophic). In the example, only two values are different from zero, i.e. the first, and the fourth category. The variable `WaterTank.Empty` was specified in Figure 7.

We will now improve the modelling by also including the possibility of efficient use of water trucks for distribution of water to the consumers. In the example we now assume that efficient use of water trucks will reduce consequence category 4 (critical) to consequence category 3 (serious). The corresponding event tree is shown in Figure 9.

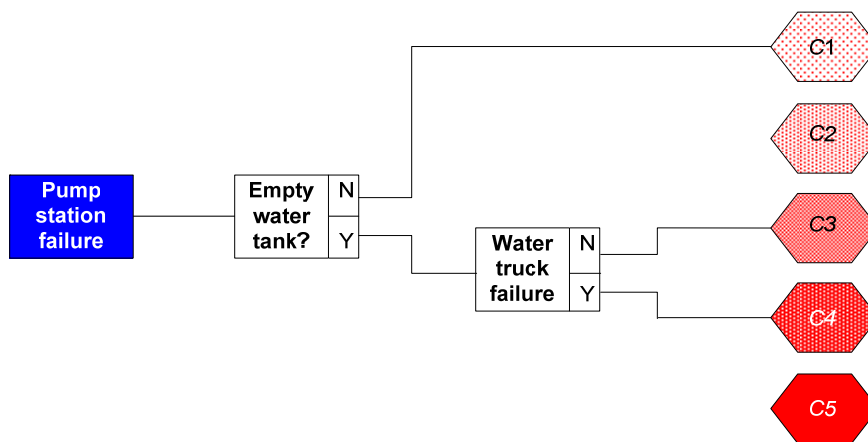


Figure 9 Event tree with water tank and water trucks as barriers

To model the event tree we will assume that the probability of failure of efficient use of water trucks is influenced by the vulnerability factor `OperationalProcedures`. To load the quality of this factor into the model, we use the `LoadRIF` statement in Figure 10:

```
LoadRIF OperationalProcedures AS Procedures
Quality = 4
End Load
```

Figure 10 Vulnerability factor

The syntax is similar to the LoadSCF statement. Here we have used the same scoring regime as defined by the general vulnerability factors in Table 2, hence a value of 4 represents “Unfavourable”.

To complete the event tree statements corresponding to the event tree in Figure 9 we write:

```
WaterTruckFailure = RIF1To5(Procedures.Quality, 0.01, 0.9)
LifelineUnavailability = Dist(1-WaterTank.Empty, 0, _
WaterTank.Empty*(1-WaterTruckFailure), _
WaterTank.Empty*WaterTruckFailure, 0)
```

Figure 11 Statements to complete the event tree analysis

The first line in Figure 11 assigns a probability to the variable WaterTruckFailure by use of the RIF1To5(<RIFValue>, <LowProb>, <HighProb>) function. This function calculates a failure probability according to the value of <RIFValue>. When the RIF value takes the best value (1) the <LowProb> will be returned and when the <RIF value takes the worst value (5) the <HighProb> will be returned. Between these two values a exponential interpolation is performed. In the example we have assumed that the probability of water truck failure is 1% in the best situation, and 90% in the worst situation.

4 Main events and societal critical functions (SCFs)

The main events and societal critical functions to include in the analysis is listed in Table 6 and Table 7 respectively. The code structure is used for easy references.

Table 6 List of main events

Events in hierarchy				Code values			
L1	L2	L3	L4	L1	L2	L3	L4
Natural catastrophe (N)	Meteorological (M)	Strong wind (1)	Storm, hurricane (1)	N	NM	NM1	NM11
			Whirlwind, tornado (2)	N	NM	NM1	NM12
		Flooding (2)	Seasonal flooding (1)	N	NM	NM2	NM21
			Storm flooding (2)	N	NM	NM2	NM22
			Spring flooding (3)	N	NM	NM2	NM23
		Climatic change with increased average weather values (3)	Increased sea level (1)	N	NM	NM3	NM31
			Increased temperature (2)	N	NM	NM3	NM32
			Increased rainfall (3)	N	NM	NM3	NM33
		Geological/Geotechnical (G)	Snow slide (1)	Snow slide over infrastructure (1)	N	NG	NG1
	Snow slide over buildings (2)			N	NG	NG1	NG12
	Landslide (2)		Land slide over infrastructure (1)	N	NG	NG2	NG21
			Land slide over buildings (2)	N	NG	NG2	NG22
			Land slide into water (3)	N	NG	NG2	NG23
	Earthquake (3)		Less than 5 Richter (1)	N	NG	NG3	NG31
			5 Richter or more (2)	N	NG	NG3	NG32
	Tsunami (4)		National impact (1)	N	NG	NG4	NG41
			Regional impact (2)	N	NG	NG4	NG42
	Volcanism (5)		Not in use (1)	N	NG	NG5	NG51
			National downfall fallout(2)	N	NG	NG5	NG52
	Calderac explosion (6)		Not in use(1)	N	NG	NG6	NG61
		Global impact, national downfall fallout (2)	N	NG	NG6	NG62	
	Fire, natural (F)	Forrest-, ling-, grass fire (1)	Fire related to infrastructure (1)	N	NF	NF1	NF11
			Fire related to other buildings (2)	N	NF	NF1	NF12
	Cosmic (C)	Meteorite (asteroid) (1)	National impact (1)	N	NC	NC1	NC11
			Regional impact (2)	N	NC	NC1	NC12
			Global impact (3)	N	NC	NC1	NC13
		Comet (2)	Urban impact (1)	N	NC	NC2	NC21
National impact (2)	N		NC	NC2	NC22		
Medical biological catastrophe (B)	Plants and animals (P)	Transferable disease (1)	Zoonotic (between humans and animals) (1)	B	BP	BP1	BP11
			Non-zoonotic (2)	B	BP	BP1	BP12
	Humans (H)	Pandemic (1)	Flu (1)	B	BH	BH1	BH11
			SARS (2)	B	BH	BH1	BH12
			Not in use (3)	B	BH	BH1	BH13
Technical catastrophe (T)	Accident (A)	Release of dangerous substances (1)	Toxic chemicals (1)	T	TA	TA1	TA11
			Seveso installations (2)	T	TA	TA1	TA12
			Nuclear reactor (3)	T	TA	TA1	TA13

Events in hierarchy				Code values			
L1	L2	L3	L4	L1	L2	L3	L4
			Other radiological sources (4)	T	TA	TA1	TA14
			Biological release (5)	T	TA	TA1	TA15
			Maritime contamination (6)	T	TA	TA1	TA16
		Huge fire (2)	Gas terminal (1)	T	TA	TA2	TA21
			Oil refinery (2)	T	TA	TA2	TA22
			Fuel depot (3)	T	TA	TA2	TA23
			Onshore pipeline (4)	T	TA	TA2	TA24
			Offshore pipeline (5)	T	TA	TA2	TA25
			Offshore oil installation (6)	T	TA	TA2	TA26
			Chemical plant (7)	T	TA	TA2	TA27
		Explosion (3)	Gas terminal (1)	T	TA	TA3	TA31
			Oil refinery (2)	T	TA	TA3	TA32
			Fuel depot (3)	T	TA	TA3	TA33
			Onshore pipeline (4)	T	TA	TA3	TA34
			Offshore pipeline (5)	T	TA	TA3	TA35
			Offshore oil installation (6)	T	TA	TA3	TA36
			Chemical plant (7)	T	TA	TA3	TA37
		Transportation accident (4)	Sinking or burning passenger ship (1)	T	TA	TA4	TA41
			Harbour accident (2)	T	TA	TA4	TA42
			Aircraft crash (3)	T	TA	TA4	TA43
			Aircraft crash in urban area (4)	T	TA	TA4	TA44
			Train accident (5)	T	TA	TA4	TA45
			Road accident, pile up (6)	T	TA	TA4	TA46
			Dangerous goods (7)	T	TA	TA4	TA47
		Structural collapse (5)	Breaking of a dyke (1)	T	TA	TA5	TA51
			Bridges (2)	T	TA	TA5	TA52
			Buildings (3)	T	TA	TA5	TA53
	Failure to deliver (critical infrastructure) (D)	Lack of water (1)	Water source (1)	T	TL	TL1	TL11
			Waterworks and purification (2)	T	TL	TL1	TL12
			Pipelines (3)	T	TL	TL1	TL13
		Lack of food (2)	Production (1)	T	TL	TL2	TL21
			Import (2)	T	TL	TL2	TL22
			Distribution (3)	T	TL	TL2	TL23
		Sewage and refuse collection failure (3)	Sewer (1)	T	TL	TL3	TL31
			Surface Water (2)	T	TL	TL3	TL32
			Refuse collection (3)	T	TL	TL3	TL33
		Lack of transportation services (4)	Air travel (1)	T	TL	TL4	TL41
			Rail (2)	T	TL	TL4	TL42
			Road (3)	T	TL	TL4	TL43
			Sea (4)	T	TL	TL4	TL44
		Lack of financial services (5)	Bank services (1)	T	TL	TL5	TL51
			Securities services (2)	T	TL	TL5	TL52
		Lack of energy supply (6)	Production (1)	T	TL	TL6	TL61
			Transformation (2)	T	TL	TL6	TL62
			Main distribution network (3)	T	TL	TL6	TL63

Events in hierarchy				Code values			
L1	L2	L3	L4	L1	L2	L3	L4
			Regional and local distribution network (4)	T	TL	TL6	TL64
		Lack of ICT (7)	Traditional phone (1)	T	TL	TL7	TL71
			Mobile phone (2)	T	TL	TL7	TL72
			Internet (3)	T	TL	TL7	TL73
Dysfunctional human behaviour (D)	Individual (I)	Psychotic (1)	Unable to act in critical situation (1)	D	DI	DI1	DI11
			(Criminal) use of violence (2)	D	DI	DI1	DI12
		Negligent (2)	Failure in attitude, rigidity (1)	D	DI	DI2	DI21
			Naivety (2)	D	DI	DI2	DI22
	Collective (C)	System failure (1)	Lack of objective communications (1)	D	DC	DC1	DC11
			Lack of competence development (2)	D	DC	DC1	DC12
		Organisational defect (2)	Wrong use of, or lack of resources (1)	D	DC	DC2	DC21
			Non-existing objective (2)	D	DC	DC2	DC22
		Conflicting objectives (3)	Procrastinate behaviour (1)	D	DC	DC3	DC31
			Pursuit inadequate objectives (2)	D	DC	DC3	DC32
(Malicious) acts against nation, inhabitants, or interest (M)	Crime (C)	Organised crime (1)	Smuggling (1)	M	MC	MC1	MC11
			Drugs and weapon arm trade (2)	M	MC	MC1	MC12
			Trafficking (3)	M	MC	MC1	MC13
			Cybercrime (4)	M	MC	MC1	MC14
		Sabotage (2)	Attack against installations (1)	M	MC	MC2	MC21
			Forcible violent protest, "disturbance" (2)	M	MC	MC2	MC22
			Will full plundering (3)	M	MC	MC2	MC23
			Data hacking (4)	M	MC	MC2	MC24
		Espionage (3)	Political (1)	M	MC	MC3	MC31
			Military (2)	M	MC	MC3	MC32
			Industrial (3)	M	MC	MC3	MC33
		Terrorism (T)	Conventional terrorism (1)	Attack against person (1)	M	MT	MT1
	Hostage-taking (2)			M	MT	MT1	MT12
	Explosives used against crowds (3)			M	MT	MT1	MT13
	CBRN-terrorism (2)		Chemical attack (1)	M	MT	MT2	MT21
		Biological attack (2)	M	MT	MT2	MT22	
		Radiological attack (3)	M	MT	MT2	MT23	
		Nuclear attack (4)	M	MT	MT2	MT24	
	Security policy challenge in peacetime (S)	Not in use (1)	Resource economical (1)	M	MS	MS1	MS11
			Military (2)	M	MS	MS1	MS12
Euro/Atlantic (2)		Political/economical pressure (1)	M	MS	MS2	MS21	
		Political/organisational setback (2)	M	MS	MS2	MS22	
Not in use (3)		Not in use	M	MS	MS3	MS31	
	Not in use	M	MS	MS3	MS32		
War (W)	Physical war (1)	National (1)	M	MW	MW1	MW11	

Events in hierarchy				Code values			
L1	L2	L3	L4	L1	L2	L3	L4
			Nearby regions (2)	M	MW	MW1	MW12
			Not in use (3)	M	MW	MW1	MW13
		Computer network operations (CNO) (2)	Distributed attack (1)	M	MW	MW2	MW21

Table 7 List of societal critical functions

Societal critical function hierarchy				Codes			
L1	L2	L3	L4	L1	L2	L3	L4
Critical infrastructure, basic (B)	Electrical power (1)	Production plants (1)	Class 1	B	B1	B11	B111
			Class 2	B	B1	B11	B112
			Class 3	B	B1	B11	B113
		Transformer and transformer cubicle front (2)	Class 1	B	B1	B12	B121
			Class 2	B	B1	B12	B122
			Class 3	B	B1	B12	B123
		Distribution net (3)	Class 1	B	B1	B13	B131
			Class 2	B	B1	B13	B132
			Class 3	B	B1	B13	B133
		Dams, barrages (4)		B	B1	B14	B14
		Control centres and SCADA-systems (5)		B	B1	B15	B15
		Mobile backup systems (6)		B	B1	B16	B16
		Electronic communication (2)	Phone and cable systems (1)	National centrals	B	B2	B21
	Nodes			B	B2	B21	B212
	Important switchboards and other important user applications			B	B2	B21	B213
	Mobile phones (2)		National centrals	B	B2	B22	B221
			Nodes	B	B2	B22	B222
			Base stations	B	B2	B22	B223
	Internet (3)		NIX'es etc	B	B2	B23	B231
			Internet Service Providers	B	B2	B23	B232
	Closed communication systems for the authorities (4)		Digital net of army	B	B2	B24	B241
			Rescue net	B	B2	B24	B242
	Radio communication (5)		Aviation control central	B	B2	B25	B251
			Costal radio	B	B2	B25	B252
			Broadcasting	B	B2	B25	B253
	Satellite based infrastructures, earth based stations (6)		For meteorology, communication, Broadcasting, Navigation, Environment monitoring	B	B2	B26	B26

Societal critical function hierarchy				Codes			
L1	L2	L3	L4	L1	L2	L3	L4
		Mobile backup systems (7)		B	B2	B27	B27
Critical infrastructure, remaining (C)	Water and sewage systems (1)	Water sources (1)	Catchments	C	C1	C11	C111
			Surface water	C	C1	C11	C112
			Groundwater	C	C1	C11	C113
			River	C	C1	C11	C114
		Backup systems for water (2)	C	C1	C12	C12	
		Purification plants (3)	Coagulation	C	C1	C13	C131
			Filtration	C	C1	C13	C132
			Chlorination	C	C1	C13	C133
			UV	C	C1	C13	C134
			CO2	C	C1	C13	C135
			pH adjustment	C	C1	C13	C136
			Pumps	C	C1	C13	C137
		Distribution networks (4)	Mains	C	C1	C14	C141
			Tunnels	C	C1	C14	C142
			Pipes	C	C1	C14	C143
			Water tanks	C	C1	C14	C144
			Valves	C	C1	C14	C145
	Pumps		C	C1	C14	C146	
	Sewage systems (5)	C	C1	C15	C15		
	Control centres and SCADA-systems (6)	C	C1	C16	C16		
	Oil- and gas supply	Offshore installations (1)	C	C2	C21	C21	
		Pipelines (2)	C	C2	C22	C22	
		Land terminals and refineries (3)	C	C2	C23	C23	
		Depots (4)	C	C2	C24	C24	
		Control centres and SCADA-systems (5)	C	C2	C25	C25	
	Transport (3)	Airports (1)	C	C3	C31	C31	
		Railway stations and terminals (2)	C	C3	C32	C32	
		Road transportation terminals (3)	C	C3	C33	C33	
		Sea terminals, harbours (4)	C	C3	C34	C34	
	Bank and finance (4)	National clearing systems (1)	C	C4	C41	C41	
		Payments system (2)	C	C4	C42	C42	
Securities systems(3)		C	C4	C43	C43		
Other critical infrastructure	Food support(1)	Logistics system (1)	O	O1	O11	O11	
		Hygiene and safety	O	O1	O12	O12	

Societal critical function hierarchy				Codes			
L1	L2	L3	L4	L1	L2	L3	L4
(O)		(2)					
	Sanitation (2)	Waste transportation (1)		O	O2	O21	O21
		Waste depot (2)		O	O2	O22	O22
	Health, social and social security services (3)	Specialist health services hospitals (1)		O	O3	O31	O31
		Primary health services (2)		O	O3	O32	O32
		Social services (3)		O	O3	O33	O33
		Support of medicines (4)		O	O3	O34	O34
		Laboratories (5)		O	O3	O35	O35
		Systems for social security services		O	O3	O36	O36
		Police, emergency- and rescue services (4)	Police registers (1)		O	O4	O41
	Police stations (2)			O	O4	O42	O42
	Emergency and rescue services (3)			O	O4	O43	O43
	Fire brigade (4)			O	O4	O44	O44
	Public management (5)	Parliament (1)		O	O5	O51	O51
		Government and administration, crisis management (2)		O	O5	O52	O52
		The judiciary (3)		O	O5	O53	O53
		Head of defence (4)		O	O5	O54	O54
	Media and news communication (6)	Radio- and television companies (1)		O	O6	O61	O61
		Press, hard copies(2)		O	O6	O62	O62
		Internet papers (3)		O	O6	O63	O63
		Public information services (4)		O	O6	O64	O64
	Important industries (7)	Chemical plants and depots (1)		O	O7	O71	O71
		Nuclear reactors and nuclear depots (2)		O	O7	O72	O72
		Defence industry (3)		O	O7	O73	O73
		Control centres and SCADA-systems (4)		O	O7	O74	O74
	National symbols (8)	Buildings cultural institutions and monuments (1)		O	O8	O81	O81
		Mobile objects (2)		O	O8	O82	O82
		Institutional evection		O	O8	O83	O83

5 Using the computerized tool - InfraRisk

When the InfraRisk tool is loaded the main menu shown in Figure 12 appears.

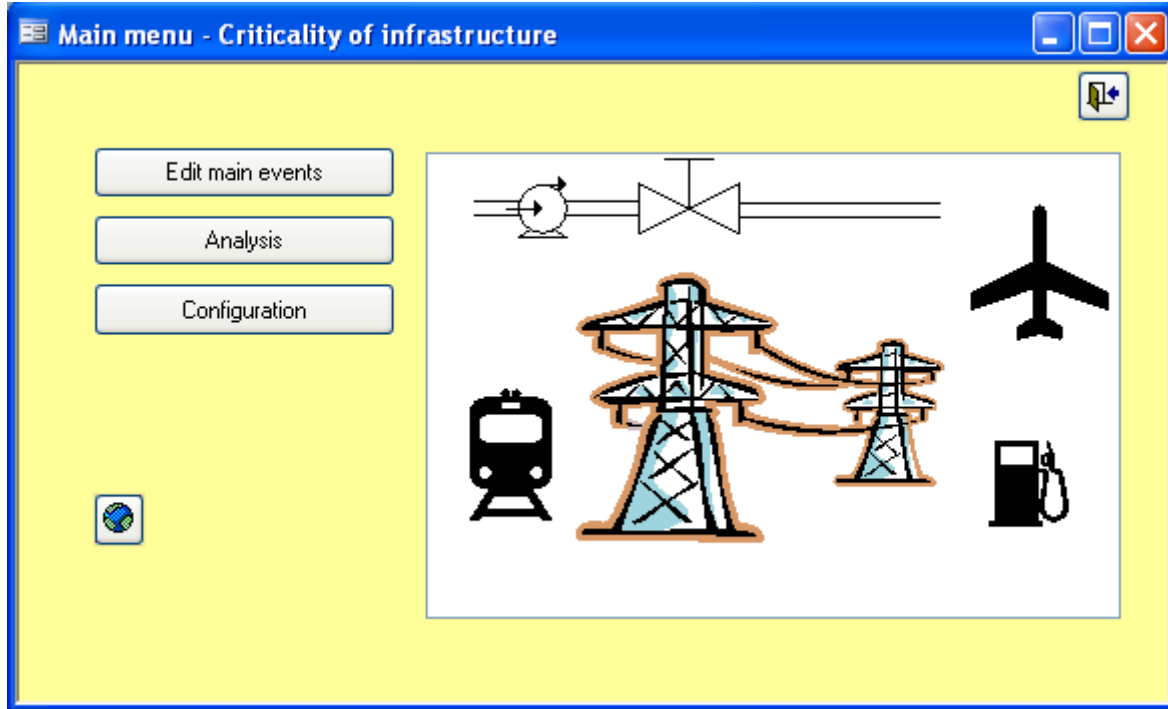


Figure 12 Main menu of InfraRisk

5.1 Analyzing main events

Figure 13 Screen for analyzing main events

Press the **Edit main events** button from the main menu to load the screen for analyzing main events as shown in Figure 13. The main event is described by up to four levels of detail according to Table 6 on page 20.

When pressing the **New event** or **Change event** buttons in Figure 13 the main event may be chosen from a hierarchy menu. When a simplified analysis mode is chosen, the frequency and consequence assessments are made directly according to procedures in sections 2.4.3 and 2.4.4. In the left part of the screen it is possible to add SCFs relevant for the risk scenario by clicking the **Add** button. A new SCF could then be chosen from a hierarchical menu corresponding to the SCFs in Table 7. When a new SCF is added the type and strength of relation between the SCF and the main event should be defined according to values shown in Table 1. Also it should be indicated whether the SCF typically occurs before (initiating event) or after (barrier function) the main event.

Vulnerability or risk factors are defined in the browser in the middle of the screen in Figure 13. To add a new factor move to the New record (*****) row and choose a factor from the list. Also for the vulnerability or risk factors it should be indicated whether they act before or after the main event. The value of the factor is chosen from a list corresponding to Table 2.

Note that when frequency and consequence values are assessed, the risk for each consequence dimension is calculated according to the current calibration of the risk matrix in Table 5.

The lifeline quality and unavailability dimensions could either be specified directly, or they could be calculated from a “Duration” and “Involved persons” assessment. In this case the

consequences are determined by the current calibration of matrixes for duration and involved persons, see Table 4.

By clicking the View risk matrix button (📊) in Figure 13 all main events are plotted in a risk matrix as shown in Figure 14. By clicking in one cell, the corresponding main events are filtered out and viewed. Note that the risk matrix is presented for one dimension at the time, use the buttons at the bottom of the screen to move between the various dimensions.

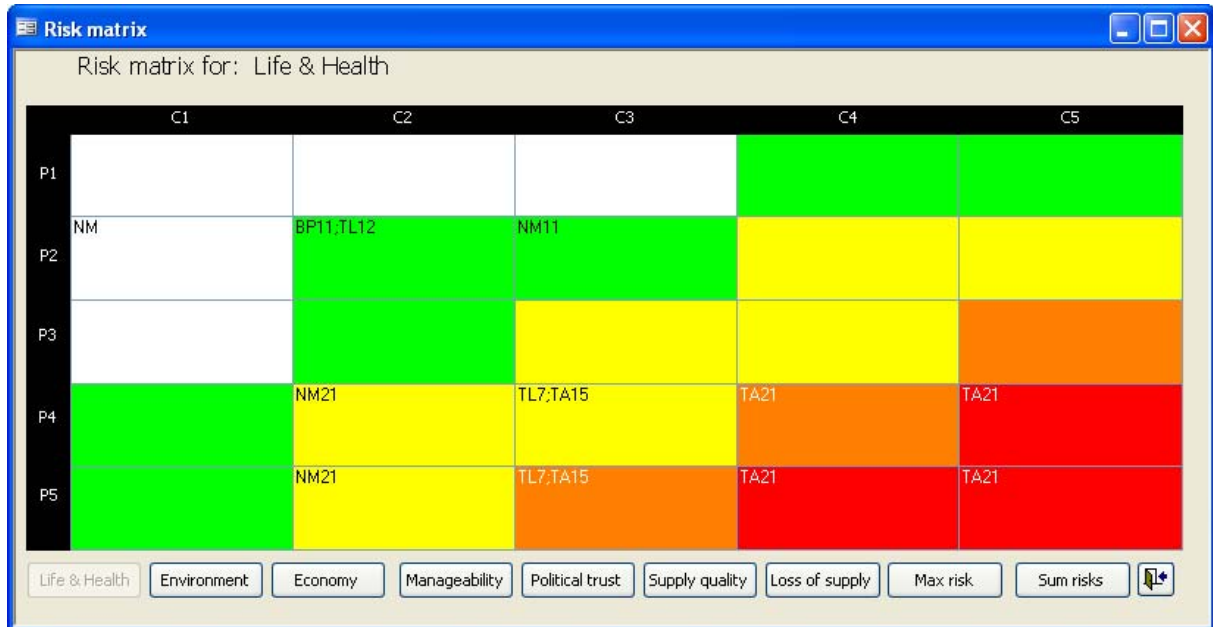


Figure 14 Plot main events in the risk matrix

If a comprehensive analysis mode is chosen (see Chapter 3) the detailed model specification is entered in a text editor loaded by pressing the (📄) button in Figure 13. The text editor is shown in Figure 15. When the model is completely specified, and the editor window is closed, it is necessary to compile it by pressing the compile button (🔧) from 13. When the model is compiled the frequency and consequence fields in Figure 13 will be updated if no errors occur during compilation. Note also that the result of the compilation is shown in a separate window. It is recommended to check the result in this window, since errors are likely to be introduced during the model specification.

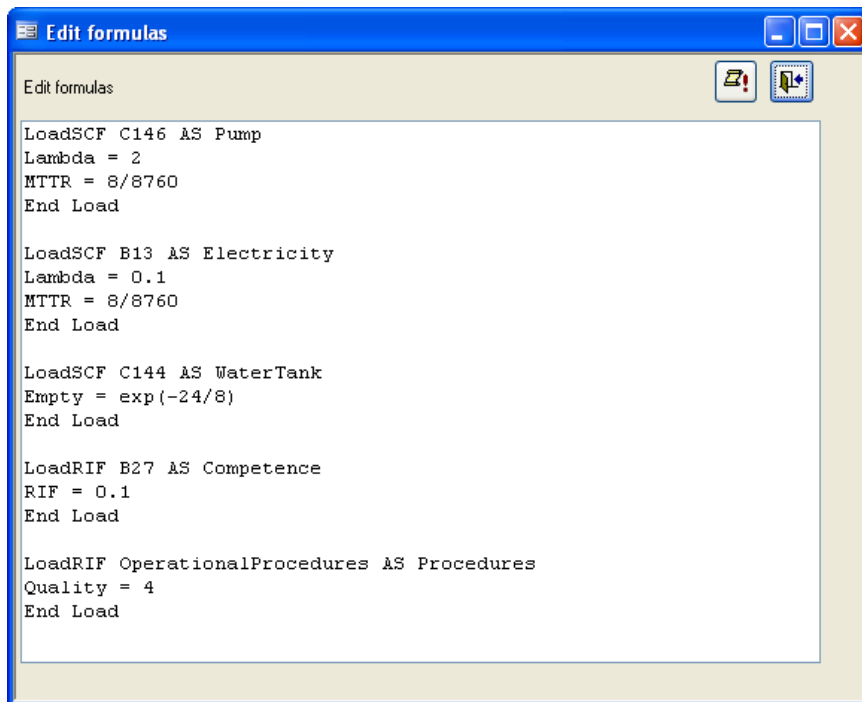



Figure 15 Text editor for specifying the detailed model

5.2 Filtering events

Press the filter button () at the bottom of Main Event specification form in Figure 13 to activate the filter prompt. Enter the WHERE clause of the SQL statement to filter out selected records. Special functions available here are:

```
SCF(<SCF code>)
MainEvent(<Event code>)
```

For example specify

```
SCF ("C33")
```

to select "Critical infrastructure, remaining (C); Transport (3); Metro/Tram (3)". See the code list in Table 7 for a list of SCFs. Similar, specify:

```
MainEvent("TA2")
```

to filter out Main events of type "Technical catastrophes, accident and huge fire". See Table 6 for a complete list of Main Events.

In order to clear the filter specify

```
True
```

in the filter command field.

Advanced filtering requires understanding of the name structure of the tblMainEvents.

5.3 Configuration

The various matrixes used in InfraRisk may be calibrated from the **Configuration** menu available from the main menu. For example press the **Edit risk matrix** from the configuration matrix. In the risk matrix you now click on a cell, and then you could change the colour/text of the cell as shown in Figure 16.

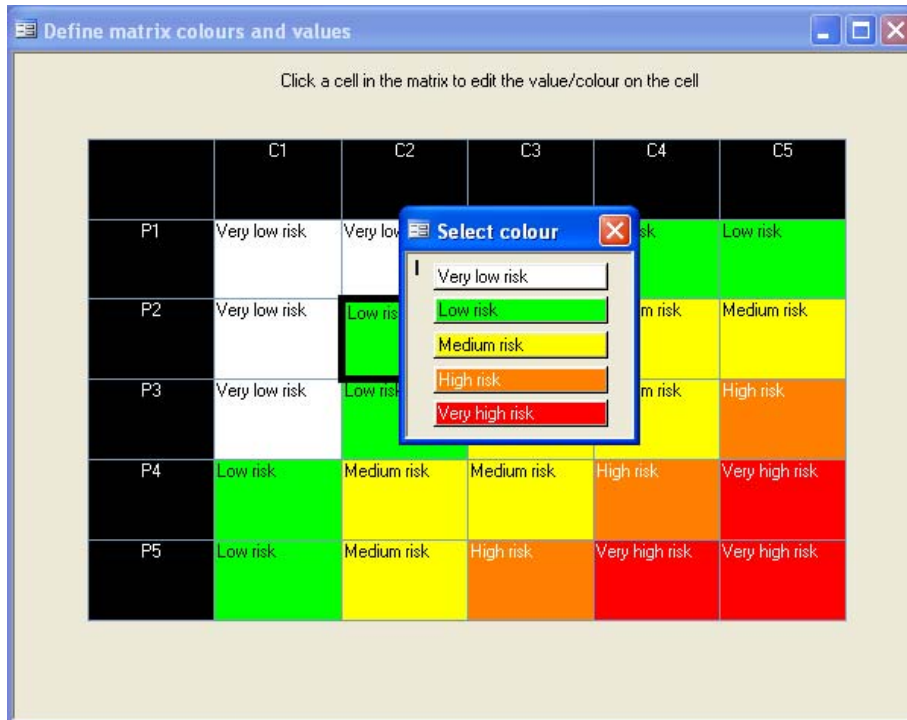


Figure 16 Calibration of risk matrixes

Note that the consequence dimensions for lifeline quality and unavailability also could be calibrated from the configuration menu.

5.4 Analysis

From the main menu, press the **Analysis** button to get access to the various analysis available in the InfraRisk program. Currently only three analyses are available:

5.4.1 SCF ranking

The SCF ranking is based on the result from the simplified analysis described in Chapter 2. For each main event where a SCF is involved, the risk is calculated by multiplying the frequency with the sum of consequences. Then each SCF achieves a score which is the importance contribution times the risk. By summing over all main events for all SCFs it is possible to establish a ranking of SCFs. Note that the frequency and consequence values are given on a logarithmic scale, hence it is necessary to use the exponential function during the

calculation in InfraRisk. The SCF ranking is the only importance measure for the SCF that could be constructed if only a simplified analysis is conducted.

5.4.2 SCF improvement potential

The SCF improvement potential measure could be calculated for each SCF if the comprehensive analysis has been conducted according to Chapter 3. The improvement potential represents the reduction in risk if the SCF is replaced with a “perfect” SCF. To calculate the improvement potential, InfraRisk replaces all the attributes for the SCF with zero. This means that when the attributes are described, see Figure 4 on page 16, all attributes should be defined such that a zero represents a perfect SCF. For example a barrier probability should always represent failure of the barrier, hence a zero value will then be a barrier that never fails.

5.4.3 SCF listing

In the SCF listing all SCFs are listed with a sublist of all main events for which the SCF is included.

5.4.4 More analyses...

More analyses are to be included in InfraRisk.....

5.4.5 Summary of commands and functions

Below we give a brief summary of commands and functions available in the InfraRisk programming language. Arguments are shown in brackets (< >), and optional arguments are shown in square brackets ([]).

LoadSCF

```
LoadSCF <SCF-ID> [AS <Alias>]
<Parameter1> = <expression>
[<Parameter2> = <expression>
:]
End Load
```

Where <SCF-ID> is the ID of the SCF according to Table 7. <Alias> is an optional name for the SCF to enhance readability. After the load statement an arbitrary number of parameter (SCF attributes) assignment could be defined. Note that to refer to the attribute always add the alias name (or SCF-ID if no alias is given) with a punctuation in front of the attribute name, e.g., Pump.Probability. In the assignment the <expression> could either be a number, or a formula. Always terminate the LoadSCF with an End Load statement.

LoadRIF


```

LoadRIF <RIF> [AS <Alias>]
<Parameter1> = <expression>
[<Parameter2> = <expression>
:]
End Load

```

The LoadRIF construct is similar to the LoadSCF. Currently the InfraRisk program do not support any analysis of the vulnerability factors, but to be compatible with future versions of InfraRisk, the <RIF> argument should be according to dropdown list for the RIFs in Figure 13.

AndGate

```
AndGate(<Prob1>, <Prob2> [ , ... , <ProbN> ] )
```

The AndGate returns the occurrence probability of an AND gate. Two or more arguments could be specified. The arguments are either numeric values, reference to a variable, or a function returning a probability (e.g., another gate).

fAndGate

```
fAndGate(<Freq1>, <MDT>, <Freq2>, <MDT> [ , ... , <FreqN>, <MDTN> ] )
```

The fAndGate is used to when we want to find frequencies rather than probabilities for the AND gate. We then have to specify both frequencies, and mean down time (MDT) for each input. The frequencies and MDTs are given in pair.

OrGate

```
OrGate(<Prob1>, <Prob2> [ , ... , <ProbN> ] )
```

The ORGate returns the occurrence probability of an OR gate. The arguments are specified as for the ANDGate.

fOrGate

```
fOrGate(<Freq1>, <MDT>, <Freq2>, <MDT> [ , ... , <FreqN>, <MDTN> ] )
```

The fOrGate is supported for symmetric reasons only since the output will be identical to the ORGate function. This means that the <MDT> values are not used.

KooNGate

```
KooNGate(<K>, <Prob1>, <Prob2> [ , ... , <ProbN> ] )
```

The first argument, <K>, represents the number of inputs occurrences that are critical. This means that if <K> or more inputs occurs, then the KooN gate will occur. The remaining arguments are as for the ANDGate.

fKooNGate

```
fKooNGate(<K>, <Freq1>, <MDT>, <Freq2>, <MDT> [ , ... , <FreqN>, <MDTN> ] )
```

The fKooNGate is used when we are seeking the frequency of the KooN gate.

RIF1To5

```
RIF1To5(<RIFValue>, <LowProb>, <HighProb> )
```

This function calculates a failure probability according to the value of <RIFValue>. When the RIF value takes the best value (1) the <LowProb> will be returned and when the <RIF value takes the worst value (5) the <HighProb> will be returned. Between these two values an exponential interpolation is performed, i.e. $RIF1to5(x,l,h) = A \cdot \exp(B \cdot x)$, where $B = [\ln(h/l)]/4$, and $A = l \cdot \exp(-B)$.

Reserved variables

The InfraRisk program supports a set of reserved variable names which have a special meaning. When these variables are set, the frequency and/or consequence values for the main event are set. The reserved words are;

- Frequency (set the frequency of the main event)
- LifeAndHealth (set the consequence distribution for life and health)
- Environment (set the consequence distribution for environment)
- Economy (set the consequence distribution for economy)
- Manageability (set the consequence distribution for manageability)
- PoliticalTrust (set the consequence distribution for political trust)
- LifelineQuality (set the consequence distribution for lifeline quality)
- LifelineUnavailability (set the consequence distribution for lifeline unavailability)

The frequency variables must be set by a statement returning a single number, e.g., a `fAndGate` statement. The remaining variables must be set with the `Dist()` function, see example on in Figure 8 page 18.

bFailure

`bFailure(<InFreq>, <FailProb>)`

The <InFreq> is the probability that the barrier (in an ETA) is activated, and <FailProb> is the conditional probability that the barrier fails given it is activated. The `bFailure` function returns in fact an array of two elements, the first element is the rate of failure of the barrier (combination of activation and failure), and the second element is the rate of success of the barrier. To refer to these two numbers, use the suffixes `.No`, and `.Yes`. For example:

```

` In the example the analysis starts when a fire has started.
`
FireNotMitigated = bFailure(1, 0.01)
`
` Assume only two possible outcomes
`
LifeAndHealth      =      Dist(FireNotMitigated.Yes,0,
FireNotMitigated.No,0,0)
```

(Note that an apostrophe (‘) is use to mark comments in the text editor for commands.

Index

AndGate	15, 33	example of use	15
bFailure.....	34	Main event	5
Bow tie	12	MainEvent() filter function.....	30
Consequence classes	9	Main menu	27
ETA	12	OrGate.....	15, 33
Event tree		probability	8
example	18	Reserved variable names	34
event tree analysis	<i>See</i> ETA	RIF1To5.....	33
fAndGate	33	risk matrix	
Fault tree		calibration	31
example	14	plot events.....	29
fault tree analysis.....	<i>See</i> FTA	Risk matrix.....	11
Filter	30	SCF	
fKooNGate	33	definition.....	6
fOrGate.....	33	improvement potential	32
Frequency analysis		ranking	31
Comprehensive analysis.....	14	SCF() filter function.....	30
FTA	12	Societal critical functions.....	<i>See</i> SCF
KooNGate.....	15, 33	SQL.....	30
LoadRIF	32	TOP event	14
LoadSCF.....	32	Vulnerability Factor.....	7