CZECH TECHNICAL UNIVERSITY IN PRAGUE
FACULTY OF ELECTRICAL ENGINEERING

DIPLOMA THESIS

Risk Analysis of Tunnels

Prague, 2009

Author: Samuel Privara

České vysoké učení technické v Praze
Fakulta elektrotechnická

Katedra řídicí techniky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Student: **Bc. Samuel Prívara**

Studijní program: Elektrotechnika a informatika (magisterský), strukturovaný
Obor: Kybernetika a měření, blok KM1 - Řídicí technika

Název tématu: **Rizikové analýzy tunelů**

Pokyny pro vypracování:

1. Seznamte se s metodami rizikových analýz, jak se provádějí v oblasti posuzování rizik tunelů a s jejich alternativami.
2. Vyberte jednu alternativní metodu a podle ní zpracujte rizikovou analýzu modelového příkladu (Strahovský tunel).
3. Proveďte kvalitativní a kvantitativní ohodnocení jednotlivých variant navrhovaných bezpečnostních opatření Strahovského tunelu.

Seznam odborné literatury:

[1] Rudolf Hörhan a kol., Tunnel-Risikoanalysemodell, Vídeň, 2008
[2] U. S. Department of Transportation, FAA System Safety Handbook, Washington, 2000
[3] Bernhard Kohl a kol., Risk Analysis for Road Tunnels, Paříž, 2008

Vedoucí: Ing. Lukáš Ferkl, Ph.D.

Platnost zadání: do konce zimního semestru 2009/10

prof. Ing. Michael Šebek, DrSc.
vedoucí katedry

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE Fakulta elektrotechnická L.S.

doc. Ing. Boris Šimák, CSc.
děkan

V Praze dne 27. 2. 2009

Prohlášení

Prohlašuji, že jsem svou diplomovou práci vypracoval samostatně a použil jsem pouze podklady (literaturu, projekty, SW atd.) uvedené v přiloženém seznamu.

V Praze dne _____ _____
podpis

Acknowledgements

I would like to convey my gratitude to my supervisor Ing. Lukáš Ferkl, Ph.D, who created perfect conditions for elaborating this thesis and was always willing to consult any problem that occurred. Special thanks belongs to him for his great and laborious correction of the thesis. Many thanks belong also to Ing. Ondrej Nývlt who had many perfect ideas and contributed with his valuable suggestions.

Abstract

Many approaches to Risk Analysis in tunnels have been proposed by both international and national authorities over the last few years. They address the specific environment of tunnels and try to estimate the risk levels in order to diminish it in an affective manner to make the tunnels safer. Many topics have been discussed and a large number of important risk factors and hazards in tunnels have been identified. However, the concept of Risk Analysis in the scope of tunnel risks is still under development; particularly an overall idea about the Risk Management concept is still missing. This thesis introduces the concept of Risk Analysis in the scope of Risk Management trying to both explain traditional methods used in Risk Analysis and employs methods well-known in aeronautics and aircraft industry, yet, still unused and unknown in tunnels. The objective of this thesis also includes a case study of Strahov Tunel which uses Risk Analysis methods traditionally used by aircraft industry – particularly National Aeronautics and Space Administration (NASA), Federal Aviation Association (FAA) and United States Department of Defence (DoD). The Risk Analysis proposed in **Chapter 3 – Case Study** was developed for Strahov Tunnel (as a part of Technical Documentation), where it was applied as of 2009. This method is supposed to be applied for other Czech tunnels, especially new tunnels built in Prague, e.g. Blanka tunnel.

Anotácia

V poslednej dobe bolo rôznymi organizáciami navrhnuté množstvo rôznych prístupov k analýze rizík, ktoré sa snažia zohľadniť špecifické vlastnosti cestných tunelov. Snažia sa urobiť tunely bezpečnejšími prostredníctvom odhadov úrovne rizík a ich efektívnym znížením. Napriek tomu, že sa o tejto tematike vedú rozsiahle diskusie a bolo identifikovaných množstvo hlavných kontribučných faktorov k celkovému riziku, celkový koncept rizikových analýz v prostredí tunelu je stále v počiatočných štádiach vývoja a ucelená koncepcia nebola dosiaľ predstavená. Diplomová práca prezentuje rizikovú analýzu ako časť širšieho konceptu managementu rizík, pričom vysvetľuje tradičné metódy ako aj nové myšlienky prevzaté z leteckého priemyslu, ktoré doteraz neboli použité na analýzu rizík v tuneloch. Práca prezentuje praktický príklad použitia rizikovej analýzy využívaných často Národným úradom pre letectvo a kozmonautiku (NASA), Federálnym úradom pre letectvo (FAA) a Ministerstvom obrany Spojených štátov amerických (US DoD) na mestskom tuneli Strahov Praha, kde bola táto analýza nasadená ako súčasť Technickej dokomentácie v roku 2009, pričom sa predpokladá jej nasadenie pre novo stavané tunely, napr. Blanka.

Contents

Definitions and Notations

Accident	An incident with situations unsafe for the people in tunnel
Basic event	The bottom or "leaf" events of a fault tree. The limit of resolution of the fault tree
Common cause failure	Multiple component faults that occur at the same time and that are due to a common cause
Consequence analysis	Procedure of description and/or calculation consequences
Corrective action	A documented design, process, procedure, or materials change implemented and validated to correct the cause of the failure or design deficiency
Criticality	A relative measure of the consequences of a failure mode and its frequency of occurrences
End effect	The consequences a failure mode has on the operation, function, or status of the highest level
Failure	An unacceptable deviation from the design tolerance, an incorrect output, the incapacity to perform the desired function
Failure effect	The consequences a failure mode has on the predation, function, or status of an item. Failure effects are classified as local effect, next higher level, and end effect
Failure mode	The manner by which a failure is observed. Generally describes the way the failure occurs and its impact on equipment operation
Fault	A defect, imperfection, mistake or flaw of varying severity that occurs within some hardware or software component or system. "Fault" is a general term and can range from a minor defect to a failure. The manifestation of a fault in a system or the information that is processed by the system or a manifestation in the internal system state.
FN curve	Graph representing cumulative frequency distribution of N units of consequences. FN stands for the annual frequency of occurrence F to have a scenario likely to cause an effect (generally, the number of fatalities) equal to or higher than N. In other words FN are curves relating the probability of causing N or more fatalities (F) to N per year. In fact, it is the complementary cumulative distribution function. Such curves may be used to express societal risk criteria and to describe the safety levels of particular facilities.

Harm	Physical injury or damage to the health of people, damage to the property of environment
Hazard	Potential source of harm
Hazard identification	A process of recognition of hazards or process of definition of hazard characteristics
Local effect	The consequences a failure mode has on the operation, function, or status of the specific item being analyzed
Minimal cut set	A smallest combination of basic events whose occurrence results in the occurrence of the top event of a fault tree
Minimal path set	A smallest combination of basic events whose nonoccurrence results in the nonoccurrence of the top event of the success tree
Next higher level effect	The consequences a failure mode has on the operation, functions, or status of the items in the next higher level above the lever under consideration
Probability	Extent of event occurrence evaluated numerically as a number between 0 and 1
Probability analysis	Procedure of probability description and/or calculation
Residual risk	Risk remaining after safety measures and precautions have been implemented
Risk	Combination of the probability and severity of the harm or failure
Risk analysis	Systematic use information to identify the hazards and estimate the risk
Risk assessment	Process of risk analysis and risk evaluation
Risk evaluation	Process based upon risk analysis to determine whether or not the tolerable risk has been achieved
Risk reduction	Actions taken to reduce the risk probability and/or negative consequences
Safety	Absence of unacceptable level of risk
Safety analysis	Systematic use information to identify the hazards and estimate the safety level
Safety assessment	Process of safety analysis and safety evaluation
Safety evaluation	Process based upon safety analysis to determine whether or not freedom from unacceptable has been achieved
Safety management	Process undertaken by the tunnel management organisation to attain and maintain a compliant level of safety
Scenario analysis	Risk Analysis where a set of scenarios is defined, risk estimated for each scenario and effects of mishaps studied
Severity	The consequences of a failure mode. Severity considerers the worst potential consequence of a failure, determined by the degree of injury, property damage, or system damage that could occur

Single failure point	The failure of an item which would result in a failure of the system and is not compensated for by redundancy or alternative operational procedure
State of component fault	A fault of a component due to either the failure of the component or the failure of a command to the component
State of system fault	A fault with a system-level effect and which is not necessarily localized at a given component
Top event	The initial event of a fault tree or success tree. Also called the undesired event in the case of a fault tree
Trigger level	Warning or control limit applied to the level of risk, which can be predetermined to the particular risk to take control action
Undesired event	The top event of the fault tree

List of Figures

List of Tables

Chapter 1

Introduction

1.1 State of the Art

1.1.1 Relationship of the Risk Analysis and Risk Management

In the state of the art, Risk Analyses (RA) are not considered as stand-alone tools, but are rather incorporated into a more complex Risk Management system (RM), which forms a part of a decision making process. RM provides means for quality management, risk mitigation, production and maintenance planning, safety and reliability analysis, etc.

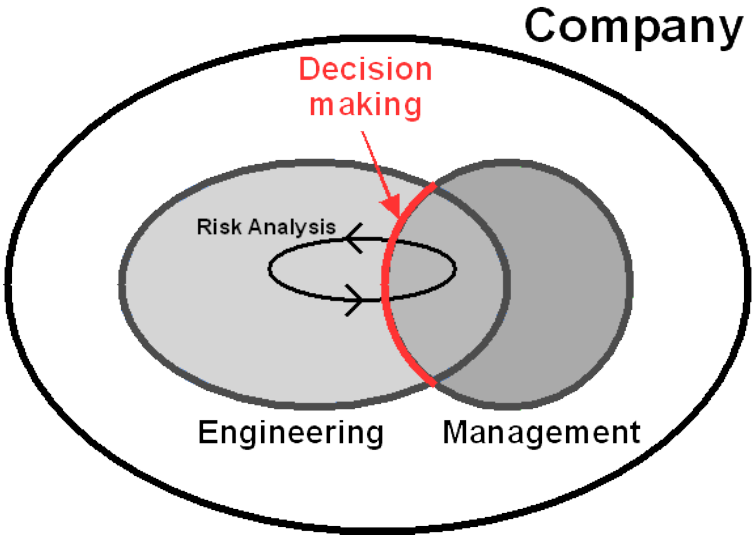


Figure 1.1: Risk analysis as a part of a risk management process providing means for sound decision making.

As illustrated in Fig. 1.1, the RM process has two major parts, which correspond to the engineering and managing departments of a company. The engineering departments perform the technical analysis which must provide a clear interface for the decision makers in the company management in order to carry out sound decisions.

In order to be efficient and to provide meaningful results, the RM process has to be scheduled for the entire lifetime of a system, as illustrated in Fig. 1.2 (FAA System Safety Handbook (2000)). It is clear that each phase of the system life stage requires different

approaches with respect to corresponding needs of decision making. Another factor is the input data available for the respective RA methods. If properly scheduled, the RM of a system is a continuous process that naturally follows the life cycle of the system. This continuity not only ensures appropriate results of the respective RA methods, but also saves significant amount of effort and resources needed for risk evaluation.

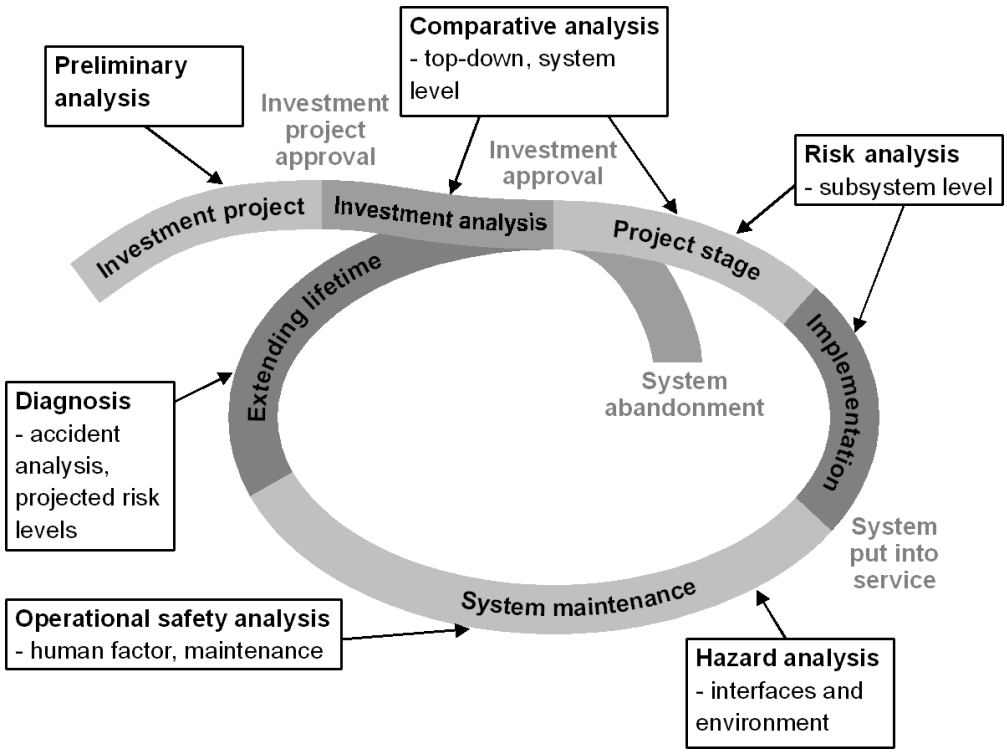


Figure 1.2: The role of risk analyses in the system life cycle.

1.1.2 Risk Analyses in Tunnels

Risk analysis is a tool developed initially in industries with potentially dangerous applications (chemical plants, nuclear power plants). The purpose of risk analysis is establishing the proactive safety strategy by investigating potential risks. In last 15 years risk analysis methods were also adapted in tunnel safety.
Risk analysis in tunnel context is:

- systematic approach analyzing interrelations in potential accidents or incidents, identifying weak points of the system etc.
- not a single method but a name for the whole family of different approaches
- quantitative or qualitative expression of risk

Risk analysis should be used to check consistency and optimality of safety planing, to choose between alternatives, etc. (PIARC – Risk Analysis for Road Tunnels (2008)). Risk analysis in tunnel enables comparison of safety measures in terms of risk reduction as well as risk-based cost/effectivness analysis, which can evaluate the cost of risk reduction. The process of risk analysis in tunnels is usually divided into hazard definition (all

hazards must be identified and structured), probability analysis (identified hazards get probability evaluation) and consequence analysis (consequences of hazards are investigated).

1.2 Risk Management

According to NASA Probabilistic Risk Assesment... (2002a), Risk Management (RM) is a process in which the project team is responsible for managing (identifying, analyzing, planning, tracking, controlling, and communicating) the risks[1] within the team and with the management. NASA introduced a new expression – Continuous Risk Management (CRM), which is a well-established tool within NASA that promotes proactive identification and control of departures from project/program objectives. NASA has also introduced a complete structural hierarchy of the Risk Management Responsibilities, which are, however, out of the scope and interest of this thesis. CRM is an iterative and adaptive process that is intended to promote the successful execution of program intent.

RM process begins with the project/program formulation and must continue throughout the all project/program life cycle. The steps used in the CRM process are as follows (see Fig. 1.3, NPR8000.4 (2002), Dezfuli et al. (2007)):

1. **Identify**
   Identify individual risks by identifying scenarios having adverse consequences (deviations from program intent). Both, the undesirable event and the consequences of that event to the project/program must be clearly identified.

   - How are risks identified?
   - Is the identification process effective?

2. **Analyze**
   Estimate the likelihood and consequence components of the risk as well as the time in which the action must be performed.

   - How are risks analyzed? For example, does the project employ Fault Tree Analysis (FTA), Failure Mode, Effects and Criticality Analysis (FMECA), or Probabilistic Risk Assessment (PRA)?
   - Is the analysis process effective?
   - Has each risk been assessed and quantified as to probability and consequences (including cost consequences)?
   - Are risks prioritized[2]?
   - Are risks updated when a change in program phase occurs, or when significant changes in program scope, budget, or schedule occur?

[1] Risk is characterized by the probability/frequency of the project failure and undesirable consequences, i.e. risk is defined as the expected value of the consequences.

[2] The risks should be classified before the prioritization.

Figure 1.3: The Continuous Risk Management (CRM) cycle.

3. **Plan**
   Plan the Track and Control actions. Decide what will be tracked, decision thresholds for corrective action, and proposed risk control actions. There is a variety of approaches to the risk: mitigation (the aim is to eliminate the risk, or to reduce its likelihood), acceptation (documented and tested recovery plan should be made in order to respond to the consequences of the accepted risk in case of its occurrence), research (collecting, analyzing and evaluating additional information leads to better future decision), and monitoring (monitoring of the risk behavior).

   - Has responsibility to address each risk been assigned to the person?
   - Have mitigation plans been prepared/implemented?
   - Have adequate resources been assigned for effective implementation of the risk mitigation plans?

4. **Track**
   Track project/program performance compared to its plan. This involves collecting, evaluating and analyzing risk data to determine the trends of the risks. Tracking should answer the question if the risk reduction and mitigation precautions are effective or the risk trends are approaching trigger levels.

   - How are risks and risk trends tracked?
   - Is the risk tracking effective?
   - Are all mitigated and monitored risks being regularly tracked to ascertain trends and ensure that trigger levels are not being exceeded?

- Does the project/program maintain a risk profile (estimated risks for the project/program life cycle according to Fig. 1.2)? A copy should be requested.

5. **Control**
   Given an emergent risk issue, execute the appropriate control action, and verify its effectiveness. Control action is the feedback process based on current monitoring data. Actions include change of the current plan, closing the risk, accepting a new plan or continuation in the current plan.

   - Was the acceptance of primary risks accomplished early and with the concurrence of the Governing Program Management Council? Are these considered formally open or closed?[3]
   - Were all risks dispositioned prior to delivery?

6. **Communicate and Document**
   This is an element of each of the previous steps. Focus on understanding and communicating all risk information throughout each program phase. Effective, open and ongoing communication within the team is essential. Documentation process ensures that the RM rules are well understood, implemented and maintained.

   - Does the project/program have an RM Plan document signed by project/program management? A copy of the RM Plan should be requested.
   - Do the contents meet the intent of the requirements defined by applicable standards/regulations?
   - Does the project/program have a Risk List? A copy should be requested of at least a sample of the list.
   - Is the Risk List easily accessible to program/project team members?
   - Are all risk acceptances documented in accordance with applicable standards/-regulations?
   - Are risks regularly presented by the project/program to the Governing Program Management Council? Copies of representative presentations should be requested.
   - Is a system RM database used as a tool to provide current, up-to-date information to the project/program team and all involved parties?

1.3 Risk Optimization

One of the primary objectives of any RM process is to balance the **cost of safety** with the **cost of accidents**. It is very difficult to achieve as there is only a small evidence about the cost of accidents, while the cost of safety is usually known quite well. The problem is illustrated in Fig. 1.4.

The principle problem is to evaluate the total system risk. In any RA method, there are two factors that act against each other:

[3] closing of risk means the acceptation of residual risk

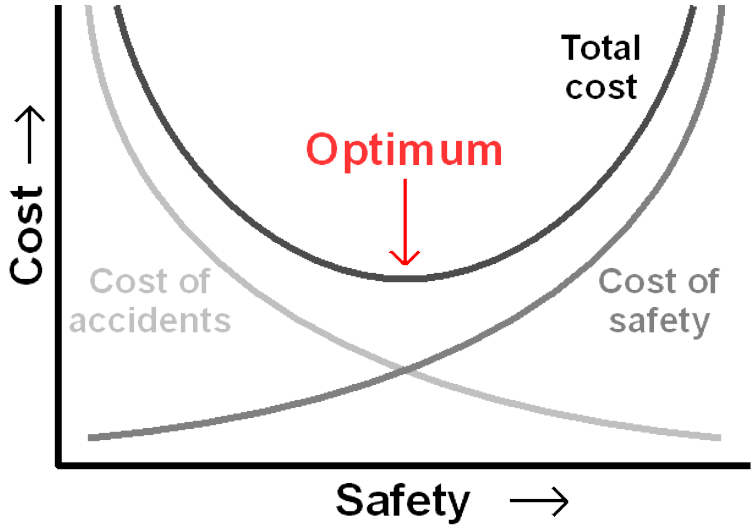


Figure 1.4: Risk Management – balance of cost of safety and cost of accidents.

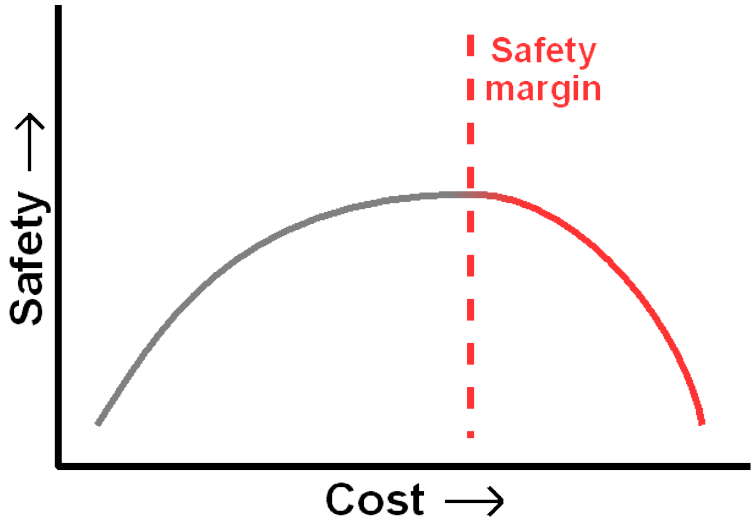


Figure 1.5: Safety Margin – a "too safe" approach can decrease the overall system safety.

- A risk estimate has to be "on the safe side", i.e. the calculated risk has to be greater or equal than the actual risk.
- The higher the calculated risk is, the higher will be the cost of appropriate mitigation measures.

This implies that complex methods that provide realistic risk estimates result in lower safety costs, because the risks are mitigated in an efficient way. This is a very important point emphasized in all basic safety documents in aerospace industry (NASA Probabilistic Risk Assesment... (2002a), FAA System Safety Handbook (2000), MIL-STD-756B (1981), MIL-STD-882D (2000)) and is closely related to conditional probabilities.

Another problem is that "being on the safe side" does not necessarily mean "being on the safe side". Incorporating too many safety measures without any reflection of conditional probabilities leads to actual decrease of the real safety, as illustrated in Fig. 1.5.

1.4 Objectives of the Thesis

This thesis should provide insight into a variety of possible risk analysis methods, explain the basic principles of the most important ones, compare traditional risk analysis methods used in tunnels (PIARC – Integrated Approach to Road Tunnel Safety (2007) and PIARC – Risk Analysis for Road Tunnels (2008)) and an alternative approach (Fault Tree Analysis) (NASA Probabilistic Risk Assesment... (2002a), FAA System Safety Handbook (2000), MIL-STD-756B (1981), MIL-STD-882D (2000), NASA Fault Trees... (2002b)) taken from different industries. It tries to show the advantages of use of the proven methods and its applicability to the tunnels with ease and convenience and thus provides alternative approach to this problem. The provided analysis is applied in the Strahov Tunnel as of 2009.

1.5 Outline of the Thesis

- **Chapter 1 – Introduction** presents the topic and goals of the thesis. It introduces concept of Risk Management and Risk Analysis as inevitable part of decision making and engineering.
- **Chapter 2 – Methods of Risk analysis Used in Tunnels** describes variety of methods used in different industries with special accent on those used in tunnels.
- **Chapter 3 – Alternative Approach to Tunnel Risk Analyses** introduces new methods into the tunnel Risk Analysis. Two most popular and well-known methods, Fault Tree analysis (FTA) and Failure Mode, Effects and Criticality analysis (FMECA) used by (among others) National Aeronautics and Space Administration (NASA), Federal Aviation Association (FAA) or United States Department of Defence (DoD) were chosen and described.
- **Chapter 4 – Case Study – Strahov Tunnel** provides a practical insight into the Risk analysis of the Strahov Tunnel, where both Fault Tree Analyses as well as Event Tree Analyses were used.
- **Chapter 5 – Incorporating Aviation Experience into Tunnel RA Methods** compares the traditional approach and methods from aviation industry in tunnel Risk Analysis.
- **Chapter 6 – Conclusions** summarizes goals and results of the thesis.

Chapter 2

Methods of Risk Analyses Used in Tunnels

Although the idea of risk analysis in tunnels is fairly old, it was effectively born in 1999 after Mont Blanc (39 fatalities), Tauern (12 fatalities) and St.Gothard (2001: 11 fatalities) catastrophes (PIARC – Integrated Approach to Road Tunnel Safety (2007)). After these accidents it was clear that it is necessary to systematically analyze, evaluate and mitigate the risk.

It is important to emphasize here, that most of the currently used methods for risk analysis and estimation counts with fire as the "initiating" and to the overall risk most contributing factor. There are, however, several pitfalls when considering fire. Above all, one has to realize, that although fire has probably the most serious consequences on the tunnel (equipment, people, etc.), its occurrence is quite rare. Speaking strictly statistically, the number of fire occurrence is unsatisfactory to have sound statistical meaning. Yet another problem is with expressing of the "power" of fire (e.g. heat release rate, etc.), because fires of different intensities have, of course, different influence.

Risk analysis (RA) in tunnels, as well as anywhere else, is not a separate tool, but is incorporated into a Risk Assessment Process (RAP) that is composed of (PIARC – Integrated Approach to Road Tunnel Safety (2007), PIARC – Risk Analysis for Road Tunnels (2008)):

1. **Risk analysis** that studies the possible failures (mishaps) and the consequences

2. **Risk evaluation** that gives level of estimated risk whose acceptability must be decided later on. Several kinds of risk criteria can be introduced as follows:

    - expert judgment
    - guidelines, directives, standards
    - threshold values
    - cost-effectiveness parameter: cost of safety
    - individual risk: probability of injury/death of one specific person per time period
    - total expected fatalities in a specific tunnel per time period

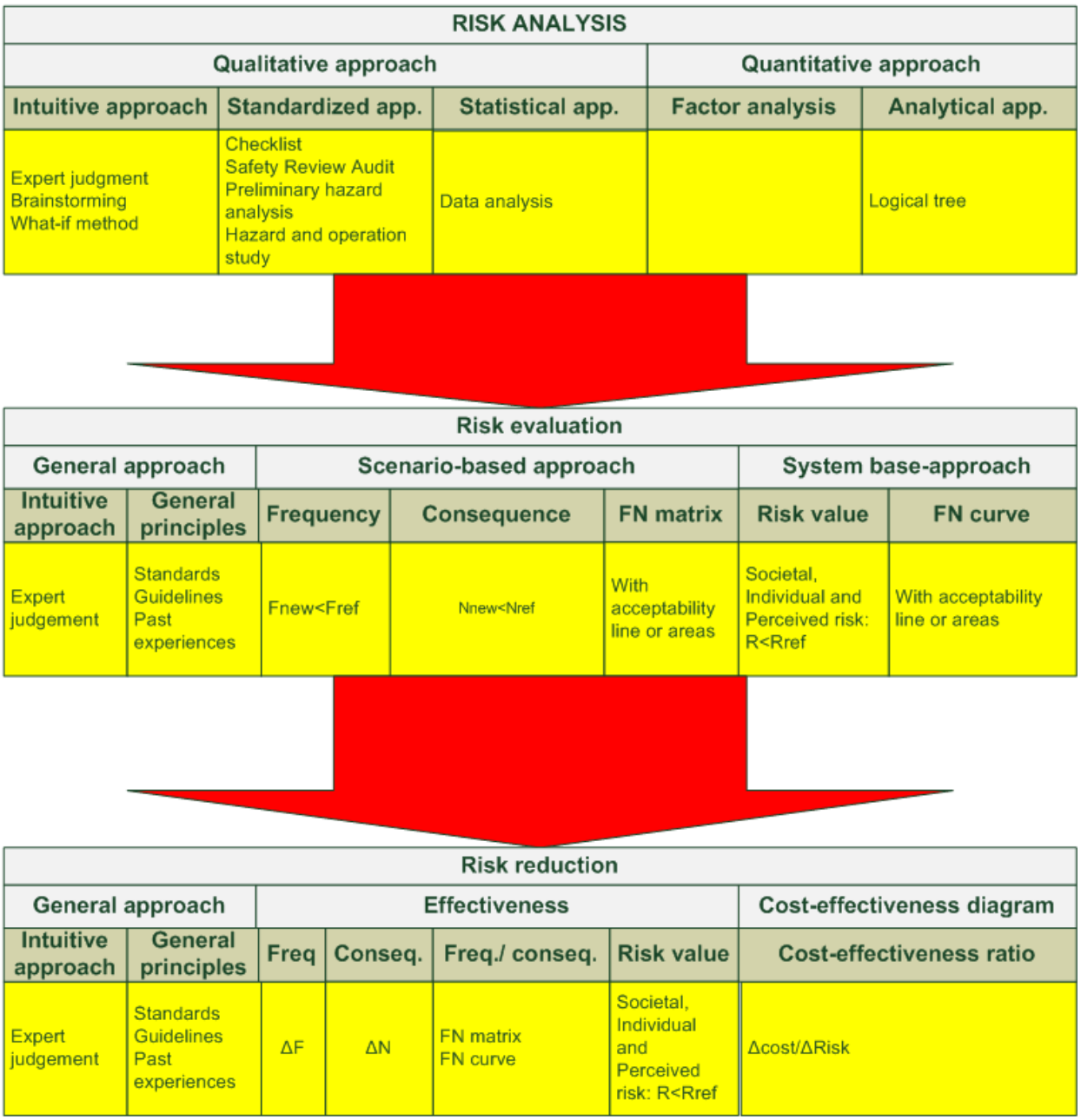


Figure 2.1: Risk Assessment Process

3. **Risk reduction and planning of safety measures** is made upon request of risk level from previous point. If the risk level is not acceptable, safety measures have to be introduced to meet the risk level specificiation/request.

For better understanding, RAP is depicted in Fig. 2.1.

RA is explicitly requested in EU tunnels by EU Directive on the minimum system requirements. Methods of RA[1] used in tunnels can be divided into two major groups, quantitative and qualitative methods.

- **Qualitative methods:** These methods are based upon arbitrarily definable evaluation standards. They are often simple, flexible and can be used for many kinds of problems. The pitfall of this kind of method is an unclear weight of subjective impression and evaluation.

- **Quantitative methods:** The risk in these methods is quantified and the system is structured in some manner. Quantitative methods also enable incorporation of interrelationships, interferences and correlations among different elements subjected to analysis. The main advantage, comparing to qualitative methods, is transparent representation of the estimated risk and better understanding of correlations. However, this kind of methods is often time and money consuming; moreover, they can be carried out only when quantitative data are available.

Two basic principles are used in tunnel risk analysis methods:

- **Scenario-based approach:** a set of relevant scenarios is defined (RVS 09.03.11 (2008)) and the probability of each scenario is estimated, risk evaluated and effect analyzed. This kind is used especially for the cases such as optimization of escape routes in tunnels, planning of emergency response measures etc. Each scenario has its own, separately done risk assessment. Both quantitative as well as qualitative methods can be used. Example of the scenario-base approach is depicted in Fig. 2.2

- **System-based approach:** the main difference compared to the scenario-based approach is an assessment of the risk. In this approach, the probabilities are estimated and the risk is assessed for the whole system. This is used when the whole system, such as tunnel, is taken into an account, or its subsystems, such as ventilation etc. Qualitative methods must be used (PIARC – Risk Analysis for Road Tunnels (2008)). Example of the system-base approach is depicted in Fig. 2.3

The risk assessment methods used in road tunnels are chosen according to the variety of criteria, such as national standards and regulations, international norms, or the objective of the analysis (PIARC – Risk Analysis for Road Tunnels (2008)), and depend e.g. on the complexity and characteristics of the analyzed tunnel, the availability of specific data, performance of subsystems etc. The oldest analyses made use of expert judgments, but these can be used only for simple system and with abundant data. Later on, expert judgments were not able to keep risk analysis and risk evaluation apart, or were not able to make any reasonable analysis at all. Increasing complexity of the systems lead to the use of quantitative methods such as logical trees, consequences models or event trees. With starting of quantitative methods, the role of expert judgement has changed in favor of supplementary role, when e.g. data are missing or are incomplete. This is particularly important when speaking about road tunnel incidents, where data are often missing or miss statistical importance. Moreover, only few countries have published their statistics.

[1] The short review of selected risk analysis methods is in Appendix B.

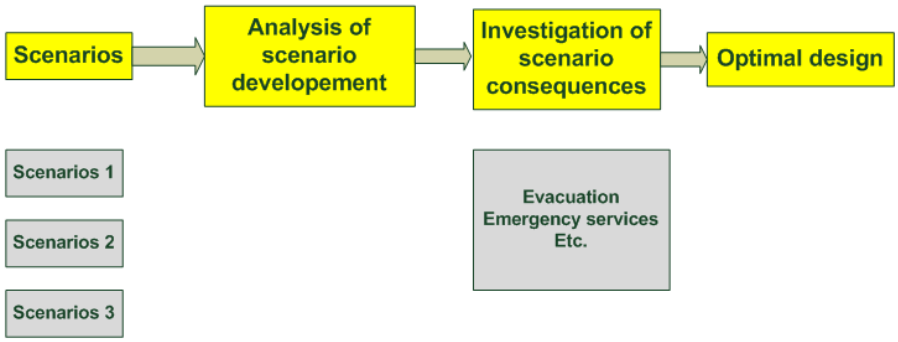


Figure 2.2: Scenario-based approach

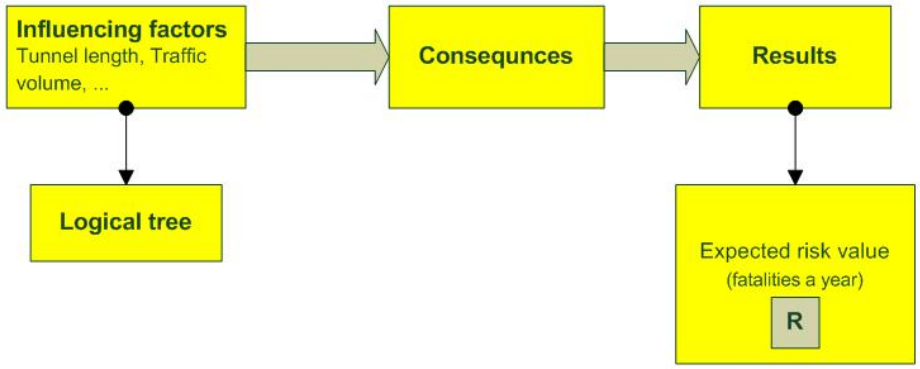


Figure 2.3: System-based approach

2.1 Risk Analysis in Selected PIARC Member Countries

Incident rates for different tunnels are not same, and depend on many factors. To get proper results, the correction factors have to be introduced for different country, location, geometry of the tunnel, traffic complexity and time line. Some countries have been using risk analysis methods for several years, yet in many countries it is a new expression (PIARC – Risk Analysis for Road Tunnels (2008)). Brief survey of methods in selected countries is listed as follows:

- **France.** As a consequence of the Mont Blanc Tunnel fire, safety regulations have been completely remade and new methodology "Specific Hazard Investigation" was introduced. This method is scenario-based and allows investigation of quantitative elements, such as smoke or fire flow. A quantitative assessment of frequencies of trigger events is performed followed by ranking of trigger events, which leads to standardized Frequency-Consequence matrix (Frequency-Consequence matrix will be explained more in detail in Chapter 3, Section 3.4). Thereafter a quantitative consequence analysis is carried out for a set of scenarios selected in the Frequency-Consequence matrix. The specific hazard investigation should result in the compliance of the investigated tunnel with French technical instruction and/or EU Directive. It specifically provides recommendations for risk reduction, evaluates the adequacy of measures taken to reduce the risk, ensure the absence of common fail-

ure mode, etc. This method allows the comparison of risk level of different tunnels, enables modeling of interaction of smoke propagation and the procedure of self-rescue. The main disadvantage of this method is high costs, especially in the case of simpler situations. This model, however, does not count with the investigation of risk of transportation of dangerous goods, and therefore model DG QRA developed by OECD/PIARC is being used (PIARC – Risk Analysis for Road Tunnels (2008)).

- **The United Kingdom.** The use of risk analysis has a long tradition in the UK and tunnel safety analysis has been standardized by 1978. The United Kingdom is characteristic for using a rather big variety of qualitative analyses (Risk Priority Number method), deterministic scenarios analysis, as well as ad-hoc probability risk analysis.

- **The Netherlands.** Deterministic, scenario-based risk analysis method "Dutch scenario analysis for road tunnels" has been introduced to optimize the management of processes of an accident. This method also enables implementation of several quantitative features. The scenario analysis is a deterministic method identifying possible weak points in the tunnel as such. The Dutch put special focus on self-rescue and emergency response. The consequence analysis is done in a qualitative way, however later on, some quantitative data are added (number of people in tunnel, casualties, ...). Defined scenarios[2] are evaluated against criteria and conclusions and recommendations are made. However, there are no risk calculations, thus there can be no cost-effectiveness assessed. Another approach in use is system-based TunPrim spreadsheet model for quantitative risk analysis with emphasis on twin tube tunnels with unidirectional traffic and longitudinal ventilation. This model counts with statistical data – frequencies of initial events from which an event tree is constructed and frequencies of scenarios are calculated. The resulting expected risk represents the average number of fatalities per year and societal risk – FN curves (FN curves will be explained later). Risk acceptance criteria have been defined as 10^{-7} per person-kilometer and societal risk as $10^{-1}N^2$ per km per year, where N is lower bound on the number of fatalities. The model can be used to calculate the risk reduction by adding risk-reducing devices, to support decision making process for the selection of safety measures, to asses new or existing tunnels, etc.

- **Norway.** Deterministic model "TUSI" is used for tunnel of the total length greater than 500 m. The odds of this method are nonexistence of consequence assessment and no standardized risk level, which are subjectively judged by tunnel management.

- **USA.** Deterministic and probabilistic methods are used mainly for several fire scenarios. Most of the methods count with the knowledge data base exploiting past experience. The old tunnels have been upgraded on the basis of the US National Fire Protection Agency standard for "Road Tunnels, Bridges, and other Limited Access Highways" (NFPA502). However, there is no national safety assessment document, and the implementation of some risk assessment is reserved for the respective states.

[2]Selection of the specific scenario as relevant is dependent on its frequency.

- **Austria.** After several years of using past experience and prescriptive guidelines Austria has started to use methodology of integrated quantitative analysis. Risk assessment concept was based upon the minimum safety requirements defined by EU Directive and the OECD/PIARC DG QRA model for transportation of dangerous goods is being used.
  Austrian Tunnel Risk Model TuRisMo RVS 09.03.11 (2008) is a set of quantitative methods that basically comprises quantitative frequency analysis (event trees for analyzing the sequences of the events from initial event that are quantified) and quantitative consequence analysis (quantification of the consequences of the effects of tunnel accidents). The shares of risk are separately estimated for mechanical effect, fires and transportation of dangerous goods. Risk assessment and evaluation is done by comparison of risk reducing effects of different safety measures and precautions as well as by comparing the risk of investigated tunnel and reference[3] tunnel. The TuRisMo model covers longitudinal as well as transverse ventilation tunnels and counts with several kinds of tunnel accidents with injuries. It enables modeling of both smoke propagation and self rescue procedure in case of fire. Distribution of different accident consequence classes are not included and therefore the model is not suited for investigation of accidents with low probabilities and high consequences, thus it is not suitable for investigation of dangerous good transport accident effects.

- **Czech Republic.** Mainly quantitative models are used, but commercial models are only at the stage of development. The EU Directive 2004/54/*EC* on minimum safety requirements for tunnels was implemented into the law as 80/2006 in 2006. This act applies for all road tunnel with total length over 500m. As a standard for tunnel construction "ČSN 737507" is used. Basic provision for the design of technological equipment of road tunnels in provided in Technical specification TP 98 and TP 154. Safety assessment methods are included in Technical specification "Road tunnel safety", that are established on fault tree charts or Bayesian network (Prague city ring). For the transportation of dangerous goods, the OECD/PIARC DG QRA model is being used.

- **Germany.** Mainly prescriptive guidelines (RABT) are in use as well as risk-based approach in specific cases. There is no unified approach and many different model for tunnels are used. Due to EU Directive a new quantitative methodology is being developed. For transportation of dangerous goods the OECD/PIARC DG QRA model is being used.

- **Italy.** belongs to the countries with no or little experience with risk analyses. The effort to implement EU Directive lead to establishing a research in this area and a kind of quantitative analysis has been introduced (event trees, smoke propagation model, etc.). The Italian approach is based upon quantitative probability estimates and quantitative consequence analysis (scenarios). The method introduced event trees (logical trees) where a set of triggering initial events is identified and consequence analysis performed. Probability quantification for the trigger events are base upon a statistical approach – the fire rates in tunnels, while the probability quantification of other events is derived from the reliability performance of the tunnel ele-

[3]Reference tunnel is a tunnel of the same length and characteristics as the tunnel under investigation and complying with the minimum safety requirements of EU Directives.

ments (equipment). Consequence analysis is focused on smoke flow, temperature, concentration of toxic substances and visibility, because these factors particularly influence the process of self-rescue. The method is used for existing as well as new tunnels, especially for choosing of additional equipment or alternative safety measures.

- **Switzerland.** "Ordinance on Protection against Major Accidents" is Swiss implementation of quantitative risk analysis which is, however, limited to the evaluation of transport of dangerous goods and therefore this methodology can not be extended to risk evaluation in road tunnels. At the moment no other risk analysis methods are being developed.

- **Japan.** There is absolutely no risk analysis performed in Japan, nor the plans for the future implementation. There have been, however, developed and introduced many safety measures and precautions. Protection of life is the top priority in the case of the fire and therefore there is an effort to satisfy an early detection of an accident and fire, control traffic, evacuation of the tunnel users and extinguishing of the fire. Safety features consist of preventive measures (awareness of the tunnel users of potential dangers, appropriate ventilation system installation, tunnel management, etc.) and emergency facility based measures. (Tunnels in Japan are classified into five categories with respect to their length, traffic volume, etc. The classification was determined by the probability of accidents based upon the past experience)

- **OECD/PIARC.** The main purpose of Dangerous Goods Quantitative Transportation Assessment (DG QRA) is to assess the risk relative to the dangerous goods transport in a quantitative way. Consequences and frequencies of the respective scenarios are simultaneously evaluated and societal risk is assessed. QRA has the following steps (Charlotte et al. (2008)):

  - choice of a restricted number of Dangerous Goods
  - choice of scenarios
  - identification of physical effects of the selected scenarios
  - evaluation of effects identified in previous step
  - possibilities of escape/sheltering and/or rescue
  - determination of each scenario frequency

  FN curves and their expected values are the major outputs of the QRA model. FN curve is a log-log plot of the frequency of events which causes at least N fatalities against the number N. If the frequency scale is replaced by annual probability, then the resultant curve is called fN curve. Although FN curves are constructed based on historical data, they in fact represent current situation and form the basis of developing societal acceptability and tolerability levels. The example of societal risk criteria is depicted in Fig. 2.4. Acceptable[4] risk refers to the level of risk which requires no further reduction. Tolerable[5] risk refers to the risk level assessment in exchange for

[4] A risk which everyone impacted is prepared to accept. Reduction of such a risk is not required unless reasonably practicable measures are available at low cost in terms of money, time and effort.

[5] A range of a risk that society can (and is prepare to) live with. It is a range of risk regarded as non-negligible and needing to be kept under review and reduced further if possible.

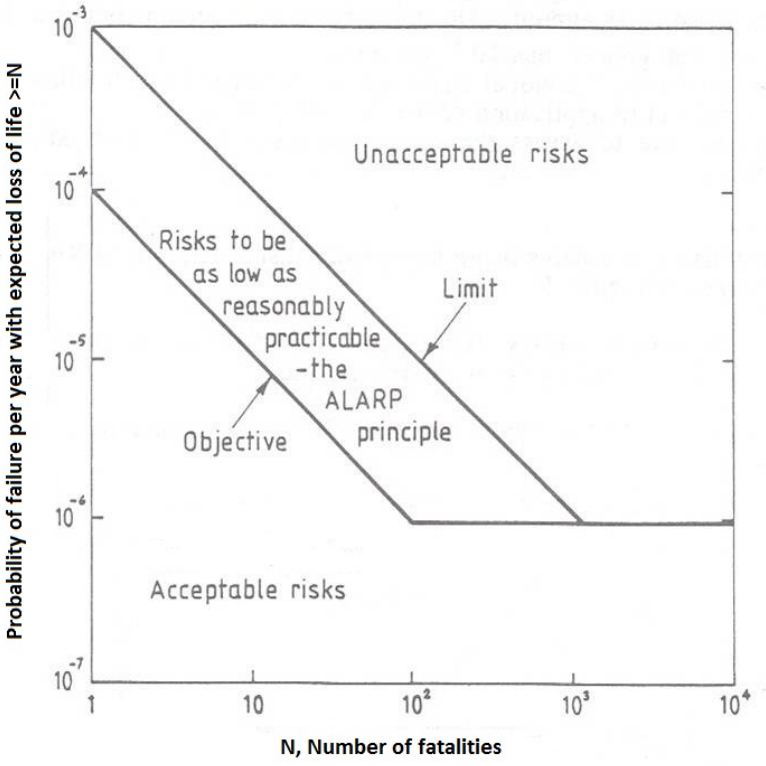


Figure 2.4: FN curves and societal risk criteria

certain benefits. It is up to the society to decide whether to accept or tolerate the risk. Between the tolerable and acceptable risk (see Fig. 2.5) stands risk level expressed by **As Low as Reasonable Practicable** principle, (ALARP[6]). The example of FN curves (based upon different regions) is depicted in Fig. 2.6.

Yet another approach is given in PIARC – Risk Analysis for Road Tunnels (2008), where in the first step an expected societal risk ("intrinsic risk" – expected number of fatalities caused by transportation of dangerous goods per year) value for the tunnel is calculated whilst the following data are needed: DG traffic volume and composition (personal vehicles, buses, HGV, etc.), accidental rate along the routes and tunnel characteristics (length, geometry of ventilation, emergency exits, number of tubes, etc.). The second step of DG QRA is carried out only if the intrinsic risk exceeds certain limit: DG QRA enables comparison up to three alternative routes, where the following steps are carried out:

- data collection for the alternative routes
- calculation of intrinsic risk for comparison of the routes – FN curves
- comparison of the curves and the sensitivity study

The combination of quantitative frequency and consequence analyses allows the calculation of FN curves.

The whole process of DG QRA is depicted in Fig. 2.7.

[6]It is a risk level lower than the limit of tolerability; tolerable only if the risk reduction is impracticable or if its cost is too high and is disproportional to the improvements gained.

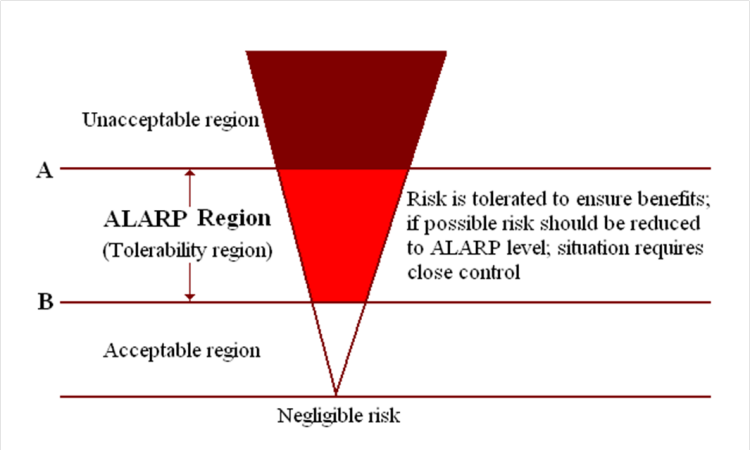


Figure 2.5: Levels of risk

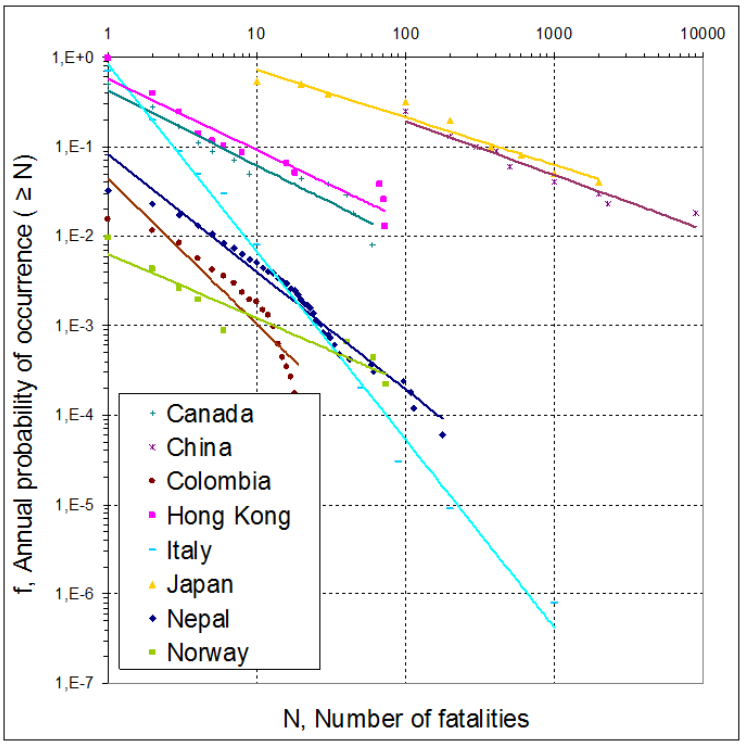


Figure 2.6: FN curves

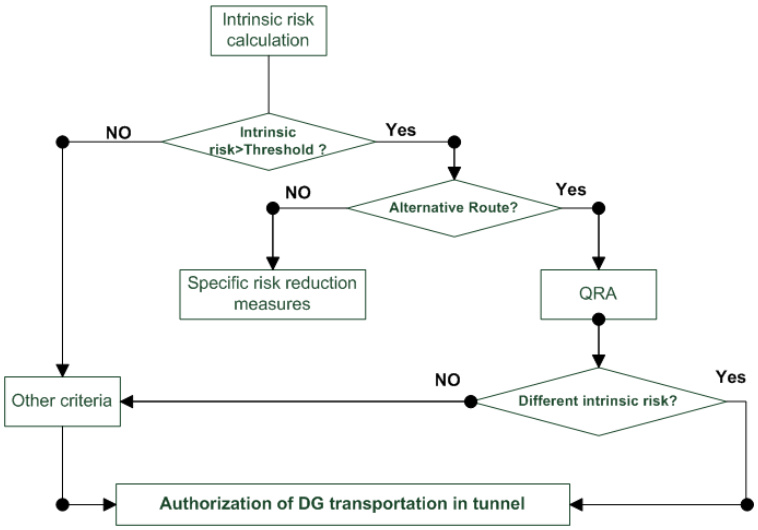


Figure 2.7: The DG QRA model

The value of intrinsic risk is obtained by applying DG QRA for tunnel (all DG are expected to go through tunnel). If intrinsic risk is greater than certain threshold, say 0.001, then a QRA is performed to compare tunnel under investigation to alternative routes. If intrinsic risk is lower than that threshold, then the risk value caused by DG is out of interest. When a second step (QRA study) is needed, then the model is used to compare the risk value of DG transportation through the tunnel to the risk value of DG transportation via alternative routes. The result of DG QRA is proposal for decision making process of administration whether or not to give an authorization of full/partial/no dangerous goods transportation for the tunnel under investigation.

The main problems of the current methodology used in tunnels is probably is statistical validity of fire occurrence. Because of the lack of data, the fire probability density functions are very raw and very often highly imprecise approximations of the real properties of fire. Therefore there is an effort to introduce an alternative approach that could deal with this statistical pitfalls. A possible way seems to be a usage of successfully industry-applied and yearly proved methods based upon fault tree and event tree analyses, which will be described in following chapters.

Chapter 3

Alternative Approach to Tunnel Risk Analyses

As was already stated in the previous chapter, the current methods used in the risk analysis for road tunnels have several serious problems, such as lack of statistical data of fires, non-quantified results of the analysis and therefore only "experienced-based" mitigation of the risk decisions, no unified and standardized approach to the risk analysis, thus an existence of a number of ad hoc methods, etc. The effort of this thesis is an introduction of comprehensible, widely applicable and acceptable, yet clear approach to the estimation and assessment of the risk in the tunnel. The Probabilistic Risk Assessment (PRA) with Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) widely used in aerospace, nuclear, chemical and other industries could be very conveniently applied also for common tunnel analysis. The goal of the usage of these methods is to get clear, comprehensible numerical results of both the risk analysis and costs, i.e. the results should provide unambiguous decision tool for management. The results should include current risk levels of investigated object, the contribution to the overall risk of its individual components or the sets of components, the numerical dicrease/increase of the risk when a safety equipment is added/removed and above all, also an economic cost of the risk mitigation. All of these above mentioned criteria are fully satisfiable by using of the PRA, FTA and ETA.

One of the most important objectives of NASA according to its own words is to add Probabilistic Risk Assessment (PRA) to its repertoire of expertise in proven methods to reduce risk. Fault Tree Analysis (FTA) (NASA Fault Trees... (2002b)) is one of the most important techniques used in PRA today. Importance of PRA and FTA begun to grow after the Three Mile Island nuclear disaster (1979) and Challenger accident (1986: FMECA used). But the real importance of PRA was recognized in 1990 when it was necessary to know how much do multibillion investments to NASA Space Shuttles contribute to overall system safety. Because of logical, systematic and comprehensive approach of PRA and FTA, they have been proven to be capable of uncovering design and operational weaknesses and evaluate reliability. Moreover, the strength of PRA and FTA is, that they are both analysis and decision support tools. Having clear and explicit outputs, they are naturally engaged into the Risk Management process (NASA Probabilistic Risk Assesment... (2002a)). A PRA process can be itemized as follows (NASA Probabilistic Risk Assesment... (2002a)):

1. **Definition of the Objective.** The objective of the risk assessment must be properly defined and the undesirable consequences, end states, are identified. The project

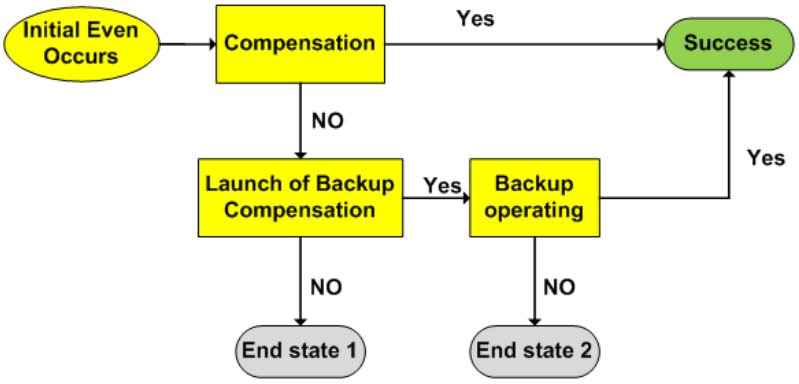


Figure 3.1: Event Sequence Diagram

success criteria are necessary to define risk assessment end states (ES_j) in Eq. (3.1)).

2. **Familiarization with the System.** All relevant design, operational and engineering information are gathered to get familiar with the system and its behavior. These may include design manuals, design blueprints and technical documentations, operations and maintenance manuals, operations and maintenance logs and personnel.

3. **Identification of IEs.** Initial Events (IE) or Trigger Events of the event sequences (scenarios) are identified and analyzed by means of master logic diagrams (MLD) or FMEA/FMECA analyses.

4. **Modeling of the Scenarios.** Each accident scenario is developed in inductive manner with probabilistic tool named Event Tree (ET). An ET starts with IE and continues through the scenario (pivotal events) until the end state is reached. In fact, one step was omitted: Accident progression is modeled by inductive, success oriented graphic tool called Event Sequence Diagram and ET is only its formal derivative. The process of accident progression modeling is launched by Event Sequence Diagram because the morphology of an Event Sequence Diagram is less rigidly structured, permits the complex relationships among IEs and subsequent event sequences and is more understandable for managers and non-technical personnel. On the other hand ET is a formal derivative of Event Sequence Diagram and enables convenient linking ET and Fault Tree (FT) and successive evaluation. One Event Sequence Diagram is developed for each IE and the objective is to depict all possible paths from IE to the end states. ET is a quantitative graphic tool that displays relationships among IEs and subsequent responses. For better understanding the derivation of ET from Event Sequence Diagram, see Fig. 3.1 and Fig. 3.2, respectively.

5. **Modeling of the Failures.** Each failure (complementary success) of pivotal event in accident scenario is modeled in deductive manner by means of FT. The top event of FT (more about FT is provided in Chapter 3) (negation of the system success criterion) is a given as negation of the pivotal event defined in an accident scenario. Fig. 3.3 shows the relationship of the FT and ET.

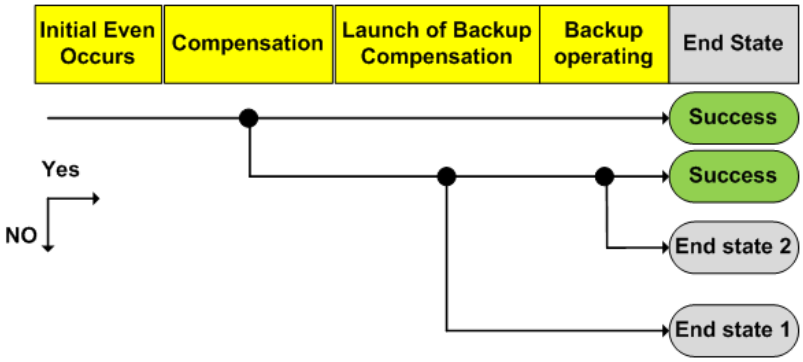


Figure 3.2: Event Tree

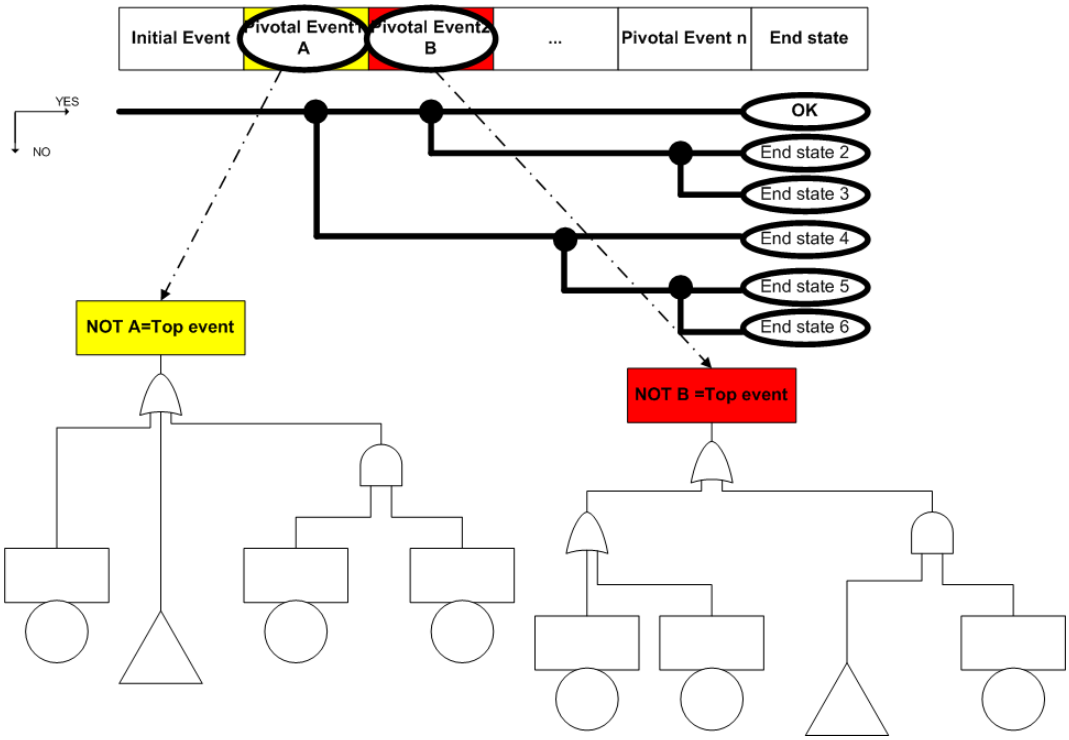


Figure 3.3: Event and Fault Tree relationship

6. **Collection, Analysis and Development of the Data.** Various types of data are collected (Chapter 3, Section 3.2: Steps of the Fault Tree Analysis, FT Evaluation) to quantify the accident scenarios and accident contributors.

7. **Quantification and Integration.** The frequency of occurrence of each end state in the ET is the product of the IE frequency and the (conditional) probabilities of the pivotal events along the scenario path linking the IE to the end state. Scenarios are grouped according to the end state of the scenario defining the consequences and thereafter end states are grouped and their frequencies are summed up. The mathematically correct way of calculation of the expression for the frequency of a specific scenario, $\Lambda_{j,k}$ is as follows:

$$\Lambda_{j,k} = \Lambda(ES_{j,k}) = \lambda_j p(ES_{j,k}|IE_j), \tag{3.1}$$

where λ_j stands for the frequency of the j-th IE and $p(ES_{j,k}|IE_j)$ denotes the conditional probability for the end state of the event sequence ES_k (without initiating event IE_j), in the event tree initiated by IE_j given that IE_j has occurred.

8. **Uncertainty Analysis.** This analysis is performed to evaluate the rank of knowledge/confidence in the calculated numerical risk results (e.g. by Monte Carlo methods).

9. **Sensitivity Analysis.** This analysis is performed to show which inputs' or elements' changes cause the greatest changes in risk results. The uncertainty associated with some PRA assumptions is handled by performing sensitivity studies. PRA uses assumptions when data are missing or information lacking and can have significant impact on the PRA results. Sensitivity analysis uses e.g. examination of the risk metric to identify dependence-suspect minimal cut sets (more about minimal cut sets in Chapter 3, Section 3.2), minimal cut sets containing failure of components, of which more than two have common property which makes them susceptible to dependant failures.

10. **Importance Ranking.** Ranking of risk scenarios provides insight regarding the contribution of individual events to the total risk. Scenario risk ranking shows the importance of group failures, not the individual events. If the event with significant contribution to the risk is in the structure of many low frequency scenarios, it may be absent in the definition of the dominant risk scenario and scenario risk ranking will not capture the risk importance of this event. To address this issue quantitative importance measures are calculated. When the importance measures are calculated, the events are ranked according to the relative value of the importance measure and treated further with respect to their rank (more about importance measures in Chapter 3, Section 3.2).

This full PRA process can be truncated to "limited scope" PRA. The truncated PRA does not mean, that some of the steps would be missing at all, but it means, that only major contributors instead of all will be identified and evaluated.

The **interpretation and presentation** of the result of PRA is crucial. The level of detail and the style of the presentation of risk results depends on the risk assessment objectives. Graphical and tabular displays are effective means for conveying the results of a risk assessment. The following type of information is generated in typical PRA:

- total likelihood of various end states
- list of dominant risk scenarios and the likelihood of each scenario
- list of relative ranking of each scenario to the total end state likelihood
- total mission risk
- importance measures
- risk curves, and others.

3.1 Deductive vs. Inductive Methods

In a deductive analysis it is postulated, that a system has already failed and the task is to find out what modes of system behavior contributed to this failure. Deductive methods, such as Fault Tree Analysis (FTA), are applied to determine **how** a given system state can occur, while inductive methods try to determine **what** system states are possible. In inductive approach, a particular fault is postulated and the task is to find out the effect of that failure on the system. In other words, induction means reasoning from the individual case to a general conclusion. Among inductive methods one can count e.g. What-if method, Parts Counts Approach (most conservative one, assuming, that simple component failure leads to a system failure), Failure Mode and Effect Analysis (FMEA: identifies failure probabilities, failure modes and failure effect), or Failure Mode, Effects and Criticality Analysis (FMECA: similar to FMEA, but criticality of the failure is analyzed more in detail). All inductive techniques post one of the most hazardous pitfalls of the risk analysis: the project becomes only a matter of filling out forms instead of proper analysis. Moreover, FMEA as well as FMECA analyzes only single component fault and their system effects and does not consider combinations of the component faults. Oftentimes inductive methods are called bottom-up, while deductive methods are called top-down. FTA is an appropriate analysis when an undesired event is given, while the FMEA/FMECA and/or other inductive analyses are appropriate to use when the set of initiating events are identified and the goal is to figure out the consequences. For initiating events that can possibly lead to multiple failure states are the event trees proper choice to determine the consequences and enumerate the possible scenarios.

3.2 Fault Tree Analysis

FTA is a deductive, failure-based approach that starts with an undesired event (top event), and then determines its causes using backward-stepping approach. The symbols used in a FTA indicate the type of the event and the type of the relationships involved. The fault tree (FT) is a qualitative model with the possibility of quantitative evaluation that provides the information about the probability of the top event. FTA can be applied to both an existing system and to a system that is being designed. For system in design, FTA

can provide an estimate of the failure probability and contributors using generic data. FTA can be also used as a supporting tool of a performance-based design. In an existing system FTA can identify weaknesses, evaluate possible upgrades, monitor and predict behavior. A FT can be transformed into its logical complement, a success tree (ST), that shows the specific ways the undesired event can be prevented from occurring.

FTA is an analytical technique[1], where an undesired state is specified and the system, its environment and operation modes are then analyzed. A FT is a graphical mode, thus depicts the interrelationships of basic events that lead to the top event. The top event corresponds to some particular failure mode, and thus the FT includes **only** those faults, that **contribute** to this top event. A FT is composed of a complex of entities, "gates", that permit or prohibit the passage of fault up the tree. The gates thus show relationships of events needed for the occurrence of a fault at the output of the gate. The implicit supposition is, that outcomes are binary events.

The qualitative evaluations transform the FT logic into logically equivalent forms. These obtained results are minimal cut sets (MCS) of the top event. A cut set (CS) is a combination of basic events that can cause the top event. It is now clear, that a MCS is the smallest such a combination. Because the basic events are the bottom events, the MCSs relate the top event directly to the basic event causes. The structure of MCSs can provide valuable information e.g. MCS with single event means, that the occurrence of this single event causes the whole system failure. The upgrade and prevention actions should be firstly focused on these single event MCSs.

Even though FTs are of qualitative nature, a FT can be quantified and evaluated. The quantitative evaluations of a FT consist of the determination of top event probability and basic event importance. This is typically done by determination of basic events probabilities, calculation of the probabilities of MCS, those are summed up and the result is the probability of the top event. The MCSs are very often sorted by probability thus they can provide useful criterion of "severity" of the respective MCSs. The most influenced MCSs (MCSs with the highest probability) are called dominant cut sets. Top event frequencies, failure or occurrence rates etc. can also be calculated. Moreover, the calculation of time-varying probability values is also possible thus it enables to calculate probability density function of the time of the first top event occurrence. Quantified importance allows actions and resources to be prioritized according to the importance of the event causing the top event. For different applications different importance measures can be calculated e.g. how much will decrease the top event probability when some event is eliminated from occurring or how much is certain event contributing to the top event probability etc.

As mentioned above, a Success Tree (ST) is logical complement of a FT. Success is, however, specifically defined as the top event not occurring. The ST identifies the minimal sets (minimal path sets – MPSs) of basic events that need to be prevented in order to top event will not occur. Each of the MPSs can be quantified to prioritize the most effective methods for prevention of the top event. From an analytical point of view there are some several advantages that arise from failure space instead of success space perspective e.g. the definition of what is failure is much more straightforward that the definition of what is success. Another advantage of FT over ST is that from practical standpoint there

[1]The symbols used in FTA are included in Appendix C.

are generally more ways to success than that there are to failure.

3.2.1 Extent of Usage of FTA

FTA has a great range of use and it can be used throughout the system life cycle (see Fig. 1.2). A variety of major FTA uses is provided as follows:

- FTA can clarify and simplify the system logic and causes of the top event occurrence. FT is graphical tool to express the logic of the fault propagation through the system. Interactions and relationships can be easily depicted by use of the various types of gates. The failures of similar classes can be categorized according to the variety of criteria.

- Prioritization of contributing events can be done by sorting minimal cut sets with following evaluation, thus the counter-actions, safety measures and resource allocation can be accordingly prioritized. From the past experience it was shown, that $10 - 20\%$ of basic events contribute up to 80% of the top event probability (FAA System Safety Handbook (2000)).

- FTA as a proactive tool preventing the top event to occur that is able to identify the weak points of the system, which can be thereafter analyzed and corrected before the top event occurs. FTA moreover enables to evaluate the cost-performance of upgrades/corrections made to the system. Every upgrade of the system or parts of the system should be focused on the impact of the upgrade on the top event probability.

- Performance monitoring of the system is done with respect to probability of the top event. The basic events updates, ageing of the system, trending, etc. cause the need for re-evaluation of the top event probability with new information taken into account. The performance monitoring enables early identification of aggravating component/subsystem, thus its early substitution without top event occurrence.

- Optimization of resource allocation can be also done by FTA which not only identifies the most important events that are major contributors to the top event probability, but also identifies the minor and negligible events where the safety measures can be relaxed. According to FAA System Safety Handbook (2000) in some applications up to 40% of resources can be saved without significant impact on the top event probability.

- FTA can be also used as a design tool, that can evaluate and compare several alternatives and helps to choose the most suitable one that satisfies the design requirements.

- FTA can be used as a diagnostic tool to identify (and remedy) causes of the top event. This also includes the investigation of the most efficient corrective measure.

3.2.2 Steps of the FTA

The Fault Tree Analysis should consist of the following steps (FAA System Safety Handbook (2000)):

1. **Identification of the objective.** Definition of the proper and valid objective of the analysis is crucial.

2. **Definition of the top event.** Top event is the event for which the failure causes are identified and probability is calculated. Correct formulation of the top event is extremely important. Even though this seems to be obvious and easy, this is the source of the most frequent design errors. If either of afore-mentioned is incorrectly defined, then the whole analysis will be incorrect. The top event must be defined with respect to criteria defining the occurrence of the top event. This is often done by defining failure of the system as the opposite to the system success. From the practical viewpoint the system under study is first defined and a particular failure mode is selected to be the top event.

3. **Definition of the scope of the analysis.** The scope of the analysis determines the failure modes to include. The scope also includes the boundary conditions (initial states and assumed inputs of the system) for the analysis as well as the design version historical time period. The definition of boundaries means the clear and unambiguous limitation what is and what is not the objective of the analysis.

4. **Definition of the resolution of the analysis.** Resolution of the analysis defines to which level of detail will be the analysis carried out. The level of detail should depend on amount of data that are possible to be obtained at certain detail levels.

5. **Definition of the ground rules.** Ground rules establish the way how the events and gates are named and also determine the manner of modeling of the specific failures. The ground rules defined in FAA System Safety Handbook (2000) are as follows:

   - **Write the statements that are entered in the event boxes as faults; state precisely what the fault is and the conditions under which it occurs. Do not mix successes with faults.** The"what-condition" describes the relevant failed state of the component. The "when-condition" describes the condition of the system. Thereafter necessary and sufficient events resulting to the fault described by each boxed statement are determined.
   - **Classify the event as a "state of component fault" or "state of the system fault."** This classification is made by answering the question if the given fault is the component failure or not. This classification enables to recognize the faults as localized to the component or those with direct influence on the system. For the "state of the system" events one has to look for the necessary and sufficient immediate causes.

6. **Construction of the fault tree.** The most important thing is to "think in small" (FAA System Safety Handbook (2000)) i.e. necessary and sufficient immediate events that result in the event are identified for each event. In other words, for given top event one determines the immediate, necessary, and sufficient causes for the occurrence of the top event. The immediate, necessary, and sufficient causes of the top event

are now treated as sub-top events and one has to determine their immediate, necessary, and sufficient causes. It means that the sub-top events correspond to the top events in the subsystem fault tree. This insures thinking "in small" and proper backstepping which finally ends with the basic events. In a particular analysis, concept of hierarchy – system, subsystem and components, is introduced for convenience and for setting the boundaries to the problem. In constructing FT, the basic concept of failure effects, failure modes and failure mechanisms is important in introducing proper relationships among the events. Failure effects are addressed when the concern **why** a particular failure is of interest, i.e. what are its effects on the system. Failure modes describe **what** aspect of component failure are of concern and failure mechanism provides answer to the question **how** can a particular failure mode occur. The system failure modes are the "top events" that the analyst can consider. The investigated immediate causes for its occurrence will be failure mechanisms. Proceeding step by step, the analyst will arrive at the components failure-basic causes (basic events), which are defined by resolution of the tree. The construction ground rules follow as:

- The resolution of the fault tree should be determined by the highest level for which data exist. Modeling of the lower level jeopardize the analysis with larger uncertainties or erroneous probabilities
- The wiring or piping should not be modeled (wiring/piping fault have significantly lower probability than analyzed faults)
- Out of design conditions should not be modeled because the component is not intended to be used outside its operating environment
- Common cause failure contributors on all identical active components should be modeled
- Human errors that involves human committing of an unforseen action should not be modeled (unconstrained state space)

7. **Evaluation of the fault tree.** This step includes both qualitative and quantitative evaluation. The qualitative evaluation identifies minimal cut sets that are thereafter sorted by the cut set order (number or events in the set). The evaluation includes application of Boolean algebra to the FT. Those events of the tree that are initiated by other events are called faults, while those that are basic events of the FT are called "failures". The faults and failures are related to each other by the gates. Because the gates relate the faults and failures in the same way as the Boolean operations, the Boolean algebraic representation can be used.

   Quantitative evaluation provides the probability of the top event, dominant cut sets, as well as any event that is of interest. Cut sets are then sorted by probability and low probable sets are excluded from further analysis. Described more in detail, to get the probability of the top event, one has to know the probabilities of the basic events. These probabilities are then propagated upwards through the tree using the Boolean relationships. Alternatively, minimal cut sets can be generated from the FT[2] and then used to compute the probability of the top event. The top event is in

[2]Most of the current FTA software uses this method.

fact a union of the minimal cut sets, thus the probability of the top event can be approximated[3] as a sum of the probabilities of the minimal cut sets i.e.

$$p(TE) = \sum_{i=1}^{n} p(MCS_i), \tag{3.2}$$

where

$$p(MCS_i) = p(BE_1)p(BE_2)\dots p(BE_k), \tag{3.3}$$

with the notation as follows: TE stands for top event, BE is an acronym for basic event and MCS means minimal cut set. Minimal cut set (MCS) is an intersection of the basic events, thus the probability of a MCS_i can be calculated as a product of the basic events probabilities.
The input data for basic events can be of four basic types:

- **Pure event probability.**
- **Event occurrence probability.** An event occurrence rate and the time interval must be supplied to calculate the event occurrence probability. The event occurrence rate is defined as

  $$\lambda_e = \lambda_0 d + \lambda_N(1-d), \tag{3.4}$$

  where $d = \frac{\text{total operating time}}{\text{total project time}}$, λ_0 is the event occurrence rate in the operating state and λ_N is the component failure rate in idle state. The event occurrence probability P_e is computed as

  $$P_e = 1 - e^{-\lambda_e t}, \tag{3.5}$$

  where λ_e is the event occurrence rate and t is the time interval.
- **Component failure probability.** To compute component failure probability, a component failure rate and a time elapsed project time must be provided (sum of the time in which the component is in operating mode and idle mode). The failure rate is defined as

  $$\lambda_{fr} = \lambda_0 d + \lambda_N(1-d), \tag{3.6}$$

  where $d = \frac{\text{total operating time}}{\text{total project time}}$, λ_0 is the component failure rate in the operating state and λ_N is the component failure rate in idle state. The component failure probability P_{fr} is computed as

  $$P_{fr} = 1 - e^{-\lambda_{fr} t}, \tag{3.7}$$

  where λ_{fr} is the component failure rate and t is the time interval.
- **Component unavailability.** If the component is repairable the input data can have the form of unavailability and a component failure rate and repair time must be provided. Unavailability can be expressed as follows:

  $$\begin{aligned} q &= \frac{\lambda_0\tau}{1+\lambda_0\tau} \text{ for operating component} \\ q &= \frac{\frac{1}{2}\lambda_s\tau}{1+\frac{1}{2}\lambda_s\tau} + 1 - e^{-\lambda_0\tau} \text{ for standby component,} \end{aligned} \tag{3.8}$$

[3]The approximation is good if the $p(MCS_i) < 0.1$ otherwise the union must be computed by different approach considering intersection of the MCSs.

where λ_0 is an failure rate for an operating component, τ is an average repair time, λ_s is component failure rate in standby regime T is the test/inspection interval.

8. **Interpreting and presenting of the results.** The results must be properly interpreted to have desired impact. The presentation is important to make decision maker to take the results of the analysis seriously and with respect, not just as a bunch of intangible numbers.

As it was already said at the beginning of this chapter (description of the Probabilistic Risk Assessment Process), one of the greatest advantages of the FTA is the ability to express the contribution of the respective event to the overall probability. At the time of decision making process, it is useful to have the events sorted according to some criterion/criteria. This is especially useful e.g. in the case, when (as it is always) the budget is limited and one has to decide which safety measures are crucial to implement and/or which critical elements in the system have to be "neutralized". This ranking is enabled by importance measures. Four basic types of importance measures can be calculated for different types of applications as follows:

- **Fussel-Vesely Importance.** Alternative name for this measure is the Top Contribution Importance and reflects the contribution of individual MCS containing the basic event x_i to the overall risk. The F-V is calculated as follows:

$$I_{x_i}^{FV} = \frac{p(\bigcup_J MCS_j^{x_i})}{p(\bigcup_J MCS_j)} = \frac{p(\bigcup_J MCS_j^{x_i})}{p(TE)}, \tag{3.9}$$

  where $p(\bigcup_J MCS_j^{x_i})$ is probability of the union of the MCSs containing event x_i and $p(\bigcup_J MCS_j)$ is probability of the union of all MCSs. The Fussel-Vesely Importance measure shows the conditional probability that at least one MCS containing basic event x_i will occur, given that the system has failed. Alternative calculation of the Fussel-Vesely Importance measures follows as:

$$I_{x_i}^{FV} = \frac{p(TE) - p(TE|x_i = 0)}{p(TE)} \tag{3.10}$$

- **Risk Reduction Worth.** Alternative name is Top Decrease Sensitivity and implies the decrease of the probability of the top event under assumption of non-occurrence of a given event. For the basic events the Risk Reduction Worth shows the amount by which the risk decreases assuming that respective basic event, i.e. failure, will not occur. The Risk Reduction Worth is calculated by re-quantifying the FT with the probability of the given event set to 0.0 and mathematically as:

$$I_{x_i}^{RRW} = \frac{p(\bigcup_J MCS_j)}{p(TE|x_i = 0)} = \frac{p(TE)}{p(TE|x_i = 0)} \tag{3.11}$$

Risk Reduction Worth and Fussel-Vesely Importance measures are used to identify hardware elements, that are the biggest contributors to the overall risk. One can see, that there is a relationship between Fussel-Vesely Importance and Risk Reduction Worth, that can be expressed as:

$$I_{x_i}^{FV} = 1 - \frac{1}{I_{x_i}^{RRW}}. \tag{3.12}$$

- **Risk Achievement Worth.** With alternative name Top Increase Sensitivity, it expresses a change in the risk when the probability of a basic event is set to 1.0, it means that Risk Achievement Worth shows the amount of change of the overall risk under assumption of the total failure of a basic event. This importance measure enables optimization of the prevention activities deployment since it shows the events with the greatest impact on the system. The Risk Achievement Worth is calculated by re-quantifying the FT with the probability of the given event set to 1.0 and mathematically as:

$$I_{x_i}^{RAW} = \frac{p(TE|x_i = 1)}{p(\bigcup_J MCS_j)} = \frac{p(TE|x_i = 0)}{p(TE)} \tag{3.13}$$

  RAW measure is useful for assessing which basic events of the risk model are the most crucial for causing the system to have a higher risk.

- **Birnbaum's Importance Measure.** Birnbaum's Importance Measure presents the rate of change in the top event probability as a result of the change in the probability of a given event, and mathematically as:

$$I_{x_i}^{BM} = \frac{\partial R}{\partial x_i} \tag{3.14}$$

  Birnbaum's Importance Measure is related to the Risk Reduction Worth and Risk Achievement Worth as

$$I_{x_i}^{BM} = p(TE) I_{x_i}^{RAW} - \frac{p(TE)}{I_{x_i}^{RRW}} \tag{3.15}$$

The steps of FTA are depicted in Fig. 3.4 for better understanding. The feedback from step 6 and/or 7 expresses the possibility of correction and/or modification of steps 4 and 5.

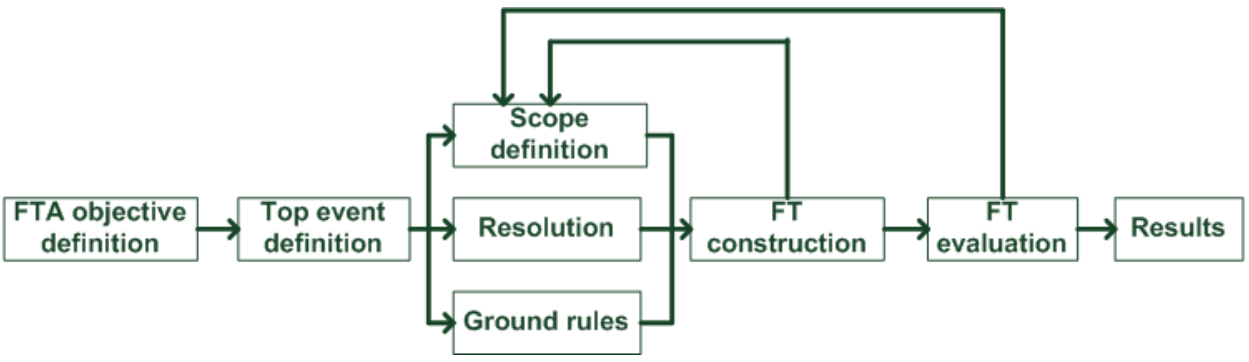


Figure 3.4: Fault tree analysis

3.2.3 Extensions to the FTA

3.2.3.1 Time and Phase Dependent Analysis

In the case that a project has several phases or time intervals, the probability of the top event represents the total system failure probability over the time interval. Different phases and intervals and their contribution can be modeled by an FT. These time and phase dependent events, however, cannot be directly modeled by currently available software (NASA Fault Trees... (2002b)). There are several methods how to deal with this problem. One of these methods is modeling of the time dependence by dividing the basic event into several new basic events. Each of them represents the corresponding time interval (Fig. 3.5).

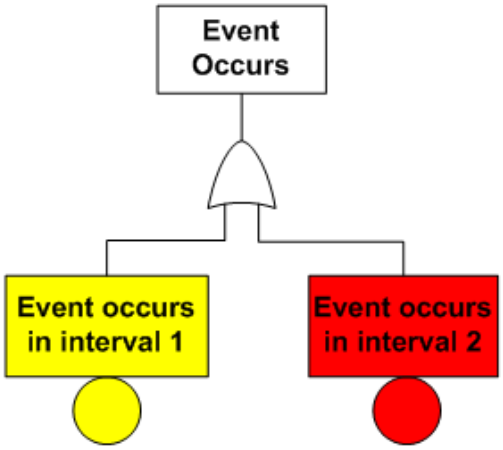


Figure 3.5: Time interval events

The new basic events occurrences in subintervals are joined together with OR gate to compose the original basic event. After obtaining of the MCSs they must be divided into as many groups as is the number of the new basic events created from the original one. Every MCS will have the respective $interval_i$ event, i.e. mutually exclusive events that can not occur in the same time interval, can not be in the same MCS. The sum of the respective MCSs will be the probability of the top event for the respective time interval.

3.2.3.2 Common Cause Failures

Two events are said to be dependent if

$$p(x,y) \neq p(x)p(y). \tag{3.16}$$

There are several classifications of dependencies, e.g.:

1. **Intrinsic.** The functionality of one component is affected by the functionality of other component. Intrinsic dependencies can be further subclassified as:

(a) **Functional Requirement Dependency.** Functional status of the component X determines the functional requirements of Y, e.g.: Y is not needed when X works or Y is needed when X works, etc.

(b) **Functional Input Dependency.** Functional status of Y is directly dependent on functional status of X, e.g.: Y works if X works

(c) **Cascade Failure.** The failure of one component cause the failure of another.

2. **Extrinsic.** Extrinsic dependencies do not origin from the system design or system itself, but are caused by external factors.

(a) **Physical.** Dependencies due to common environmental factors.

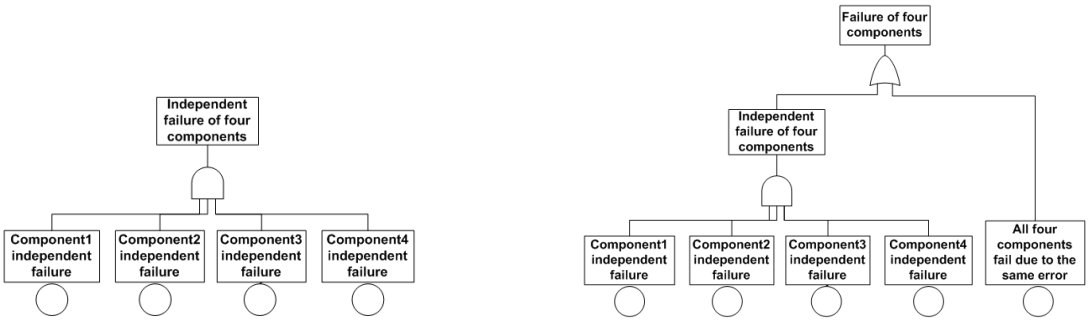
(b) **Human Interactions.** Same maintenance error can cause multiple failures of the same origin.

In PRA process, many extrinsic and some intrinsic dependencies are not explicitly modeled to construct manageable models. Dependant failures whose root causes are not explicitly modeled are called Common cause failures (CCFs). They represent failures of two and more components due to the same cause. The proper identification of CCFs is crucial, because neglecting of the CCFs contribution to the top event can significantly depreciate the analysis. CCFs are very often:

- design or material deficiency with a number of components with a same potential malfunction
- common environment, such as dust, radiation, vibration causing the failure of multiple components at once
- common installation errors caused by erroneous installation procedure
- common maintenance errors

CCFs are significant for active redundant components when the contribution to the TE increases with the increasing redundancy. CCF probability influences all components in the redundant set and extremely increases the probability, that all components in the set will fail. As an example, consider a system consisting of four redundant components, each with failure probability $p_{ind} = 10^{-3}$ and with the CCF $p_{CCF} = 10^{-2}$ (it means that all three components fail in one case out of a hundred due to a common cause). If the CCF probability is ignored, then the FT is depicted in Fig. 3.6(a)[4]

[4]For simplicity the rule of maximum three inputs to one gate is not obeyed.



(a) FT without CCF modeled (b) FT with CCF modeled

Figure 3.6: Fault tree with and without CCF modeled

end corresponding probability of the system failure is calculated as

$$p(\overline{S}_{ind}) = p_{ind}^4 = 10^{-12}, \tag{3.17}$$

which is fairly unlikely to happen. On the other hand, when the CCF is taken into account

$$p(\overline{S}_{CCF}) = p_{ind} p_{CCF} = 10^{-5}. \tag{3.18}$$

That is an enormous difference and with increasing number of components the difference grows even bigger. CCF must be separately modeled as depicted in Fig. 3.6(b). In fact, Eq. (3.18) and Fig. 3.6(b) describe a little different approach. To clarify this difference another method how to deal with CCFs has to be introduced – β factor. Each component (which has the same influence factor as some other component) is divided into independent failing component and a component affected by CCFs only. Then a total component failure frequency is a sum of independent failure frequency and common cause failure frequency, i.e.

$$p(Total) = (\lambda_I t)^n + \lambda_C t = [(1-\beta)\lambda_T t]^n + \beta\lambda_T t, \tag{3.19}$$

where λ_T is failure frequency, λ_I is independent failure frequency, $\beta = \frac{\lambda_C}{\lambda_T}$ is β factor, $\lambda_C = \beta\lambda_T$ is common cause failure frequency, and n is a number of affected components. Fig. 3.6(b) already agrees[5] with Eq. (3.19), where the total component failure frequency is a sum of its independent failure frequency (in the example 10^{-7} times lower than the independent probability and therefore is omitted) and the common cause failure frequency. There is an other option to model CCFs: Let $p(C_{AB})$ be the probability of the concurrent occurrence of A and B failures and $p(A)$, $p(B)$ be the probabilities of independent failures of components A and B, respectively. Then $p(C_{A,B})$ can be computed as

$$p(C_{A,B}) = gp(A), \tag{3.20}$$

where g is of generic value, typically in the range between 0.05 and 0.1 and can be more accurately found in tables of common cause factor (NASA Probabilistic Risk Assesment... (2002a)).

[5]To be absolutely accurate one has to remark, that Eq. (3.19) uses frequencies, while the previous example used probabilities. The logic is, however, the same. Moreover, the common cause factor was considered for concurrent failure of all three components. However, this could be modeled in more complex way, where three common cause factors would represent concurrent failures of respective couples of components, and the fourth would represent the concurrent failure of all three components.

3.2.3.3 Dynamic FTA

When the dynamics is taken into account a Dynamic Fault Tree (DFT) must be used. The DFT methodology was introduced in order to enable interconnection of the FTA and Markov analysis, where Markov chains are commonly used to asses the reliability and performance of fault tolerant systems. The original Markov models have clearly big disadvantage in being too large, whilst the DFT interconnect both, the mathematical power of Markov models and simplicity of the FT.

3.3 Human Reliability Analysis

The objective of the Human Reliability Analysis (HRA) is to study interactions between humans and the system. The human performance is influenced by many factors (NASA Probabilistic Risk Assesment... (2002a)) called Performance Shaping Factors (PFC) that can be of two types:

- External PSFs such as the complexity, written procedures, stress, etc.
- Internal PSFs such as operator training, experience, motivation, etc.

The human-system interaction (HI) can be classified into several categories based upon factors such as the timing of the HI with respect to initiating event (IE), human error type, cognitive behavior of humans responding to the accident, etc. HI based on their timing with respect to IE or accidents are of following types:

1. **Type A.** Routine actions evoked by maintenance, testing or calibrations. This type of HIs is explicitly modeled and is included in the system FT. Among these errors belong maintenance errors, testing and calibration errors, etc.

2. **Type B.** Interactions related to the IE such as human errors causing loss of power, etc. These interactions are included in databases for assessing IE frequencies and do not require explicit modeling (there is, however, an exception: when a FT is developed to assess a specific IE frequency, then human errors causing IE are modeled).

3. **Type C.** Interactions invoked after the IE occurred, emergency actions, such as backing up of an automatic system or actuating a manual safety system, etc. Type C HIs are explicitly modeled and are included at different levels of PRA (FTs, ETs, etc). This type of HIs can be further developed more in detail as:

   (a) **Cognitive response** Human failure to perform adequate response within the time available can be further expanded as:

   - **Skill-based (S)** Response requires little or no cognitive effort. The response of the operator is fast, more or less automatic, based upon training.
   - **Rule-base (R)** Response is determined by rules. The response of the operator requires his/her checking of the list of rules and procedures, thus the response is slower and tends to have some errors.

- **Knowledge-based (K)** Response requires initiative, problem solving and decision making. Operator must rely on his/her experience and knowledge of the system. This behavior shows most errors.

(b) **Action response** Human failure to perform corrective actions after the correct diagnosis of the accident has been made within the available time.

According to NASA Probabilistic Risk Assesment... (2002a) there exist two basic types of human errors or HI:

1. **Errors of Omission.** The personnel omit the step in the procedure or the entire task.
2. **Errors of Commission.** This type of error can be further divided as:
   (a) Selection error, where personnel select wrong control or malposition it or issue wrong command.
   (b) Errors of sequence.
   (c) Timing errors, where the action is performed too early or too late.
   (d) Qualitative errors, where the action is of undesired size.

Conservative human error probabilities (HEPs) estimates are used in the PRA models to perform initial quantification of HIs. HIs with insignificant impact on the risk are excluded from further analysis. In principle, human basic events or HEPs can be quantified using any probability distribution, however, because of the usual lack of human data, special models have been developed. One of these models is Technique for Human Error Rate Prediction, originally developed for nuclear industry. It enables prediction of the human error probabilities. Human Error Rate Prediction can be characterized as follows:

- HI is represented by HRA event tree (Fig. 3.7) and is used to combine HEPs and action response.

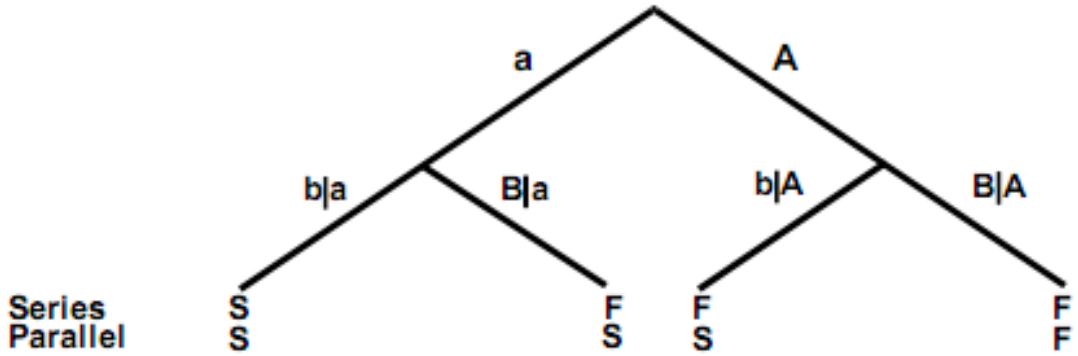


Figure 3.7: HRA Event Tree (NASA Probabilistic Risk Assesment... (2002a))

- For the cognitive response two models have been developed:
  - Alarm Response Model (ARM), where response to alarms after an accident had occurred dominates the cognitive response.
  - Time Reliability Curve (TRC) where the decision-making process is strongly dependent on time and dominates the cognitive response. TRCs are used to quantify HEP associated with the cognitive response of Type C HIs, mathematically described as

$$p(\overline{R}) = p(T_r > T_w) = \int_0^\infty f_{T_w}(t)[1 - F_{T_r}(t)]dt, \tag{3.21}$$

    where $\overline{R}$ stands for non-response in time t, T_r stands for crew response time and T_w represents available time window for a specific HI, $f_{T_w}(t)$ is density function and $F_{T_r}(t)$ is cumulative probability distribution. $[1 - F_{T_r}(t)]$ represents complementary cumulative distribution of crew response time and is called TRC.

- For the action response tasks such as using control buttons, breaker operation outside a control room, emergency operating procedures steps, etc. are used in a task analysis.

For both cognitive and action responses, basic human error probability estimates have been provided (performance shaping factors) must be average/normal e.g. optimum stress, well trained operator, etc.) and are assumed to have lognormal distribution.

In is important to emphasize, that the results of the HRA are the input data for basic events of FTA. It means, that after construction of FT, one has to identify the way of "filling-up" the basic event probabilities and in case, that the basic event is a subject of some human action, or is human-related, the probability for this basic event is oftentimes acquired by HRA.

3.4 Failure Mode, Effects and Criticality Analysis

In addition to FTA, inductive approaches, Failure Mode and Effects Analysis (FMEA) and Failure Mode, Effects and Criticality Analysis (FMECA) (MIL-STD-1629A (1980)), are used in safety analysis and risk and reliability analysis. These are forward-stepping approaches that begin with a basic event and investigate the end effects. The FMECA is, according to MIL-STD-1629A (1980), and MIL-STD-756B (1981), "an essential function in design from concept through development". FMECA has to be used in an iterative manner to correspond with system design. The greatest effectiveness of FMECA is at the earliest stages of the design process, while the biggest weakness of this analysis is its limited use in improvements designs. Even though there has been some attempts to combine several FMECAs to make a fault tree, this should be done under no circumstances. This always produced erroneous model NASA Fault Trees... (2002b).

FMECA was developed by the U.S. Military – introduced by Military Procedure MIL-P-1629 "Procedures for performing a failure mode, effects and criticality analysis" dated November 9, 1949. The objective of the FMECA is to identify all modes (within defined scope) of failure within a system design, however the most important purpose is early identification of all catastrophic and critical failure possibilities. The FMECA identifies these failures (each potential failure is ranked by the severity of the effect), the effects of these failures on the system, and suggests how to mitigate the risk or avoid the failures. Therefore, the FMECA should be employed as soon as possible in the early stages of the design. To summarize previous, according to MIL-STD-1629A (1980) the purpose of the FMECA is "to study results or effects of item failure on system operation and to classify each potential failure according to its severity". The FMECA has the greatest impact on costs, so it should be initiated early in the design process. The locked-in cost[6] versus the total cost of a product is illustrated in Rausand and Høyland (2004) in the Fig. 3.8.

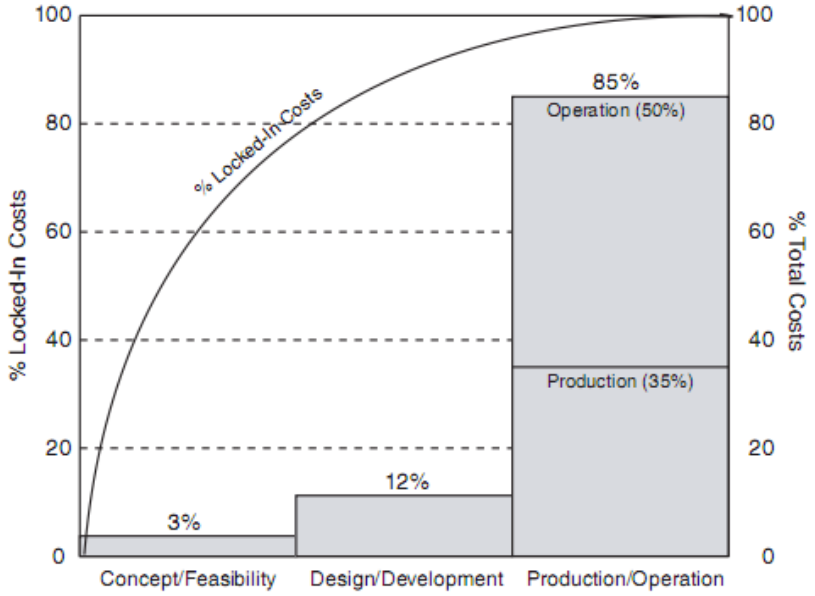


Figure 3.8: Locked-in cost versus total cost

Among others, FMECA can be used for variety of other purposes such as safety analysis, survivability, maintenance plans, etc. It can also provide historical documentation for future reference and basis for quantitative reliability.

Rausand and Høyland (2004) present three types of FMECA:

1. **Design FMECA** should eliminate failures during design. Each identified failure

[6]In economics, vendor/proprietary lock-in create barriers to market entry; or customer lock-in, makes a customer dependent on a vendor for products and services, unable to use another vendor without substantial switching costs. Here it means additional cost of switching the process, technology etc. in the respective phase of the project, i.e. to change something what has already been developed and is in operation is much more expansive (85% of total cost of a product) than switching the procedure e.g. at the phase of development.

mode should be assigned a severity classification to establish priorities for corrective actions

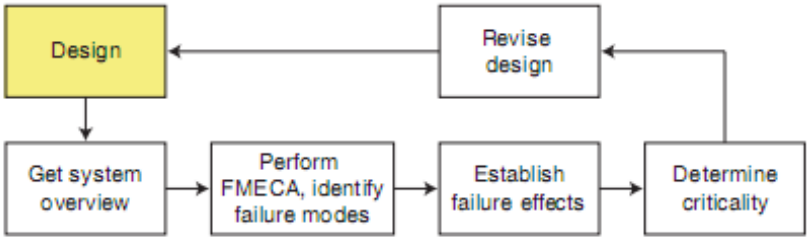


Figure 3.9: FMECA in design

2. **Process FMECA** is aimed at problems related to the manufacturing, operation and maintenance of the equipment

3. **System FMECA** analyses the whole systems and searches for potential failures. It is considered to be combination of previous two

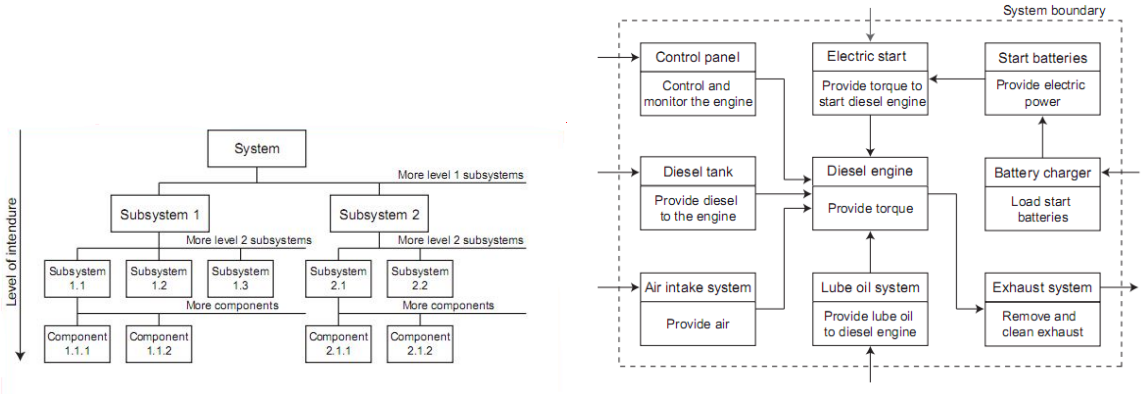
3.4.1 Basic Steps of FMECA Analysis

The basic steps in FMECA analysis as introduced in Rausand and Høyland (2004) and MIL-STD-1629A (1980) are as follows:

1. **FMECA prerequisites**
   System to be analyzed has to have properly defined boundaries, main objective and functions, expected performance, failure definitions as well as the conditions[7] in which the system will operate. All available information that describes system (including plan, drawings, specifications, schemas, functional descriptions etc.) has to be collected. Moreover, information from internal and external sources as well as previous designs, personnel experience should be employed.

2. **System structure analysis**
   System has to be divided into functional elements, units. The scope and resolution are given by the analysis objective. Functional and reliability block diagrams are often constructed to illustrate the interrelationships and interdependencies of functional entities. Alternative modes of operations require separate block diagrams depending upon the definition of the system. Functional decomposition example is depicted in Fig. 3.10(a) and Fig. 3.10(b), respectively. Analysis should be carried out on the highest possible level in the system hierarchy. When it discovers failure (even a potential failure), then the corresponding subsystem has to be analyzed (and further expanded) into greater detail. The analysis started on low level provides on the

[7] Environmental profiles for different environmental conditions should be defined.



(a) Structural decomposition (b) Functional block diagrams

Figure 3.10: Functional decomposition of the system

one hand complete system information, but on the other hand it cost a lot of money, time and resources and is very often useless.

3. **Failure analysis and preparation of FMECA worksheets**
   Worksheet format is not rigidly given and may have many different forms which are oftentimes determined by customer request or management system.
   Analysts must consider all functions of each system element (component, subsystem) as well as all its operational modes and effects of these modes. If there exists an adverse effect, the element has to be examined further in greater detail, otherwise further analyzing is not necessary.

   Fig. 3.11 shows FMECA worksheet with its twelve columns. This is one of the most often used formats of FMECA worksheets. The particular columns have meaning as follows:

   - 1^{st} **column:** Each element is uniquely referenced. A serial number or other reference identification number is assigned for traceability purposes
   - 2^{nd} **column:** Each element's functionalities must be listed – checklist may be used
   - 3^{rd} **column:** Operational modes of each element are listed (running, idle, etc.)
   - 4^{th} **column:** Potential failure modes of each function and operational mode of each element must be listed. Failure mode is defined as a nonfulfillment of the functional requirements of the function in 2^{nd} column. Potential failure mode should be determined by examination of element's outputs. Each failure mode should be examined in relation to the:
     - Failure to operate at a prescribed time
     - Failure to cease operation at a prescribed time
     - Degradation or loss of output

     ⋮

System: Performed by:

Ref. drawing no.: Date: Page: of

Description of unit			Description of failure			Effect of failure		Failure rate	Severity ranking	Risk reducing measures	Comments
Ref. no	Function	Operational mode	Failure mode	Failure cause or mechanism	Detection of failure	On the subsystem	On the system function				
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)

Figure 3.11: FMECA worksheet

- 5^{th} **column:** Failure modes in 4^{th} column are studied and failure mechanisms that can cause or contribute to a failure are identified and listed
- 6^{th} **column:** Possibilities for detection of identified failure modes are listed (diagnostic testing, proof testing...) Some applications require an extra column for the rank of likelihood that the failure will be detected prior to the system delivery to the end-user/customer

Rank	Description
1-2	Very high probability that the defect will be detected. Verification and/or controls will almost certainly detect the existence of a deficiency or defect.
3-4	High probability that the defect will be detected. Verification and/or controls have a good chance of detecting the existence of a deficiency/defect.
5-7	Moderate probability that the defect will be detected. Verification and/or controls are likely to detect the existence of a deficiency or defect.
8-9	Low probability that the defect will be detected. Verification and/or control not likely to detect the existence of a deficiency or defect.
10	Very low (or zero) probability that the defect will be detected. Verification and/or controls will not or cannot detect the existence of a deficiency/defect

Table 3.1: Failure detection likelihood ranks

- 7^{th} **column:** The effects of each failure mode on the other components in the same subsystem are listed (**local** effects and **next higher level** effects). The consequences of each failure mode on other element or function should be identified, evaluated and recorded. Local effects concentrate specifically on the impact a failure mode has on the operation and function of the element in the level under consideration. Next higher level effects concentrate on the impact

a failure has on the operation and function of the elements in the next higher level above the level under consideration

- 8^{th} **column:** The effects of each failure mode on the system are listed (global effects or **end** effect). The consequences of each failure mode on system or system function should be identified, evaluated and recorded. The end effects evaluate and define the total effect a failure has on the operation, function or/and status of the system
- 9^{th} **column:** Failure rates for each failure mode are listed
- 10^{th} **column:** Severity classifications are assigned to provide a qualitative measure of the worst potential effect of the failure considered on the system level. Every failure mode should be assigned to proper severity class. Severity classification provides the basis for establishing corrective action priorities. The severity classes can be introduced as follows:

Category	Rank	Severity Class	Description
I	10	Catastrophic	Failure results in major injury or death of personnel or system loss
II	7-9	Critical	Failure results in minor injury to personnel, personnel exposure to harmful chemicals or radiation, or fire or a release of chemical to the environment
III	4-6	Major	Failure results in a low level of exposure to personnel, or activates facility alarm system. Minor property or system damage, which will result in delay or loss of availability
IV	1-3	Minor (Negligible)	Failure results in minor system damage but does not cause injury to personnel, allow any kind of exposure to operational or service personnel or allow any release of chemicals into the environment

Table 3.2: Severity classes

First priority should be given to the elimination of the Category I and Category II failure modes.

- 11^{th} **column:** List of correcting actions. Action that can reduce the frequency of the failure modes should be also recorded
- 12^{th} **column:** Other information, comments

4. **Risk Ranking and Objective Revision** The risk associated to failure mode is a function of the frequency of the failure mode and the potential end effects (severity) of the failure mode. The risk related to the failure modes can be presented by:

   (a) Risk matrix (Frequency-Consequence matrix), which is composed of two basic components, the Frequency matrix (for example see Table 3.3) and Consequence matrix (for example see Table 3.4). The Frequency matrix expresses how

No.	Frequency category	Yearly frequency
6	very often	>10
5	often	1-10
4	probable	0.1-1
3	moderate	0.01-0.1
2	rare	0.001-0.01
1	very rare	0.0001-0.001
0	extremely rare	<0.0001

Table 3.3: Frequency matrix

	Non-negligible	Marginal	Considerable	Serious	Very serious
Type of consequence	0	1	2	3	4
Employees					
Public					
Environment					

Table 3.4: Consequence matrix

often undesired event of interest occur in both qualitative ("often, rarely, etc.") and quantitative (0.1) way. The Consequence matrix enables also quantitative, as well as qualitative ("serious, negligible") description .

The risk matrix is a combination of risks and consequences. The risk associated to failure mode is a function of the frequency of the failure mode and the potential end effects (severity) of the failure mode. The examples of risk matrices are depicted in Fig. 3.13 and Fig. 3.12(a) and Fig. 3.12(b). ALARP stands for As Low As Reasonably Practicable.

(b) risk priority number (RPN), which can be evaluated as

$$RPN = SOD, \tag{3.22}$$

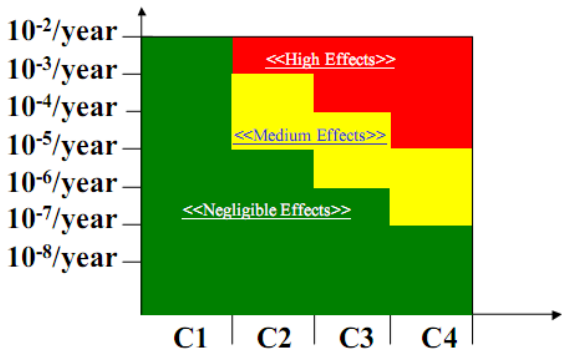
where S stands for the rank of the occurrence of the failure mode, O stands for the rank of the severity of the failure mode and finally D represents the rank of the likelihood the failure will be detected prior to delivery the system to the end-user/customer. The ranks are scaled $1 - 10$. The smaller RPN the better. The RPN is however not rigorously defined and strongly depends on application and the FMECA standard that is used and therefore RPN of different companies may have (and often has) different meaning.

Review of objectives should:

(a) decide whether of not is the system acceptable

(b) identify feasible improvements to reduce the risk (reducing the likelihood of the failure occurrence, reducing the effects of the failure or increasing the likelihood of early failure detection)

Every improvement has to be documented as well as corresponding revisions and updates of FMECA worksheets and RPN.



(a)

Ranking		Consequence				
		Nonexisting/ negligible	Marginal	Considerable	Serious	Very serious
Frequency		0	1	2	3	4
Very often	6	6	7	8	9	10
Often	5	5	6	7	8	9
Moderate	4	4	5	6	7	8
Probable	3	3	4	5	6	7
Rare	2	2	3	4	5	6
Very rare	1	1	2	3	4	5
Extremely rare	0	0	1	2	3	4

(b)

Figure 3.12: Risk matrices

Frequency/ consequence	1 Very unlikely	2 Remote	3 Occasional	4 Probable	5 Frequent
Catastrophic					
Critical					
Major					
Minor					

Acceptable - only ALARP actions considered

Acceptable - use ALARP principle and consider further investigations

Not acceptable - risk reducing measures required

Figure 3.13: Risk priority matrix

5. **Corrective Actions**
   Decision changes, safety devices, procedure and/or training may significantly reduce the risk. The risk can be significantly reduced and the failures and failure effects can be reduced or nullified by either design provisions (redundant elements, safety or relief devices, alternative modes of operation) or operator actions.

The results of the FMECA should be documented in a report that clearly identifies the level of analysis, documents the data sources and techniques and includes analysis results. The used ground rules, assumptions, block and functional diagrams should be also added. Report should also highlight the Category I and Category II (according to the Table 3.2) failure modes – the potential single failure modes. These single failure points should be listed separately. Summary of the report should provide conclusions and recommendations based upon the analysis.

The FMECA comprises of three main phases as follows (Kmenta (2002)):

Phase	Question	Output
Identify	What can go wrong?	Failure descriptions Causes → Failure modes → Effects
Analyze	How likely is a failure?	Failure rates
	What are the consequences?	RPN
Act	What can be done?	Design solutions
	How can be the causes eliminated?	Test plans
	How can be the severity reduced?	Error proofing

Table 3.5: FMECA main phases

For better understanding of the complexness of FMEA/FMECA analysis a simplified analysis of a SOS phone box is shown in Fig. 3.14.

3.4.2 FMECA in Short

One can see, that these are very similar to Continuous Risk Management from Chapter 1. FMECA is one of the most beneficial and used risk analysis. Individual failure modes are listed in an organized and evaluated manner, thus enabling verification of system integrity, identification of possible pitfalls and quantification of the risk. It is important to remind, that each single element failure is to be considered as the only failure in the system. If single element failure detection is impossible, the analysis should be extended to the effects of a second failure, which in combination with first undetectable failure could possibly lead do Catastrophic of Critical failure modes. Finally, the pros and cons of FMECA are summarized as follows:

Advantages

- Structured and reliable method for evaluating system
- Easy to learn the concept and applications
- Evaluation of system is easy to do

Disdvantages

- The process of FMECA can be time and money consuming
- Not suitable for multiple failures
- Tend to forget and omit human error

It is obvious, that FMECA/FMECA and the concept of Continuous Risk Management described in Chapter 1 have a common base and many similarities. The more detail comparison is performed in Table 3.6.

No.	Description of unit			Description of failure			Effect of failure		Risk reducing measures	Comments
	Unit	Function	Operational mode	Failure mode	Failure cause or mechanism	Detection of failure	On the subsystem	On the system function		
1	**Activation switch**	Activate the phone	Active	The lever does not switch on	Mechanical failure - dirt	N/A	Phone does not work	Operator is not informed	Frequent checks, robust design	
2				The switch does not close circuit	Electrical failure - corrosion	N/A	Phone does not work	Operator is not informed	Frequent checks, switch for aggressive environment	
3			Passive	False connection	Wear-off, false switch	Operator	N/A	False alarm	Frequent checks	
4	**Microphone**	Connect to operator	Active	Microphone not working	Corrosion	Operator: phone active, no signal	Person in tunnel thinks phone not working	No interaction operator-person in tunnel	Frequent checks, corrosion-resistant technology	
5				Poor quality signal	Distorsion	Noisy signal	Poor connection	False information for the operator	Install sound barrier	
6					Corrosion				Frequent checks, corrosion-resistant technology	
7					Interference				Follow EM compatibility rules	
8	**Speaker**	Connect to person in tunnel	Active	Speaker not working	Corrosion	Operator: no interaction from the tunnel	Person in tunnel thinks phone not working	No interaction operator-person in tunnel	Frequent checks, corrosion-resistant technology	Operator can still give information to the tunnel with help of other safety devices
9				Poor quality signal	Distorsion	Noisy signal	Poor connection	False information for the person in tunnel	Install sound barrier	
10					Corrosion				Frequent checks, corrosion-resistant technology	
11					Interference				Follow EM compatibility rules	
12	**Connection line**	Connect phone to operator centre	Active	Connection interrupted	Mechanical failure	Result of other accident	Phone does not work	Operator is not informed	Communication line redundancy, wireless technology	
13					Communication failure	Watch-dog system	Phone does not work	Operator is not informed	Use separate circuits, robust industrial networks	
14					Communication interference	Noisy signal	Poor connection	Operator is not informed	Follow EM compatibility rules, use optical network, filters	
15					Network failure	Software detection	Poor or connection	Operator is not informed	Implement emergency communication protocol, use separate circuits	
16			Passive	False alarm	Communication failure	Watch-dog system	N/A	Watch-dog triggers false alarm	Happens sooner or later - coordination with other devices	
17	**Interface to operator**	Connect the phone to the operator	Active	No connection	Bad addressing	CRC check	Phone not connected	Operator is not informed	Handshake communication, redial	
18				Connection to wrong phone	Wrong dial	No interaction with the tunnel	Phone not connected	Operator is not informed	Redial, software measures	

Figure 3.14: FMEA example

FMEA/FMECA	Continuous Risk Management
Systems structure analysis; the system is divided into fundamental elements.	Identification of the risks
Failure analysis (function, description of the failure, effect of the failure, etc.)	Risk analysis; risk data are transformed into decision making information; impact, probability and time frame is calculated for each risk.
Risk ranking, risk assessing, prioritizing and planning of the corrective actions.	Planning of the Track an Control actions to mitigate the risk
Corrective actions and risk reevaluation.	Tracking of the risk indicators and comparing the actual and planned performances.
Reviews and updates of the analysis.	Control of the process and correction of the deviations from the mitigation plans.
The most of the FMEA/FMECA steps are directly filled into the FMEA/FMECA forms.	Each of the previous steps is documented.

Table 3.6: FMEA/FMECA and Continuous Risk Management

Chapter 4

Case Study – Strahov Tunnel

Directives of European Union require new Technical Documentation every ten years. Because Strahov tunnel was required to have new Technical Documentation as of 2009, Technická správa komunikací Praha asked Satra s.r.o. to elaborate new Technical Documentation for Strahov Tunel. Risk analysis is an integral part of Technical Documentation that was supposed to be made by Feramat Cybernetics, s.r.o. In the state of the art, Strahov tunnel has several safety problems with both aged and missing equipment that is about to be replaced (or newly installed). Among others e.g. new video recognition system for transportation of dangerous goods (which is usually strictly prohibited in city tunnel as it is in Strahov tunnel), new longitudinal fans with sufficient performance capable to cope with fire up to 30 MW, "soft stop[1]", and other equipment which is supposed to eliminate the danger of the accident (fire especially), or when occur, to suppress it in a sufficient manner, providing enough time for escape. The analysis provides not only the risk levels incurred by the current safety measures, but also evaluates the contribution of new elements in the tunnel. The analysis also enables prioritizing of the safety measures with respect to the risk reduction and the cost which is great advantage considering the price of some tunnel equipment (millions of crowns).

4.1 Basic Characteristics

Strahov tunnel is bidirectional tunnel (see Fig. 4.1) opened after long (12 years) and difficult process of building and applying the control system. The actual capacity of a tunnel tube is $43,000$ vehicles per day (transportation of dangerous goods is prohibited). It is part of the Prague City Ring which includes also tunnels Mrazovka and Blanka (under construction). Actual length of Strahov tunnel is 2 km; the length of Western Tube (WT) is 1997 m, the length of Middle Tube (MT) is 1990 m with two portals at Malovanka and Mrazovka. Daily average number of vehicles in WT is 32000 and 25200 in MT, 4 % of heavy vehicle included. The tunnel of Strahov contains 8 emergency exits with fireproof doors (fire resistance 90 minutes, overpressure 1 kPa), gas proof walls, and one special "open" emergency exit ("the wall hole"), which causes serious ventilation problems. The emergency exits in WT are $73 - 422$ m away from each other and $98 - 403$ m in MT. Cur-

[1] By means of the soft stop it should be possible to stop drive-in to the tunnel in case of accident (surprisingly many drivers either ignore the regular stop signal and red lights, or they do not see them).

rently there is no longitudinal ventilation system in the Strahov tunnel, but it is about to be installed. There are 25 SOS boxes in the Strahov tunnel placed 54–226 m from each other. The tunnel is powered by 22 kV distribution network of PRE, a.s., and a emergency power supply – two pieces of 220 V, 330 Ah batteries. The Strahov tunnel has its own video surveillance system composed of two separate parts. The first circle is connected to the automatic traffic congestion recognition (63 recording devices). The second video circle is independent on the first and serves for the operators supervising the tunnel. The tunnel is outfitted with fire detection signalization device, Linear Heat Detection system, which serves for the fire detection. The Czech and international authorities are requesting the proper quantitative analysis of the tunnel in order to classify the tunnel into a specific risk class. Because the equipment in the tunnel is quite old, there is a great effort to outfit the tunnel with new safety devices. In order to perform this effectively from both risk reducing and cost effective point of view, a proper analysis had to be performed.

4.2 Probabilistic Risk Assessment

The goal of the analysis is to evaluate current state of the safety of the Strahov tunnel. Several options of safety solutions will be proposed based upon this analysis providing both quantitative (risk analysis) and cost support. The final table will be composed of the respective variants, its risk probabilities and cost of equipment and will serve as a basic decision making and support tool in the process of outfitting the Strahov tunnel. Due to the large result differences of the variety of analysis devoted to human behavior, it was decided, that only contribution of "technical part" of the tunnel will be taken into an account and analysed and therefore the analysis of evacuation and human behavior during the accident was omitted.

The risk analysis for the Strahov tunnel makes use of event tree (ET) and fault tree analyses (FT) (Chapter 3). The whole tunnel (analysis) was divided into a three separate sections:

- **Fire and Smoke Detection** section (FSD)
- **Fire and Smoke Control: tube Affected by fire** (FSCA)
- **Smoke Control: Escape Tube** (SCET)

One can see the scheme expressed as event tree scheme in Fig. 4.2.

A fire is the most serious and problematic threat to any tunnel without any further discussion. Therefore, a fire was chosen as an initial event (IE). Fire occurs in tunnel with some probability (given by variety factors) and has different consequences on tunnel users and tunnel itself depending on incredible broad variety of causes such as tunnel equipment, tunnel users behavior, tunnel operator reactions and the proper reaction and subsequent actions of the rescue services. However, the probability of the occurrence of the fire is enormously low, and the statistical data are insufficient. Many studies (PIARC – Integrated Approach to Road Tunnel Safety (2007) and PIARC – Risk Analysis for Road Tunnels (2008)) have been provided, but neither one had solved the issue of the fire in the sufficient manner. According to the statistical data, there was only one fire of insignificant

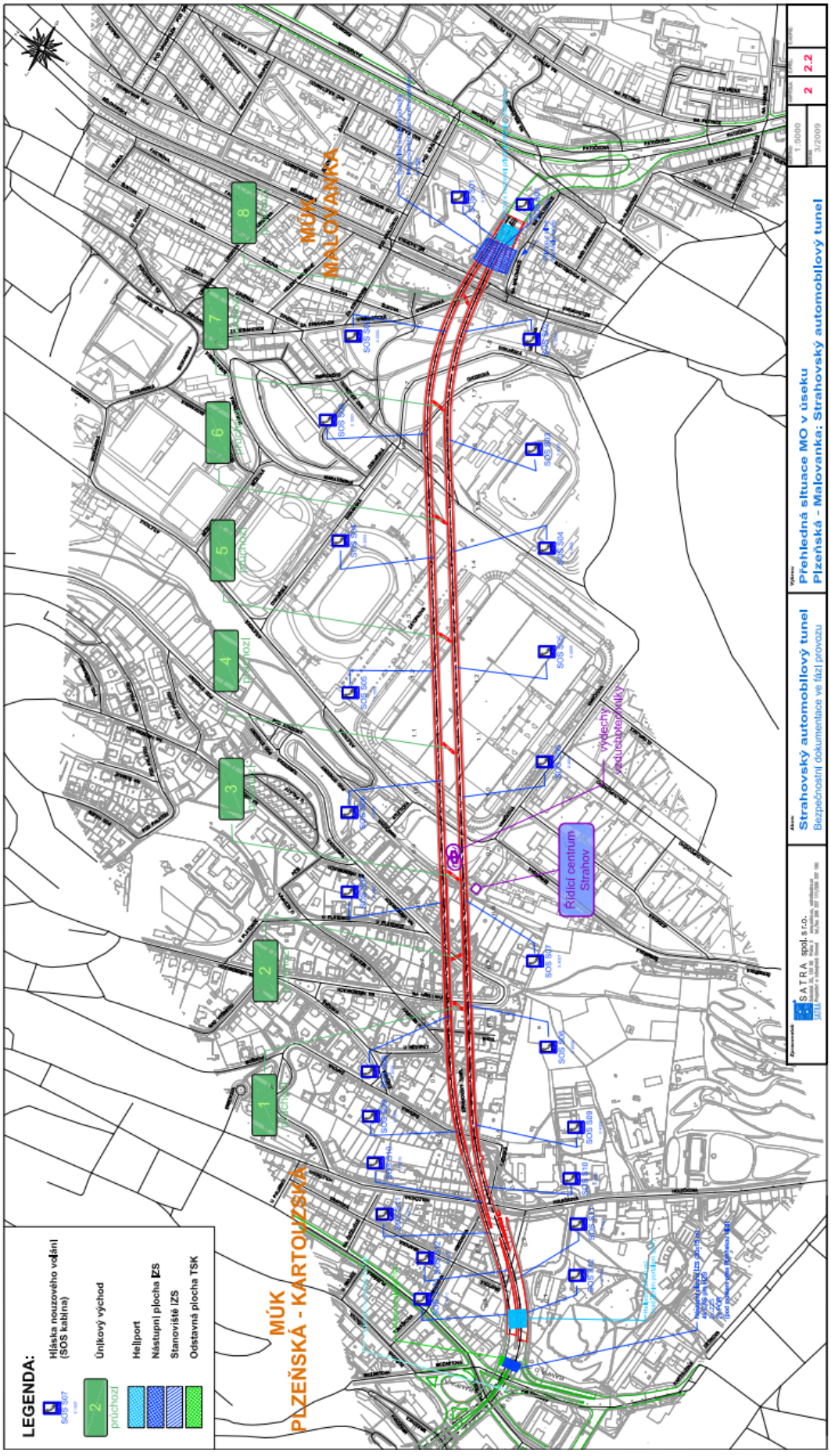


Figure 4.1: Blueprint of the Strahov tunnel

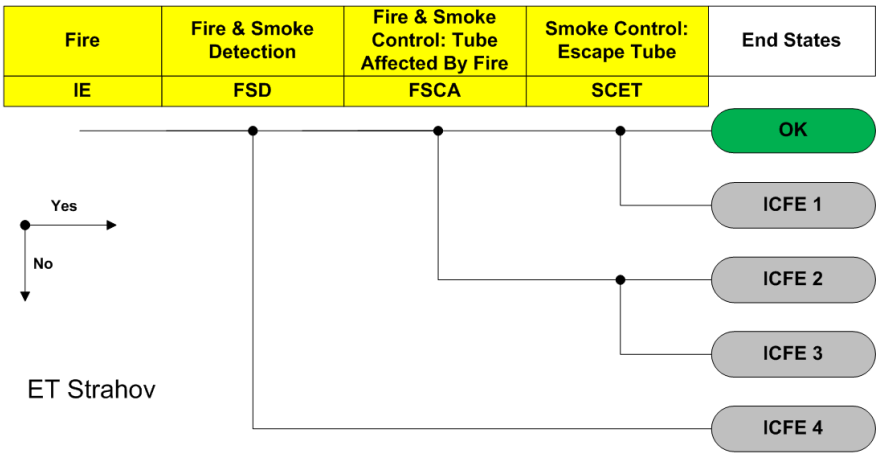


Figure 4.2: Event tree of Strahov tunnel

importance, since the Strahov tunnel had been opened! There were no casualties, nor injuries, and the driver was able to extinguish the fire itself. Therefore, the whole analysis will be done without the initial event "fire" i.e. the whole analysis will be a comparison of the variety of the safety measures and precautions.

The second event in the event sequence (Fig. 4.2) is Fire and Smoke Detection (FSD). The corresponding FT (Fig. 4.3) was developed for FSD that provides the probability contribution of the FSD to the overall probability in the event sequence. The similar logic holds for the consequent events in the event sequence, FSCA and SCET, respectively. The FTs are constructed in a such a way, that they comply with everything what was said in Chapter 3, Section 3.2.

One can see (Fig. 4.2), that the event sequences can end up to 5 different states depending on the combinations "en route". The horizontal direction (Fig. 4.2) means, that the corresponding subsystem reacted correctly (e.g. FSD detected and properly identified fire) whilst the vertical directions means, that the subsystem failed to fulfill its task. The "matrix" of various "yes" and "no" directions represents the options of the scenario development in the tunnel. For the purposes of Strahov tunnel, only state "OK[2]" is in interest. All other states mean, that the lives of people will be somehow endangered.

The meaning of the respective events in FSD, FSCA and SCET are explained in Table 4.1, Table 4.2, Table 4.3, respectively.

The structure of the tunnel risks depicted in Fig. 4.3, Fig. 4.4, and Fig. 4.5 had to be constructed with the help of many people who are experts in respective areas. One of the greatest problem however, (and one probably can say that this holds for every tunnel) is data. Data for basic events of the respective fault trees had to be exploited from several sources. Thereafter the minimal cut sets were computed as was introduced in Chapter 3 followed by the calculation of an overall probability of "tunnel failure". The results in-

[2]State OK means, that fire was properly and in time detected, the control system had correctly reacted in less than 10 minutes in the case of personal vehicle accident or in less than 7 minutes in the case of heavy goods vehicle.

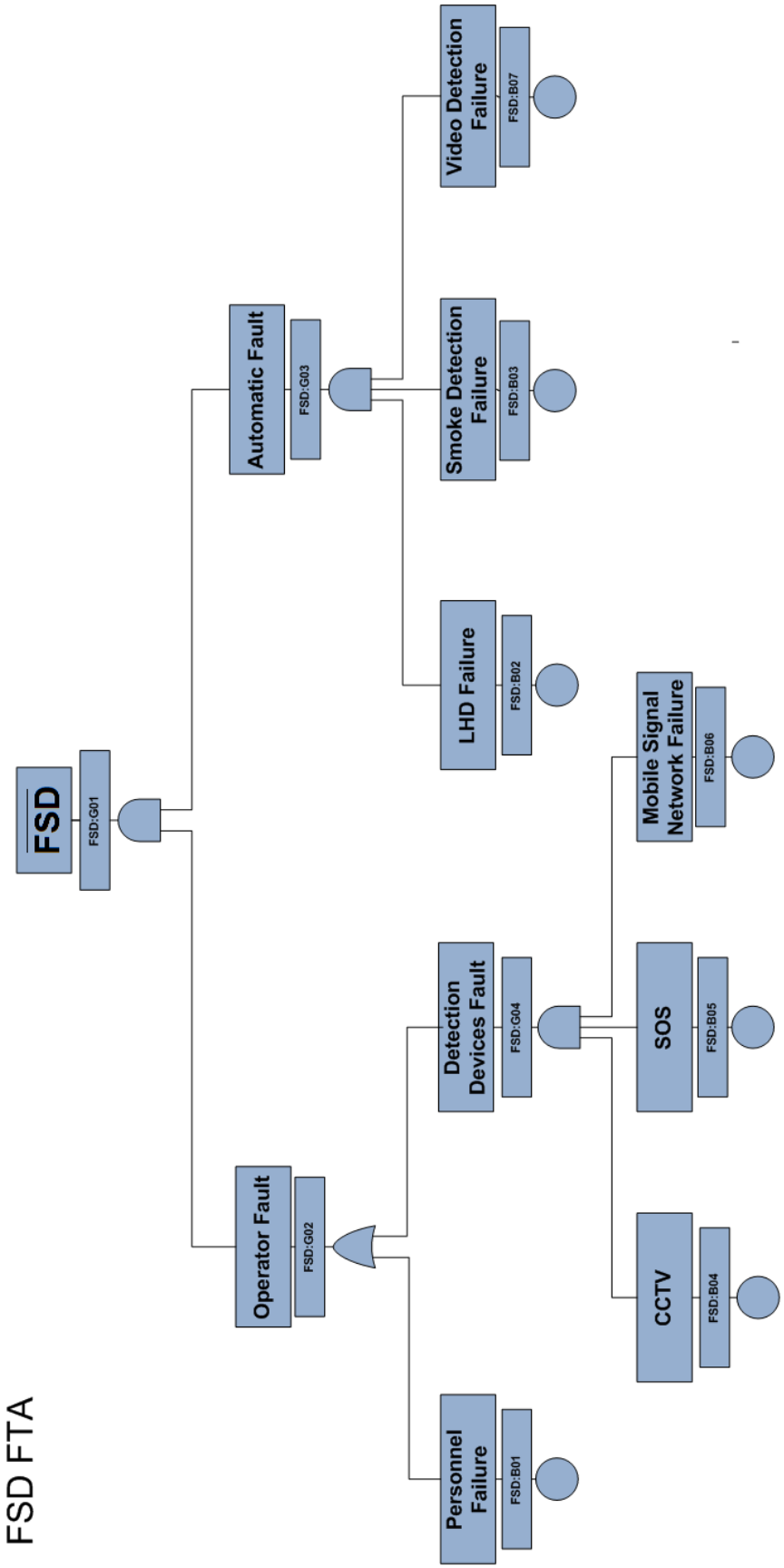


Figure 4.3: FSD Fault Tree

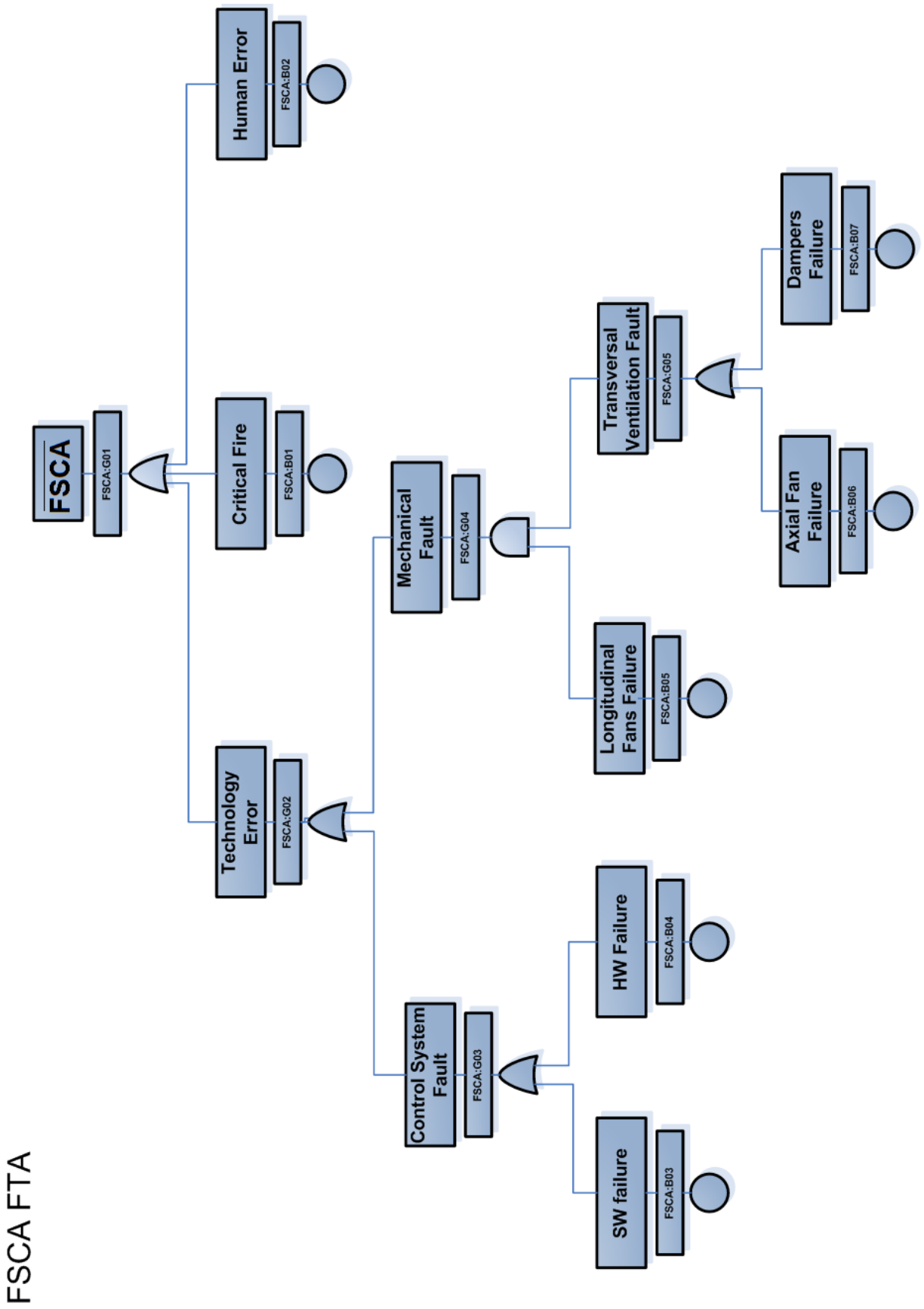


Figure 4.4: FSCA Fault Tree

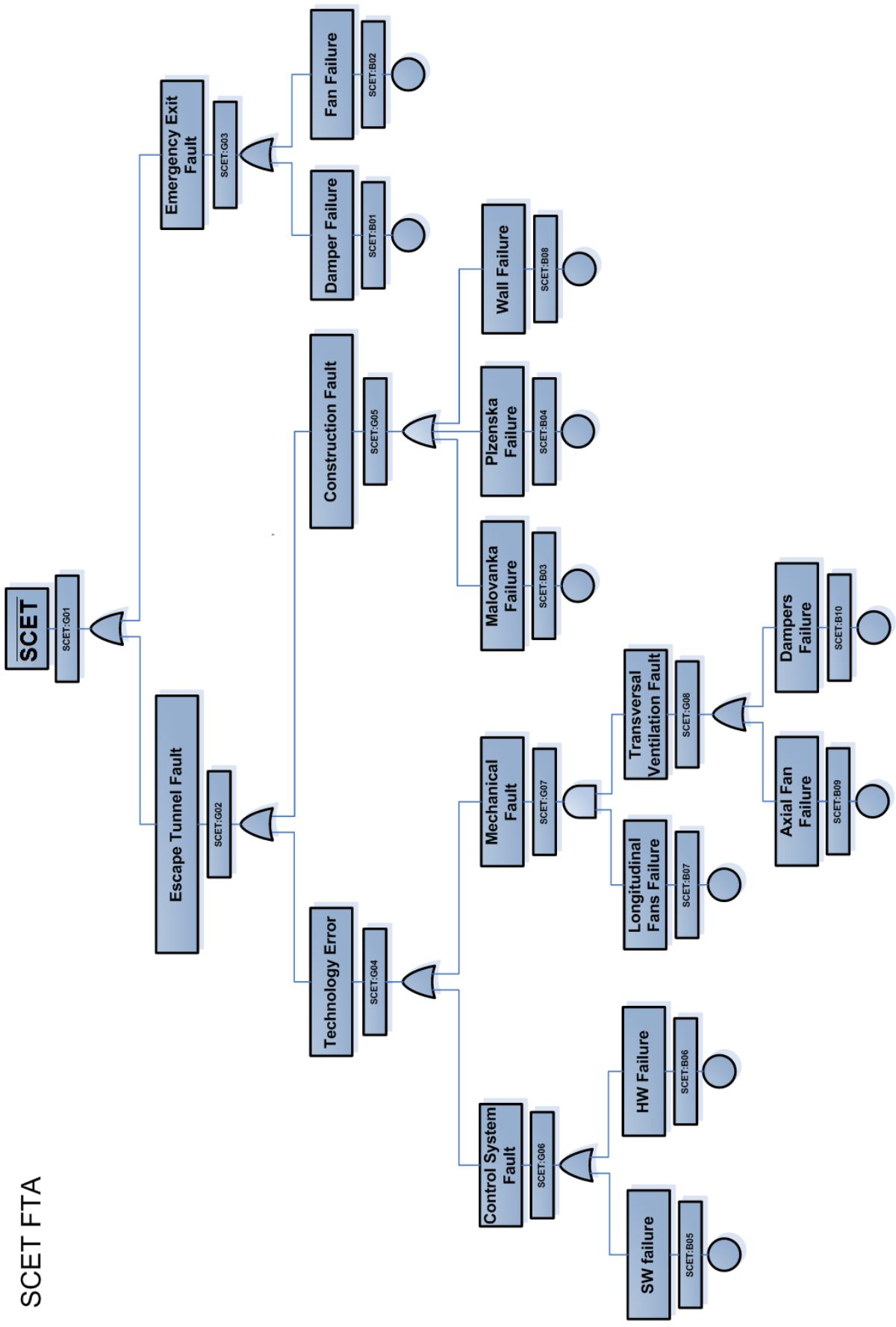


Figure 4.5: SCET Fault Tree

Code	Name	Description
FSD:G01	non FSD	Top event, FSD did not correctly and in time detected and identified the fire and propagation of smoke
FSD:G02	Operator Fault	Personal fault of the operator – improper reaction or proper reaction not in time
FSD:G03	Automatic Fault	Fault of automatic detection equipment
FSD:G04	Detection Devices Fault	Fault of "other" safety equipment
FSD:B01	Personnel Failure	Improper human reaction
FSD:B02	LHD Failure	Linear heat detection sensor failure
FSD:B03	Smoke Detection Failure	Smoke sensitive sensors failure
FSD:B04	CCTV	Failure of the CCTV
FSD:B05	SOS	SOS box is not working
FSD:B06	Mobile Signal Network Failure	There is no network signal in the tunnel
FSD:B07	Video Detection	Video detection failure

Table 4.1: Events of FSD Fault Tree

Code	Name	Description
FSCA:G01	non FSCA	Top event, the fire and smoke have not developed in affected tube thanks to safety measures
FSCA:G02	Technology Error	Variety of technological equipment failed to control and suppress smoke propagation
FSCA:G03	Control System Fault	Control system failed to properly launch fans
FSCA:G04	Mechanical Fault	Mechanical fault of fans
FSCA:G05	Transversal Ventilation Fault	Mechanical failure of transversal fan or/and dampers
FSCA:B01	Critical Fire	Fire with performance over 30MW. This performance can not be treated with ventilation system installed currently or planned to install
FSCA:B02	Human Error	Operator failed to launch the fire sequence properly and in time
FSCA:B03	SW Failure	SW failure of control system
FSCA:B04	HW Failure	HW failure of control system
FSCA:B05	Longitudinal Fans Failure	Mechanical failure of longitudinal fan
FSCA:B06	Axial Fans Failure	Mechanical failure of axial fans
FSCA:B07	Dampers Failure	Mechanical failure of dampers

Table 4.2: Events of FSCA Fault Tree

Code	Name	Description
SCET:G01	non SCET	Top event, smoke reached escape tunnel due to failure of safety measures and inadvertent operation condtitions
SCET:G02	Escape tunnel Fault	Smoke in the escape tunnel due to technical or tunnel construction failures
SCET:G03	Emergency Exit Fault	Smoke in the emergency exit due to failure of damper or fan
SCET:G04	Technology Error	Failure of technology or improper construction cause smoke in the escape tunnel
SCET:G05	Construction Fault	Improper construction at the portals or inside the tunnel (there is a huge passage "whole" between tubes that can cause smoke propagation from affected tube into escape tube)
SCET:G06	Control System Fault	Control system failed to properly launch fans
SCET:G07	Mechanical Fault	Mechanical fault of fans
SCET:G09	Transversal Ventilation Fault	Mechanical failure of transversal fan or/and dampers
SCET:B01	Damper Failure	Damper is unusable in the emergency exit
SCET:B02	Fan Failure	Emergency exit fan failed to operate properly
SCET:B03	Malovanka Failure	see Construction Fault
SCET:B04	Plzenska Failure	see Construction Fault
SCET:B05	SW Failure	SW failure of control system
SCET:B06	HW Failure	HW failure of control system
SCET:B07	Longitudinal Fans Failure	Mechanical failure of longitudinal fan
SCET:B08	Wall Failure	see Construction Fault
SCET:B09	Axial Fan Failure	Mechanical failure of axial fans
SCET:B10	Dampers Failure	Mechanical failure of dampers

Table 4.3: Events of SCET Fault Tree

Results of PRA analysis for Strahov Tunnel

probabilities: human error = 0.1 and HW failure= 0.1

		Smokde detection	Longitudinal Ventilation	Faster fans	Dampers	Dampers-emergency exits	Fans-emregency exits	Malovanka-wall	Plzenska-wall	SW	Wall in the tunnel	Cost
1	0.6089	1	1	1	1	1	1	1	1	1	1	99,000,000.00 Kč
2	0.6082	0	1	1	1	1	1	1	1	1	1	94,000,000.00 Kč
3	0.6059	1	1	0	1	1	1	1	1	1	1	94,000,000.00 Kč
4	0.6053	0	1	0	1	1	1	1	1	1	1	89,000,000.00 Kč
5	0.5843	1	1	1	1	1	1	1	0	1	1	99,000,000.00 Kč
6	0.5837	0	1	1	1	1	1	1	0	1	1	94,000,000.00 Kč
7	0.5814	1	1	0	1	1	1	1	0	1	1	94,000,000.00 Kč
8	0.5808	0	1	0	1	1	1	1	0	1	1	89,000,000.00 Kč
9	0.5541	1	1	1	1	1	1	1	1	1	0	89,000,000.00 Kč
10	0.5535	1	1	1	1	1	1	0	1	1	1	89,000,000.00 Kč
11	0.5535	0	1	1	1	1	1	1	1	1	0	84,000,000.00 Kč
12	0.5533	1	1	1	0	1	1	1	1	1	1	49,000,000.00 Kč
13	0.5533	1	1	0	0	1	1	1	1	1	1	44,000,000.00 Kč
14	0.553	0	1	1	1	1	1	0	1	1	1	84,000,000.00 Kč
15	0.5528	0	1	1	0	1	1	1	1	1	1	44,000,000.00 Kč
16	0.5528	0	1	0	0	1	1	1	1	1	1	39,000,000.00 Kč
17	0.5514	1	1	0	1	1	1	1	1	1	0	84,000,000.00 Kč
18	0.5508	1	1	0	1	1	1	0	1	1	1	84,000,000.00 Kč
19	0.5508	0	1	0	1	1	1	1	1	1	0	79,000,000.00 Kč
20	0.5502	0	1	0	1	1	1	0	1	1	1	79,000,000.00 Kč
21	0.5317	1	1	1	1	1	1	1	0	1	0	89,000,000.00 Kč
22	0.5314	1	0	1	1	1	1	1	1	1	1	89,000,000.00 Kč
23	0.5312	1	1	1	1	1	1	0	0	1	1	89,000,000.00 Kč
24	0.5311	0	1	1	1	1	1	1	0	1	0	84,000,000.00 Kč
25	0.531	1	1	1	0	1	1	1	0	1	1	49,000,000.00 Kč
26	0.531	1	1	0	0	1	1	1	0	1	1	44,000,000.00 Kč
27	0.5309	0	0	1	1	1	1	1	1	1	1	84,000,000.00 Kč
28	0.5306	0	1	1	1	1	1	0	0	1	1	84,000,000.00 Kč
29	0.5304	0	1	1	0	1	1	1	0	1	1	44,000,000.00 Kč
30	0.5304	0	1	0	0	1	1	1	0	1	1	39,000,000.00 Kč
31	0.5291	1	1	0	1	1	1	1	0	1	0	84,000,000.00 Kč
32	0.5285	1	1	0	1	1	1	0	0	1	1	84,000,000.00 Kč
33	0.5285	0	1	0	1	1	1	1	0	1	0	79,000,000.00 Kč
34	0.528	0	1	0	1	1	1	0	0	1	1	79,000,000.00 Kč
35	0.5099	1	0	1	1	1	1	1	0	1	1	89,000,000.00 Kč
36	0.5094	0	0	1	1	1	1	1	0	1	1	84,000,000.00 Kč
37	0.5037	1	1	1	1	1	1	0	1	1	0	79,000,000.00 Kč
38	0.5035	1	1	1	0	1	1	1	1	1	0	39,000,000.00 Kč
39	0.5035	1	1	0	0	1	1	1	1	1	0	34,000,000.00 Kč
40	0.5032	0	1	1	1	1	1	0	1	1	0	74,000,000.00 Kč
41	0.503	1	1	1	0	1	1	0	1	1	1	39,000,000.00 Kč
42	0.503	1	1	0	0	1	1	0	1	1	1	34,000,000.00 Kč
43	0.503	0	1	1	0	1	1	1	1	1	0	34,000,000.00 Kč
44	0.503	0	1	0	0	1	1	1	1	1	0	29,000,000.00 Kč
45	0.5025	0	1	1	0	1	1	0	1	1	1	34,000,000.00 Kč
46	0.5025	0	1	0	0	1	1	0	1	1	1	29,000,000.00 Kč
47	0.5012	1	1	0	1	1	1	0	1	1	0	74,000,000.00 Kč
48	0.5007	0	1	0	1	1	1	0	1	1	0	69,000,000.00 Kč
49	0.4836	1	0	1	1	1	1	1	1	1	0	79,000,000.00 Kč
50	0.4834	1	1	1	1	1	1	0	0	1	0	79,000,000.00 Kč

Figure 4.6: Numerical results of PRA analysis including cost analysis with probability of human error 0.1 an probability of HW failure 0.1

Results of PRA analysis for Strahov Tunnel

probabilities: human error = 0.7 and HW failure= 0.5

		Smokde detection	Longitudinal Ventilation	Faster fans	Dampers	Dampers-emergency exits	Fans-emregency exits	Malovanka-wall	Plzenska-wall	SW	Wall in the tunnel	Cost
1	0.0626	1	1	1	1	1	1	1	1	1	1	99,000,000.00 Kč
2	0.0623	1	1	0	1	1	1	1	1	1	1	94,000,000.00 Kč
3	0.0622	0	1	1	1	1	1	1	1	1	1	94,000,000.00 Kč
4	0.0619	0	1	0	1	1	1	1	1	1	1	89,000,000.00 Kč
5	0.0601	1	1	1	1	1	1	1	0	1	1	99,000,000.00 Kč
6	0.0598	1	1	0	1	1	1	1	0	1	1	94,000,000.00 Kč
7	0.0597	0	1	1	1	1	1	1	0	1	1	94,000,000.00 Kč
8	0.0594	0	1	0	1	1	1	1	0	1	1	89,000,000.00 Kč
9	0.057	1	1	1	1	1	1	1	1	1	0	89,000,000.00 Kč
10	0.0569	1	1	1	1	1	1	0	1	1	1	89,000,000.00 Kč
11	0.0569	1	1	1	0	1	1	1	1	1	1	49,000,000.00 Kč
12	0.0569	1	1	0	0	1	1	1	1	1	1	44,000,000.00 Kč
13	0.0567	1	1	0	1	1	1	1	1	1	0	84,000,000.00 Kč
14	0.0567	1	1	0	1	1	1	0	1	1	1	84,000,000.00 Kč
15	0.0566	0	1	1	1	1	1	1	1	1	0	84,000,000.00 Kč
16	0.0565	0	1	1	1	1	1	0	1	1	1	84,000,000.00 Kč
17	0.0565	0	1	1	0	1	1	1	1	1	1	44,000,000.00 Kč
18	0.0565	0	1	0	0	1	1	1	1	1	1	39,000,000.00 Kč
19	0.0563	0	1	0	1	1	1	1	1	1	0	79,000,000.00 Kč
20	0.0563	0	1	0	1	1	1	0	1	1	1	79,000,000.00 Kč
21	0.0547	1	1	1	1	1	1	1	0	1	0	89,000,000.00 Kč
22	0.0547	1	0	1	1	1	1	1	1	1	1	89,000,000.00 Kč
23	0.0546	1	1	1	1	1	1	0	0	1	1	89,000,000.00 Kč
24	0.0546	1	1	1	0	1	1	1	0	1	1	49,000,000.00 Kč
25	0.0546	1	1	0	0	1	1	1	0	1	1	44,000,000.00 Kč
26	0.0544	1	1	0	1	1	1	1	0	1	0	84,000,000.00 Kč
27	0.0544	1	1	0	1	1	1	0	0	1	1	84,000,000.00 Kč
28	0.0543	0	1	1	1	1	1	1	0	1	0	84,000,000.00 Kč
29	0.0543	0	0	1	1	1	1	1	1	1	1	84,000,000.00 Kč
30	0.0543	0	1	1	1	1	1	0	0	1	1	84,000,000.00 Kč
31	0.0542	0	1	1	0	1	1	1	0	1	1	44,000,000.00 Kč
32	0.0542	0	1	0	0	1	1	1	0	1	1	39,000,000.00 Kč
33	0.0541	0	1	0	1	1	1	1	0	1	0	79,000,000.00 Kč
34	0.054	0	1	0	1	1	1	0	0	1	1	79,000,000.00 Kč
35	0.0525	1	0	1	1	1	1	1	0	1	1	89,000,000.00 Kč
36	0.0521	0	0	1	1	1	1	1	0	1	1	84,000,000.00 Kč
37	0.0518	1	1	1	1	1	1	0	1	1	0	79,000,000.00 Kč
38	0.0518	1	1	1	0	1	1	1	1	1	0	39,000,000.00 Kč
39	0.0518	1	1	0	0	1	1	1	1	1	0	34,000,000.00 Kč
40	0.0517	1	1	1	0	1	1	0	1	1	1	39,000,000.00 Kč
41	0.0517	1	1	0	0	1	1	0	1	1	1	34,000,000.00 Kč
42	0.0516	1	1	0	1	1	1	0	1	1	0	74,000,000.00 Kč
43	0.0515	0	1	1	1	1	1	0	1	1	0	74,000,000.00 Kč
44	0.0514	0	1	1	0	1	1	1	1	1	0	34,000,000.00 Kč
45	0.0514	0	1	0	0	1	1	1	1	1	0	29,000,000.00 Kč
46	0.0514	0	1	1	0	1	1	0	1	1	1	34,000,000.00 Kč
47	0.0514	0	1	0	0	1	1	0	1	1	1	29,000,000.00 Kč
48	0.0512	0	1	0	1	1	1	0	1	1	0	69,000,000.00 Kč
49	0.0497	1	0	1	1	1	1	1	1	1	0	79,000,000.00 Kč
50	0.0497	1	1	1	1	1	1	0	0	1	0	79,000,000.00 Kč

Figure 4.7: Numerical results of PRA analysis including cost analysis with probability of human error 0.7 an probability of HW failure 0.5

cluding the costs are depicted in Fig. 4.6, Fig. 4.6 and in Appendix E in Fig. E.1- Fig. E.6. The first column shows an order of scenarios, second column provides the probability, then 10 columns with occurrence/nonoccurrence of respective equipment follow (each zero means, that the safety measure is not applied, each one means, that the safety item was taken into an account) and the cost of the respective solution is provided in the last column. The results show various possibilities of human and HW fault because these two according to the performed analysis contribute in a greatest manner to the overall probability. In Fig. 4.6 one can see, that the overall probability is quite "good" if the new equipment (especially new HW complying the EU norms) was provided and the staff properly trained. These results are in sharp contrast with Fig. 4.7. This figure reflects the current situation, when according to the analysis, every bigger accident that occurs in the tunnel means a major problem.

One can see (Fig. 4.6, Fig. 4.7) one of the main advantages of the performed style of risk analysis, when it enables the cost comparison of the results, e.g. by inspection in Fig. 4.6 items 11, 12, 13 have almost identical or identical probability, but the cost of the measurement is completely different.

4.2.1 Safety Precautions Proposal

Based upon the risk analysis of the current state of the Strahov tunnel, several safety precautions had been proposed:

- **Smoke Detection Device.** The device is currently not installed (formally: the probability of failure is 1). The smoke detection is inevitable to successfully identify and localize the initiating fire and therefore the smoke detectors will be installed close to dampers (next to the axial fans). The newly installed detectors have probability of failure lower than 0.01 and the estimated cost is 5 million Kc.

- **Longitudinal Ventilation.** The longitudinal fans are currently not installed, but they are key part of successful management of the smoke and fire, thus enable the safe evacuation of people. There will be installed four longitudinal fans at the each and of the tube (16 altogether). This precaution cost 10 million Kc and the probability of failure is lower than 0.02.

- **Power Supply for the Axial Fans.** The current system of power supply is slow (3 minutes, probability of failure 0.1) due to the fact, that the axial fans start up is in star-triangle configuration. This configuration causing slow start up should be replaced by frequency converters that enable faster start up (less than 1.5 minutes) and have a lower probability of failure (0.05). The cost is estimated to 5 million Kc.

- **Dampers.** Current dampers are not an integral part of the control system, i.e. they have their own logic of start – thermal fuse cut-outs (75 °C). It has already been proved, that the current system of start up is completely unreliable and unsuitable with probability of failure close to 1. Therefore there will be installed 48 new dampers into the tunnel with surface of 10 m^2. This, however, requires also some construction works and the tunnel roof will not stay intact. The new system of dampers (probability of failure less than 0.02) should be a part of control system. The new damper system is one of the most expensive solutions for the tunnel with estimated cost of 50 million Kc.

- **Dampers and Fans in the Emergency Exits.** Current Dampers and fans in the emergency exits do not have sufficient performance in order to maintain the pressure in emergency exits and therefore have probability of failure close to 1. There should be installed new high-performance dampers and fans (approximate cost 0.5 million Kc) with probability of failure less than 0.01.

- **Malovanka Portal.** In the case of accident in Western Tube (WT) there should be no smoke in the Middle Tube (MT) due to the fact, that both natural and forced air flow in the MT is in the outward direction. The problem is likely to occur when there is an accident in MT, because it takes $4-6$ minutes to change the direction of the air flow. Therefore the most critical fire could occur in the upper part of the MT (the speed of smoke development is about 3 m/s, thus it takes about $4-6$ minutes). This negative effect can be fought by building-up the wall at the Malovanka portal which would disable the smoke penetration into the other tube. The probability of smoke penetration after this construction adjustment (approximate cost is 10 million Kc) is less than 0.01.

- **Plzenska Portal.** In the state of the art, there is partially built wall at the Plzenska portal with probability of failure 0.05. Because there is almost no space left for the construction work described above, in the near future, there will be no adjustments to the Plzenska portal.

- **Tunnel Wall.** There is an open space, "the hole" inside of the tunnel that enables the free passage from one tube to another. It was built with intention of traffic control for the case of existence of three tubes, however, there is no useful usage of it in the state of art. In contrary, it poses serious threat to the tunnel safety, because it enables smoke penetration between the tubes, thus disables effective evacuation in the case of accident. Because of these reasons, "the hole" should be walled-up thus lowering the probability of failure form current 0.09 to 0 (according to unpublished CFD fire simulations performed by Satra, s.r.o.)with an approximate cost of 10 million Kc.

- **Software.** The current software (SW) has been never tested (hardware-in-the-loop), nor it passed the exams of Fire Department. Even though there was only one minor fire in the existence of Strahov tunnel, the control system software did not work correctly. Therefore it is considered highly unreliable with approximate probability of failure more than 0.9. The proposed solution includes thorough testing, hardware-in-the-loop tests, etc. and the goal probability of failure under 0.05 with approximate cost of the solution estimated to 8 million Kc.

- **Staff.** The tunnel operators are not trained on regular basis, the do not have any simulator training or model situations training. It is therefore inevitable to introduce training procedures on regular basis.

It is certainly proper to mention a fact, that the whole scheme used for Fault Tree Analysis can be rearranged and redrafted as a Petri Nets. They provide certain mathematical advantages such as easy algebraic computations of some properties (e.g. Minimal Cut Sets, etc.). Some of the schemes are redrawn as Petri nets and shown in Appendix D.

Chapter 5

Incorporating Aviation Experience into Tunnel RA Methods

5.1 Aviation as an "Inspiration"

Incorporating aviation experience into tunnel RA methods does not mean that all the tunneling experience must be forgotten. The RA methods used in both aviation and tunneling are quite similar, only the aviation has about 80 years longer experience and tunneling may well profit from it.

As an example of an "inspiration", we can show a link between the Fault Trees, as presented in this document, and Event Trees, as presented e.g. in RVS 09.03.11 (2008).

The failures of events of the Event Tree (called pivotal events) are used as top events of the respective Fault Trees. It is not necessary to develop a FT for every pivotal event. If applicable probabilistic data are available from similar systems or testing, these data can be assigned directly to the pivotal events without further modeling.

The combination of Fault Trees and Event Trees has many advantages over their separate use, for example:

- The ET is easier to construct than the FT, so it is advantageous to use it as a first estimate of the risk model
- The ET simplifies the search for the top event of a FT
- The FT enables easy incorporation of probability uncertainties
- The FT brings deeper knowledge about the risk dependencies, including the Minimal Cut Sets
- The ET-FT (with the corresponding Minimal Cut Sets) linking provides a straightforward method for defining and simulating risk scenarios, including accident progression

5.2 Comments on PIARC documents

If one compares the PIARC documents PIARC – Integrated Approach to Road Tunnel Safety (2007) and PIARC – Risk Analysis for Road Tunnels (2008) with the FAA and NASA resources and methods, one can see the differences and possible improvements to PIARC methods as follows.

- **Life Cycle of Tunnel** There is no exact definition of Life Cycle of tunnels and its stages in PIARC documents in contrast to the aircraft industry (for example FAA System Safety Handbook (2000)), where the Life Cycle of the project is well defined (as illustrated in Figure 1.2 therein). The PIARC documents comprise of the description of a "Safety Circle", which is analogous to the CRM circle (FAA System Safety Handbook, chapter 1.3 and Figure 1.3), but there is no exact description of the relationship between the Safety Circle and the Risk Management of a tunnel. According to the FAA System Safety Handbook, the Life Cycle should also include the final stage – System abandonment, which is not considered in PIARC documents, but presents some hazards and risks as well.

  A detailed description of the Life Cycle, along with suitable methods for hazard identification, evaluation and risk mitigation, could decrease the expenses for risk management, as identification and control of hazards and risks in early stages of a project (with respect to the later stages) is more cost-effective than in the later stages.

- **Interactions** Figure 1 of the PIARC – Integrated Approach to Road Tunnel Safety shows the major contributors to tunnel safety, which is similar to a "5M Model" of the FAA System Safety Handbook. However, the PIARC document does not solve the interactions between the respective risk contributors, which also present significant hazards.

- **Hazard analysis** There is little attention paid to the identification and evaluation of hazards and risks in the PIARC documents, whereas this issue represents a significant part of the NASA and FAA documents. The PIARC documents use terms such as severity and probability of events/scenarios, but there is an important difference between an event/scenario and a hazard.

- **Other comments to PIARC documents** Main emphasis of PIARC projects is fire safety of tunnels, but from statistics we can see, that most fatalities in tunnels result from accidents which do not involve fire. This is a frequently discussed issue and we think that the problem may be that we are not aware of documents that address accidents not involving fires.

Chapter 6

Conclusions

The purpose of this document was to show possibilities of expanding traditional approach to risk analysis in tunnels of methods taken from industries with a long and successful tradition. Moreover it should point at the fact, that the main focus in tunneling is put on Risk **Analysis** methods, not on Risk **Management**. This makes a big difference.

The RA methods in tunneling of the state of the art are in fact the Event Trees (e.g. RVS 09.03.11 (2008)) or Parts Count (e.g. SafeT project). If not incorporated into a Risk Management system, these methods cannot be fully exploited and their application becomes more expensive. If a RA method is incorporated into a Risk Management system and properly focused on the decision making process (as illustrated in Fig. 1.1), it may reveal more results which can help reducing the risks and optimizing the safety costs. Furthermore, if more accurate methods are used for subsystems or scenarios that are particularly important or expensive, further savings can be made while avoiding excessive expenditures on safety systems. In general, economic aspects of safety is a very sensitive issue ("we must do everything to reduce risks"), but it should not be fully neglected. Moreover, some of the new or refurbished tunnels already suffer from the phenomenon of excessive safety, which means that the risks of the failure of the safety system actually outweigh the risks they should mitigate (see Day, 2008).

There are several risk management handbooks in aviation industry which describe general principles of risk management and analysis methods (e.g. MIL-STD-882D (2000), FAA System Safety Handbook (2000) or NASA Probabilistic Risk Assesment... (2002a)) which could be advantageously used as a basis for a similar handbook that would be available for tunnel experts. It should be noted that these documents are very easy to read, yet they are of high scientific value. Moreover, they are available on the Internet for free.

The thesis tried to show the extent of the Risk Management and especially Risk Analyses. From the practical standpoint the risk analysis of Strahov tunnel was performed and successfully applied and is part of the Technical Documentation of Strahov Tunnel. One can clearly see the big advantages of mathematically based recommendations (both economical and safety) to outfitting the tunnel with new equipment.

Bibliography

FAA System Safety Handbook. Federal Aviation Administration, Washington, DC, December 2000.

Bouissou Charlotte, Ruffin Emmanuel, Defert Raphaël, and Dannin Eric Prats Franck. *A new QRA Model for rail transportation of Hazardous Goods*. Institut National de l'Environnement Industriel et des Risques (INERIS), Parc Technologique Alata, F-60550 Verneuil-en-Halatte, FRANCE, 2008.

John R. Day. The hazards of trying to improve the safety of tunnels. In *Proceedings of the 4th Conference 'Tunnel Safety and Ventilation'*, pages 234–240, Graz, 2008.

MIL-STD-1629A: Procedures for Performing a Failure Mode, Effects and Criticality Analysis. Department of Defence of the U.S.A., Washington, DC, November 1980.

MIL-STD-756B: Reliability Modeling and Prediction. Department of Defence of the U.S.A., Washington, DC, November 1981.

MIL-STD-882D: Standard Practice for System Safety. Department of Defence of the U.S.A., Washington, DC, February 2000.

Homayoon Dezfuli, Robert Youngblood, and Joshua Reinert. Managing risk within a decision analysis framework. In *Proceedings of the Second IAASS Conference*, Chicago, May 2007.

Steven Kmenta. Scenario-based fmea (using expected cost). In *IIE Workshop 'A New Perspection on Evaluating Risk in FMEA'*, 2002.

Risk Management Procedural Requirements. NASA, Office of Safety and Mission Assurance, Washington, DC, April 2002. NASA Procedural Requirements NPR 8000.4.

RVS 09.03.11: Tunnel-Risikoanalysemodell. Österreichische Forschungsgesellschaft Strasse — Schiene -– Verkehr, Wien, 2008.

Integrated Approach to Road Tunnel Safety. PIARC, La Defense, 2007.

Risk Analysis for Road Tunnels. PIARC, La Defense, 2008.

Marvin Rausand and Arnold Høyland. *System Reliability Theory, Models, Statistical Methods, and Applications*. John Wiley & Sons, Inc, Hoboken, NJ, USA, 2004.

Michael Stamatelatos, George Apostolakis, Homayoon Dezfuli, Chester Everline, Sergio Guarro, Parviz Moieni, Ali Mosleh, Todd Paulos, and Robert Youngblood. *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*. NASA Office of Safety and Mission Assurance, Washington, DC, August 2002a. Version 1.1.

Michael Stamatelatos, William Vesely, Joanne Dugan, Joseph Fragola, Joseph Minarick, and Jan Railsback. *Fault Tree Handbook with Aerospace Applications*. NASA Office of Safety and Mission Assurance, Washington, DC, August 2002b. Version 1.1.

Jelle Vlaanderen, Roel Vermeulen, Dick Heederik, and Hans Kromhout. *Guidelines to Evaluate Human Observational Studies for Quantitative Risk Assessment*. Utrecht University, Institute for Risk Assessment Sciences, Division Environmental Epidemiology, Utrecht, the Netherlands, 2008.

Appendix A

Probabilistic and Statistical Analysis

A.1 Failure Distributions

A.1.1 Distribution Functions

1. **Probability Mass Function (PMF)** of the discrete random variable is defined as

$$p(X = x_i) = p_i \tag{A.1}$$

and normalization condition as

$$F(x) = \sum_i p_i = 1 \tag{A.2}$$

2. **Probability Density Function (PDF)** of the continuous random variable is defined as

$$f(x) = \frac{dF(x)}{dx} \tag{A.3}$$

and

$$\int_{-\infty}^{\infty} f(x)dx = 1 \tag{A.4}$$

must hold.

3. **Cumulative Distribution Function (CDF)** of random variable X (both continuous and discrete) is defined as

$$F(x) = p(X \leq x) \tag{A.5}$$

and has properties as follows:

- $\lim_{x \to -\infty} F(x) = 0$
- $\lim_{x \to +\infty} F(x) = 1$
- F is nondecreasing function of x
- $F(x) = \int_{-\infty}^{x} f(k)dk$

A.1.2 Moments

1. **Mean, average**

$$E[x] = \mu_x = \begin{cases} \int_{-\infty}^{\infty} x f(x) dx & \text{continuous random variable} \\ \sum_i x_i p_i & \text{discrete random variable} \end{cases} \tag{A.6}$$

2. **Variance**

$$E[(x-\mu_x)^2] = \sigma^2 = \begin{cases} \int_{-\infty}^{\infty} (x-\mu_x)^2 f(x) dx & \text{continuous random variable} \\ \sum_i (x_i - \mu_p)^2 p_i & \text{discrete random variable} \end{cases} \tag{A.7}$$

3. **Coefficient of variation**

$$cov = \frac{\sigma}{\mu} \tag{A.8}$$

4. **Mode** has a little different meaning for continuous and discrete random variable. For CRV the mode is such x for which $f(x)$ has a maximum, whilst for DRV is mode such x for which p_i is the largest.

5. **Median** is such x_m for which $F(x_m) = 0.5$.

A.1.3 Basic Distributions

1. **Binomial**

$$F(k; n, q) = p(X \leq k) = \sum_{i=0}^{k} \binom{n}{i} q^i (1-q)^{n-i}, \tag{A.9}$$

where q is a probability of a failure, n is a number of trials, k is the number of failures and $p(X \leq k)$ is a probability of k failures in n trials. The moments of the binomial distribution are

$$\begin{aligned} \mu &= qn \\ \sigma^2 &= nq(1-q) \end{aligned} \tag{A.10}$$

and Eq. (A.9) must satisfy Eq. (A.2).

2. **Exponential**

$$F(t, \lambda) = \begin{cases} 1 - e^{-\lambda t} & \text{for } t > 0 \\ 0 \end{cases} \tag{A.11}$$

3. **Lognormal PDF**

$$f(x; \mu, \sigma) = \frac{1}{x\sigma\sqrt{2\pi}} e^{-\frac{(\ln(x)-\mu)^2}{2\sigma^2}} \tag{A.12}$$

4. **Weibull**

$$F = \begin{cases} 1 - e^{-(\lambda t)^b} & \text{for } t > 0 \\ 0 \end{cases} \tag{A.13}$$

where $b > 0$ and $\lambda > 0$

5. **Poisson** which is used frequently for the computation of the Initial event probability.

$$p(k) = e^{-\lambda t} \frac{(\lambda t)^k}{k!}, \tag{A.14}$$

where λ is the frequency of the events k. The moments of the binomial distribution are

$$\begin{aligned} \mu &= \lambda t \\ \sigma^2 &= \lambda t \end{aligned} \tag{A.15}$$

A.1.4 Failure Nomenclature and Definitions

1. **Failure Distribution and Failure Density** $F(t)$ and $f(t)$[1]

2. **Reliability**

$$R(t) = 1 - F(t) \tag{A.16}$$

3. **Mean Time to Failure**

$$T_{mean} = \int_0^\infty R(t)dt \tag{A.17}$$

4. **Failure Rate**

$$\lambda t = \frac{f(t)}{R(t)}, \tag{A.18}$$

where λ is an conditional probability of failure in $(t, t + dt)$ under assumption that the component has survived up to t.

A.2 Bayesian Approach

The classical interpretation of probability is based upon a limit of relative frequencies, where an experiment is repeated many times and the number of occurrences of some phenomenon is observed. Let say, that n is the number of repetitions of an experiment, k is the number of occurrence of the phenomenon A, than the probability of A is defined as

$$p(A) = \lim_{n \to \infty} \frac{k}{n}. \tag{A.19}$$

The other interpretation of the probability is the Bayesian approach, where the number of repetitions of the experiments is not inevitable. Probability is interpreted as a measure of degree of belief Stamatelatos et al. (2002a) where the probability is just an numerical

[1] $f(t)$ expresses the probability that a failure occurs between t and dt

expression of that belief. This belief is called prior probability, which is then, updated with newly coming information (oftentimes called likelihood) and the result is posterior probability; and mathematically as

$$\underbrace{p(A|B)}_{posterior} = \frac{p(A,B)}{p(B)} = \frac{p(B|A)p(A)}{p(B)} = \frac{\overbrace{p(B|A)}^{likelihood}\overbrace{p(A)}^{prior}}{\underbrace{\int p(B|A)p(A)dA}_{normalization}} \tag{A.20}$$

or

$$p(A|B) = \frac{p(B|A)p(A)}{\sum p(B|A)p(A)} \tag{A.21}$$

for the discrete case.

Appendix B

Risk Analysis Methods

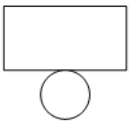
Method	Description
Cause and Consequence	CCA is used for determination of relevant event scenarios by linking Fault Tree and Event Tree analyzes, where failures that can lead to a critical event are analyzed by FTA and consequences are analyzed by ETA
Checklist	Simple qualitative method containing list of tasks/questions to check. It can be use for regular checking of processes. Thanks to the low complexity it takes a big advantage in simpler structures or well defined system with constrained failure possibilities. For more complex system the method becomes cumbersome and uses as supportive tool
Double failure matrix	Is an inductive method that is similar to FMEA/FMECA, but is able to work with the effect of double failures. The faults are categorized into several severity classes and system effects
Event Tree analysis	Initial event is defined and all consequent events are identified and analyzed. The method is a graphical method that depicts possible events of the system that can result in failure/harm. The events can be quantified and several analyzed performed (consequence analysis, frequency analysis, etc.). The main disadvantage is unclarity for the large trees

Expert judgment	Estimation of several experts from the respective field that can be of quantitative and/or qualitative kind. Experts can asses frequency, consequences and risk values, evaluate safety measures etc. The main disadvantage is that the method strongly depends on personal judgment, experience and knowledge of individual and is feasible only for low complex system
Fault hazard analysis	This method is suitable for the project conducted by many organizations where the cross organizational interface problems are to be identified. This analyzes is very similar to FMEA/FMECA although there are some differences
Fault Tree analysis	The method is described in Chapter 3 in detail
Preliminary hazard analysis	Method for assessment of potential hazard on personnel and other humans. PHA should be carried out in the earliest stages of the product development to eliminate costly changes in design. PHA identifies all possible hazards, identify those events, that can potentially transform hazards into accidents and finally the potential accidents are evaluated to provide basis for decision making whether or not correcting measures should be taken
Reliability block diagram	The subsystems/elements of the system are represented by the blocks. The RBD are used to represent active components of the system, where the dependencies in the system can be explicitly addressed. The blocks are then combined as system-success pathways
Safety review	The system is analyzed and tested to identify possible weak points. The goal of the analysis is to identify and fix weak points, to improve the current system. It is often used as a first overview of potential problems requiring small effort
Simulation	All safety devices/measures can fail with certain probability which is tested by modeling and simulating of some process for several times. Using statistical language the probability density function is substituted with sufficient amount of the samples (result of the simulations). The method is extremely precise when repeating sufficient simulations, but enormously costly

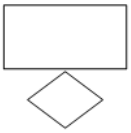
Statistical data	Requires satisfactory amount of data to perform analysis of distribution and deviations. The method is excellent for well-established method with sufficient data, where the results of the analysis can be used for risk reduction. The result from this quantitative analysis have to be interpreted considering the conditions of data acquiring
What if method	Low complex team method where answers for possible scenarios are looked for. It can be used for identification and analysis of hazards, finding simple correlations, etc. The strongest as well as the weakest point of this method is composition of the decision making team

Appendix C

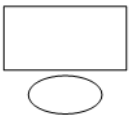
Symbols Used in Fault Tree Analysis



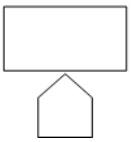
Basic Event: Basic initiating Fault, often HW failure



Undeveloped Event: Event without further development because of the lack of data



Conditioning Event: Used with PRIORITY AND and INHIBIT gates



House Event: An event expected to occur

AND gate: Output fault occurs if all input faults occur

OR gate: Output fault occurs if at least on of the input faults occurs

PRIORITY AND gate: Output fault occurs if all of the input faults occur in a specific sequence -CONDITIONING EVENT

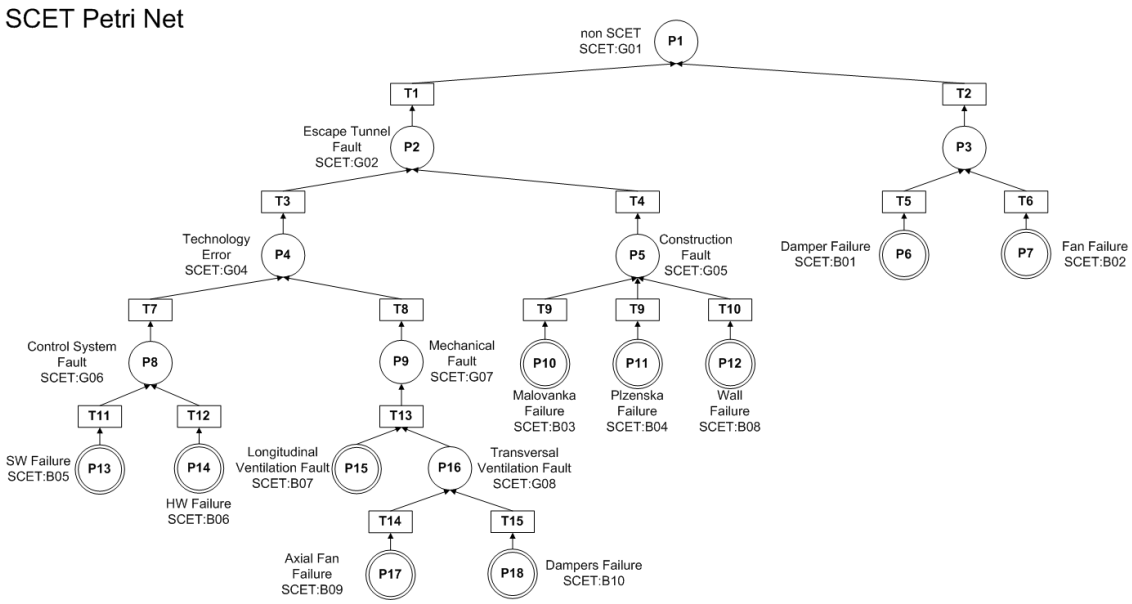
XOR gate: Output fault occurs if exactly one of the input faults occur

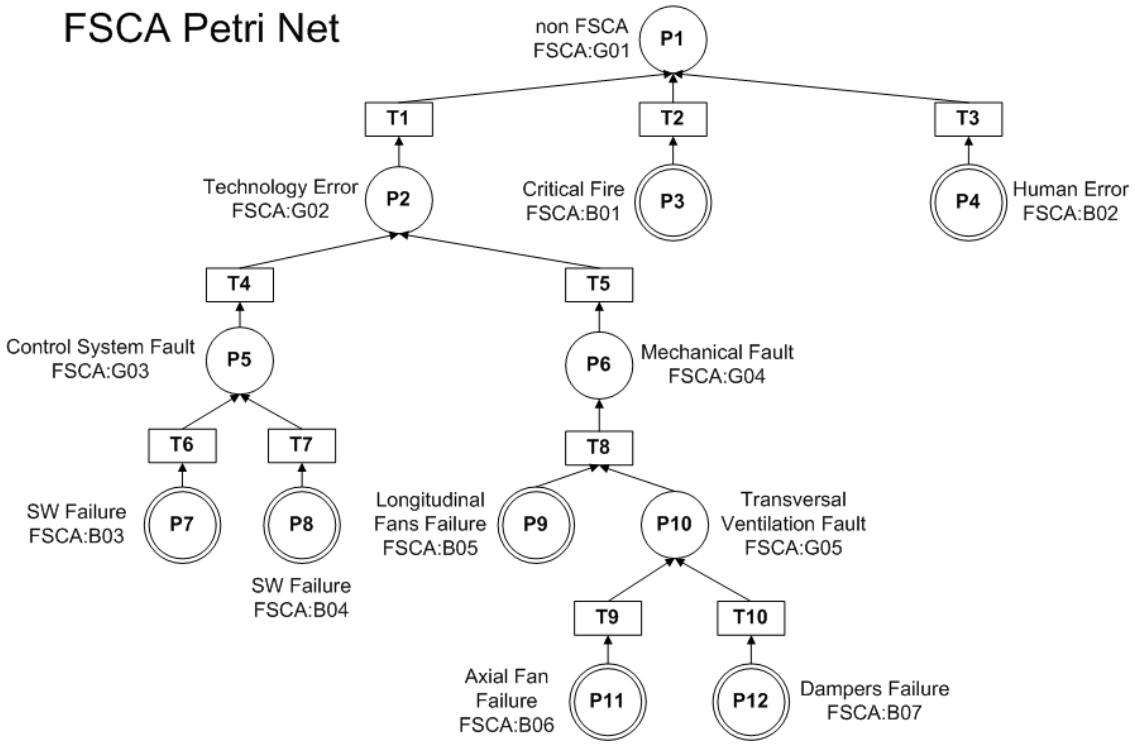
INHIBIT gate: Output fault occurs if single input fault occurs in the presence of an enabling condition-CONDITIONING EVENT

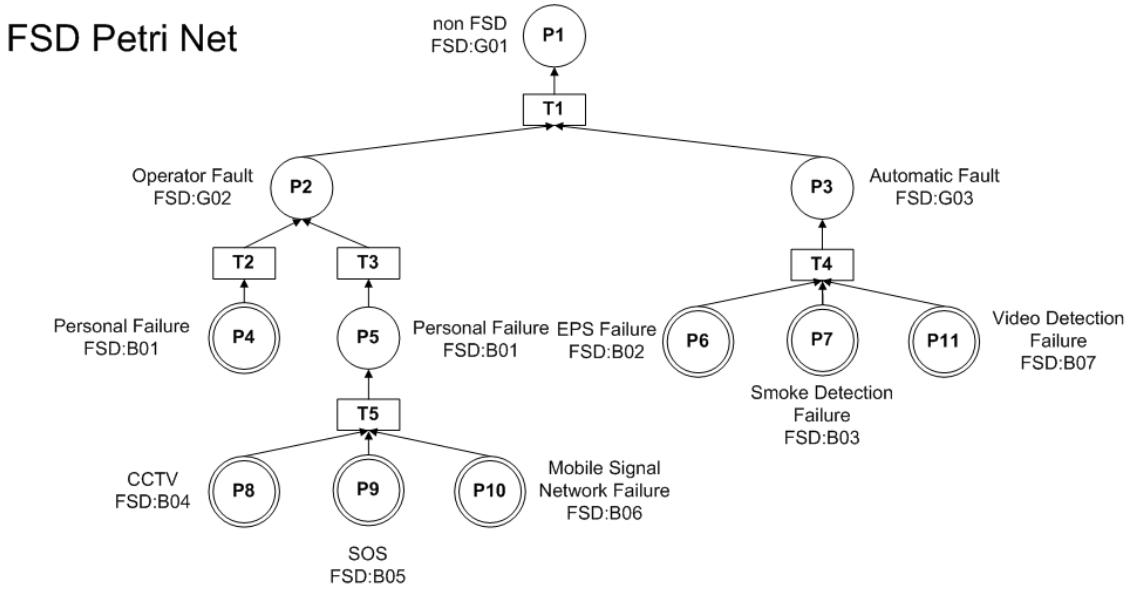
TRANSFER symbol: Indicates further development of the tree

Appendix D

Fault Tree Schemes as Petri Nets




FSCA Petri Net
non FSCA
FSCA:G01
P1
T1
T2
T3
Technology Error
FSCA:G02
P2
Critical Fire
FSCA:B01
P3
P4
Human Error
FSCA:B02
T4
T5
Control System Fault
FSCA:G03
P5
P6
Mechanical Fault
FSCA:G04
T6
T7
T8
SW Failure
FSCA:B03
P7
P8
SW Failure
FSCA:B04
Longitudinal
Fans Failure
FSCA:B05
P9
P10
Transversal
Ventilation Fault
FSCA:G05
T9
T10
Axial Fan
Failure
FSCA:B06
P11
P12
Dampers Failure
FSCA:B07


FSD Petri Net
non FSD
FSD:G01
P1
T1
Operator Fault
FSD:G02
P2
P3
Automatic Fault
FSD:G03
T2
T3
T4
Personal Failure
FSD:B01
P4
P5
Personal Failure
FSD:B01
EPS Failure
FSD:B02
P6
P7
P11
Video Detection
Failure
FSD:B07
Smoke Detection
Failure
FSD:B03
T5
CCTV
FSD:B04
P8
P9
P10
Mobile Signal
Network Failure
FSD:B06
SOS
FSD:B05

Appendix E

Numerical Results of PRA Analysis Including Cost Analysis with Various Probability of Human and HW Faults

Results of PRA analysis for Strahov Tunnel

probabilities: human error = 0.1 and HW failure= 0.1

		Smokde detection	Longitudinal Ventilation	Faster fans	Dampers	Dampers-emergency exits	Fans-emregency exits	Malovanka-wall	Plzenska-wall	SW	Wall in the tunnel	Cost
1	0.6089	1	1	1	1	1	1	1	1	1	1	99,000,000.00 Kč
2	0.6082	0	1	1	1	1	1	1	1	1	1	94,000,000.00 Kč
3	0.6059	1	1	0	1	1	1	1	1	1	1	94,000,000.00 Kč
4	0.6053	0	1	0	1	1	1	1	1	1	1	89,000,000.00 Kč
5	0.5843	1	1	1	1	1	1	1	0	1	1	99,000,000.00 Kč
6	0.5837	0	1	1	1	1	1	1	0	1	1	94,000,000.00 Kč
7	0.5814	1	1	0	1	1	1	1	0	1	1	94,000,000.00 Kč
8	0.5808	0	1	0	1	1	1	1	0	1	1	89,000,000.00 Kč
9	0.5541	1	1	1	1	1	1	1	1	1	0	89,000,000.00 Kč
10	0.5535	1	1	1	1	1	1	0	1	1	1	89,000,000.00 Kč
11	0.5535	0	1	1	1	1	1	1	1	1	0	84,000,000.00 Kč
12	0.5533	1	1	1	0	1	1	1	1	1	1	49,000,000.00 Kč
13	0.5533	1	1	0	0	1	1	1	1	1	1	44,000,000.00 Kč
14	0.553	0	1	1	1	1	1	0	1	1	1	84,000,000.00 Kč
15	0.5528	0	1	1	0	1	1	1	1	1	1	44,000,000.00 Kč
16	0.5528	0	1	0	0	1	1	1	1	1	1	39,000,000.00 Kč
17	0.5514	1	1	0	1	1	1	1	1	1	0	84,000,000.00 Kč
18	0.5508	1	1	0	1	1	1	0	1	1	1	84,000,000.00 Kč
19	0.5508	0	1	0	1	1	1	1	1	1	0	79,000,000.00 Kč
20	0.5502	0	1	0	1	1	1	0	1	1	1	79,000,000.00 Kč
21	0.5317	1	1	1	1	1	1	1	0	1	0	89,000,000.00 Kč
22	0.5314	1	0	1	1	1	1	1	1	1	1	89,000,000.00 Kč
23	0.5312	1	1	1	1	1	1	0	0	1	1	89,000,000.00 Kč
24	0.5311	0	1	1	1	1	1	1	0	1	0	84,000,000.00 Kč
25	0.531	1	1	1	0	1	1	1	0	1	1	49,000,000.00 Kč
26	0.531	1	1	0	0	1	1	1	0	1	1	44,000,000.00 Kč
27	0.5309	0	0	1	1	1	1	1	1	1	1	84,000,000.00 Kč
28	0.5306	0	1	1	1	1	1	0	0	1	1	84,000,000.00 Kč
29	0.5304	0	1	1	0	1	1	1	0	1	1	44,000,000.00 Kč
30	0.5304	0	1	0	0	1	1	1	0	1	1	39,000,000.00 Kč
31	0.5291	1	1	0	1	1	1	1	0	1	0	84,000,000.00 Kč
32	0.5285	1	1	0	1	1	1	0	0	1	1	84,000,000.00 Kč
33	0.5285	0	1	0	1	1	1	1	0	1	0	79,000,000.00 Kč
34	0.528	0	1	0	1	1	1	0	0	1	1	79,000,000.00 Kč
35	0.5099	1	0	1	1	1	1	1	0	1	1	89,000,000.00 Kč
36	0.5094	0	0	1	1	1	1	1	0	1	1	84,000,000.00 Kč
37	0.5037	1	1	1	1	1	1	0	1	1	0	79,000,000.00 Kč
38	0.5035	1	1	1	0	1	1	1	1	1	0	39,000,000.00 Kč
39	0.5035	1	1	0	0	1	1	1	1	1	0	34,000,000.00 Kč
40	0.5032	0	1	1	1	1	1	0	1	1	0	74,000,000.00 Kč
41	0.503	1	1	1	0	1	1	0	1	1	1	39,000,000.00 Kč
42	0.503	1	1	0	0	1	1	0	1	1	1	34,000,000.00 Kč
43	0.503	0	1	1	0	1	1	1	1	1	0	34,000,000.00 Kč
44	0.503	0	1	0	0	1	1	1	1	1	0	29,000,000.00 Kč
45	0.5025	0	1	1	0	1	1	0	1	1	1	34,000,000.00 Kč
46	0.5025	0	1	0	0	1	1	0	1	1	1	29,000,000.00 Kč
47	0.5012	1	1	0	1	1	1	0	1	1	0	74,000,000.00 Kč
48	0.5007	0	1	0	1	1	1	0	1	1	0	69,000,000.00 Kč
49	0.4836	1	0	1	1	1	1	1	1	1	0	79,000,000.00 Kč
50	0.4834	1	1	1	1	1	1	0	0	1	0	79,000,000.00 Kč

Figure E.1: Numerical results of PRA analysis including cost analysis with probability of human error 0.1 an probability of HW failure 0.1

Results of PRA analysis for Strahov Tunnel

probabilities: human error = 0.1 and HW failure= 0.5

		Smokde detection	Longitudinal Ventilation	Faster fans	Dampers	Dampers-emergency exits	Fans-emregency exits	Malovanka-wall	Plzenska-wall	SW	Wall in the tunnel	Cost
1	0.1879	1	1	1	1	1	1	1	1	1	1	99,000,000.00 Kč
2	0.1877	0	1	1	1	1	1	1	1	1	1	94,000,000.00 Kč
3	0.187	1	1	0	1	1	1	1	1	1	1	94,000,000.00 Kč
4	0.1868	0	1	0	1	1	1	1	1	1	1	89,000,000.00 Kč
5	0.1803	1	1	1	1	1	1	1	0	1	1	99,000,000.00 Kč
6	0.1801	0	1	1	1	1	1	1	0	1	1	94,000,000.00 Kč
7	0.1794	1	1	0	1	1	1	1	0	1	1	94,000,000.00 Kč
8	0.1793	0	1	0	1	1	1	1	0	1	1	89,000,000.00 Kč
9	0.171	1	1	1	1	1	1	1	1	1	0	89,000,000.00 Kč
10	0.1708	1	1	1	1	1	1	0	1	1	1	89,000,000.00 Kč
11	0.1708	0	1	1	1	1	1	1	1	1	0	84,000,000.00 Kč
12	0.1708	1	1	1	0	1	1	1	1	1	1	49,000,000.00 Kč
13	0.1708	1	1	0	0	1	1	1	1	1	1	44,000,000.00 Kč
14	0.1707	0	1	1	1	1	1	0	1	1	1	84,000,000.00 Kč
15	0.1706	0	1	1	0	1	1	1	1	1	1	44,000,000.00 Kč
16	0.1706	0	1	0	0	1	1	1	1	1	1	39,000,000.00 Kč
17	0.1702	1	1	0	1	1	1	1	1	1	0	84,000,000.00 Kč
18	0.17	1	1	0	1	1	1	0	1	1	1	84,000,000.00 Kč
19	0.17	0	1	0	1	1	1	1	1	1	0	79,000,000.00 Kč
20	0.1698	0	1	0	1	1	1	0	1	1	1	79,000,000.00 Kč
21	0.1641	1	1	1	1	1	1	1	0	1	0	89,000,000.00 Kč
22	0.164	1	0	1	1	1	1	1	1	1	1	89,000,000.00 Kč
23	0.1639	1	1	1	1	1	1	0	0	1	1	89,000,000.00 Kč
24	0.1639	0	1	1	1	1	1	1	0	1	0	84,000,000.00 Kč
25	0.1639	1	1	1	0	1	1	1	0	1	1	49,000,000.00 Kč
26	0.1639	1	1	0	0	1	1	1	0	1	1	44,000,000.00 Kč
27	0.1638	0	0	1	1	1	1	1	1	1	1	84,000,000.00 Kč
28	0.1638	0	1	1	1	1	1	0	0	1	1	84,000,000.00 Kč
29	0.1637	0	1	1	0	1	1	1	0	1	1	44,000,000.00 Kč
30	0.1637	0	1	0	0	1	1	1	0	1	1	39,000,000.00 Kč
31	0.1633	1	1	0	1	1	1	1	0	1	0	84,000,000.00 Kč
32	0.1631	1	1	0	1	1	1	0	0	1	1	84,000,000.00 Kč
33	0.1631	0	1	0	1	1	1	1	0	1	0	79,000,000.00 Kč
34	0.163	0	1	0	1	1	1	0	0	1	1	79,000,000.00 Kč
35	0.1574	1	0	1	1	1	1	1	0	1	1	89,000,000.00 Kč
36	0.1572	0	0	1	1	1	1	1	0	1	1	84,000,000.00 Kč
37	0.1555	1	1	1	1	1	1	0	1	1	0	79,000,000.00 Kč
38	0.1554	1	1	1	0	1	1	1	1	1	0	39,000,000.00 Kč
39	0.1554	1	1	0	0	1	1	1	1	1	0	34,000,000.00 Kč
40	0.1553	0	1	1	1	1	1	0	1	1	0	74,000,000.00 Kč
41	0.1553	1	1	1	0	1	1	0	1	1	1	39,000,000.00 Kč
42	0.1553	1	1	0	0	1	1	0	1	1	1	34,000,000.00 Kč
43	0.1552	0	1	1	0	1	1	1	1	1	0	34,000,000.00 Kč
44	0.1552	0	1	0	0	1	1	1	1	1	0	29,000,000.00 Kč
45	0.1551	0	1	1	0	1	1	0	1	1	1	34,000,000.00 Kč
46	0.1551	0	1	0	0	1	1	0	1	1	1	29,000,000.00 Kč
47	0.1547	1	1	0	1	1	1	0	1	1	0	74,000,000.00 Kč
48	0.1545	0	1	0	1	1	1	0	1	1	0	69,000,000.00 Kč
49	0.1493	1	0	1	1	1	1	1	1	1	0	79,000,000.00 Kč
50	0.1492	1	1	1	1	1	1	0	0	1	0	79,000,000.00 Kč

Figure E.2: Numerical results of PRA analysis including cost analysis with probability of human error 0.1 an probability of HW failure 0.5

Results of PRA analysis for Strahov Tunnel

probabilities: human error = 0.4 and HW failure= 0.1

		Smokde detection	Longitudinal Ventilation	Faster fans	Dampers	Dampers-emergency exits	Fans-emregency exits	Malovanka-wall	Plzenska-wall	SW	Wall in the tunnel	Cost
1	0.4059	1	1	1	1	1	1	1	1	1	1	99,000,000.00 Kč
2	0.4043	0	1	1	1	1	1	1	1	1	1	94,000,000.00 Kč
3	0.4039	1	1	0	1	1	1	1	1	1	1	94,000,000.00 Kč
4	0.4023	0	1	0	1	1	1	1	1	1	1	89,000,000.00 Kč
5	0.3895	1	1	1	1	1	1	1	0	1	1	99,000,000.00 Kč
6	0.388	0	1	1	1	1	1	1	0	1	1	94,000,000.00 Kč
7	0.3876	1	1	0	1	1	1	1	0	1	1	94,000,000.00 Kč
8	0.386	0	1	0	1	1	1	1	0	1	1	89,000,000.00 Kč
9	0.3694	1	1	1	1	1	1	1	1	1	0	89,000,000.00 Kč
10	0.369	1	1	1	1	1	1	0	1	1	1	89,000,000.00 Kč
11	0.3689	1	1	1	0	1	1	1	1	1	1	49,000,000.00 Kč
12	0.3689	1	1	0	0	1	1	1	1	1	1	44,000,000.00 Kč
13	0.3679	0	1	1	1	1	1	1	1	1	0	84,000,000.00 Kč
14	0.3676	1	1	0	1	1	1	1	1	1	0	84,000,000.00 Kč
15	0.3675	0	1	1	1	1	1	0	1	1	1	84,000,000.00 Kč
16	0.3674	0	1	1	0	1	1	1	1	1	1	44,000,000.00 Kč
17	0.3674	0	1	0	0	1	1	1	1	1	1	39,000,000.00 Kč
18	0.3672	1	1	0	1	1	1	0	1	1	1	84,000,000.00 Kč
19	0.3661	0	1	0	1	1	1	1	1	1	0	79,000,000.00 Kč
20	0.3657	0	1	0	1	1	1	0	1	1	1	79,000,000.00 Kč
21	0.3544	1	1	1	1	1	1	1	0	1	0	89,000,000.00 Kč
22	0.3543	1	0	1	1	1	1	1	1	1	1	89,000,000.00 Kč
23	0.3541	1	1	1	1	1	1	0	0	1	1	89,000,000.00 Kč
24	0.354	1	1	1	0	1	1	1	0	1	1	49,000,000.00 Kč
25	0.354	1	1	0	0	1	1	1	0	1	1	44,000,000.00 Kč
26	0.353	0	1	1	1	1	1	1	0	1	0	84,000,000.00 Kč
27	0.3529	0	0	1	1	1	1	1	1	1	1	84,000,000.00 Kč
28	0.3527	1	1	0	1	1	1	1	0	1	0	84,000,000.00 Kč
29	0.3527	0	1	1	1	1	1	0	0	1	1	84,000,000.00 Kč
30	0.3526	0	1	1	0	1	1	1	0	1	1	44,000,000.00 Kč
31	0.3526	0	1	0	0	1	1	1	0	1	1	39,000,000.00 Kč
32	0.3524	1	1	0	1	1	1	0	0	1	1	84,000,000.00 Kč
33	0.3513	0	1	0	1	1	1	1	0	1	0	79,000,000.00 Kč
34	0.351	0	1	0	1	1	1	0	0	1	1	79,000,000.00 Kč
35	0.3399	1	0	1	1	1	1	1	0	1	1	89,000,000.00 Kč
36	0.3386	0	0	1	1	1	1	1	0	1	1	84,000,000.00 Kč
37	0.3358	1	1	1	1	1	1	0	1	1	0	79,000,000.00 Kč
38	0.3357	1	1	1	0	1	1	1	1	1	0	39,000,000.00 Kč
39	0.3357	1	1	0	0	1	1	1	1	1	0	34,000,000.00 Kč
40	0.3353	1	1	1	0	1	1	0	1	1	1	39,000,000.00 Kč
41	0.3353	1	1	0	0	1	1	0	1	1	1	34,000,000.00 Kč
42	0.3345	0	1	1	1	1	1	0	1	1	0	74,000,000.00 Kč
43	0.3343	0	1	1	0	1	1	1	1	1	0	34,000,000.00 Kč
44	0.3343	0	1	0	0	1	1	1	1	1	0	29,000,000.00 Kč
45	0.3341	1	1	0	1	1	1	0	1	1	0	74,000,000.00 Kč
46	0.334	0	1	1	0	1	1	0	1	1	1	34,000,000.00 Kč
47	0.334	0	1	0	0	1	1	0	1	1	1	29,000,000.00 Kč
48	0.3328	0	1	0	1	1	1	0	1	1	0	69,000,000.00 Kč
49	0.3224	1	0	1	1	1	1	1	1	1	0	79,000,000.00 Kč
50	0.3222	1	1	1	1	1	1	0	0	1	0	79,000,000.00 Kč

Figure E.3: Numerical results of PRA analysis including cost analysis with probability of human error 0.4 an probability of HW failure 0.1

Results of PRA analysis for Strahov Tunnel

probabilities: human error = 0.4 and HW failure= 0.5

		Smokde detection	Longitudinal Ventilation	Faster fans	Dampers	Dampers-emergency exits	Fans-emregency exits	Malovanka-wall	Plzenska-wall	SW	Wall in the tunnel	Cost
1	0.1253	1	1	1	1	1	1	1	1	1	1	99,000,000.00 Kč
2	0.1248	0	1	1	1	1	1	1	1	1	1	94,000,000.00 Kč
3	0.1247	1	1	0	1	1	1	1	1	1	1	94,000,000.00 Kč
4	0.1242	0	1	0	1	1	1	1	1	1	1	89,000,000.00 Kč
5	0.1202	1	1	1	1	1	1	1	0	1	1	99,000,000.00 Kč
6	0.1197	0	1	1	1	1	1	1	0	1	1	94,000,000.00 Kč
7	0.1196	1	1	0	1	1	1	1	0	1	1	94,000,000.00 Kč
8	0.1192	0	1	0	1	1	1	1	0	1	1	89,000,000.00 Kč
9	0.114	1	1	1	1	1	1	1	1	1	0	89,000,000.00 Kč
10	0.1139	1	1	1	1	1	1	0	1	1	1	89,000,000.00 Kč
11	0.1138	1	1	1	0	1	1	1	1	1	1	49,000,000.00 Kč
12	0.1138	1	1	0	0	1	1	1	1	1	1	44,000,000.00 Kč
13	0.1135	0	1	1	1	1	1	1	1	1	0	84,000,000.00 Kč
14	0.1134	1	1	0	1	1	1	1	1	1	0	84,000,000.00 Kč
15	0.1134	0	1	1	1	1	1	0	1	1	1	84,000,000.00 Kč
16	0.1134	0	1	1	0	1	1	1	1	1	1	44,000,000.00 Kč
17	0.1134	0	1	0	0	1	1	1	1	1	1	39,000,000.00 Kč
18	0.1133	1	1	0	1	1	1	0	1	1	1	84,000,000.00 Kč
19	0.113	0	1	0	1	1	1	1	1	1	0	79,000,000.00 Kč
20	0.1129	0	1	0	1	1	1	0	1	1	1	79,000,000.00 Kč
21	0.1094	1	1	1	1	1	1	1	0	1	0	89,000,000.00 Kč
22	0.1093	1	0	1	1	1	1	1	1	1	1	89,000,000.00 Kč
23	0.1093	1	1	1	1	1	1	0	0	1	1	89,000,000.00 Kč
24	0.1092	1	1	1	0	1	1	1	0	1	1	49,000,000.00 Kč
25	0.1092	1	1	0	0	1	1	1	0	1	1	44,000,000.00 Kč
26	0.109	0	1	1	1	1	1	1	0	1	0	84,000,000.00 Kč
27	0.1089	0	0	1	1	1	1	1	1	1	1	84,000,000.00 Kč
28	0.1089	1	1	0	1	1	1	1	0	1	0	84,000,000.00 Kč
29	0.1089	0	1	1	1	1	1	0	0	1	1	84,000,000.00 Kč
30	0.1088	0	1	1	0	1	1	1	0	1	1	44,000,000.00 Kč
31	0.1088	0	1	0	0	1	1	1	0	1	1	39,000,000.00 Kč
32	0.1088	1	1	0	1	1	1	0	0	1	1	84,000,000.00 Kč
33	0.1084	0	1	0	1	1	1	1	0	1	0	79,000,000.00 Kč
34	0.1083	0	1	0	1	1	1	0	0	1	1	79,000,000.00 Kč
35	0.1049	1	0	1	1	1	1	1	0	1	1	89,000,000.00 Kč
36	0.1045	0	0	1	1	1	1	1	0	1	1	84,000,000.00 Kč
37	0.1036	1	1	1	1	1	1	0	1	1	0	79,000,000.00 Kč
38	0.1036	1	1	1	0	1	1	1	1	1	0	39,000,000.00 Kč
39	0.1036	1	1	0	0	1	1	1	1	1	0	34,000,000.00 Kč
40	0.1035	1	1	1	0	1	1	0	1	1	1	39,000,000.00 Kč
41	0.1035	1	1	0	0	1	1	0	1	1	1	34,000,000.00 Kč
42	0.1032	0	1	1	1	1	1	0	1	1	0	74,000,000.00 Kč
43	0.1032	0	1	1	0	1	1	1	1	1	0	34,000,000.00 Kč
44	0.1032	0	1	0	0	1	1	1	1	1	0	29,000,000.00 Kč
45	0.1031	1	1	0	1	1	1	0	1	1	0	74,000,000.00 Kč
46	0.1031	0	1	1	0	1	1	0	1	1	1	34,000,000.00 Kč
47	0.1031	0	1	0	0	1	1	0	1	1	1	29,000,000.00 Kč
48	0.1027	0	1	0	1	1	1	0	1	1	0	69,000,000.00 Kč
49	0.0995	1	0	1	1	1	1	1	1	1	0	79,000,000.00 Kč
50	0.0995	1	1	1	1	1	1	0	0	1	0	79,000,000.00 Kč

Figure E.4: Numerical results of PRA analysis including cost analysis with probability of human error 0.4 an probability of HW failure 0.5

Results of PRA analysis for Strahov Tunnel

probabilities: human error = 0.7 and HW failure= 0.1

		Smokde detection	Longitudinal Ventilation	Faster fans	Dampers	Dampers-emergency exits	Fans-emregency exits	Malovanka-wall	Plzenska-wall	SW	Wall in the tunnel	Cost
1	0.2029	1	1	1	1	1	1	1	1	1	1	99,000,000.00 Kč
2	0.2019	1	1	0	1	1	1	1	1	1	1	94,000,000.00 Kč
3	0.2015	0	1	1	1	1	1	1	1	1	1	94,000,000.00 Kč
4	0.2005	0	1	0	1	1	1	1	1	1	1	89,000,000.00 Kč
5	0.1947	1	1	1	1	1	1	1	0	1	1	99,000,000.00 Kč
6	0.1938	1	1	0	1	1	1	1	0	1	1	94,000,000.00 Kč
7	0.1934	0	1	1	1	1	1	1	0	1	1	94,000,000.00 Kč
8	0.1924	0	1	0	1	1	1	1	0	1	1	89,000,000.00 Kč
9	0.1847	1	1	1	1	1	1	1	1	1	0	89,000,000.00 Kč
10	0.1845	1	1	1	1	1	1	0	1	1	1	89,000,000.00 Kč
11	0.1844	1	1	1	0	1	1	1	1	1	1	49,000,000.00 Kč
12	0.1844	1	1	0	0	1	1	1	1	1	1	44,000,000.00 Kč
13	0.1838	1	1	0	1	1	1	1	1	1	0	84,000,000.00 Kč
14	0.1836	1	1	0	1	1	1	0	1	1	1	84,000,000.00 Kč
15	0.1834	0	1	1	1	1	1	1	1	1	0	84,000,000.00 Kč
16	0.1832	0	1	1	1	1	1	0	1	1	1	84,000,000.00 Kč
17	0.1831	0	1	1	0	1	1	1	1	1	1	44,000,000.00 Kč
18	0.1831	0	1	0	0	1	1	1	1	1	1	39,000,000.00 Kč
19	0.1825	0	1	0	1	1	1	1	1	1	0	79,000,000.00 Kč
20	0.1823	0	1	0	1	1	1	0	1	1	1	79,000,000.00 Kč
21	0.1772	1	1	1	1	1	1	1	0	1	0	89,000,000.00 Kč
22	0.1771	1	0	1	1	1	1	1	1	1	1	89,000,000.00 Kč
23	0.177	1	1	1	1	1	1	0	0	1	1	89,000,000.00 Kč
24	0.177	1	1	1	0	1	1	1	0	1	1	49,000,000.00 Kč
25	0.177	1	1	0	0	1	1	1	0	1	1	44,000,000.00 Kč
26	0.1763	1	1	0	1	1	1	1	0	1	0	84,000,000.00 Kč
27	0.1762	1	1	0	1	1	1	0	0	1	1	84,000,000.00 Kč
28	0.176	0	1	1	1	1	1	1	0	1	0	84,000,000.00 Kč
29	0.1759	0	0	1	1	1	1	1	1	1	1	84,000,000.00 Kč
30	0.1758	0	1	1	1	1	1	0	0	1	1	84,000,000.00 Kč
31	0.1757	0	1	1	0	1	1	1	0	1	1	44,000,000.00 Kč
32	0.1757	0	1	0	0	1	1	1	0	1	1	39,000,000.00 Kč
33	0.1751	0	1	0	1	1	1	1	0	1	0	79,000,000.00 Kč
34	0.1749	0	1	0	1	1	1	0	0	1	1	79,000,000.00 Kč
35	0.17	1	0	1	1	1	1	1	0	1	1	89,000,000.00 Kč
36	0.1688	0	0	1	1	1	1	1	0	1	1	84,000,000.00 Kč
37	0.1679	1	1	1	1	1	1	0	1	1	0	79,000,000.00 Kč
38	0.1678	1	1	1	0	1	1	1	1	1	0	39,000,000.00 Kč
39	0.1678	1	1	0	0	1	1	1	1	1	0	34,000,000.00 Kč
40	0.1677	1	1	1	0	1	1	0	1	1	1	39,000,000.00 Kč
41	0.1677	1	1	0	0	1	1	0	1	1	1	34,000,000.00 Kč
42	0.1671	1	1	0	1	1	1	0	1	1	0	74,000,000.00 Kč
43	0.1667	0	1	1	1	1	1	0	1	1	0	74,000,000.00 Kč
44	0.1667	0	1	1	0	1	1	1	1	1	0	34,000,000.00 Kč
45	0.1667	0	1	0	0	1	1	1	1	1	0	29,000,000.00 Kč
46	0.1665	0	1	1	0	1	1	0	1	1	1	34,000,000.00 Kč
47	0.1665	0	1	0	0	1	1	0	1	1	1	29,000,000.00 Kč
48	0.1659	0	1	0	1	1	1	0	1	1	0	69,000,000.00 Kč
49	0.1612	1	0	1	1	1	1	1	1	1	0	79,000,000.00 Kč
50	0.1611	1	1	1	1	1	1	0	0	1	0	79,000,000.00 Kč

Figure E.5: Numerical results of PRA analysis including cost analysis with probability of human error 0.7 an probability of HW failure 0.1

Results of PRA analysis for Strahov Tunnel

probabilities: human error = 0.7 and HW failure= 0.5

		Smokde detection	Longitudinal Ventilation	Faster fans	Dampers	Dampers-emergency exits	Fans-emregency exits	Malovanka-wall	Plzenska-wall	SW	Wall in the tunnel	Cost
1	0.0626	1	1	1	1	1	1	1	1	1	1	99,000,000.00 Kč
2	0.0623	1	1	0	1	1	1	1	1	1	1	94,000,000.00 Kč
3	0.0622	0	1	1	1	1	1	1	1	1	1	94,000,000.00 Kč
4	0.0619	0	1	0	1	1	1	1	1	1	1	89,000,000.00 Kč
5	0.0601	1	1	1	1	1	1	1	0	1	1	99,000,000.00 Kč
6	0.0598	1	1	0	1	1	1	1	0	1	1	94,000,000.00 Kč
7	0.0597	0	1	1	1	1	1	1	0	1	1	94,000,000.00 Kč
8	0.0594	0	1	0	1	1	1	1	0	1	1	89,000,000.00 Kč
9	0.057	1	1	1	1	1	1	1	1	1	0	89,000,000.00 Kč
10	0.0569	1	1	1	1	1	1	0	1	1	1	89,000,000.00 Kč
11	0.0569	1	1	1	0	1	1	1	1	1	1	49,000,000.00 Kč
12	0.0569	1	1	0	0	1	1	1	1	1	1	44,000,000.00 Kč
13	0.0567	1	1	0	1	1	1	1	1	1	0	84,000,000.00 Kč
14	0.0567	1	1	0	1	1	1	0	1	1	1	84,000,000.00 Kč
15	0.0566	0	1	1	1	1	1	1	1	1	0	84,000,000.00 Kč
16	0.0565	0	1	1	1	1	1	0	1	1	1	84,000,000.00 Kč
17	0.0565	0	1	1	0	1	1	1	1	1	1	44,000,000.00 Kč
18	0.0565	0	1	0	0	1	1	1	1	1	1	39,000,000.00 Kč
19	0.0563	0	1	0	1	1	1	1	1	1	0	79,000,000.00 Kč
20	0.0563	0	1	0	1	1	1	0	1	1	1	79,000,000.00 Kč
21	0.0547	1	1	1	1	1	1	1	0	1	0	89,000,000.00 Kč
22	0.0547	1	0	1	1	1	1	1	1	1	1	89,000,000.00 Kč
23	0.0546	1	1	1	1	1	1	0	0	1	1	89,000,000.00 Kč
24	0.0546	1	1	1	0	1	1	1	0	1	1	49,000,000.00 Kč
25	0.0546	1	1	0	0	1	1	1	0	1	1	44,000,000.00 Kč
26	0.0544	1	1	0	1	1	1	1	0	1	0	84,000,000.00 Kč
27	0.0544	1	1	0	1	1	1	0	0	1	1	84,000,000.00 Kč
28	0.0543	0	1	1	1	1	1	1	0	1	0	84,000,000.00 Kč
29	0.0543	0	0	1	1	1	1	1	1	1	1	84,000,000.00 Kč
30	0.0543	0	1	1	1	1	1	0	0	1	1	84,000,000.00 Kč
31	0.0542	0	1	1	0	1	1	1	0	1	1	44,000,000.00 Kč
32	0.0542	0	1	0	0	1	1	1	0	1	1	39,000,000.00 Kč
33	0.0541	0	1	0	1	1	1	1	0	1	0	79,000,000.00 Kč
34	0.054	0	1	0	1	1	1	0	0	1	1	79,000,000.00 Kč
35	0.0525	1	0	1	1	1	1	1	0	1	1	89,000,000.00 Kč
36	0.0521	0	0	1	1	1	1	1	0	1	1	84,000,000.00 Kč
37	0.0518	1	1	1	1	1	1	0	1	1	0	79,000,000.00 Kč
38	0.0518	1	1	1	0	1	1	1	1	1	0	39,000,000.00 Kč
39	0.0518	1	1	0	0	1	1	1	1	1	0	34,000,000.00 Kč
40	0.0517	1	1	1	0	1	1	0	1	1	1	39,000,000.00 Kč
41	0.0517	1	1	0	0	1	1	0	1	1	1	34,000,000.00 Kč
42	0.0516	1	1	0	1	1	1	0	1	1	0	74,000,000.00 Kč
43	0.0515	0	1	1	1	1	1	0	1	1	0	74,000,000.00 Kč
44	0.0514	0	1	1	0	1	1	1	1	1	0	34,000,000.00 Kč
45	0.0514	0	1	0	0	1	1	1	1	1	0	29,000,000.00 Kč
46	0.0514	0	1	1	0	1	1	0	1	1	1	34,000,000.00 Kč
47	0.0514	0	1	0	0	1	1	0	1	1	1	29,000,000.00 Kč
48	0.0512	0	1	0	1	1	1	0	1	1	0	69,000,000.00 Kč
49	0.0497	1	0	1	1	1	1	1	1	1	0	79,000,000.00 Kč
50	0.0497	1	1	1	1	1	1	0	0	1	0	79,000,000.00 Kč

Figure E.6: Numerical results of PRA analysis including cost analysis with probability of human error 0.7 an probability of HW failure 0.5