Making sense of risks

B. Hovestad

F.J. Bex

Technical Report UU-CS-2016-006
May 2016

Department of Information and Computing Sciences
Utrecht University, Utrecht, The Netherlands
www.cs.uu.nl

ISSN: 0924-3275

Department of Information and Computing Sciences
Utrecht University
P.O. Box 80.089
3508 TB Utrecht
The Netherlands

Abstract

Risk management is relevant in a large array of industries and other fields concerned with acting upon risks in a timely manner. Several dynamic sub-processes lay at the foundation of risk management. A sub-process that plays a central role is risk assessment, which revolves around the identification and analyses of risks and mitigating measures.

To conduct a risk assessment, several methods and tools have been developed, ranging from simple to more complex ones. In this thesis an analysis is made of different methods and tools. The analysis is based on literature research and experiences and insights of our case organization, the Dutch police force. The results from the analysis show that the methods and tools are either too simple, in these sense that risk scenarios are not sufficiently analyzed, or too complex due to the requirement of complex mathematical, statistical or formal knowledge.

This thesis proposes a risk assessment model based on the hybrid theory by Bex, Van Koppen, Prakken, and Verheij (2010). The hybrid theory enables to make sense of evidential data and has its roots in artificial intelligence and law. Translated to risk assessment, a model based on the hybrid theory can enable to make sense of risks by providing an accessible, systematic and dynamic way of identifying and analyzing risk scenarios and mitigating measures. The case study has revealed how reoccurring patterns of risks can be identified and applied in practice.

Because the model consists of abstract concepts, which are not difficult to understand by an everyday reasoner, the model can be used to develop risk assessment methods and tools, such as the iTable application of the Dutch police force.

Keywords: *Risk management*, *Risk assessment*, *Scenario building*, *The hybrid theory*

Contents

List of Tables

List of Figures

Terminology

The terminology that is used throughout this thesis is listed and defined. The definitions are according to the ISO/IEC Guide 73[1] and in some cases complemented for clarification purposes.

Risk - combination of the probability of an event and its consequences.

Risk management - a continuous management process with the objective to identify, analyze, and assess potential hazards in a system or related to an activity, and to identify and introduce risk control measures to eliminate or reduce potential harms to people, the environment, or other assets (Rausand, 2011, p.10).

Risk assessment - overall process of risk analysis and risk evaluation.

Risk analysis - process to comprehend the nature of risk and to determine the level of risk.

Risk identification - process of finding, recognizing and describing risks.

Risk estimation - process used to assign values to the probability and consequences.

Risk evaluation - process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Risk treatment - process of selection and implementation of measures to modify risk.

Residual risk - risk remaining after risk treatment.

Event - occurrence of a particular set of circumstances. An event can be one or more occurrences, and can have several causes.

Consequence - outcome of an event. An event can lead to a range of consequences. Furthermore, a consequence can be certain or uncertain and can have positive or negative effects

[1] https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

on objectives.

Impact - related to the consequence of an event, but often expressed in qualitative or quantitative scales or values.

Probability - measure of the chance of occurrence expressed in qualitative terms or as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty.

Scenario - a single event or a sequence of events (Rausand, 2011, p.57). A scenario offers a way of communicating about obtaining a joint picture of future uncertainties and factors that influence decisions (Bergmans et al., 2009, p.17).

Hazard - a source of potential harm.

Threat - hazard with a high potential of harm (Rausand, 2011, p.72).

Risk factor - term used to indicate both hazards and threats.

Control - a measure that is modifying risk.

1

Introduction

In everyday life we come across a variety of situations where we aim to control and eventually mitigate risks. Whether it is a change of plans to intercept unexpected sick leave at work, installing snow tires before traveling to your favorite winter sports location to be able to face slippery roads, or putting on a kitchen apron to protect yourself from oil spatters. By adopting measures we aim to control the probability and impact of possible unwanted effects. Being able to cope with risk by seeking and adapting controls to mitigate risks is the essence of risk management. Risk management is not unique to one specific environment and is widely applied in different fields and industries. One could for example think of risk management in a financial institution to measure and manage market, credit, and operational risks across a range of business activities (Rosenberg & Schuermann, 2006). Also, in the IT industry risk management plays an important role (Stoneburner, Goguen, & Feringa, 2002) e.g. an unskilled business analyst or software architect could lead to poor system design which finally has its effects on the costs of the system for both the company and the client. By implementing risk management, IT managers can balance the operational and economic costs of risk mitigating measures by protecting their IT systems and company data (Stoneburner et al., 2002). In sum, risk management is a valuable asset which can be applied in a wide range of fields to support and possibly improve decision-making.

To study risk management in practice, in this thesis the Dutch police force is used as a case organization. Within the Dutch police force, we target risk assessment on supporter flows around football events in the Netherlands, that is on predicting and analyzing risks that occur before and after a football match. The reason for focusing on football events is that there is a significant amount of data and knowledge available on these events, which enables in-depth research and analysis of risks, controls and scenarios.

1.1 Risk assessment methods and tools

Before diving into methods and tools, definitions should be provided for a *method* and a *tool*. The definitions are adapted from van de Weerd and Brinkkemper (2008, p. 275-276), to fit the context of this thesis. A method is "an approach to perform a procedure, based on a specific way of thinking, consisting of directions and rules, structured in a systematic way in activities with corresponding products", and a tool is "a possibly automated means to support a part of a process". These definitions clearly distinguish between a method and a tool, and provide a better understanding of terminology used in this section.

Several risk assessment methods and tools exist. Some of them are generally applicable, while others are developed for a specific field of research or a particular industry. One of the most basic tools is a risk matrix. However, risk matrices are only useful as an approximate tool for risk analysis (Cox, 2008). A more advanced risk assessment tool is, for instance, a Bayesian network, which can reflect the states of (some part) of a world that is being modeled, and describes the relationship between these states in terms of probability (Fenton & Neil, 2012).

Even though current risk assessment methods and tools offer solutions in some domains, there are some shortcomings[1]. On the one hand the methods and tools are too simple in the sense that they do not provide sufficient means to construct scenarios which support the analyses and eventually mitigation of risks, or are too time-consuming (Hopkin, 2012). This applies to tools such as risk matrices or flowcharts (Cox, 2008), as well as to cause and effect diagrams and a structured what-if technique (SWIFT) (Rausand, 2011). On the other hand, the current advanced methods and tools are too complex due to the requirement of knowledge on mathematical, statistical or complex formal models (Fenton & Neil, 2011). This is the case with common and complex risk assessment methods and tools, such as Bayesian networks, Markov methods, petri nets, hazard and operability studies (HAZOP), and fault tree analysis (FTA) (Rausand, 2011). The downside of requiring specific knowledge or actually being able to acquire and process this knowledge is also pointed out by Fenton and Neil (2012), who believe that for many people (for example in the legal domain) any attempt to use Bayesian networks is unsuccessful due to its requirement of specific knowledge on Bayes' theorem. This does not solely apply to Bayesian networks, but can also be extended to the other currently existing complex risk assessment tools, since they all depend on some sort of mathematical or statistical model. This dependency increases the complexity and decreases the ease of use and applicability of a method. Especially, when there is insufficient knowledge on these methods available within the organization. In Section 2.3.2, we will go into further detail on both the simple and more complex methods and tools.

All in all, the current risk assessment methods and tools can be improved upon. Existing methods and tools provide insufficient means to construct useful and coherent scenarios along with the analysis of risks and controls to mitigate these risks. This is due to the requirement of

[1] see Section 3.4 for a detailed overview of current methods and tools

specific and extensive knowledge on mathematical, statistical and formal methods. The requirement of specific knowledge becomes a hurdle in performing risk assessment when the parties that have to perform a risk assessment lack this knowledge.

The formal problem statement for this research project is defined as follows:

Problem statement

Current risk assessment methods and tools are inadequate due to too simple approaches, or too complex approaches that require in-depth knowledge on mathematical, statistical or formal methods. This inadequacy results in insufficient identification and analysis of scenarios, risks, and controls. Consequently, decreasing the possibility to capture and act upon risks. To increase this possibility, a risk assessment model is needed which enables the identification and analysis of scenarios, risks and controls, while not requiring mathematical knowledge.

1.2 Case study: Dutch police force

To research the applicability of our risk assessment model and to validate our findings, a case study is performed at the Dutch police force. The findings in this section are mainly based on the work by den Hengst, Rovers, and Regterschot (2014). Currently, the risk assessment methods and tools aimed around events at the Dutch police force are inadequate. As mentioned above, this thesis targets risk assessment around football events. Too many risks are not anticipated and acted upon when it comes to riots between violent cores of supporter groups (hooligans). Moreover, occasional disturbers, or in terms of the police, “ultras” and “opportunist” are not identified, even though in some cases they are responsible for violence or disturbance (den Hengst et al., 2014).

The current practice of risk assessment at the Dutch police force usually and mainly limits itself to: risk identification and risk analyses. These processes are generally seen as the risk assessment process. However, after finishing the risk analysis, the last stages of identifying and applying controls are often omitted. Events, incidents, situational and environmental changes can lead to new and uncontrolled risks. According to Adang and Brown (2008), the risk assessment process at the police force is not adapted to be able to cope with dynamically developing situations. Furthermore, there is insufficient knowledge and know-how on mathematical and statistical methods within the Dutch police force, hindering the thorough use of existing complex risk assessment methods and tools.

Finally, there is a lack of insight in possible scenarios. In the context of football events and football supporter flows, this lack of insight in possible scenarios manifests itself in for instance unpredicted violent clashes between groups of hooligans of different fan clubs. Needless to say, such situations have negative impact not only on the security and safety of football events, but also on the safety of society.

This research project is part of a larger project at the Dutch police force (project "RISK"). The aim of the overall project is to improve the risk assessment process based on hooliganism around supporter flows. For this reason, a risk assessment model is required, which enables the development of coherent scenarios. To support this risk assessment process around football supporter flows, an application will be developed for an " iTable". The iTable is a touchscreen based platform, and is currently used at the Dutch police force to support the decision-making process around special events (e.g. protection of political figures). The information concerning the events and the severity of risks can be loaded into the iTable application, where an interactive map is used as a basis for the interface. Next, the decision-maker(s) (usually not more than 10 people) gather around the iTable, and by means of discussions and input from the different team members, scenarios can be established by plotting elements on the map, such as camera positions, locations of vehicles, nearest hospitals, getaway routes etc. This can help the decision-makers in understanding and making sense of the situation and possible risks at hand, subsequently enabling the identification of controls.

The goal of this thesis is to develop the underlying risk assessment model. This model is based on an argumentative-narrative approach as proposed in the hybrid theory by Bex et al. (2010). The hybrid theory has its roots in the field of artificial intelligence and law and provides a means to make sense of evidential data and facts by constructing, attacking and supporting possible stories (also known as scenarios). Being able to construct and discuss scenarios is valuable to risk assessment, since scenarios can increase the understanding and improve the identification of risks and controls. Eventually, risks can be acted upon more timely and effectively.

The hybrid theory consists of two main components: stories and arguments. Stories are a coherent sequence of events and are needed to organize facts into one or more hypothesis. Arguments can then be used to support or attack the facts and given arguments in the stories. By using arguments based on evidence and commonsense knowledge, one can argue about not only the stories, but also the coherence of the stories, that is, whether the story is consistent, complete and plausible (Bex, 2011). Also, arguments can be given to support or attack explanatory or causal relations in a story. In addition, applying the hybrid theory allows the model to be formally specified (in order to facilitate implementation). At the same time, according to Bex et al. (2010) the hybrid theory enables the model to be natural so that it can be used by an everyday reasoner such as a crime analyst, who cannot be expected to have in-depth knowledge of mathematical or formal models. An in-depth overview of the hybrid theory is given in Chapter 5. A risk assessment model based on the hybrid theory diminishes the gaps that exist in current risk assessment methods and tools, and offers a sound way to determine, analyze and ultimately act upon risks without the requirements of mathematical knowledge. Furthermore, this model can function as a framework for future risk assessment methods and tools, by providing a means to construct and discuss coherent scenarios, weigh up the risks and controls, and to facilitate a more effective decision-making process.

1.3 Research questions

The research questions are formulated by taking into account the problem statement and research objective. The main research question is defined as:

Main RQ: How can a risk assessment model be developed which enables the identification and analysis of scenarios, risks and controls, while not requiring complex mathematical, statistical or formal knowledge?

An answer to the main question can contribute to the field of risk management by proposing a risk assessment model which enables to reason in detail about risks and controls, in order to facilitate the decision-making process, and which does not require in-depth knowledge on mathematical, statistical or complex formal models.

To answer the main research question, the following sub-questions are defined:

RQ 1: Which methods and tools are available to support and perform risk assessment?
By answering this question, an overview is developed of current risk assessment methods and tools. This overview provides us with an understanding of the state of the art in the field of risk assessment.

RQ 2: What are the drivers and requirements of using a method for risk assessment?
Since our research objective is to develop a risk assessment model based on the hybrid theory by Bex et al. (2010), the advantages and disadvantages of using a formal method for risk assessment is elaborated on, to gain an understanding of the applicability of a formal method. Furthermore, requirements for using a method for risk assessment are explored.

RQ 3: What are the limitations of current risk assessment methods and tools?
With an understanding of current methods and tools, limitations within these two can be identified and analyzed, while also enabling the extraction of best practices, resulting in requirements for the development of our risk assessment model.

RQ 4: How can the hybrid theory be applied to risk assessment?
By knowing what the drivers and requirements are for using a risk assessment method method, we assess how the hybrid theory can be used in risk assessment. This knowledge enables the identification of components to implement in our risk assessment model. The results from the case study can support the improvement of our model and can help in identifying best practices.

a) How can the concepts of the hybrid theory be translated to risk assessment?

b) How can risk assessment be supported by stories and arguments?

c) How can coherent scenarios be defined?

RQ 5: What is the added value of risk assessment based on the hybrid theory?
With an understanding of how the hybrid theory can be applied to risk assessment, we can assess added value of using the hybrid theory for risk assessment. This provides us with advantages and limitations to take into account when developing a risk assessment model based on the hybrid theory.

1.4 Research approach

To conduct the research project, the research framework approach by Verschuren, Doorewaard, and Mellion (2010) is adopted and depicted in Figure 1.1.

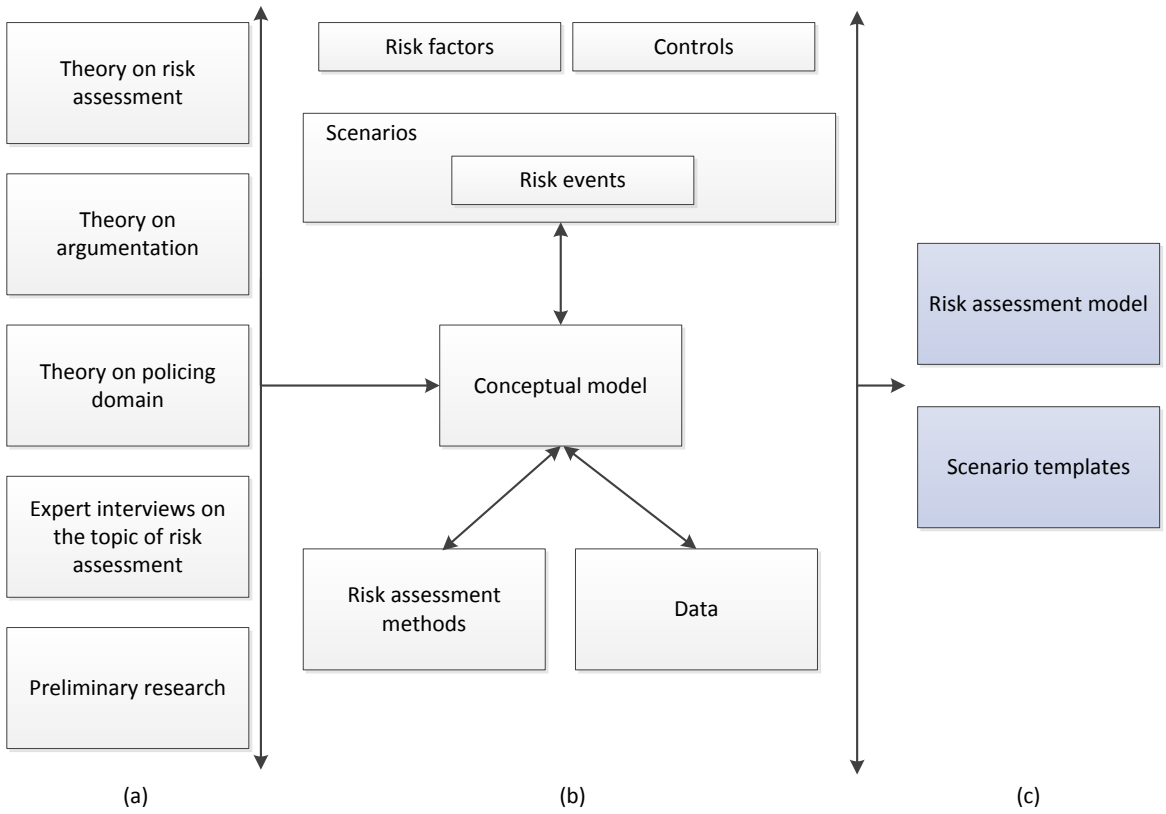

Figure 1.1: Research model

First, a theoretical framework is constructed (a), which results in a conceptual model (b) containing knowledge on the topics as defined on the left side of Figure 1.1. By use of the conceptual model, the construction of scenarios can be investigated, in addition to analysis of risk factors

and controls. Furthermore, current risk assessment tools can be analyzed to determine possible shortcomings or flaws.

By knowing how people reason with risks and controls in the policing domain and by developing insight in scenarios and risk assessment methods and tools, an understanding of risk assessment can be developed which servers as an input for the risk assessment model. Furthermore, by means of expert interviews possible scenario schemes will be uncovered which can support risk analyst in quickly constructing risk scenarios (c).

As depicted in Figure 1.1, the research process starts with developing a sound theoretical foundation. In order to guide this process the *snowball method* (Streeton, Cooke, & Campbell, 2004) is used. This method enables us to identify, filter and gather relevant literature referenced by other studies, thereby uncovering literature which would otherwise remained hidden (Atkinson & Flint, 2001).

For this research two libraries were selected as the main research libraries. First, Google Scholar[2], a commonly used database by researchers, because of the significant amount of literature and topics. In addition, the Web of Science[3] database is consulted to retrieve literature and find cited references. Both of these databases are accessible through the subscription of Utrecht University.

Furthermore, qualitative methods were applied, such as interviews and observations to capture the current risk assessments process and to identify gaps. Also, this leads to insights in how people discuss scenarios and deal with scenarios. The research will be guided according to the design science framework as defined by von Alan et al. (2004). Even though design science originates from the field of Information Systems, it can also be applied in the context of this research project, because it can aid in designing new artifacts such as models or methods. More concrete, the design science paradigm seeks to extend the boundaries of human and organizational capabilities by creating new and innovative artifacts (von Alan et al., 2004).

This research describes the process of integrating the hybrid theory (Bex et al., 2010) with the risk assessment process to create a risk assessment model. Because artifacts are created, extended and integrated, we can relate this research with the design science paradigm. The artifacts will be produced according to the design science research guidelines by von Alan et al. (2004) to ensure that knowledge and understanding of a design problem and its solution are acquired in the building and application of an artifact. Finally, to evaluate the designed artifacts, methodologies are available in the knowledge base, which can demonstrate the efficacy and goodness of an artifact. Example methodologies are case studies or the construction of detailed scenarios.

When applying the design science framework to this research the model in Figure 1.2 on page 11 is constructed.

[2]http://scholar.google.com
[3]https://webofknowledge.com

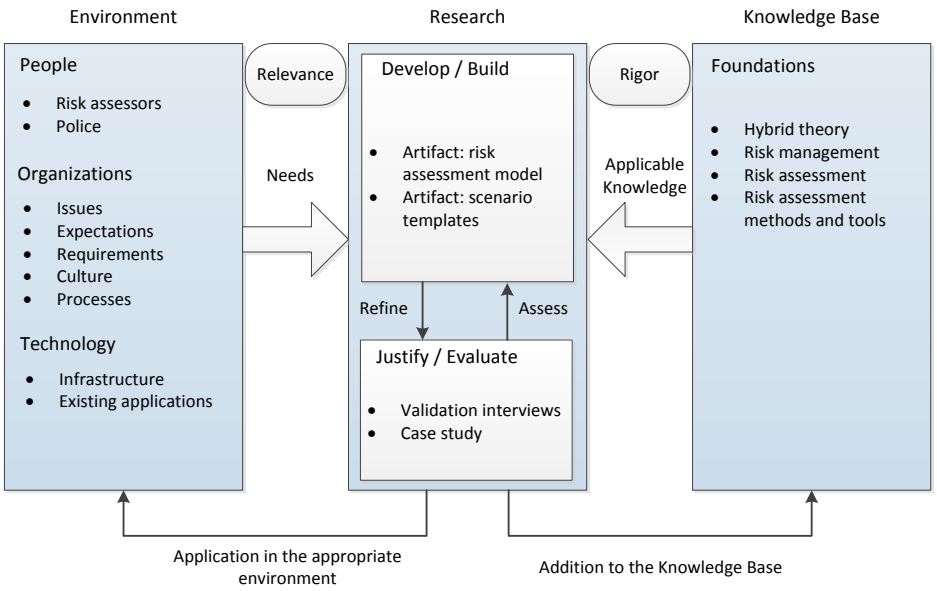

Figure 1.2: Design science model applied to this research (adapted from von Alan et al. (2004))

The results of the literature review are presented in the theoretical framework, represented in Chapter 2, Chapter 3, and Chapter 5.

1.5 Relevance

1.5.1 Scientific Relevance

Over the last years, risk management has found its ways through different fields of research and different industries. As mentioned earlier, risk assessment is an integral part of the overall risk management process. To perform risk assessment several methods and tools are available (Fenton & Neil, 2012; Hopkin, 2012; Rausand, 2011)[4]. However, when applying these methods and tools in the policing domain, they do not seem to be adequate due too large complex data sets combined with an often insufficient level of insight into mathematics and complex analytical thinking.

This research aims at integrating the hybrid theory by Bex et al. (2010) with the risk assessment process in order to facilitate a more natural and rational way of uncovering risks and scenarios. This research will propose a model to improve the efficiency and quality of current risk assessment methods and tools. By doing so we add knowledge to the field of risk management which can ultimately be applied outside the policing domain. Furthermore, the results from this project can function as a source for future research in the field of risk assessment.

1.5.2 Social Relevance

In addition to the scientific relevance, there is a social trigger to the project. The current lack of insights in risks and measures in the policing domain results in inefficient assessment of risks. Often there is an overview of what the risks are, however no deep understanding is generated which is necessary to identify new risks and consequences, and to apply suiting and sufficient mitigating measures (den Hengst et al., 2014). The Dutch police force has developed many risk assessment methods and tools to execute and support risk management. However, none of these methods seem to fully satisfy the analysis of risks due to a lack of quality (den Hengst et al., 2014). The findings of this research will enrich the knowledge of risk assessment in the policing domain and can aid in decreasing risks and increasing reliability of the decision-making process.

1.6 Outline

To develop an understanding of the context of this thesis, first an introduction to the concepts, principles and processes of risk management is provided in Chapter 2. Furthermore, the limitations of current risk assessment methods and tools are discussed. The knowledge from that chapter will form the foundation for the remainder of the thesis.

[4] see Section 2.3.2 for a detailed overview of methods and tools

In Chapter 3 an overview is provided of risk management and assessment at the Dutch police force. Furthermore, the different risk assessment methods and tools at the Dutch police force will be described, after which their limitations are discussed.

With the knowledge about possibilities and limitations of risk assessment methods and tools, requirements for a risk assessment model can be defined. These requirements are discussed in Chapter 4.

To develop a risk assessment model which can incorporate the defined requirements, we base our model on the hybrid theory by Bex et al. (2010). The hybrid theory and its different concepts are explained in Chapter 5.

In Chapter 6 it is explained how the hybrid theory can be translated to risk assessment by discussing the different concepts that constitute our risk assessment model. To clarify how the model can be applied to a situation which requires the assessment of risks, examples are provided throughout the chapter.

The case study conducted at the Dutch police force is explained, analyzed and discussed in Chapter 7.

By using the knowledge extracted from the literature study and the case study, the main research question and its sub-question are answered in Chapter 8.

Finally, in Chapter 9 the limitations of our research and risk assessment model are discussed. Furthermore, interesting possibilities for future research of our risk assessment model will be suggested and described.

2

Introduction to Risk Management

To be able to give a proper insight into risk management it is important to define the concepts of risk management and risk. There are many accepted definitions of risk management. Stoneburner et al. (2002, p. 1) define risk management as "the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level", while as defined by the ISO 3100 standard[1], risk management consists of "coordinated activities to direct and control an organization with regard to risks". However, one well-accepted and more complete definition of risk management is: "A continuous management process with the objective to identify, analyze, and assess potential hazards [in a system or related to an activity], and to identify and introduce risk control measures to eliminate or reduce potential harms to people, the environment, or other assets" (Rausand, 2011, p. 10).

An essential part of the overall risk management process is risk assessment. Risk assessments are performed primarily for the purpose of providing information and insight to those who make decisions about how that risk should be managed. Risk assessment is defined by the ISO/IEC Guide 73[2] as "the overall process of risk analysis and risk evaluation". The overall risk management process combines risk assessment with decisions on how to control the risks. An overview of the risk assessment process is provided in Section 2.3.2. However, first the concepts and principles of risk management are elaborated on.

[1] http://www.iso.org/iso/home/standards/iso31000.htm
[2] https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

2.1 Risk management concepts

Within the context of risk management several concepts can be distinguished which play a key role in understanding and conducting a risk assessment. Common approaches to risk assessment view risk as in 2.1.1:

Definition of risk

$$\text{Risk} = \text{probability(scenario)} \times \text{impact(scenario)} \tag{2.1.1}$$

To clarify the different concepts that come into play when talking about risk assessment, an overview of the concepts is depicted in Figure 2.1, based on the bow-tie method as described by Hopkin (2012). The bow-tie method depicts the relationships between identified risk events, its triggers and consequences, and controls to reduce the probability and impact of the risk event, and to mitigate it consequences (Rausand, 2011). This makes the bow-tie model ideal for providing a comprehensive overview of risk management concepts.

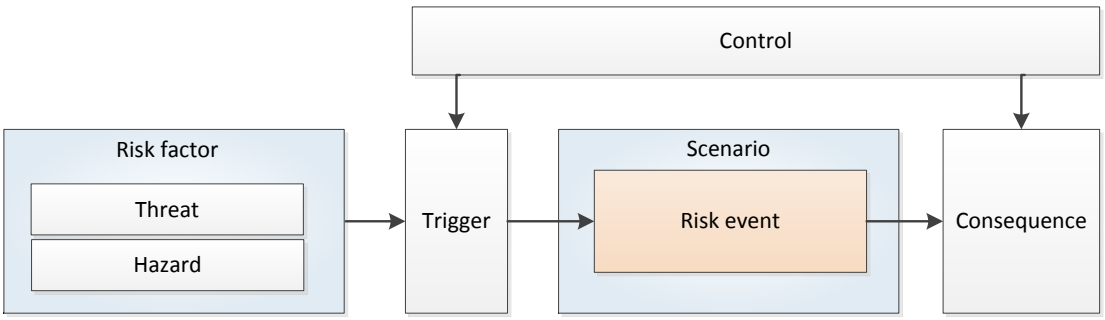

Figure 2.1: Concepts of risk management

Risk management revolves around the identification of hazards and threats (also known as risk factors). When *triggered*, these risk factors result in a *risk event*. The risk events have consequences, which should be identified. Recalling the example as described in Chapter 1, slippery roads can be seen as our risk factor. This risk factor could trigger a risk event, such as losing control of the car. One or more risk events form a *scenario*, in this case for instance a traffic incident. This risk event brings along certain *consequences* e.g. a damaged car. To influence the impact and probability of triggers and consequences, both proactive and reactive controls (measures) can be applied. An example of a proactive control could be to install new tires. On the one hand, this will have minor effect on the impact of the traffic incident. On the other hand, it will possibly reduce the probability of losing grip on a slippery road and therefore

a traffic incident. A reactive control could for example be having a proper insurance to decrease the financial impact of the damaged car.

2.2 Risk management principles

According to Hopkin (2012), there are several principles that lay at the foundation of risk management. The main principle is that risk management should deliver value, which means that the activities are designed to achieve the best possible outcome, while at the same time reducing the uncertainty of outcomes. Furthermore, Hopkin (2012) mentions that successful risk management should be:

- comprehensive, systematic, and structured
- dynamic, iterative, and responsive to change
- proportionate to the level of risk

Rausand (2011) compiled a comparable list aimed at the risk assessment process. However, Rausand (2011, p. 10-12) adds to this list that a "[risk analysis] process should be transparent and understandable by all stakeholders to whom the report will be presented". This principle is relevant, since a vague or underdeveloped analysis could result in an unclear situational view, resulting in inefficient mitigation of risks.

Since risk management is a dynamic and iterative process, the occurrence probability of events and incidents changes due to new risks that emerge, or due to adaptation of existing risks in a dynamic environment (den Hengst et al., 2014). This can be illustrated by for example the traffic accident, for which a set of risks and controls is defined. However, the probability, impact and even the risks itself can change as the accident is taking place. To perform solid risk management, it is vital that not only during the preparation phases attention is payed to the identification and analysis of risks and controls, also during the occurrence of an event possible risks and controls should be evaluated against the current situation (den Hengst et al., 2014).

2.3 Risk management processes

Risk management is sometimes a misunderstood term, in which there are misconceptions in terms of the relationship between different processes of risk management. An important distinction that for instance has to be made when talking about risk management, is the difference between risk management and risk assessment. Often these terms are used to refer to the same processes, however, risk management consists of more than solely a risk assessment. To classify and clarify the processes of risk management, a risk management standard, as depicted in Figure 2.2, has been been developed by AIRMIC (2002).

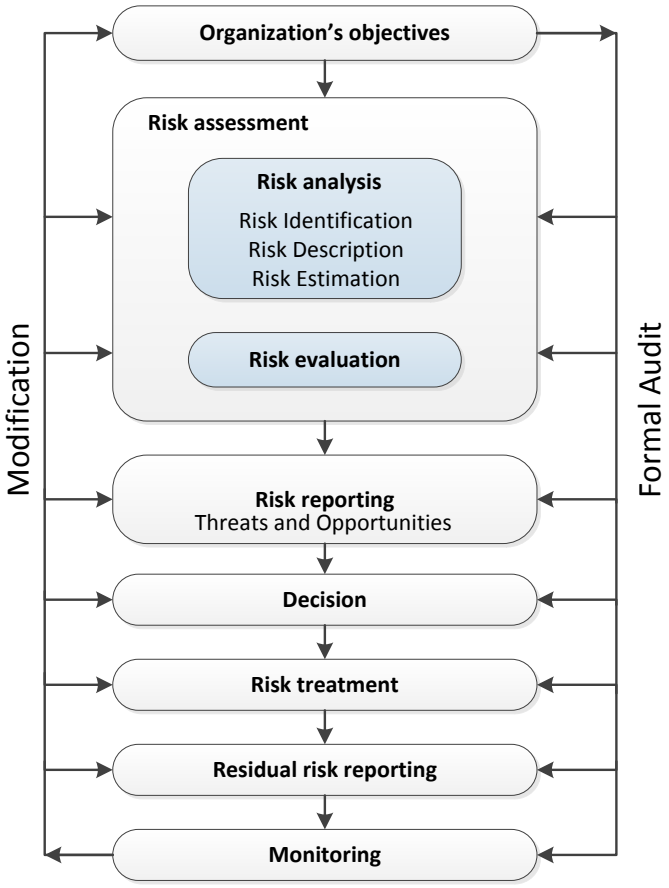

Figure 2.2: Risk management process framework (adopted from AIRMIC (2002))

From Figure 2.2 it becomes clear that the overall risk management process consists of multiple sub-processes, in its turn the risk assessment process also consists of sub-processes. Starting at the top of the model, the first process is to perform a risk analysis, consisting of risk identification, risk description, and risk estimation. After the risk analysis is performed, a risk evaluation takes place to compare the actual risks against the estimated risks. Subsequently, both the threats and the opportunities that are created by the risks are then reported to decision makers, who decide whether the risks should be dealt with or not. The report of the decision making process includes a discussion of the residual risk. Finally, the monitoring process assures that the appropriate controls are in place to mitigate the risk.

A more detailed description is provided in the following sections.

2.3.1 Organization's objectives

The first step in the risk management process is to determine and define the *organization's objectives*. By doing so, an overview can be gained of what the goal of risk management is for the organization, and what possible hurdles are that should be taken into account. Furthermore, setting objectives enables to check if the risk management process is effective, because it allows to monitor whether an objective has been reached or not.

2.3.2 Risk assessment

Risk assessment is defined by the ISO/ IEC Guide 73 as the overall process of risk analysis and risk evaluation. The following subsections will give an overview of the sub-processes of risk assessment.

Risk analysis

The risk analysis process consists of risk identification, description, estimation and finally, risk evaluation.

The first step is the *risk identification* process, which allows the early determination of possible risks that are of influence on the probability and impact of a scenario. To guide this process, several methods and tools are available such as brainstorming sessions, questionnaires, expert judgement and analysis of organization's documentation and data (Hopkin, 2012). In addition, Hopkin (2012) mentions that more complex tools and methods exist, such as fault tree analysis and flowcharts. The most commonly applied risk identification techniques are summarized in Table 2.1.

Technique	**Description**
Questionnaires and checklists	Use of structured questionnaires and checklists to collect information that will assist with the recognition of the significant risks
Interviews and brainstorming	Collecting and sharing of ideas during interviews or brainstorm sessions to discuss the risks that could impact objectives or core processes
Flowcharts and fault tree analysis	Analysis of the processes and operations to identify critical components

Table 2.1: Risk identification techniques

After risks have been identified, they should be described. The objective of *risk description* is to display the identified risks in a structured format, for example, by using a table. This table

containing risk descriptions can be used to facilitate the assessment of risks. The use of a well-designed structure is necessary to ensure a comprehensive risk identification, description and assessment process.

Solely identifying and describing risks is not really helpful in understanding risk, therefore the risks have to be analyzed to gain insight into the possible causes of risk. In the *risk estimation* stage, different *quantitative* and *qualitative* tools are available to perform an analysis on the risks. However, a method or tool is often not exclusively qualitative or quantitative. Nevertheless, this thesis distinguishes these two forms of approaches, because there is a difference in how the methods and tools are most commonly applied. Most of the findings about the different risk assessment methods and tools are based on the work by Rausand (2011).

Qualitative methods and tools are based on a simple model of risk assessment, comprising the two factors of risk: probability and impact. These factors are analyzed and assigned non-numerical values. They may include for instance high, medium, or low (Ostrom & Wilhelmsen, 2012). While these methods and tools are relatively simple in concept, it has been demonstrated to be useful for decision makers. A qualitative risk assessment is often performed when numerical data are inadequate or unavailable, resources are limited e.g. budget or expertise, and time allowed is reduced (Radu, 2009). Furthermore, it is frequently the case that a qualitative risk assessment is undertaken initially, with the intention of following up with a quantitative risk assessment if it is subsequently thought to be necessary or useful, and feasible (WHO, 2009).

Risk matrices have been widely praised and adopted as simple, effective approaches to qualitative risk assessment, since they provide a clear framework for systematic review of individual risks and collections of risks (Cox, 2008). As many risk practitioners have pointed out, constructing, using, and socializing risk matrices within an organization requires no special expertise of quantitative risk assessment methods or data analysis. An example of a risk matrix is provided in Figure 2.3.

There are two dimensions to a risk matrix, the probability and the impact. Furthermore, most risk matrices have at least three different areas:

- **Low probability - low impact** (green) indicates that the risk of an event is sufficiently controlled or not high enough. For events in this category, usually no action is taken.
- **Medium probability - medium impact** (yellow) indicates that an event that falls in this category requires monitoring and possibly measures to control the risk. Essentially, it means that if the risk is kept at the same level, we could accept it
- **High probability - high impact** (red) indicates that an event needs a significant amount of controlling measures to decrease the impact and probability of a risk event.

The risk matrix can be used from different perspectives. One could analyze the probability and impact of different scenarios, or the different risk events within these scenarios can assessed.

To illustrate the use of a risk matrix, we imagine a situation where road workers are preparing road work. During the preparation of road work, there are several scenarios that could influence

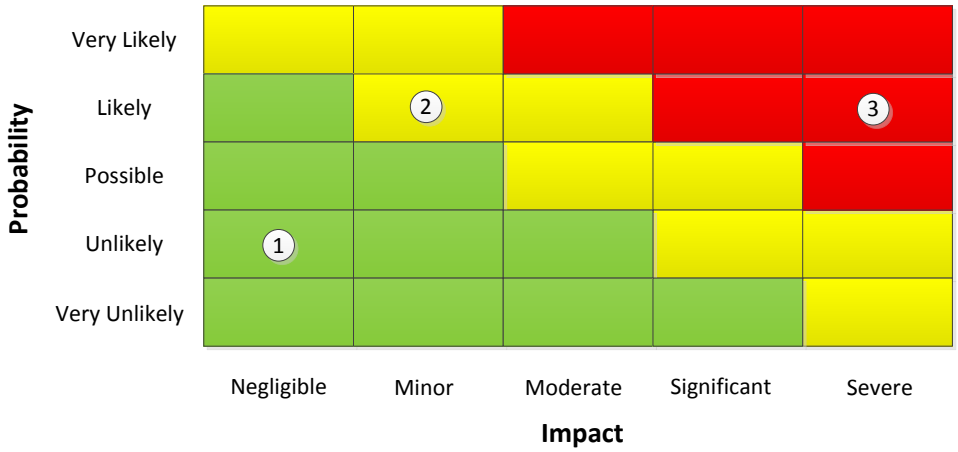

Figure 2.3: Risk matrix

the safety of the road workers. For instance, if we consider the traffic accident scenario as introduced in Section 2.1, this scenario can have a severe impact on the safety of the road workers. Furthermore, the chance of this scenario occurring is possible, thus, this scenario can be plotted on the risk matrix as (3). Another example is a "thunderstorm" scenario. Depending on the weather on the day of the road work, the occurrence probability of a thunderstorm could be likely. However, the impact of this scenario on the safety of the construction workers is probably minor. Taken the probability and impact into account, this scenario can then be plotted as (2). Now that we know the "traffic accident" scenario is in the red area of the matrix, and the "thunderstorm" scenario is in the yellow area, we can decide which scenario(s) require the most attention.

Besides the analysis of scenarios, the risk events within the scenarios can be examined. If we take the example of the traffic accident scenario, different risk events can be plotted on the risk matrix. Assuming that the risk factor is slippery roads, the "losing control of the car" event could possibly have a severe impact and likely probability on the occurrence of a traffic accident. On the risk matrix, the "losing control of the car" event could then be plotted as (3). An example of a risk event as represented by (1) could be "a leaf stuck behind the windshield wipers". The probability of this risk event is unlikely, and even if a leaf gets stuck behind a wiper, the impact is negligible. As with the analysis of scenarios, we can decide to first focus on the risk events in the red area, after which the less likely and severe risk events can be treated.

Although there are many risk matrices that have been developed, the development and application of risk matrices presents some challenges. To design an effective matrix, several characteristics have been defined by Ozog and Perry (2002):

- Be simple to use and understand

- Not require extensive knowledge of quantitative risk analysis
- Show how scenarios that are at an intolerable risk level can be mitigated to a tolerable risk level
- Provide clear guidance on what action is necessary to mitigate scenarios with intolerable risk levels

A qualitative risk assessment method is the use of a structured what-if scenarios technique (SWIFT). The SWIFT method is a systematic brainstorming session involving a group of experts with in-depth knowledge on the study object. The experts setup a checklist containing topics to gather information on, and raise what-if (or how-could) questions to identify possible risk events, causes and barriers. Subsequently, suggesting alternatives to mitigate risks. When applying SWIFT to the aforementioned example of construction workers preparing roadwork, a question could be phrased something like "what if the roadwork is extended past the set time limit?" or "how could an accident occur during road work?", By asking these questions, both risks and causes could be identified. An adapted version of the risk matrix can support this method, by serving as a tool to determine the frequency and severity of a risk event.

Hazard and operability studies (HAZOP) show similarities with SWIFT. Moreover, SWIFT can be used as an approach to identify quickly the risks for which it would be worth the investment of conducting a HAZOP (Card, Ward, & Clarkson, 2012). The main difference between SWIFT and HAZOP is that SWIFT uses what-if questions and checklists instead of guide words and process parameters, making a SWIFT analysis less detailed and thorough in comparison to a HAZOP approach. However, this also means that SWIFT is easier and faster to conduct, because SWIFT is less bound to predefined sets of rules. Applying the HAZOP method to our "roadwork example", we could define generic HAZOP guide words, such as "AFTER" and "OTHER THAN". The list of guide words is often extensive, but for illustration purposes we keep it basic. In addition to the guide words, some process parameters are defined, e.g. time and speed. During the brainstorming sessions, the HAZOP leader stimulates the discussion by asking questions, taking into account the guide words and process parameters. Such questions are for example "what could happen other than a driver ignoring the speed limit?" or "what could happen after the predetermined deadline is exceeded?". The answers to these questions can help in uncovering risk events, causes which can trigger a risk events, and possible consequences. Subsequently, frequency and severity values of risks can be estimated, and plotted on for example a risk matrix, to compare the risk of a risk event with acceptance criteria.

To identify causes and effects of a risk event, the failure mode, effects and criticality analysis (FMECA) method can be applied. The FMECA method grew out of a similar method: the failure mode and effect analysis (FMEA) (Dhillon, 2006), and has its origin in quality engineering. As can be deduced from their method names, the main difference between these two methods is that FMECA includes a criticality analysis. The added value of the criticality analysis is that it allows to add the risk priority number (RPN), which is computed by summing the frequency , severity and detectability of a failure mode, i.e. risk event. Including the RPN enables the prioritization of risks and can therefore support the decision-making process. To conduct a FMECA,

cause and effect diagrams can be used as a common and easy qualitative tool that requires no extensive training. A cause and effect diagram uses a "graphic fishbone" for depicting the cause and effect relationships between a risk event and its associated causes (Dhillon, 2006). To clarify this diagram, a cause and effect diagram tailored to our "traffic accident" scenario as introduced in Section 2.1 is illustrated in Figure 2.4 on page 22.

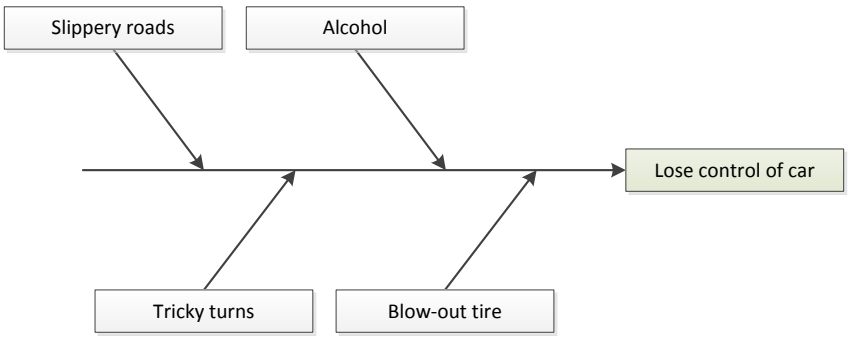

Figure 2.4: A cause and effect diagram

In this diagram, the causes which can result in the effect "losing control of the car" are depicted on the left-hand side, while the associated effect is presented on the right-hand side. In this example, the cause and effect diagram is rather simple. In practice, the different causes will possibly also consist of sub causes. By using a cause and effect diagram, risk assessor(s) are provided a means to easily understand and interpret risks.

Finally, a different kind of approach to risk assessment exist, which is based on argumentation. Krause, Fox, and Judson (1993) describe work to develop sound qualitative methods for risk assessment. Such methods can be used to express the reliability and accuracy of the evidence concerning a potential risk. Different approaches to define the state of evidence concerning risk estimates exists, but will not be elaborated on in this thesis. It is important to understand that risk classifications are often tailored to the organizational context of risk. In their work, Krause et al. (1993) focus on carcinogenic risk of chemical compounds and thus use classifications specific to that field. The general point that can be extracted from their research is that arguments for and against identified risk should be used when analyzing risks. Having constructed relevant arguments, a risk report can be generated based on the available evidence. The risk analysts can then ask for further explanation of available risks to generate additional explanations.

A method based on an argumentation based approach is RISA (RIsk assessment in Security Argumentation), which focuses on argumentation to guide the identification of risk and mitigating measures. The RISA method uses public catalogs of security expertise and empirical evidence to support risk assessment (Franqueira et al., 2011) and is an extension of the Security Framework by Haley, Laney, Moffett, and Nuseibeh (2008) in which the relevance of argumentation for risk assessment is addressed. In their Security Framework, software artifacts are separated into W (the system context), S (the specification of a system) and R (a description of the requirements). A schematic overview of the RISA method is provided in Figure 2.5 on page 24.

The contribution of RISA is to provide a systemic approach to assess risks associated with 'security arguments', i.e. arguments inferred from formal reasoning about to what extent a security requirement can be mitigated, taking into account the system context. The different catalogs are used to quickly identify known attacks and weaknesses, which are stored according to a standard schema. Even though this method is aimed at software systems, we could apply this method to our traffic accident example to illustrate its use.

Suppose we want to assess risks that could occur when we are driving from point A to point B. A *functional requirement* could be 'let the driver safely go from point A to point B'. The second step in the RISA method is to identify *security goals*, for instance to protect the driver from sliding of the road. To reach this goal, *security requirements* are described, e.g. roads need to be clean. This requirement can be satisfied by some *security functions*: sprinkle salt on roads, install winter tires. Prakken, Ionita, and Wieringa (2013) have further investigated the idea to formalize risk assessment in argumentation logic and have proposed a dialogue game, which can support the identification of security requirements.

With an understanding of the requirements, the *outer arguments* can be constructed. These outer arguments consist of one or more premises, which may represent risks, and can thus help in *identifying risks*. Outer arguments rely on properties of W and S, which represent the domain behaviour premises. The domain behaviour premises are the assumptions that are made about risk and which can turn out to be incorrect. The premises in an argument can be challenged by finding facts (based on arguments) about the argument (in a catalog), which form the risk related to the specific premise. These *inner arguments* are used to question the outer arguments'

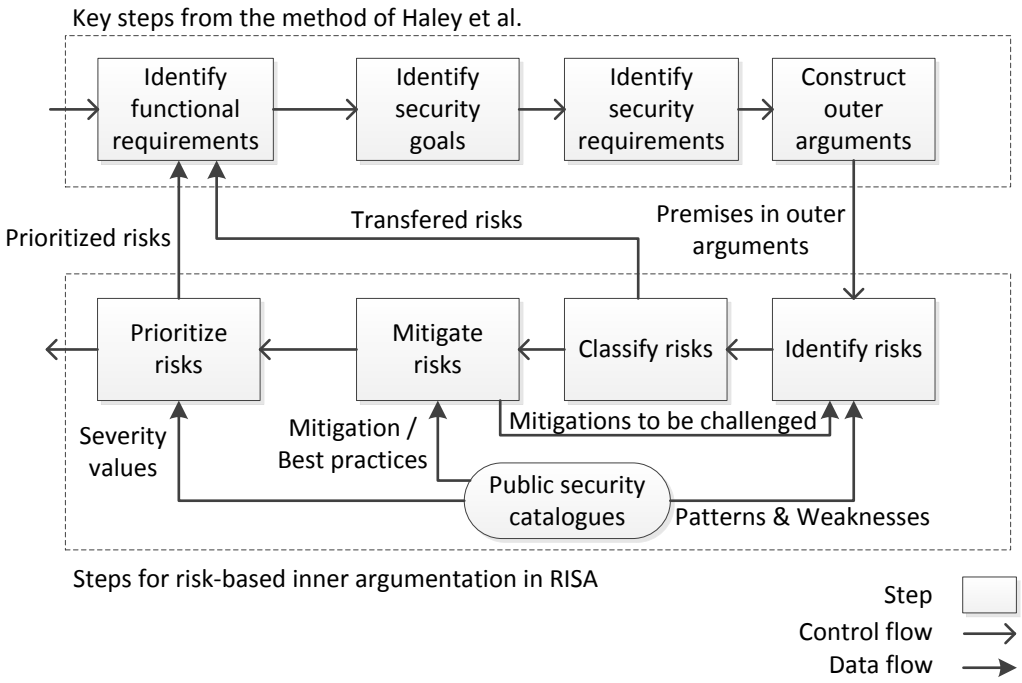

Figure 2.5: Schematic overview of the RISA method (adopted from Franqueira et al. (2011))

premises. As an example, we consider 'driver enters the road → (then) driver accelerates' as one of our domain behaviour premises (Figure 2.6 on page 25).

By means of inner arguments, the premises could be assigned some risks. For example, the premise with the ground 'driver enters the road' that implies the claim 'driver accelerates' could have a risk 'roads are slippery due to mud'. However, one could also argue about the identified risk by introducing new arguments that could rebut the established arguments. The risks are then *classified* into two groups. One group contains risks that cannot be mitigated by the system, e.g. the driving skills of the person driving down the road. In the other group are risks that should be mitigated by the system, e.g. the road conditions, safety signs, guardrails, et cetera.

Each of the identified risks could be mitigated, but mitigations may also introduce new risks, so for each mitigation a new iteration in step 5 is needed (Figure 2.5 on page 24). By mitigating all of the risks, we can be more certain that the driver can move from point A to B via the road without serious risks. In sum, the RISA method uses public catalogs with risk information and reasons about these risks by identifying, classifying, mitigating and prioritizing risks. These risks are then again used in the reasoning process to uncover more risks.

Quantitative methods and tools aim to deal with the subjectivity of qualitative methods and

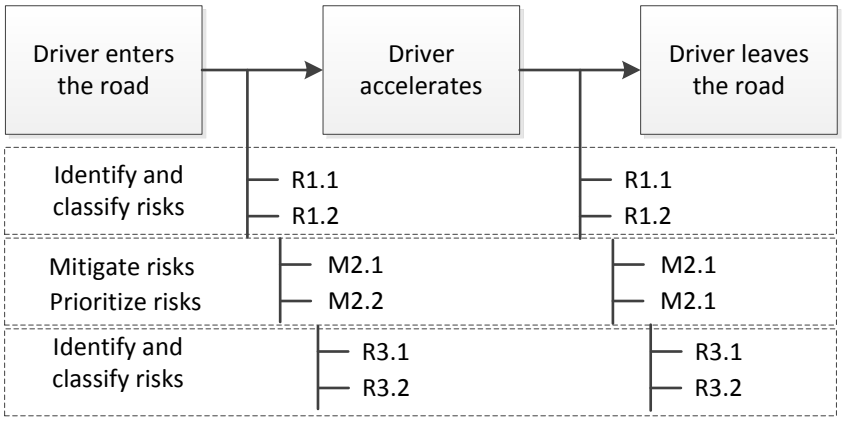

Figure 2.6: Premises of the traffic accident to be challenged via risk-based inner argumentation (adapted from Franqueira et al. (2011))

models. The added value of quantitative methods is that numerical values can be assigned to the probability and impact. This enables a more objective comparison and analysis of risks in contrast to purely qualitative tools, such as a risk matrix or cause and effect diagrams.

A popular quantitative tool for assessing risks and decision analysis is a Bayesian network, which reflect the states of (some part) of a world that is being modeled, and describes the relation between these states in terms of probability (Fenton & Neil, 2012). A Bayesian network is sometimes referred to as a Bayesian belief network, causal network, or belief network (Rausand, 2011). Perhaps the most important aspect of a Bayesian network is that it is a direct representation of the world, representing relationships and not merely the flow of information during reasoning (Fenton & Neil, 2012). Furthermore, reasoning with Bayesian networks is not bound to top-down only, but also supports bottom-up reasoning. The added value of this combined approach to reasoning lies in the ability to analyze risk from effect to consequence and vice versa , making it flexible and useful for risk assessment and decision making (Fenton & Neil, 2012). A simple Bayesian network based on the “traffic accident” scenario is visualized in Figure 2.7.

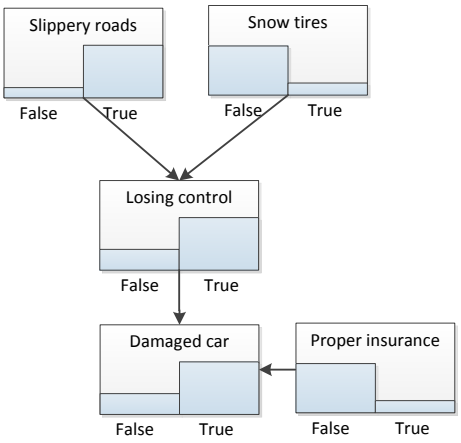

Figure 2.7: A Bayesian network

In addition to the graphical model, a Bayesian network requires probability tables, which depict the probability of events in the Bayesian network. For example, the probability of a damaged car being false is 0.085 if snow tires are not installed. However, if snow tires are installed, this probability jumps to 0.85. So, we can conclude that installing snow tires might be a smart thing to do if we do not want to lose control and finally damage our car.

A common used risk assessment method is a fault tree analysis (FTA). This method is well-documented and has been used in a wide range of application areas. A fault tree is a top-down logic diagram that displays relationships between a risks event and the causes of this event, and is considered one of the most used methods for risk and reliability studies (Rausand, 2011). When conducting a FTA, first the main risk event (in terms of FTA, top event) is defined. In our example in Figure 2.8, the top event is 'lose control of car'. Then the causes (e.g slippery roads (E_1), blow-out tire (E_2)) that will lead to the top event are identified and connected through a logic gate (e.g. OR, AND, NAND, etc). Next, the events that can lead to E_1 and E_2 are identified and also connected through a logic gate. This process repeats until a suitable level of detail is reached. As with Bayesian networks, a FTA can be combined with probability calculations to determine the probability of occurrence of the top event and its underlying causes.

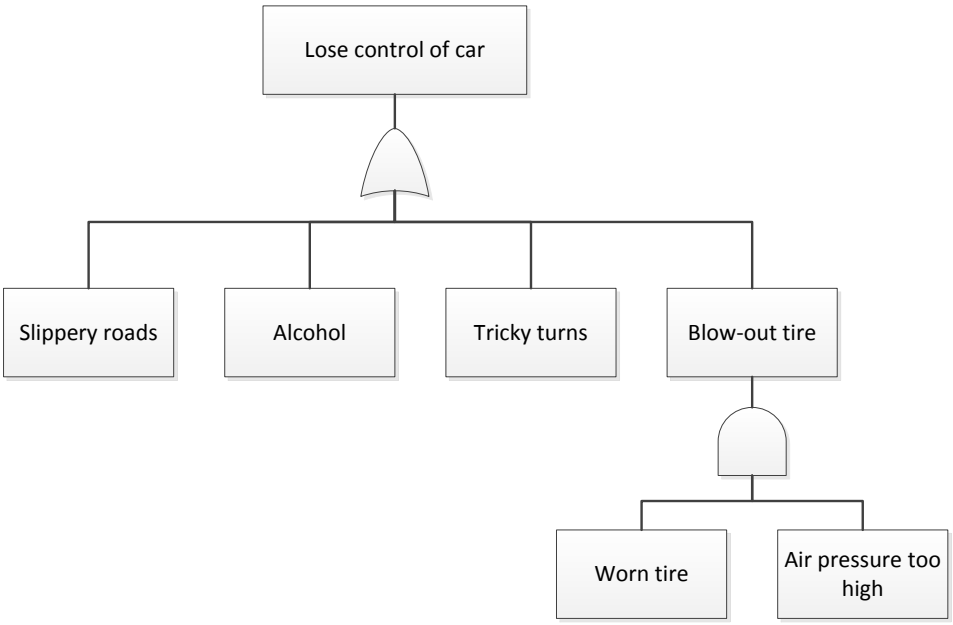

Figure 2.8: A fault-tree

A more powerful method than FTA is the Markov method (Gomes, Mota, Sampaio, Ferri, & Buzzi, 2010), aimed at the analysis of dynamic systems (Rausand, 2011). In the context of risk assessment, the Markov method is seen as complementing FTA, because it enables the analysis of small, complex and dynamic systems, which cannot be properly analyzed by using fault trees. However, in practice Markov models are more complex to handle, and thus, scarcely adopted (Gomes et al., 2010) by risk assessors.

A replacement for the Markov method are Petri nets, which can also be used as a tool for quantitative analysis of fault trees. The added value of Petri nets is expressed in the ability to include dynamic time-dependent behavior, enabling complex analysis of processes and sequences of risk events. Furthermore, Petri nets have the ability to model and improve fault tree analysis, by embedding the dynamic characteristics. An example of a Petri net tailored to our example case is depicted in Figure 2.9

This Petri net is basically a transformation of the fault-tree as depicted in Figure 2.8, but the possibility of adding different transitions (e.g. t_1, t_2) makes it more dynamic and provides a more comprehensive overview. In this example, P_1, P_2 ... P_7 are the system states. P_7 represents the "lose control of car" event which can be enabled by the transitions t_1, t_2, t_3, and t_4 if there is a token (so if one of the states is true) in either P_6, P_5, P_4, or P_3. Furthermore, if and only if P_1 and P_2 are true the transition t_5 can take place.

The discussed method and tools mainly revolve around the identification of possible causes of

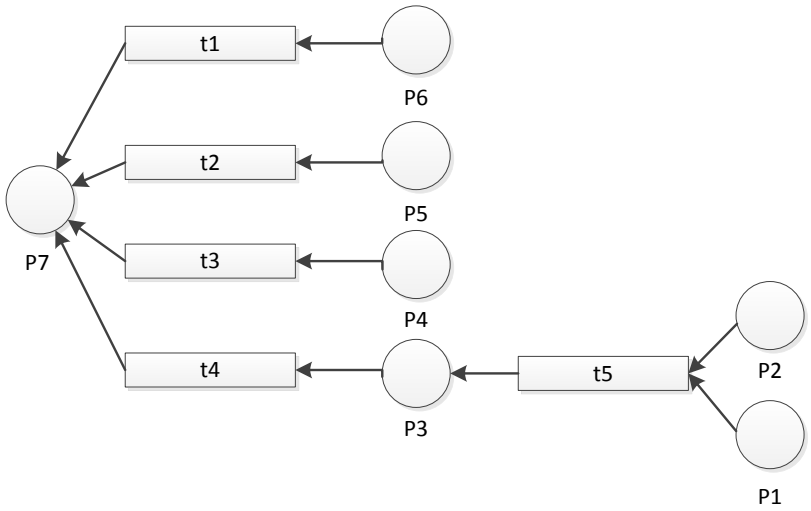

Figure 2.9: A Petri net

risk events. However, also consequences should be determined and analyzed in order to develop scenarios, and thereby a broad and in-depth understanding of the situation at hand. Event tree analysis (ETA) is by far the most commonly used method for the development and analysis of scenarios (Rausand, 2011), based on a probabilistic approach. ETA can incorporate fault-trees and is closely related to FTA (Xu & Bechta Dugan, 2004). A fault-tree and event-tree can both represent the same 'system'. Furthermore, a fault-tree can function as a branch point of an event-tree. To illustrate the use of an event-tree, we imagine the following scenario:

(A) The roads are slippery

(B) The tires lose traction

(C) ABS fails to intervene

(D) An accident cannot be avoided

If we transform this scenario to an event-tree, the tree as visualized in Figure 2.10 is created.

The event-tree should be interpreted as follows: if the roads are not slippery there is no reason for concern. If the roads are slippery, but the tires do not lose traction, the car is under control. However, if the tires do lose traction, but the ABS does not fail, the car is again stil under control, et cetera. The analysis ends when the level of detail is considered sufficient.

In the example we left out the probability values, however event-trees can include these values assigned to the different nodes to support more objective decision-making, comparable to Bayesian networks.

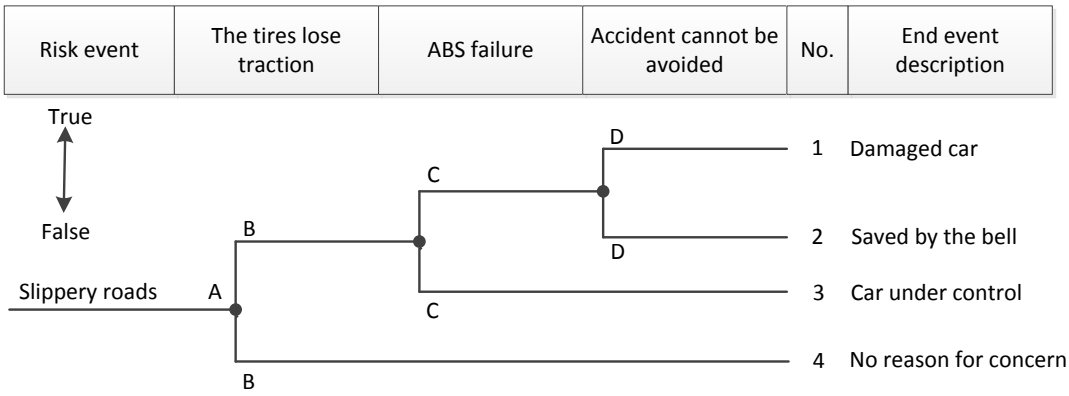

Figure 2.10: An event-tree

2.3.3 Risk evaluation

After analysis of the possible risks, a selection of most probable and highest impact scenarios is made. Furthermore, decided is whether the accompanying risks are acceptable, tolerable or whether they are serious enough to warrant treatment. The distinction between acceptable and tolerable is explained by HSE (1992, p. 2), who state that "to tolerate a risk means that we do not regard it as negligible or something we might ignore, but rather as something we need to keep under review and reduce". While, "for a risk to be 'acceptable' on the other hand means that for purposes of life or work, we are prepared to take it pretty well as it is".

To determine if a risk is acceptable, tolerable or warrants treatment, the *ALARP* principle can be adopted (Rausand, 2011). ALARP is an acronym for 'as low as reasonably practicable', and provides a framework for analyzing risk, in addition to a method to determine if the cost of a risk-reducing measure is disproportionate to the benefits it will provide, and hence if the measure should be implemented (Rausand, 2011). Alternative principles exist, such as the *ALARA principle*, the *GAMAB principle*, the *MEM principle*, the *precautionary principle*, and *societal risk criteria* (Rausand, 2011). The concepts behind these principles and criteria are almost identical, but differ on certain aspects from ALARP e.g. support for quantitative acceptance criterion or a different view on acceptability of risk. Nevertheless, the ALARP principle is considered the most common principle, and according to Aven (2007) and Aven and Vinnem (2005), risk acceptability evaluations must be based on ALARP-considerations. Because, static criteria fail to address the relationships among risks, benefits, and improvement (Rausand, 2011).

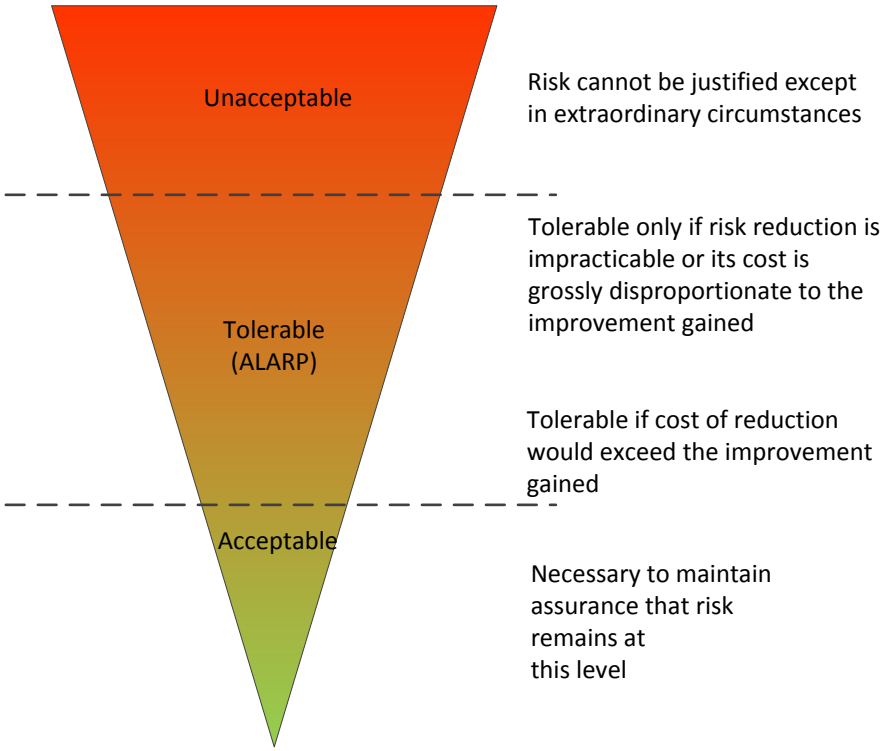

Figure 2.11: ALARP principle (adapted from Rausand (2011))

Rausand (2011) claims that the risk is mostly in the ALARP region, as depicted in Figure 2.11. However, the risk should be reduced to an ALARP level. To facilitate the determination of what reasonable risk reducing levels are, Rausand (2011) defined four components which should be considered:

- The severity of the risk event in question.
- The state of knowledge about a risk event, and the ways of preventing or mitigating its effects.
- The availability and suitability of ways to prevent the risk event or to mitigate its effects.
- The cost of preventing the risk event or mitigating its effects.

Although ALARP is useful for evaluating risk, it is recommended that practitioners interpret risk acceptance criteria as guiding benchmarks rather than rigid limits of acceptability (Rausand, 2011).

2.3.4 Risk reporting

After the risk assessment has been conducted and risks are defined, they should be reported (AIRMIC, 2002). This means that risk factors are described, that could eventually trigger a risk event. In addition, opportunities of triggering a risk factor are reported. Introducing or mitigating a risk can create opportunities to eventually mitigate other risks, since risks do not necessarily exist in isolation.

2.3.5 Risk treatment

In this stage, controls should be identified and described by an estimation of their effectiveness and the level of risk with controls in place (Berg, 2010). Furthermore, in case of the risk being greater than the tolerable risk, specific risks require additional controls or improvements in the effectiveness of the existing controls (Berg, 2010). Also, in this stage, what-if scenarios are constructed, which describe what happens if a certain control is applied to a scenario (den Hengst et al., 2014). Multi-criteria analysis methods can support the decision making by offering tools to check the probability and impact of a scenario after certain controls are applied (den Hengst et al., 2014).

To select the appropriate controls to mitigate the risk, a cost-benefit analysis should be performed on the risks and controls. This enables to decide on what a reasonable level of risk is (Rausand, 2011), and to make balanced decisions (den Hengst et al., 2014). The analysis is based on the following calculation as defined by Rausand (2011):

$$d = \frac{\text{cost of the risk reducing measure (control)}}{\text{benefit of the risk reduction}} \tag{2.3.1}$$

The value that is calculated by means of (2.3.1), is a factor *d*. To evaluate the cost and benefits, a limit d_0 should be defined. If the factor *d* as calculated by (2.3.1) is higher than d_0, the control should not be implemented. However, if the factor *d* is less than d_0, the control should be implemented.

2.3.6 Residual risk reporting

Even though in the "risk treatment" phase the aim is to treat and thereby eliminate *all* risks which have been labeled unacceptable, eliminating all risks is often not realistic. This means that there is some risk remaining after risk treatment, also known as residual risk. To treat residual risk, the previous phases should be repeated to reduce the risk to an as low as reasonably possible level.

2.3.7 Monitoring and review

The final stage in the risk management process is the monitoring and review of risks. Effective risk management requires a reporting and review structure to ensure that risks are effectively identified and assessed and that appropriate controls and responses are in place (AIRMIC, 2002).

According to AIRMIC (2002), any monitoring and review process should also determine whether:

- The measures adopted resulted in what was intended
- The procedures adopted and information gathered for undertaking the assessment were appropriate
- Improved knowledge would have helped to reach better decisions and identify what lessons could be learned for future assessments and management of risks

Also, the quality of the overall risk management process can be determined. This enables to monitor and improve the process. Several aspects have been defined by Cope (2004), which capture the quality. They are combined into the following formula as defined by den Hengst et al. (2014):

Quality of risk management

$$\text{Quality of risk management} = \text{correspondence} \times \text{coherence} \times \text{impact} \tag{2.3.2}$$

First of all, correspondence refers to the extent of which the identified risks and controls are in compliance with reality i.e. is the information that is being provided and used sufficient to map the risks. Second of all, the coherence entails if the available information is correctly analyzed, in the sense that useful information can be extracted from the risk analysis. Even though all the required information could be in place and readily available, this does not automatically mean that the information is processed in a correct manner, which subsequently affects the quality of the information. Finally, acceptance plays an important role in the risk management process. In case the risk analysis is rejected, valuable time and effort has been put into a product which is never used.

2.4 Limitations of risk assessment

As mentioned in Section 1.1, the current risk assessment methods and tools pose some limitations. The limitations of both the qualitative and quantitative side of current risk assessment are discussed in this section. To illustrate and explain the limitations of the different methods

and tools, an example case is used. This example is based on a real event from back in 2010. The background information used in the description below is based on the work by Helbing and Mukerji (2012) and Jaeger (2010).

Love land parade case

On 24 July 2010, the Love parade, a popular electronic dance music festival was held in Duisburg, Germany. Over 1.4 million visitors were expected on the 100.000 square meters large festival area. In response to concerns from the regulatory authority that the area would be too small for the expected number of visitors, the city of Duisburg added to the approval of the festival, the condition to restrict the number of concurrent visitors to 250.000. To overcome concerns regarding safety issues, a report was created, that argued that the festival area could be sufficiently well evacuated in an emergency situation. However, there were major safety concerns, since the whole event was to take place in an enclosed area, and the only way in and out was through a tunnel. When hundreds of thousands of people began to move through the tunnel towards the single entrance, people started to panic, resulting in a chain reaction of chaos, eventually creating injuries and killing people by suffocation. Three hours later more than 300 participants had been injured, 19 were dead.
During the preparation of the event, several parties were involved, ranging from the police to the organization to experts who applied complex simulations of pedestrian flows to uncover possible risks. However, the kind of accident that took place was not discussed as a possibility. Furthermore, the interaction between different risk events was not elaborated on. For instance, the organizers assumed that the possibility of inflow problems could be handled by "pushers"[3]. But, it was not considered what would happen if there was a shortage of pushers in case of a sudden increase of visitors. The lack of proper and comprehensive insight into (the interaction of) several risk factors and events led to a tragic outcome.

From the example it becomes clear that, even though advanced knowledge on pedestrian flows and mass panic was available, possible risks and controls were not properly identified and analyzed. To uncover risks and controls in more detail, and to develop a broader and better understanding of what could go wrong during the event, there was a need for more comprehensive risk assessment methods and tools. In this section we assess if the methods and tools as discussed in Section 2.3.2 could have been of value in this case and what the possible limitations are. First the applicability and limitations of the qualitative methods and tools are discussed.

As aforementioned, a popular and easy to understand risk assessment tool is a risk matrix. If we apply the concept of a risk matrix to the "Love parade case", the matrix could have supported the prioritization and analysis of risks, by creating an ordered list of less and more severe risk events. This tool does not require extensive knowledge on complex simulations and would

[3]Pushers are people, who are tasked to put pressure on visitors to keep moving

therefore be ideal as a communication vessel between the organization, the police, experts and other involved parties. However, Cox (2009) mentions that the common assumption that risk matrices do some good in helping to communicate and focus attention on the most serious problems is not necessarily justified, since risk matrices do not always provide qualitatively useful information for setting risk priorities and for identifying risks that are high enough to worry about and risks that are low enough to be neglected. The cause of this limitation, is the inability to analyze risk events simultaneously (Rausand, 2011), therefore, a risk matrix would be insufficient in the "Love parade case", because an analysis based on a risk matrix does not take into account the interaction between risk events. Also, the inability to analyze risk interactions limits the identification and mitigation of risks.

Another limitation of risk matrices can be related to the findings by Fenton and Neil (2005), who state that causal sequences of risk events can be of significant value for risk assessment. The reason for this, is that causal sequences can model multiple risks, from different perspectives, and common causes (Fenton & Neil, 2005), finally increasing the understanding of risk and turning risk into a meaningful story. In addition, consequences and controls can be captured in a causal model. However, risk matrices do not support the creation and analysis of causal sequences of events (scenarios). The inability of risk matrices to develop scenarios is also pointed Rausand (2011), who states that risk events can only be analyzed one by one rather than as a whole, while, risk decisions should be based on the accumulated risk of an activity. In the analysis of the "Love parade case" by Jaeger (2010) it is mentioned that "story-telling" would have been a valuable addition to the computer simulations, because stories (also known as scenarios) provide the opportunity to combine generalized insights with unique events. Furthermore, scenarios can give a much richer sense of the possibilities generated by a concrete situation compared to a computer model, because causes and effect of risk can be depicted in a much more accessible manner.

The concept of a risk matrix is based on the assignment of probability and impact values to scenarios or risk events. However, as mentioned in Section 2.1, assigning probability and impact values is difficult and can result in poor decision-making. The paradox involved in such an approach is that the more carefully one thinks about risk, the higher the overall risk score becomes. This could finally result in ignoring or under reporting risks to lower the risk score (Fenton & Neil, 2012). Furthermore, risks are often not independent of each other: treating one risk, may give rise to other unforeseen risk events. Taken the discussed limitations of a risk matrix approach into consideration, it becomes apparent that risk matrices would not have been of great value to risk assessment around the "Love parade", mainly because of the inability to, as Jaeger (2010) calls it, tell a story, and thereby develop scenarios.

As mentioned in Section 2.3.2, another commonly applied qualitative risk assessment method is a structured what-if technique (SWIFT) (Rausand, 2011). However, the downside of this method is that it is not always thorough, in the sense that identification of risks and controls is limited. The thoroughness of the results of a SWIFT analysis are highly dependent on checklists prepared in advance, and on the experience of the discussion leader and available knowledge within the team (Rausand, 2011). Applying this method to the "Love parade case", this method

could be valuable to identify possible risks. Questions like 'what if the 250.000 visitors limit is exceeded?' or 'what if there is a fire? Can the emergency services gain access?' could be asked. By answering the what-if questions, an overview can be gained of possible risks, but only on the topics as defined on the checklist. This means that there is a fair chance of overlooking risks that are not on the checklist. Furthermore, by asking questions based on a predefined and fixed checklist, SWIFT is not very flexible. Recalling the "Love parade case", this is undesirable, since this inflexibility can lead to missing out on potentially highly risky situations. Moreover, the inflexibility limits the development and analysis of risks and scenarios.

Methods like FMECA and HAZOP use qualitative tools, such as cause and effect diagrams, which may become very complex and requires patience from the participants (Rausand, 2011). Furthermore, cause and effect diagrams do not rank the causes in an 'if-then' manner (Rausand, 2011), but solely depict the causes that can lead to a risk event. Not being able to rank the causes in an 'if-then' manner complicates the construction of scenarios, because no insight can be gained into causal relations within scenarios. If cause and effect diagrams would have been used during the preparation of the Love parade festival, the involved parties could have developed an overview of different causes and consequences. However, since a large event such as the Love parade can have countless risks, it would have been nearly impossible and incomprehensible to create a cause and effect diagram for every single risk event. Furthermore, this would consume loads of time, which is often not available and will result in increased expenses.

Finally, the RISA method enables to reason about risk by defining formal arguments which can be challenged by arguments based on facts. However, the prioritization of risks are often based on entries from a catalog which indicates the severity of risks identified. This means that the risks are not considered as being part of a scenario where each risk can influence the severity of another risks. In the Love parade example, separate risks could have been identified using this method. However, it would have been more useful to capture the risks in a scenario to develop an understanding of the interaction between risks.

One of the most significant limitations of a quantitative approach to risk assessment is the complexity, due to the requirement of mathematical knowledge to calculate probability values. This also relates to the application of Bayesian networks, since as mentioned by Fenton and Neil (2011), while Bayes theorem is a rational way of revising beliefs in the light of observing new evidence (e.g. risks), it is not easily understood by people without a mathematical background. Furthermore, according to Rausand (2011), Bayesian networks require the use of a computer application even for very small systems. This poses difficulties to the applicability of this method, since such an application is not always readily available or requires additional costs for the development of a computer program.

The limitation of requiring a mathematical background can also be related to methods such as fault tree analysis (FTA). According to Rausand (2011), FTA is suitable for both qualitative and quantitative analysis. However, not very useful when working with dynamic systems. In addition, FTA can also become too rigid in its requirements regarding binary states and knowledge on Boolean logic (Rausand, 2011). Also, a fault-tree is single event-oriented, a separate

fault-tree must therefore be constructed for each potential risk event. So, when combining FTA with ETA, the construction of scenarios is not only a time-consuming task, but also a difficult task, because a single event-oriented approach does not allow for an easy and comprehensive overview of causal relations between risks, causes and consequences. Moreover, ETA revolves around probabilistic value calculations, which increases the complexity and efficiency if knowledge on probabilistic values is unavailable within a team of risk assessors. If these probability based methods and tools would have been adopted in the preparation of the Love parade, it is doubtful if it would have led to identification of more risks. There were some experts with knowledge on complex statistical simulations, but it cannot be expected that the other parties (police, organization) also posses this knowledge. Even though these parties can give valuable insight into the situation at hand and possible, yet unforeseen risk events are likely to be overlooked due to the difficulty of understanding probabilistic methods and tools.

Additional quantitative methods and tools can be distinguished, such as Markov methods and Petri nets. The main limitation of a Markov method is that it is not suitable for the identification of causes of risk (Rausand, 2011), and therefore provides insufficient information to construct scenarios. Furthermore, analysts may face some difficulties in translating extensive problems into a Markov model, because mainly small systems are suitable to be modeled in a Markov model. The complexity of a Markov model increase fast with the number of components in the system, and can therefore quickly become too complex to understand. According to Rausand (2011), the limitations of Markov methods also apply to Petri nets. Nevertheless, Petri nets are seen as very flexible and can be used to model any type of system/situation. For the graphical representation no special skills are required, only some basic understanding of the notation and terminology of Petri nets. However, for more complex situations and reliable decision-making, it is necessary to understand graph theory with its algorithms, theory of probability, and some reliability theory. In a situation such as the 'Love parade case', the requirement of specific knowledge on complex theories and Petri net terminology poses limitations to the effectiveness and applicability of a Petri net based approach. Furthermore, the biggest problem in the 'Love parade case' was the lack of insight into causes of risk. As aforementioned, Petri nets, like Markov methods, do not provide a way to identify causes, therefore Petri nets really would not have been of any added value in uncovering riks.

Concluding, in case one has no proper theoretical background or experience with quantitative methods, the interpretation of risks and the development of scenarios becomes near impossible. Adding to this the time most of these methods and tools consume before being able to apply them to assess risks and eventually develop scenarios, makes them less efficient for performing risk assessment in a dynamic environment, and where knowledge on mathematical and complex formal methods is scarce.

For an easy overview, the methods and tools as discussed in this section are listed in Appendix A, together with their limitations.

3

Risk assessment at the Dutch Police Force

As discussed in Section 1.2, risk assessment at the Dutch police force requires an improved and thorough approach when it comes to risk assessment around football events. First, a clear view on what an event in terms of the police is, should be obtained. According to den Hengst et al. (2014), an event can be defined as "a foreseeable or unforeseeable happening which is accessible to a gathering of people, is bound to a restricted time frame and bordered location, enables above-average risks to public order, safety, health or environment, and requires measures and collaboration from authorized authority". This thesis specifically focuses on risks that occur around football supporter flows i.e. yet unforeseen risks during the movement of hooligans from point A to point B.

This chapter will first give an overview of risk assessment at the Dutch police force aimed at football events in the Netherlands. Second, the information systems/sources and used methods and tools are elaborated on. Finally, limitations of the current risk assessment process are presented.

3.1 Background

Football matches are known to be subject of public order-incidents (den Hengst et al., 2014). According to research by the expertise centre in the field of football vandalism: "Centraal Informatiepunt Voetbalvandalisme (CIV)", every year around 600 to 700 incidents occur. Some of these incidents take place inside the football stadium. However, a significant amount of incidents take place outside the borders of the stadium: on the streets, in trains, parking lots

etc (Figure 3.1). Since hooliganism does not solely limit itself to violence inside the stadium, hooligans are increasingly becoming a threat to non-football related events.

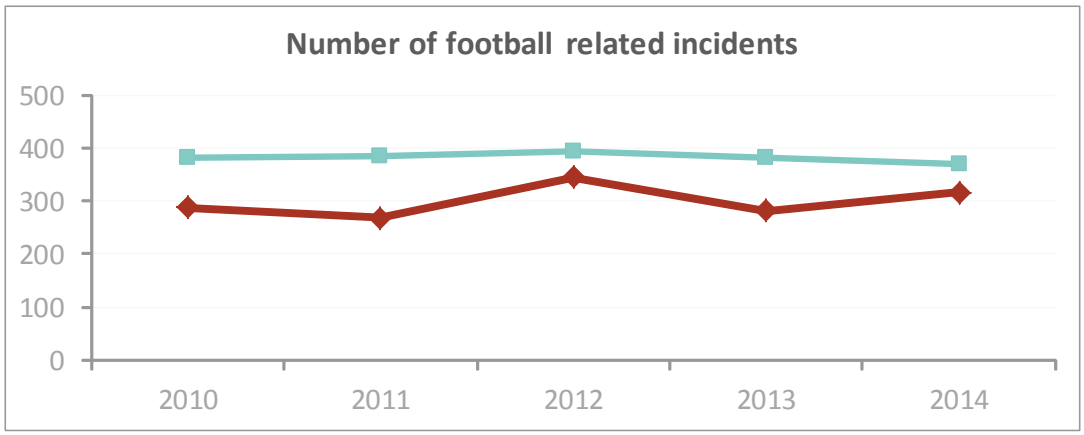

Figure 3.1: Number of football related incidents 2010 - 2014 ((CIV, 2013, 2014))

However, within the Dutch police force, there is no ready insight in how this hooligan related violence outside the football stadium evolves and where it is likely to take place. Also, there is no clear view on where violent clashes between different supporter groups are likely to take place. As a result of this lack of insight, the police forces are often missing out on possibilities to prevent vandalism or riots from escalating. One of the many examples of the damage done by hooligans is after a football match in April 2014 between two rivaling clubs: "Heracles Almelo - Ajax". While heading home from Almelo to Amsterdam, Ajax hooligans decided it was necessary to demolish the entire train they were in, resulting in a total damage of 40.000 euros. Since the train was already wrecked before it could reach its destination, the police force decided to stop the train. However, this posed a threat, because hooligans from another football club were informed of this and wanted to join the riots.

To decide on the appropriate measures to mitigate such risks around football events, six weeks prior to every professional football match, the police force, the municipality, and involved football clubs draw on the available information to assess the security risks associated with football matches. One week before the match, risk analysts evaluate the risk level, which is altered if needed. The information to perform a risk analysis is retrieved from different information sources which will be discussed in Section 3.2. After analysis of the information and discussion amongst the involved parties, models and methods, such as the CIV risk matrix as described in Section 3.3 are applied to gain insight in the possible risks. This results in the classification of a football match in a risk category as depicted in Table 3.1.

Each risk category has a specific set of risk mitigating measures, which are deemed appropriate for the level of risk. First, if a match is assigned label "A", the supporters are allowed to arrange

Risk level	Description	Explanation
A	Low risk	No extra risk of damage to persons or property compared to non-football events of a similar scale
B	Medium risk	Elevated risk of damage to persons or property due to poor spectator behavior or other circumstances
C	High risk	Potential danger to public order due to collective supporter behavior and/or extra risk due to special circumstances

Table 3.1: Risk classification of football matches

their own transport from and to the football stadium. Furthermore, there are no restrictions on the consumption of alcohol. Second, a category "B" label is assigned to a match if there is an increased chance of violence and vandalism. The measures taken by the municipality, organization and the police are restrictions on alcohol, and the possibility for supporters to make use of a so-called "combiregeling". This "combiregeling" entails that someone who bought an entrance ticket can travel to and from the stadium by bus or train, which is especially deployed for that purpose. The reason behind the "combiregeling" is that it should decrease the chance of unexpected supporter violence. Finally, if the match is assigned a "C" label, the "combiregeling" is compulsory for all supporters that travel to and from the stadium. Furthermore, there are strict prohibitions on the use and sale of alcohol.

3.2 Information systems and sources

To support risk management, different systems and databases are put in place, which can function as a source for performing risk assessments

One of the most substantial information sources is the 'Basis Voorziening Handhaving' (BVH) (enforcement information). The data source behind this system is an XML file containing cases and detailing nodes (descriptions). The relevance of this source lays in the extensiveness of the source in terms of amount of cases and detailing data.

In addition, sources such as the 'Bedrijfsprocessen Systeem' (processes information) (BPS) and 'Basis Voorziening Opsporing' (investigation information) (BVO) exist.

The expertise centre 'Centraal Informatiepunt Voetbalvandalisme' (CIV) focuses on collecting information concerning football vandalism, and distributing this information to the involved parties. The CIV was established in 1986 with the aim to collect, analyze and disseminate information on spectator behavior (Spaaij, 2013). In addition, the CIV advises on and supports in reducing football vandalism. A new data system 'Voetbal volgsysteem (VVS)' was created to facilitate this process (Spaaij, 2013). This database consists of so-called 'high-risk' supporters. From the database an overview of what are deemed to be the top 500 high-risk supporters in the Netherlands, as well as a top 10 of 'hooligans' in individual police districts, can be generated.

The objective of this data system is for all police forces to be aware who these supporters are in order to enable accurate risk assessment and to anticipate any potential misbehavior (Spaaij, 2013).

Finally, open sources such as the internet and social media are used. Also, information from the event organization and other actors can be gathered, for example general information about the event or information concerning security. Furthermore, information can be extracted from experts, employees etc. and reviews/analyses from previous years.

3.3 Methods, models, and tools

To determine risks and construct scenarios, several models and methods have been developed at the Dutch police force. On the one hand, models exist which support the identification of risks, such as the NIBRA and LOODS model. These models give guidance on what information to collect and which risk factors to take into account. On the other hand, methods exist that aim to provide the decision maker with some tools to assess risks.

3.3.1 NIBRA & LOODS

The development of the NIBRA model was initiated by the Dutch institute of fire and disaster management. The model appoints a variety of risk factors on which information should be collected, such as target audience, activities, space and organization (den Hengst et al., 2014). Among these factors are for instance the duration of an event/activity, relationship with the audience and between different groups, audience characteristics, accessibility etcetera. However, this model does not support the assessment of risk and scenarios, but merely the identification of risks (den Hengst et al., 2014).

The LOODS model aids in uncovering risks based on locations, conditions, objects, perpetrators and victims (den Hengst et al., 2014). By taking all of these aspects into account, insight in possible risks can be gained. Like the NIBRA model, this model aims solely at the identification of risks.

3.3.2 CIV risk matrix

To support the analysis of risks related to football events, a risk analysis matrix has been developed for the expertise centre 'CIV' in cooperation with the KNVB (Royal Dutch Football Association) and representatives of clubs and regional police forces. The philosophy behind this risk matrix is that it enables a systematic assessment of the security risks of football matches. Both police and clubs enter part of the risk matrix with information on risk factors and planned security and safety arrangements (Spaaij, 2013).

On the one hand, the risk matrix consists of a series of risk factors, accompanied by questions about home and away fans, such as the number of risky supporters, the number of fans with stadium bans, the mood of the supporters, the degree of rivalry between supporters groups and transport of the away fans. For a comprehensive list see Appendix B. The risk matrix itself can be found in Appendix C. For each risk factor, the risk is indicated on a five point scale. On the other hand, there are also some general factors which relate to the physical infrastructure in and around the stadium, media coverage about the match and possible match related entertainment (den Hengst et al., 2014). The risk factors are used to identify appropriate security measures, by assessing the risk on a five point scale. Among these measures are for instance restrictions on sales of alcohol, traveling and ticketing restrictions and decisions on the deployment of police officers. In addition, football clubs apply the matrix to determine the deployment of security personnel.

3.3.3 "Hooligans in beeld" (HIB)

The 'Hooligans in beeld' (HIB) method aims at documenting hooligans at supporter groups (den Hengst et al., 2014) in order to deanonymize hooligans. The focus is on collecting information concerning the role, behavior and the identity of individuals within violent groups, and the relations between groups. The collection of this data does not solely limit itself to football related events, but also focuses on gathering other available and possibly relevant data around problem behavior. Because the underlying information collecting method is dynamic, there is growing amount knowledge available which is derived from both information in systems such as the BHV and information provided by police in the field. However, den Hengst et al. (2014) and Ferwerda and Adang (2005) doubt that the method is complete, since more aspects, such as occasional disturbers should be taken into account.

3.3.4 Initiation/escalation model

The initiation/escalation model as developed by Adang (2010) aims at explaining both the initiation and escalation of collective violence. The model provides a comprehensive framework to understand why and how collective violence occurs. Furthermore, the model provides a guide as to what types of intervention can and will be effective (or counterproductive) in preventing collective violence from occurring or escalating and what types of intervention will not (Adang, 2010). According to this model, it is important to realize that the basic mechanisms for the emergence and escalation of collective violence are in essence the same for ideologically and not ideologically motivated perpetrators. Also, the factors that play a role in the emergence of collective violence differ from the factors that are responsible for the escalation of collective violence (Adang, 2007). In addition, the model clarifies why solely focusing on notorious violators is insufficient, since most violators do not act on a frequent basis, do not get caught, and are therefore not registered as violators (Muller et al., 2010).

When applying this model to an event where there is a possibility of collective violence, such as a football match, Muller et al. (2010) defined four questions which serve to support the risk analysis.

- what are potential irritants that could cause irritation or frustration at the event?
- are known (groups of) notorious violators planning on attending the event. If so, what are their intentions?
- what are specific opportunities for violence or disturbance?
- what are the social identities of the different (sub)groups visiting the event, what are the relations between these (sub)groups and the (sub)groups and authorities, police or organization? Which tensions flow out of these identities and relations?

When answering these questions and performing a risk analysis, the context of an event should be considered (Muller et al., 2010) e.g. use of alcohol and drugs, infrastructure, audience characteristics etc. Furthermore, when deciding on security and safety measures, the measures should be specifically aimed at the result of the risk analysis (Muller et al., 2010). This ensures that no counterproductive or unnecessary measures are taken, and prevents the aforementioned 'risk management of everything'.

The initiation/escalation model clearly distinguishes two types of factors, discussed in the following sub-sections.

Initiation

According to Adang (2010), collective violence is always initiated in two different ways: 1) as a response to a specific triggering event or 2) without a clear cause.

First of all, violence can initiate due to individual responses to an event, such as provocations, measures taken by the police or other identifiable causes. This type of violence is reactive (Adang, 2010), what means that it is performed in response to provocations or measures taken by the police. However, it is important to recognize that not every possible cause for violence will result in violence. Furthermore, it is not necessarily the case that individual violence results in collective violence (Adang, 2010).

Second of all, violence can initiate without a clear cause. In contrast to the aforementioned type of violence, this type is not reactive. Therefore, generally seen as coming out of the blue, even though these violent events are often planned up front (Adang, 2010). The involved parties actively search for opportunities to confront rival groups. According to Muller et al. (2010), the involved parties are nearly exclusively groups of young men (adolescents/young adults). The violence they convey is mainly aimed at comparable, rival groups of young men or representatives of a group. However, as Muller et al. (2010) mention, it is important to keep in mind that not in every situation where groups gather to use violence, this automatically results in

escalation of violence. Often there are some developing stages of violence where the groups first check if there is potential to initiate violence. In addition, the response of the police, and the willingness of rival groups to take part in collective violence is taken into account.

Escalation

To model and explain the escalation of collective violence, Adang (2010) defined two mechanisms: 1) the ability to commit violence without repercussions or negative consequences, and 2) the 'us-them' antagonism. These mechanisms can exist is isolation or can be treated as complementing each other.

As aforementioned, the first mechanism describes that collective violence can escalate when there are no repercussions or negative consequences bound to the violence. However, even in this case, only a small fraction of a group is likely to participate in direct physical violence against rival groups (Adang, 2010). The larger part chooses less risky alternatives, such as shouting, making gestures, or even remaining on the side lines. Also, according to Adang (2010), individuals are prone to avoid or mitigate unnecessary risks. Therefore, individuals try to mitigate risks by merging into a group where the focus is not on the individual. Furthermore, Adang (2010) claims that the occurrence and escalation of violence is less probable when police is present. In general, the police is more often avoided then confronted. This can also be related to football vandalism, where most clashes between hooligans and the police occur after the police have acted upon an incident.

The second mechanism, the 'us-them' antagonism, explains the frequency of collective violence (Muller et al., 2010): the more antagonistic the relationship is between two groups, the higher is the frequency of violence between these groups. Furthermore, Stott and Reicher (1998) point out that if the police treats a homogeneous group as a heterogeneous group, the members of that group develop a sense of community, thereby enabling the increase of tensions between groups and the police, and the escalation of violence.

3.4 Limitations of risk assessment

According to den Hengst et al. (2014), the current models and methods are not complete and do not deliver sufficient quality. This lack of completeness and quality is reflected in the insufficient identification of risk factors and controls, resulting in underdeveloped scenarios. A result of this is one of the aforementioned risks of risk management, 'the risk management of everything', since the models and methods do not provide a means to identify relevant information.

In general, den Hengst et al. (2014) mention that risk analysis at the Dutch police force is insufficiently systematic and too much based on (past) experience. Furthermore, Muller et al. (2010) mention that the search for an increasingly more complex and extended risk model, which contains and takes into account all possible risk factors, will finally result in an instrument which

will be inefficient and too complex to use. The reason for this is that such a model would end up as an extensive list of risk factors, lacking any structure or theoretical background (Muller et al., 2010).

However, the main limitation of the current risk assessment models and methods is that possible risk scenarios are often not sufficiently described and discussed in detail (den Hengst et al., 2014), resulting in an unclear view of risk evoking activities, people and other risk events. The same applies to controls to mitigate risks. den Hengst et al. (2014) also mentions, that in case both scenarios and controls are defined, there is not always a connection between identified risk factors, scenarios and controls. Consequently, decreasing the quality of the risk analysis, because less risk factors, scenarios and controls are acted upon. Finally, resulting in lower quality risk analysis (den Hengst et al., 2014). The lower quality is reflected in less identified risk factors, scenarios and controls. Therefore, increasing the probability and impact of risks. In Section 4.1.1, the notion and importance of scenarios is explained.

4

Requirements for a risk assessment model

In this chapter, the requirements for our risk assessment model are analyzed, taking into account the limitations and issues of current risk assessment methods and tools as discussed in Section 2.4. In addition, the principles defined in Section 2.2 are included, because the principles define the requirements for achieving the best possible outcome, while at the same time reducing the uncertainty of outcomes (Hopkin, 2012). Therefore, useful to keep in mind when defining a risk assessment model. Finally, also the limitations of risk assessment models and tools of the Dutch police force, as described in Section 3.4, and the requirements as defined by Adang and Brown (2008), are considered in the risk assessment model. These requirements are relevant, since they are based on extensive research in the policing domain in both the Netherlands and abroad (mainly The United Kingdom). Thus, originating from an environment where availability of knowledge on mathematical and statistical models is often scarce (Adang & Brown, 2008), and where scenarios are underdeveloped or not analyzed properly (den Hengst et al., 2014).

4.1 Requirements analysis

From the limitations as discussed in Section 2.4 and Section 3.4, it becomes apparent that more interactive models are needed, which take into account causal relations between risk factors, to be able to construct a complete and coherent view on possible risks, causes, consequences and controls by facilitating the construction of possible risk scenarios. At the same time, this would facilitate zooming in on relevant information (den Hengst et al., 2014). Furthermore, we derived some quality requirements from the literature: 1) the model should offer an accessible

way of assessing risks, 2) the model should offer a systematic approach, and 3) the model should enable dynamic risk assessment, where risks and controls are easily uncovered.

This following section first describes the notion and importance of coherent scenario. The identified quality requirements are discussed and explained in detail in Section 4.1.2.

4.1.1 Scenarios

The findings drawn from research into the possibilities and limitations of risk assessment methods and tools in general, and at the Dutch police force, show that current risk assessment methods and tools lack the possibility to construct and analyze coherent scenarios. The coherence measure, as defined in Section 2.3.7 is met if available information is correctly analyzed, in the sense that information to mitigate risks (to an ALARP level) can be extracted from the risk analysis (den Hengst et al., 2014). Thus, being able to develop coherent scenarios enables to mitigate risks to an as low as reasonably possible level.

In case the methods and tools, such as a Bayesian network, do facilitate in-depth assessment of risks, they are dependent on complex mathematical or statistical calculations, such as probability values. Not being able to properly construct and analyze scenarios in detail is a major shortcoming, because this limits the identification and analysis of risk factors and controls. According to Roxburgh (2009) scenarios have two benefits that make them very powerful for understanding risks.

First, scenarios expand one's thinking. People will think more broadly if they develop a range of possible outcomes. By demonstrating how and why things could quickly become better or worse, we increase our readiness for the range of future possibilities. Furthermore, scenarios force someone to ask what would have to be true for a risk to emerge. As a result, a wide range of hypothesis are tested involving changes in all sorts of underlying risks.

Second, scenarios uncover inevitable or near-inevitable futures. When developing scenarios, people will search for predetermined outcomes. Particularly unexpected outcomes are often the most dominant sources of new insight in the scenario development process.

The importance of a scenario based approach is also pointed out by Fenton and Neil (2012). In their research they propose the use of a causal framework for risk, instead of the common "Risk $=$ probability(event) $\times$ impact(event)" (2.1.1) approach. In this way, risks can be turned into meaningful stories. Turning risks into stories, can improve current risk assessment methods, by creating causal sequences of risk events which can model multiple risks, from different perspectives, and common causes (Fenton & Neil, 2005), thereby increasing the understanding of risk. Furthermore, consequences and controls can be captured in the causal model (Fenton & Neil, 2005). Finally, Fenton and Neil (2012) argue that the common approach is quite useful for prioritizing risks, however normally not very useful for assessing risks, since it is difficult and sometimes not doable to calculate probability values, because of the requirement of mathematical knowledge. All in all, adopting the concept of a causal model would benefit a risk assessment

model, because as argued by Fenton and Neil (2012), a causal approach can increase the understanding of risk, and enables the development of scenarios which tell a complete story. Finally, resulting in increased identification and analysis of risks and controls, without mathematical knowledge.

As mentioned in Section 4.1.1, scenarios enable to simultaneously examine risk factors, risk events and controls, in detail. As a result, risks can be detected and acted upon in a timely matter. As argued in Section 4.1.1, a causal model would benefit a risk assessment method by turning risks into causal structures and coherent scenarios.

4.1.2 Quality requirements

In addition to the requirement of enabling the construction of scenarios, some quality requirements can be defined. The requirements are extracted from the limitations as discussed in Section 2.4, Section 3.4, and the principles from Section 2.2 and Section 2.3.7. This section will provide an explanation of the different requirements.

Accessible

A major limitation of current risk assessment methods and tools, is that they are often dependent on complex mathematical or statistical knowledge, such as probability values. And even if they do not depend on a such knowledge, none of them provides an easy, but comprehensive method to analyze scenarios. Therfore, the model should be accessible by everyday reasoners. So to ensure the accessibility of our model, an alternative view on risk should be offered in which risk scenarios can be constructed and risk factors and controls be uncovered.

Systematic

Finally, the risk assessment model should be *systematic*, but *flexible*. A systematic approach enables a structured, and finally comprehensive risk assessment process. To be applicable in dynamic environments, the risk assessment model should also be flexible. This flexibility is reflected in the ability to identify and analyze new risks, control and scenarios, without much effort.

Dynamic

Since risk assessment and its sub-processes are iterative, but dynamic, a risk assessment model should be able to facilitate the identification of new risks and controls in each stage of the risk assessment process. This means that during the development of risk scenarios it should be possible to add new risk factors to a risk scenario, in addition to the application of controls.

The risk assessment process should be considered finished if a consensus is reached over the possible risk scenarios.

4.2 Results

Taking all the discussed requirements into consideration, a risk assessment model should enable the construction of possible risk scenarios, while being accessible, systematic and dynamic. To develop such as model, we adopt the concepts and ideas as presented in the hybrid theory by Bex et al. (2010). The hybrid theory has its roots in the fields of artificial intelligence and law, and can be used to make sense of evidential data, i.e. documents/expert opinions/etc. to support or attack a scenario. In Chapter 5, we elaborate on the hyrid theory by providing an explanation of the concepts. In sum, the hybrid theory enables the use of a causal model for the creation and analysis of causal and coherent scenarios. Thereby, improving the identification and analysis of risks and controls.

Furthermore, a model based on the hybrid theory is not dependent on the availability of mathematical or statistical knowledge to calculate probabilities. In addition, a risk assessment model based on the hybrid theory is dynamic, because new evidence can easily be added to a scenario, thereby fostering the understandability of the risk at hand.

Finally, the hybrid theory can be applied as a systematic approach, while remaining flexible. New risk, controls, and scenarios can be identified and analyzed easily.

5

The hybrid theory

In this chapter the hybrid theory as developed by Bex (2011) is described. Furthermore, the different concepts of the hybrid theory are explained and elaborated on.

5.1 Background

As explained in Section 1.2 the hybrid theory consists of a combination of two different approaches to sense-making: the story-based approach and the argument-based approach[1]. Stories can provide an overview about what happened in a case by structuring and analyzing available evidence, and are modeled as simple causal networks consisting of various events. The relations between events in a story and between the story and the evidence can be modeled as causal generalizations.

The argument-based approach can then be applied to construct arguments by performing consecutive reasoning steps, from evidence towards a conclusion. Subsequently, the arguments can be used to support or attack causal links between events in the stories and to reason about the validity of the stories. Thus, arguments can function as a connection between the evidential data and the facts of a case. In this way, arguments can be used to structure and analyze reasoning. Furthermore, arguments based on evidence can be used to attack or support other arguments. Arguments that are overruled are never considered strong enough to influence the extent to which a story conforms to the evidence. Finally, arguments can attack and support causal generalizations in a story (Bex, 2011). In this context, generalizations are general knowledge or knowledge from experience, for instance, that if a person X and Y meet, they will fight.

[1]The concepts and ideas in this chapter are largely based on the work by Bex (2011)

By supporting and attacking arguments, the *evidential support* of a story can be determined, that is, "the extent to which a story conforms to the evidence" (Bex, 2011, p.85). In the same sense, the *evidential contradiction* of a story can be defined as "the set of all pieces of evidence that contradict some element (i.e. a state, event or causal relation) in a story" (Bex, 2011, p.86). A feature of scenarios that is closely related to evidential support and contradiction, is that an *evidential* gap, which is "a state or event for which there is no direct evidence" (Bex, 2011, p.86).

As mentioned in Chapter 1, the hybrid theory enables the model to be natural so that it can be used by an everyday reasoner such as a crime analyst, who cannot be expected to have in-depth knowledge of mathematical or formal models. To assess the quality of the stories, Bex (2011) defined several criteria, which can be phrased as critical questions. These critical questions can be used to guide an analysis of what happened in a case, and can aid in uncovering sources of doubt in the stories.

To determine if a story makes sense and can be considered useful, the coherence of the story should be determined. As mentioned in Section 1.2 a story is coherent if it is plausible, consistent and complete. Firstly, the plausibility requirement can be split up in two: internal plausibility and a plausible story scheme. Internal plausibility entails that the story's events and causal relations that are not based on evidence should be plausible in that they follow from our general knowledge. If we for example would claim that John lost control of the car because he got hit by a meteorite this does not sound plausible, since we know that the chance of a meteorite hitting the earth is negligible let alone hitting a car. Secondly, the story should be consistent, what means that the story should not clearly contradict itself. For instance, if a story claims that John was driving the car at the time of the accident, while Jane was also driving the same car at the exact same moment the story clearly is not consistent. Finally, the story should be complete, that is, it should correspond to all elements of a story scheme.

In addition to stories and arguments, the hybrid theory includes the concepts of story schemes and argumentation schemes. According to Bex, Prakken, Reed, and Walton (2003) argumentation schemes play an important role in reasoning with evidence, and represent patterns in human reasoning comparable to generalizations in the form of rules. The term story schemes was coined by Bex (2009), and can be seen as scripts, which consist of a specific structure and help in understanding stories by filling in missing information. The different concepts are discussed in more detail in the following section.

5.2 Concepts of the hybrid theory

As can be deduced from the previous section, the hybrid theory is composed of several concepts. First we will discuss the notion of arguments and argumentation schemes. Second, stories and story schemes are explained. Also, we will discuss how arguments and stories can be combined to facilitate a reliable and coherent reasoning process.

Arguments are used in everyday life and give people the ability to understand and solve problems, express and defend their opinions (Dung, 1995), and to learn from each other. According to Van den Braak (2010, pp.28) arguments are "structures of inferences between different claims leading from premises to conclusions". Associated with a defeasible inference is a generalization which justifies the inference link between premises and conclusion (Bex et al., 2010). For example, if we take the "losing control of the car" scenario as mentioned above, evidence in this case could be that "Jane saw that John was texting while driving". A generalization could be "if a witness saw 'p' then p". So, by introducing and applying this generalization we could support the evidence that John lost control of the car, because there was someone who saw that John was texting. A generalization does not necessarily have to be defined as a rule, but can as mentioned above also be phrased in a non-rule based way, for instance "a witness always speaks the thruth".

To support reasoning with arguments, argumentation schemes can be used. According to Bex (2011) argumentation schemes play an important role in reasoning with evidence. In his work Bex (2011) argues that such schemes represent stereotypical patterns of how humans reason and are closely related to the above mentioned generalizations, because argumentation schemes are also viewed as conditional rules. Argumentation schemes consist of one or more premises, a conclusion and critical questions. These critical questions can point to possible sources of doubt in an argument by capturing if the premises and conclusion in the argumentation scheme can be invalidated. Negative answers to the critical questions can lead to different (types of) counterarguments (Van den Braak, 2010). A well-known example of an argumentation scheme is the scheme for argument from expert opinion (Walton, 1996).

Argumentation scheme example

Source *e* is an expert in domain *d*.
e asserts that proposition *a* is known to be true (false).
a is within *d*.
Therefore, *a* may plausibly be taken to be true (false).

In his work Walton (1996) provides this argumentation scheme with a set of critical questions which can be used in a question-answer dialogue:

Critical questions

- **Expertise Question:** How credible is *e* as an expert source?
- **Field Question:** Is *e* an expert in *d*?
- **Opinion Question:** What did *e* assert that implies *a*?

- **Trustworthiness Question:** Is *e* personally reliable as a source?
- **Consistency Question:** Is *a* consistent with what other experts assert?
- **Backup Evidence Question:** Is *a*'s assertion based on evidence?

Above (Chapter 1), it was mentioned that stories can provide information about what happened in a case, by structuring and analyzing available evidence (Bex et al., 2010). The reason why stories are useful for describing a case, is that stories are a natural way of communicating information. Bex (2011, pp. 59) defines a story as "a particular, coherent and chronologically ordered sequence of states and events". An important concept in this definition is "coherence". To determine if a story is coherent, a story should adhere to two requirements. First, the story should not contain contradictions. We can for example not claim that John is driving a car and that John is not driving a car at the same time. Second, a story should be structured as a causal combination of events. If a story is not causally structured it is very unlikely to make any sense, because the connection between one event to the following event cannot be deduced from the story. If we for instance say "I was driving in a car" followed up by "I lost control of the car", we have no clue about what caused loss of control: is it for instance because of a blown-out tire, slippery roads or ABS failure. The causal relations within a story are not necessarily explicit, but can also be implicit. However, the causal relations in a story can be made explicit by expressing them as conditional statements, which are essentially causal generalizations (Bex, 2011). So, for instance we could define a generalization "if the roads are slippery, then the driver may lose control of the car". By including this generalization in our reasoning about how the story evolved from driving a car to losing control of the car, the story makes way more sense and thus improves the understanding of the case at hand.

In addition to causal generalizations, story schemes can be distinguished. As mentioned above, story schemes can help in understanding stories by filling in missing information and represent typical stories that often occur in for example criminal cases. The difference between generalizations and story schemes is that a generalization can be seen as a general background for a single inference, while a story scheme is a more complex structure used to act as general background for a story. Such schemes are modelled as an ordered list of events or types of events together with the possible relations between these events (Bex, 2009). An example of a story scheme is:

Story scheme

- **Anomaly that the scheme explains:** person *x* is dead.
- **Central action of the scheme:** person *x* crashed vehicle *v*.
- **Other relevant information:** the reason *r*, the time of dead *t*, the place of the

accident p, the activities before the accident a.

- **Pattern of actions:** person x is conducting an activity $a \rightarrow$ person x ends up in ditch with his vehicle v for reason $r \rightarrow$ person x is dead.
- **More specific kinds of accidents with vehicles involved:** single sided accidents, accidents with more vehicles involved.

Our story, with the variables in the story scheme replaced by constants could now, for instance read: John is at a party where everybody drinks → John ends up in ditch with car because he drank alcohol → John is dead.

However, a pitfall of both generalizations and story schemes is that they might express non-realistic situations, false beliefs etc. In a story like:

> “John had a party where most of the guests were drunk. John stepped into the car. John ended up in the ditch with his car.”

Someone is likely to believe that John was drunk because most of the guests were drunk, and this could explain why he lost control of his car, even though this is not mentioned in the story and not necessarily true. So, for a story scheme to be useful it should be made explicit to increase the reliability of a story scheme by making clear how the story scheme is used and which sources were used to derive the scheme. Like with argumentation schemes, story schemes can also be accompanied by critical questions to expose sources of doubt in a story scheme.

In this section we discussed that there exist two different approaches to reasoning: the argument-based approach and the story-based approach. According to Bex, Prakken, and Verheij (2007) there are a number of reasons not to choose for one of the separate approaches. First of all, even though an argument-based approach to reasoning provides a way of analyzing and assessing reasoning with evidence, argumentative reasoning is not always the most natural way of expressing knowledge. The reason for this is that arguments do not allow to generate a complete overview of a case, because no causal relations between evidence and other elements within a case can be expressed or reasoned about. This finally limits the uncovering of new possible evidence. Second of all, because the argument-based approach is not really suited for providing an overview it is less natural when it comes to organizing a collection of evidence compared to scenarios. However, to examine in detail how individual pieces of evidential data support elements in a scenario to improve the analysis process, it is needed to include an argument-based approach. So, the story-based component enables the construction of scenarios, that is hypotheses about what happened in case, while the arguments in the argument-based component can be used to support or attack these scenarios by enabling a thorough analysis of the evidential data. What this means is that discussions about individual elements of a case, such

as pieces of evidence, generalizations and elements of a story, are possible and can be organized to give an overview of a case. To be able to accept an explanation of a story the evidence should be supported by non-overruled arguments.

6

Risk Assessment model: anRAm

In this chapter it is described how the argumentative-narrative risk assessment model (anRAm) is constructed by explaining how the hybrid theory can be related to risk assessment taking into account the challenges that will be discussed in Section 6.1. An overview of our model is provided in Section 6.2. To understand the syntax of our model, an explanation of the syntax used in anRAm is provided in Section 6.3. Subsequently, an explanation of the concepts in our model is provided given. How the concepts can be applied and combined will be touched upon in Section 6.8 and Section 6.9. To clarify and illustrate how the concepts of the hybrid theory can be translated to risk assessment we will use fictitious examples throughout this chapter, which relate to the problems the Dutch police force is facing around football supporter flows as discussed in Chapter 3.

6.1 Challenges

When applying the hybrid theory to risk assessment, there are some challenges to overcome: 1) uncovering of risk factors and controls, 2) comparing scenarios. In this section, the different challenges are introduced. How these challenges can be dealt with is explained in Section 6.9 and Section 6.10.

Challenge: Uncovering risk factors and controls

The hybrid theory usually revolves around the analysis and explanation of evidence about what *has happened* in a case. These scenarios are based on a main explanandum: the main piece of evidence that has to be explained, i.e. the conclusion of the scenario. The

explanandum can be justifiably inferred from some evidence. For instance, the event that Ajax and Feyenoord supporters had a fight some weeks ago can be justifiably inferred from a police report. Since the core of risk assessment is to identify and analyze possible risks in the future, we want to explain what *could happen*. So instead of explaining some events, we want to predict possible events. To predict future events we cannot assume there is some explanandum, because there is no justified evidence that exactly that will take place. So instead of having an explanandum which states that Ajax and Feyenoord supporters had a fight some weeks ago, in risk assessment one wants to find evidence that supports Ajax and Feyenoord supporters could get into a fight. The difference here is that in the hybrid theory the explandum can be considered a fact which is already justified, but in risk assessment we search for possible causes that could justify a possible event.

Challenge: Comparing scenarios

Since multiple scenarios can be constructed, we should be able prioritize the scenarios to compare different scenarios and decide on which ones warrant the most treatment. As mentioned in Section 6.2, risk is defined as 'probability x impact' (2.1.1). However, in our model the probability is omitted, because as argued above, a quantitative probability measure relies on complex mathematical principles. Furthermore, a probability-based approach could require a significant amount of estimated probability values from the risk analyst. A qualitative probability measure could be used instead, but as also argued above, qualitative values do not always deliver sufficient level of insight to prioritize risks. One of the requirements of our model is to keep risk assessment simple and accessible, but comprehensive.

6.2 Overview

As explained in Chapter 5, a model using the hybrid theory is based on research on how we understand the world and how humans reason (Bex, 2011). This means that no mathematical knowledge on probability values is needed, but intuitive concepts of arguments and counterarguments can be used to construct and analyze hypothetical scenarios. The different concepts of the hybrid theory and the corresponding concepts of risk assessment when applied to the hybrid theory, are depicted in Figure 6.1. The concepts with the dotted borders are newly added concepts to risk assessment and are specific to anRAm. In this section an overview is provided of the different concepts in our model. The concepts will be explained in detail in the following sections.

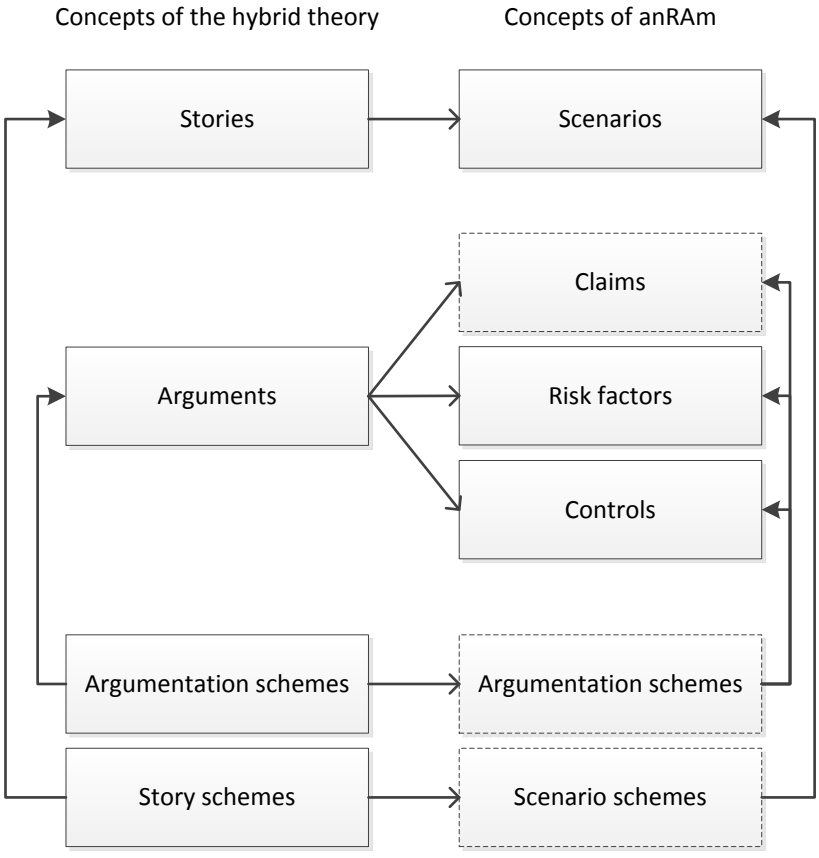

Figure 6.1: Concepts of the hybrid theory translated to risk assessment

When applying the hybrid theory to the field of risk assessment, stories can be seen as the hypothetical scenarios inferred from of one or more risk factors. In a story-based approach,

scenarios are modelled as an ordered sequence of events and serve as an hypothetical explanation of the evidence in a case. To support the construction of scenarios, the hybrid theory provides the concept of story schemes, which are essentially uninstantiated risk scenarios. In our model, these story schemes are called scenario schemes and serve the same purpose as they do in the hybrid theory: to help in understanding scenarios by filling in missing information.

In addition to stories and story schemes, the hybrid theory consists of evidential arguments and argumentation schemes. An evidential argument is an argument based on some evidence. In our model, an evidential argument can take the form of a risk factor, control or remark. In addition to evidential arguments our model consists of claims, which are the conclusion of an argument and are not necessarily supported by some evidence, because there might be no substantial evidence to do so or because there is no need to argue about the conclusion.

6.3 Syntax

The syntax used in our model to depict the different concepts is listed below. A short explanation of each different concept is given. In Section 6.2 the concepts will be explained in greater detail.

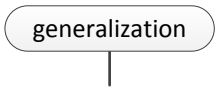

Figure 6.2: A generalization

Before explaining the syntax of scenarios and arguments, first generalizations should be explained, since they function as the glue between different elements in a scenario or argument. Generalizations are "generalized statements about how we think the world around us works, about human actions and intentions, about the environment and about the interaction between humans and their environment" (Bex, 2011, p.17). In our model, a generalization is rendered as a a rounded box (Figure 6.2). A line connects the generalization to an attack or support relation.

Figure 6.3: Support and attack links with implicit generalizations

We distinguish between two types of relations: support and attack (Figure 6.4). The links between the different risk events that construct the risk scenario express a generalization of the form '*c* causes *e*'. For instance, one risk factor can be connected to another risk factor by means of a link indicating that one risk factor causes the effect of the other risk factor. Within an argument, a link connects the evidence to a conclusion, e.g. a risk factor. In this case, the link expresses a generalization of the form '*e* is evidence for *c*'. For instance, the support link between a piece of evidence and a risk factor expresses that the relevant knowledge extracted from the evidence is evidence for a certain conclusion, in this case a risk factor. Likewise, an attack link expresses that what is extracted from the evidence is evidence against the conclusion. It depends on the type of link whether the link expresses a support or attack relation. The support link is rendered as an arrow with a closed head, while the attack link is rendered as an arrow with a square head.

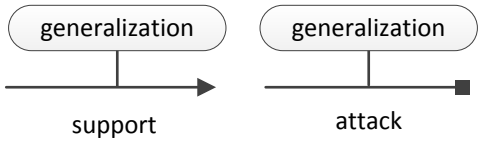

Figure 6.4: Support and attack links with explicit generalizations

In Figure 6.5 the syntax of an empty scenario is visualized as a light-blue box. A risk scenario is empty if there are no risk factors selected to construct a scenario. The *risk scenario* is inferred from risk factors which support the risk scenario. A box with a darker shade of blue sticks at the bottom of the risk scenario and indicates the total plausibility and impact of the risk scenario. The plautsibility represents the evidential support of the risk scenario and is determined by the plausibility of the different pieces of evidence that support the risk scenario. The impact of the risk scenarios represents the severity of the scenario on the situation at hand. The notions of plausibility and impact are further explained in Section 6.8.

The risk scenario is instantiated when risk events are added to the scenario, like in Figure 6.6. One risk factor supports another risk factor through a causal generalization, while the evidence which supports the risk factor is connected through an evidential generalization.

A piece of evidence is rendered as a purple box (Figure 6.7). In our model, the evidence is inferred from an evidence source. For instance, a piece of evidence which states that 'Expert *E* states that group X and Y always fight' is inferred from an evidence source 'Expert *E*'. A piece of evidence can have a plausibility and impact value of *N*, which indicates that a value of *0...n* can be assigned. How these values are derived will be explained in later on in this chapter.

From premises (i.e. evidence, and risk factors/claims/controls), conclusions can be inferred, that are risk factors (red box), controls (green box) and claims (gray box) (Figure 6.8). Note that the

Figure 6.5: An uninstantiated scenario

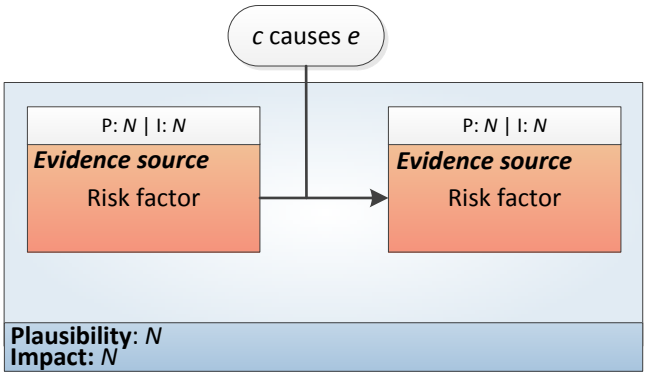

Figure 6.6: An instantiated scenario

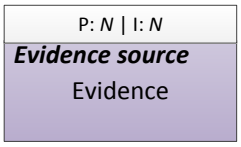

Figure 6.7: A piece of evidence

link between the piece of evidence and the risk factor, control or claim expresses a generalization of the form '*e* is evidence for *c*'. In Section 6.6 the notion of arguments is explained. The plausibility and impact values assigned to a risk factor, control or claim are determined by the total plausibility and impact values of the evidence it is being supported or attacked by.

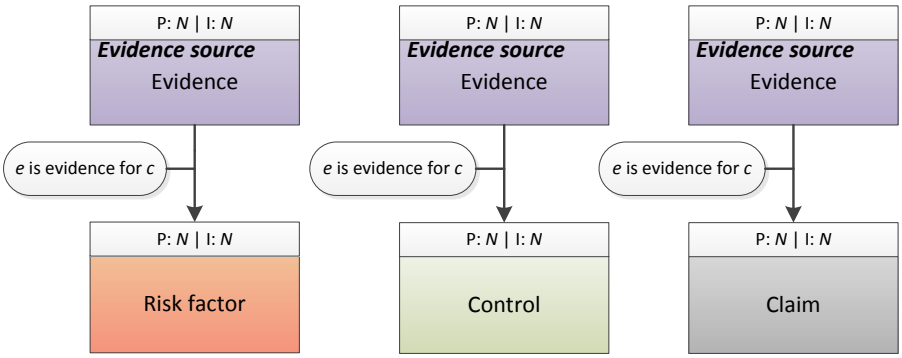

Figure 6.8: Arguments expanded with explicit generalizations

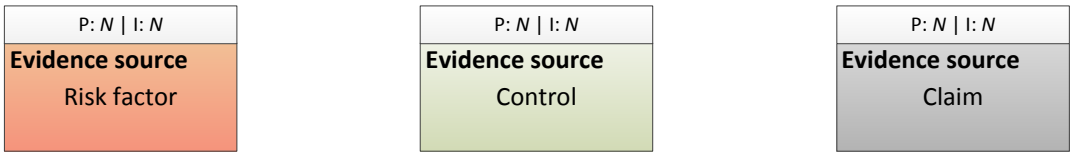

Figure 6.9: Arguments collapsed

To simplify the visualization of an argument, the evidential generalizations can be left implicit and the evidence source, plausibility and impact values, and conclusion can be aggregated into one box (Figure 6.9).

Figure 6.10: Combining arguments

In the hybrid theory, multiple arguments can be combined to infer a conclusion from more than one piece of evidence. Applied to our model, combining arguments means that either risk factors, controls or claims based on evidence can be combined through logical conjunction (AND-gate) or logical disjunction (OR/XOR-gate) (Figure 6.10). In Section 6.8 examples and an explanation of the possibilities to combine arguments is provided.

6.4 Scenarios

According to the hybrid theory, a scenario and its events are constructed from evidence (Bex, 2011). In our model, a risk scenario is constructed from risk factors which are and can be supported by available evidence (e.g. an expert who mentions that Ajax and Feyenoord always fight). In terms of risk assessment we could then say that the risk events can be considered the risk factors from which a risk scenario is inferred (Figure 6.11). Risk events can be supported attacked or by evidential arguments, which will be discussed in Section 6.6.

When developing risk scenarios, we search for possible risks in the future. As discussed above, the hybrid theory assumes there is some explanandum to be supported by evidence. The explanandum is input for the construction of a scenario. However, in risk management one cannot assume there is an explanandum, because one actually searches for explanandum that could be a possible risk. So in our model, the risk scenarios are inferred from risk indicators (i.e. risk factors). This means that the risk factors that are input for the risk scenario describe the risk. As an example, we take a risk factor supported by some evidence with states that according to a data source *D* the routes of supporter group X and Y cross. A consequence of this risk factor could be that there is going to be a fight between the two groups. So this risk factor supports a risk factor 'there is going to be a fight between supporter group X and Y'. In Section 6.8 we will explain how risk scenarios can be inferred from and supported by evidence.

In the example from Figure 6.11, a possible risk scenario is constructed from a risk factor 'the routes of Ajax and Feyenoord cross' that is supported by some evidence 'Data source iTable says that 'the routes of Ajax and Feyenoord cross". The fact that the routes cross could cause that Ajax and Feyenoord supporters get into a fight, which can be considered a risk factor. This risk factor is supported by the risk factor which states that the routes cross and can be added to the scenario. Furthermore, we could add a risk factor 'Ajax and Feyenoord always fight', which in addition to crossing routes adds to the risk of the scenario.

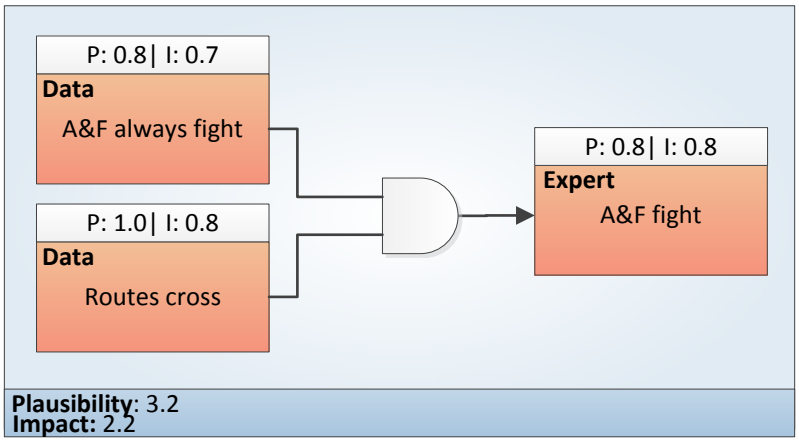

Figure 6.11: A scenario with explicit generalizations

6.5 Scenario schemes

As mentioned above, scenario schemes represent typical scenarios that often occur in for instance criminal cases. Scenario schemes can be formulated in different ways, ranging from abstract to specific and are modelled as an ordered list of events or types of events together with the possible relations between these events. Essentially, a scenario is an instantiated version of a scenario scheme, where the variables are replaced by constants. The added value of using scenario schemes for risk assessment is that such schemes enable risk analysts to develop scenarios and uncover risk factors and controls more quickly. For instance, in a case in which one wants to uncover possible risks related to football supporter flows, possible schemes include a fight scheme and a vandalism scheme.

A scenario scheme is constructed as follows:

- **Risk that the scheme explains:** group X and group Y get into a fight.
  The risk that the scheme explains is the main risk event of the risk scenario.
- **Central action of the scheme:** routes of group X and group Y cross.
  In a scenario, the events are connected through causal links. The central actions of the scheme are the events directly connected to the main event.
- **Relevant risk factors:** routes of group X and group Y cross, X and Y always fight, person Z and Q are present, person Z and Q always evoke fights.
  Relevant risk factors can be recorded in a scenario scheme.

- **Relevant controls:** change routes of group X and group Y, strictly separate person Z and person Q, deploy anti-riot squads.
  In addition, relevant controls can be made explicit.
- **Relevant information:** route A of group X and route B of group Y, person Z who is part of group X and person Y who is part of group Y.
- **Pattern of actions:** routes of group X and group Y cross $\rightarrow$ group X and group Y get into a fight.
  Patterns of action show how the risk factors are connected.

Because a scenario scheme is an abstraction of a scenario, it offers a template which shows the scenario as a connected causal sequence. The fight scheme presented above could visualized as in Figure 6.12. Subsequently, people involved in the risk assessment process can argue about the events in the scenario scheme by introducing, attacking and supporting evidence.

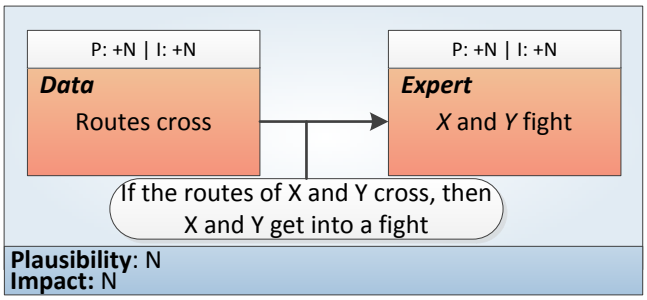

Figure 6.12: A fight scheme template

Recall that scenario schemes can be abstract, but also specific. For instance, the above scenario scheme could also be phrased as 'if the routes of Ajax and Feyenoord supporters cross they could get into a fight".

Scenario schemes can be accompanied by critical questions to uncover sources of doubt. Bex (2011, p.66) describes an intentional action scheme, that is, a scheme of initiating events, a goal, an action and consequences. However, we could also define other types of scenario schemes, since not all types of risk scenarios are based on an intentional action scheme. For instance, our fight scheme scenario could be abstracted as initiating event - consequence. Where the initiating event could be something like 'routes of X and Y cross' and the consequence is 'X and Y get into a fight'. Examples of accompanying critical questions could be:

Critical questions: Routes cross and supporters fight scheme

- **Q1:** How many risk supporters are present?
- **Q2:** How is the relationship between supporter group *X* and *Y*?
- **Q3:** Do the routes of *X* and *Y* cross?

By answering these questions, the plausibility of the scenario could be assessed in terms of what parts of the scenario still need to be supported or attacked by risk factors and controls.

6.6 Arguments

One of the main concepts of the hybrid theory is the concept of arguments, which can either attack or support a risk event or other argument. In the argument-based approach, arguments and counterarguments are used to expose sources of doubt in reasoning. According to Bex (2011), arguments can in this way be used to provide a rationally justified conclusion [about possible risks]. An argument can be defined as a pair of 'premises - conclusion'. In our model we consider three types of conclusions: 1) risk factors, 2) controls, and 3) claims (Figure 6.13). Risk factors increase the risk of a scenario, controls decrease the risk of a scenario, and claims can be used to support or attack risk factors and controls. An example of a risk factor could be 'Person A and B always fight', which can be attacked by a control, e.g. 'Separate person A and B'. A claim such as 'Separating person A and B had an effect last year' can then be used to support the control. These type of arguments that are supported by evidence are called *evidential arguments*. Evidence entails "the information that (positively or negatively) influences our belief about a particular proposition" (Bex, 2011, p.12). For instance, a risk factor 'Person A and B always fight' can be introduced by an expert 'John' (Figure 6.13). The risk factor is supported by some evidence which states that 'expert John says that 'Person A and B always fight'. The link between the evidence and the risk factor expresses a generalization. For instance, the risk factor in Figure 6.13 is based on an expert's opinion, so we could generalize that if an expert states a certain conclusion, then this conclusion can be assumed. Translated to our example, the generalization expresses 'if an expert states that Person A and B always fight, then Ajax and Person A and B always fight'. This generalization justifies the inference link between the evidence and the conclusion.

In our model, a control does not necessarily have to be supported by further evidence, since there might be no solid evidence to do so or because there is no need to argue about the control. For instance, a control 'change routes' can attack the risk scenario which contains the events that the routes of Ajax and Feyenoord supporters cross which might cause that they get into a fight. Even though this scenario could be supported by all sorts of evidence that justify that

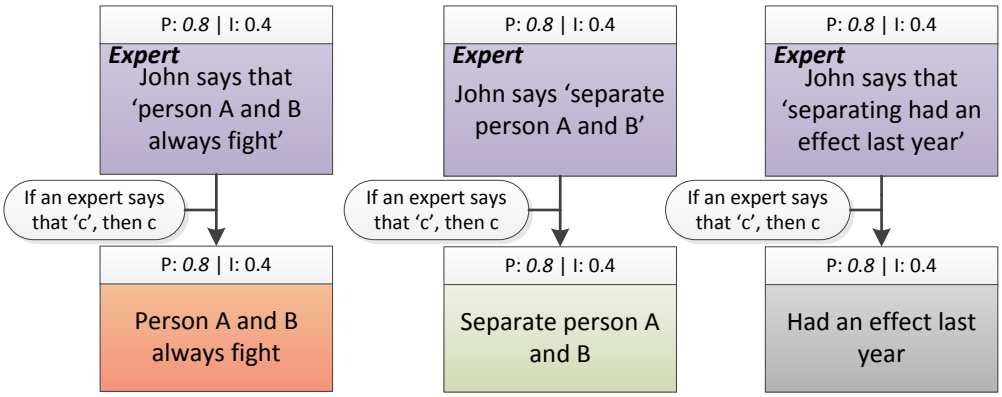

Figure 6.13: Arguments with an explicit generalization

Ajax and Feyenoord supporters could fight, changing the routes will attack all of the evidence, because the routes will not cross, which then could not result in a fight.

6.6.1 Attacking and defeating arguments

There are several possibilities by which an evidential argument can be attacked (Figure 6.14): 1) attack the conclusion, 2) attack the generalization.

For instance, we could attack the conclusion of the argument about 'Person A and B always fight' by introducing an evidential argument based on general knowledge that 'Person A and B never fight'. However, we could also attack the generalization from which the risk factor is inferred, e.g. by an expert opinion which states that the expert which claims that Person and A and B always fight is biased. By doing so we undercut the evidence and decrease the evidential support.

In order for an attacking argument to defeat another argument, some measure of strength should be assigned. As argued by Bex (2011) calculating strengths is often not easily done, because it is difficult to express how much exactly one argument is stronger than the other. Because of such difficulties, the strength of arguments should be compared relative to each other. For example, we could say that an argument by expert John is more reliable than an argument by expert Jane. To determine how much more reliable one argument is than the other argument(s) a plausibility value (P) is assigned, which is inferred from the evidence that supports the conclusion of the argument. For instance, the evidence which supports the risk factor 'Person and B always fight' from Figure 6.14 has a plausibility value of 0.5, and thus the plausibility value of the risk factor is also 0.5.

After it has been determined which arguments are stronger than others it can be determined which arguments defeat which other arguments. A rule of thumb here is that the argument

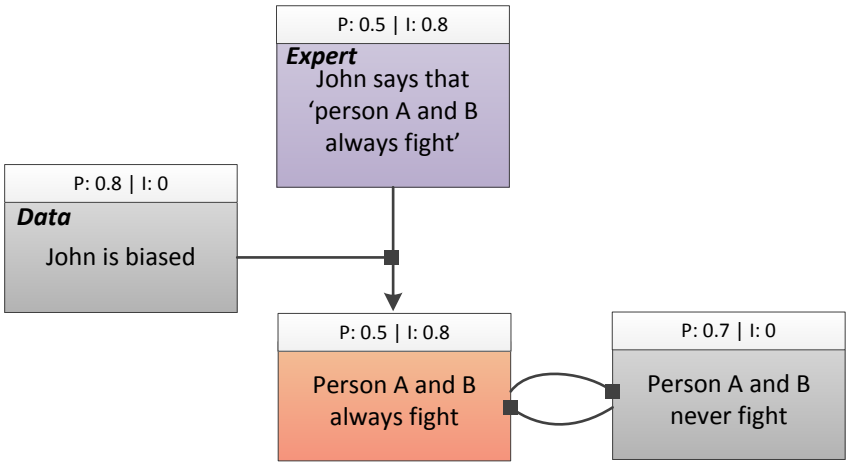

Figure 6.14: Possibilities to attack an argument

with the higher plausibility value defeats the argument with a lower plausibility value. In sum, we can say that an argument A defeats another argument B if and only if A successfully attacks B. Argument B is successfully attacked if the plausibility value of argument A is higher than the plausibility value of B.

Definition of defeat

An argument *A* defeats an argument *B* if and only if the plausibility value of *A* is greater than the plausibility value of *B*.

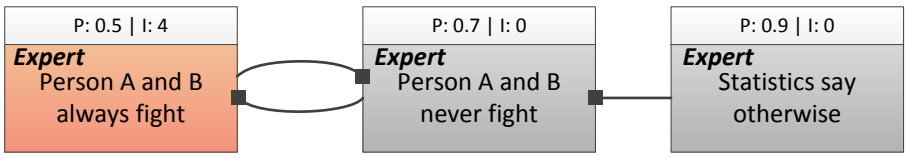

Figure 6.15: Reinstatement of arguments

Important to keep in mind when attacking and supporting arguments is what is described by Prakken and Vreeswijk (2002) as the *dialectical status* of an argument. Arguments can be classified into three kinds: 1) justified arguments, which survive the competition with their counterarguments; 2) overruled arguments, which lose the competition with their counterarguments; and 3) defensible arguments, which are involved in a tie. The dialectical status of an argument

depends on the interaction with all other arguments. According to Bex (2011) an important concept here is *reinstatement*. Suppose that argument B defeats argument A, but B is itself defeated by a third argument C; in that case C reinstates A. In the example (Figure 6.15) we have an argument 'Person A and B always fight' which is attacked by 'Person A and B never fight'. Because the rightmost argument is not attacked (Statistics say otherwise), it is justified (+) and defeats the argument 'Person A and B never fight' (-). The argument 'Person A and B always fight' is now also justified (+), because its only attacker is overruled.

6.6.2 Combining arguments

Since one argument can clash with or be dependent on another argument, multiple arguments can be combined to infer a conclusion from more than one piece of evidence. Our model enables to connect arguments through logical conjunction (AND) and disjunction (OR/XOR).

Conjunctions enable chaining arguments through an AND function which returns a 'high' value only if both the inputs to the AND-gate are high. So effectively, the AND function finds the minimum between a set of values. For example, let us take again the 'fight' scenario for which we would like to discuss and explore possible risk factors and controls. From a database we analyze data and extract knowledge that person A and B are present. But, this risk factor on its own does not support that Ajax and Feyenoord supporters get into a fight, because for that person A and person B have to be present. Information obtained from a football coordinator confirms that person A and B are present. So now we can connect these two risk factors through an AND-gate (Figure 6.16). Furthermore, for the supporters to get into a fight, the routes should cross.

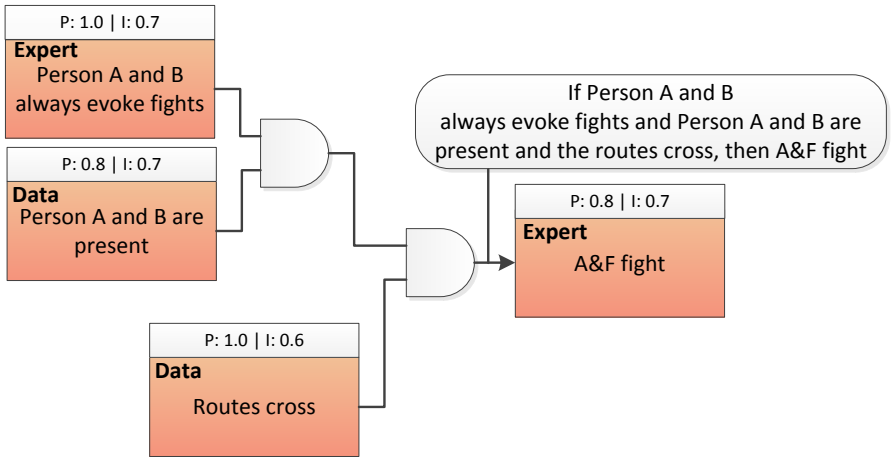

Figure 6.16: Combining arguments through an AND-gate

Disjunctions come in two forms. First of all, an OR function enables to express that one or both arguments should be true. Second of all, an XOR function enables to express a choice between arguments, that is, one of the arguments should be true. The OR and XOR function find the maximum in a set of values. For instance, if we have two risk factors 'supporters meet a gas station X' and 'supporters meet at gas station', we can use an XOR-gate to express that one of the risk factors is true, not both. (Figure 6.17)

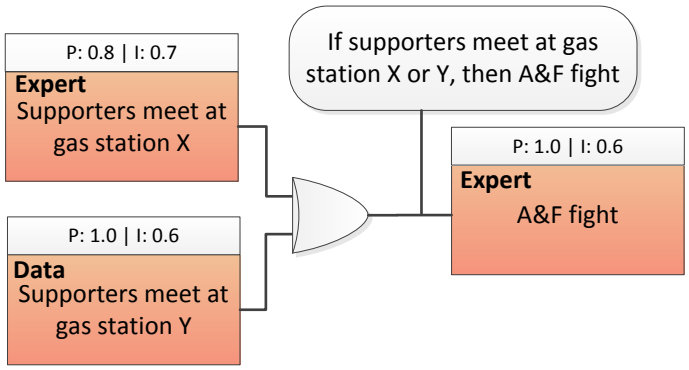

Figure 6.17: Combining arguments through an XOR-gate

The conjunctions and disjunctions can be combined. Say that we extracted information from a database which states that if Ajax and Feyenoord always fight there will be fights. From an expert we obtained data that the supporters meet at gas station X and Y. Now we can connect this knowledge through an XOR- and AND-gate (Figure 6.18).

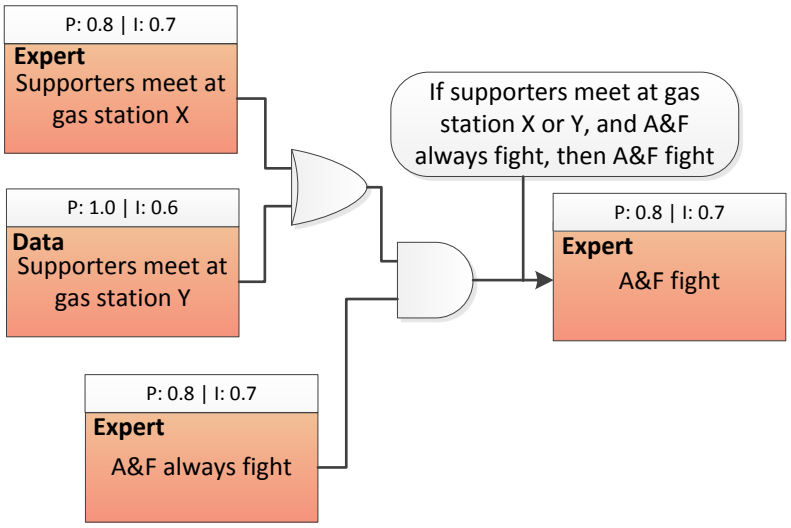

Figure 6.18: Combining gates

How the plausibility and impact values of combined arguments are determined will be explained in Section 6.8.

6.7 Argumentation schemes

Each type of evidence has its own generalization which allows us to draw a conclusion from that particular type of evidence and thus the generalization can be seen as "the glue that keeps an argument together" (Bex, 2011, p.44). Argumentation schemes are like scenario schemes, but denote a single relation between two propositions instead of multiple (causal) relations. Bex (2011) argue that there are quite a few generalizations that show similarities between kinds of reasoners. For instance, generalizations used to draw conclusions from expert testimonies often show recurring patterns. In this sense, argumentation schemes can be used, which represent stereotypical patterns of how humans reason. Every scheme is accompanied by some critical questions. As mentioned above, these critical questions can help in uncovering sources of doubt in arguments. For instance, critical questions belonging to the argumentation scheme for argument from expert opinion as discussed in Section 5.2 can be used to determine the reliability of the argument provided by someone involved in the risk assessment process. The answers to these critical questions can result in new arguments. These argumentation schemes can be attached to a piece of evidence based on its evidence source. In our model we adopt different schemes: 1) argument from expert opinion, 2) argument from documentary evidence (data), and 3) argument from general knowledge .

First of all, an argumentation scheme for argument from expert opinion can be attached to the evidence source which is based on an expert's opinion. For instance, a risk factor 'Ajax and Feyenoord always fight'. The argumentation scheme is constructed as follows (Walton, 1996):

Argumentation scheme: expert opinion

Source *e* is an expert in domain *d*.
e asserts that proposition *a* is known to be true (false).
a is within *d*.
Therefore, *a* may plausibly be taken to be true (false).

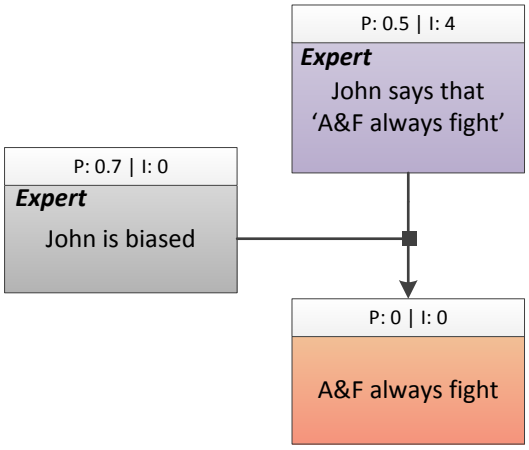

Figure 6.19: An argument derived from critical questions

In general, this scheme tells us that a proposition can be considered plausible if the source originates from an expert in a certain relevant domain and the proposition itself is also part of that domain. Applied to our example, this scheme tells that the Ajax and Feyenoord always fight may be plausible, if John is an expert in the domain of let us say 'hooligan regulation'. Attached to this scheme can be several critical questions to determine the plausibility of the control. For example, if the answer to the first questions is that John is not credible as an expert, the generalization between the evidence and the risk factor can be attacked by an argument which states that John is not credible or biased (Figure 6.19).

Critical questions: expert opinion

- **CQ1:** How credible is *E* as an expert source?
- **CQ2:** Is *E* an expert in *D*?
- **CQ3:** What did *E* assert that implies *A*?
- **CQ4:** Is *E* personally reliable as a source?
- **CQ5:** Is *A* consistent with what other experts assert?
- **CQ6:** Is *A*'s assertion based on evidence?

Second of all, an argumentation scheme for argument from documentary evidence is adopted in our model. Documentary evidence can also be seen as evidence from data (e.g. a spreadsheet, a database). The scheme is constructed as below (Walton, Reed, & Macagno, 2008, p.338):

Argumentation scheme: documentary evidence

Document *d* contains information *x* is a prima facie reason to believe *x*.

The accompanying critical questions are defined as:

Critical questions: documentary evidence

- **CQ1:** Is document *d*'s authenticity questionable?

Finally, an argumentation scheme for argument from general can applied to an argument. The argumentation is constructed as follows:

Argumentation scheme: general knowledge

It is general knowledge that '*x*' is a prima facie reason to believe *x*.

Critical questions: general knowledge

- **CQ1:** Is *x* infected by prejudice or value judgement?

6.8 Combining scenarios and arguments

In the previous sections we explained the concepts of scenario and argument. When we combine both concepts, the risk events that constitute a scenario can be considered the conclusions of evidential arguments. To illustrate how both concepts can be combined we consider the following scenario:

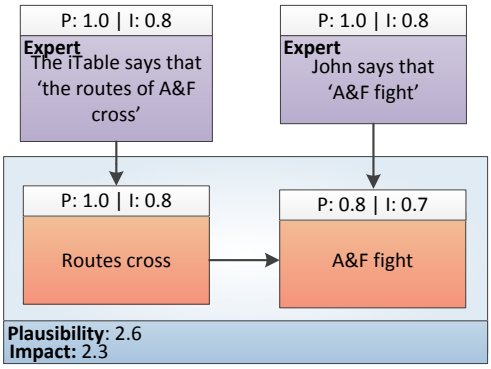

Figure 6.20: Combining scenarios and arguments

The risk events (risk factors) in the scenario are the conclusions of arguments about evidence. Both risk factors are supported by one piece of evidence. To support and attack this risk scenario, we can introduce other arguments. For instance, we can support the scenario by introducing a risk factor based on an expert opinion which states that Ajax and Feyenoord always fight (Figure 6.21). This risk factor is added to the scenario through an AND-gate, because in addition to the risk caused by crossing routes, the risk that Ajax and Feyenoord also adds to the plausibility and impact of the risk scenario. In Section 6.9 it will be explained how the plausibility and impact value are being determined.

Evidential arguments can be used to support or attack another argument. Thereby influencing the evidential support and evidential contradiction of a risk scenario. As mentioned above, the evidential support of a scenario is based on the plausibility values of the risk events and their evidence. The opposite of evidential support is evidential contradiction: all pieces of evidence that contradict some element (generalization or argument) in a risk scenario (Bex, 2011, p.85-86). By supporting a risk factor, with an argument based on evidence, the evidential support of the risk scenario increases. Likewise, attacking a risk factor with an argument based on evidence increases the evidential contradiction.

To attack the argument that 'Ajax and Feyenoord always fight', an expert Bob can introduce a claim which states that 'Ajax and Feyenoord supporters never had a fight'. If the total plausibility value of the pieces of evidence that support the claim 'Ajax and Feyenoord supporters never had a fight' is higher than the plausibility of the risk factor it attacks, the risk factor is

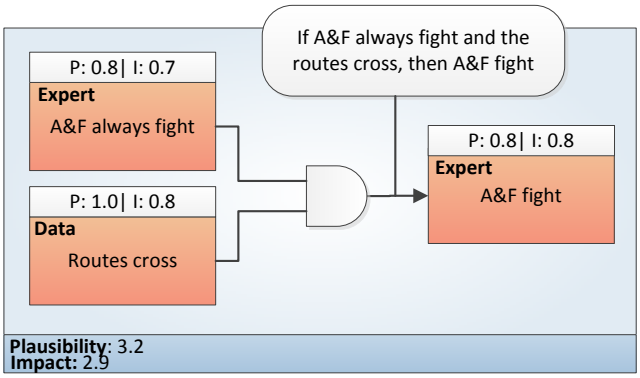

Figure 6.21: Supporting an argument

defeated (rendered in a lighter color) (Figure 6.22), and the plausibility and impact value are pf no influence anymore on the risk scenario. This means the plausibility of the risk scenario is decreased by 0.8 and the impact by 0.7, since those numbers were assigned to the risk factor.

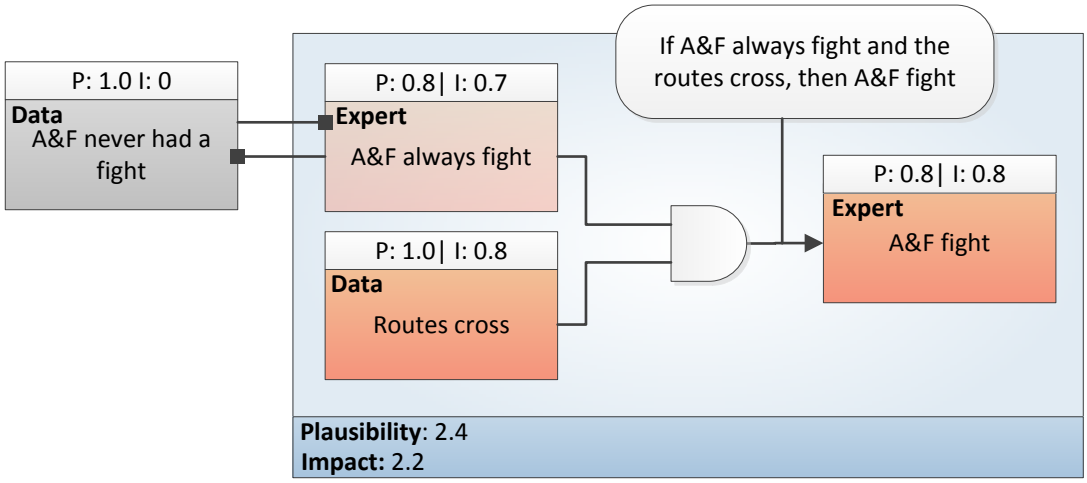

Figure 6.22: Attacking an argument

We could also apply a control 'change routes' which attacks the risk factor 'routes cross'. If we have strong evidence for the claim that by changing the routes there is no possibility anymore that Ajax and Feyenoord get into a fight, we can say that the control is stronger than all of the other arguments and defeats all possible evidence. In this case, the plausibility value of the control can be set at a value of 1.0.

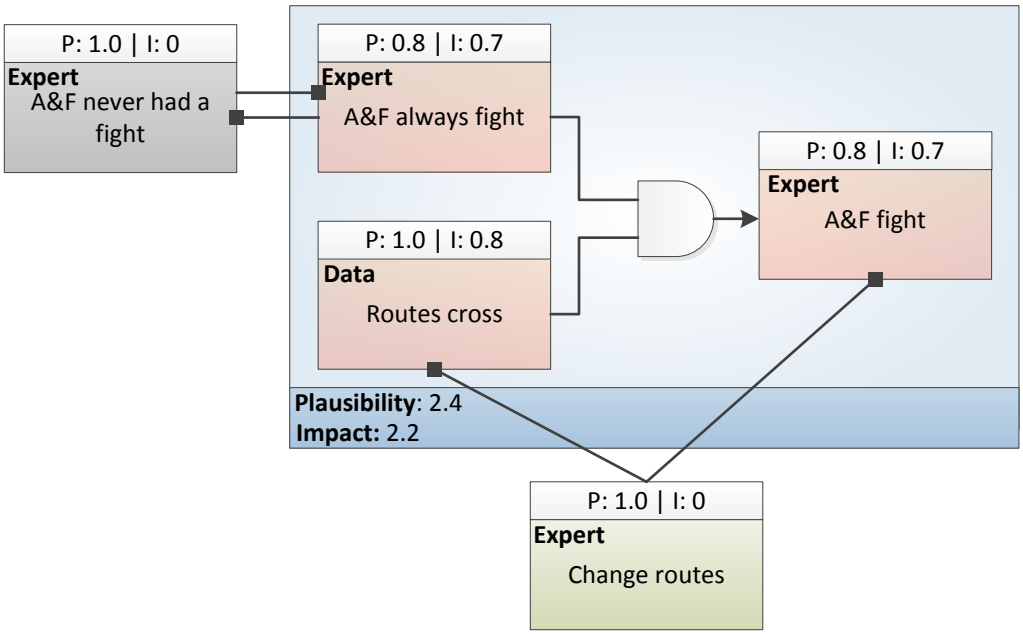

Figure 6.23: Applying a control

In some cases a control might instigate risk and lead to a new possible risk scenario. For instance, if we constructed a scenario is visualized in Figure 6.24 on page 76, the control 'Deploy anti-riot squads' can instead of mitigating risk, also instigate risk, because the presence of anti-riot squads could trigger certain violent behaviour towards these squads. However, the plausibility and impact values of 'deploy anti-riot squads' do not necessarily have to be identical, because each scenario explains a different conclusion. For instance, it could be very plausible that deploying anti-riot squads can result in a fight with the police, but this does not mean that it is also very likely that deploying anti-riot squads mitigates the plausibility of a fight between Ajax and Feyenoord.

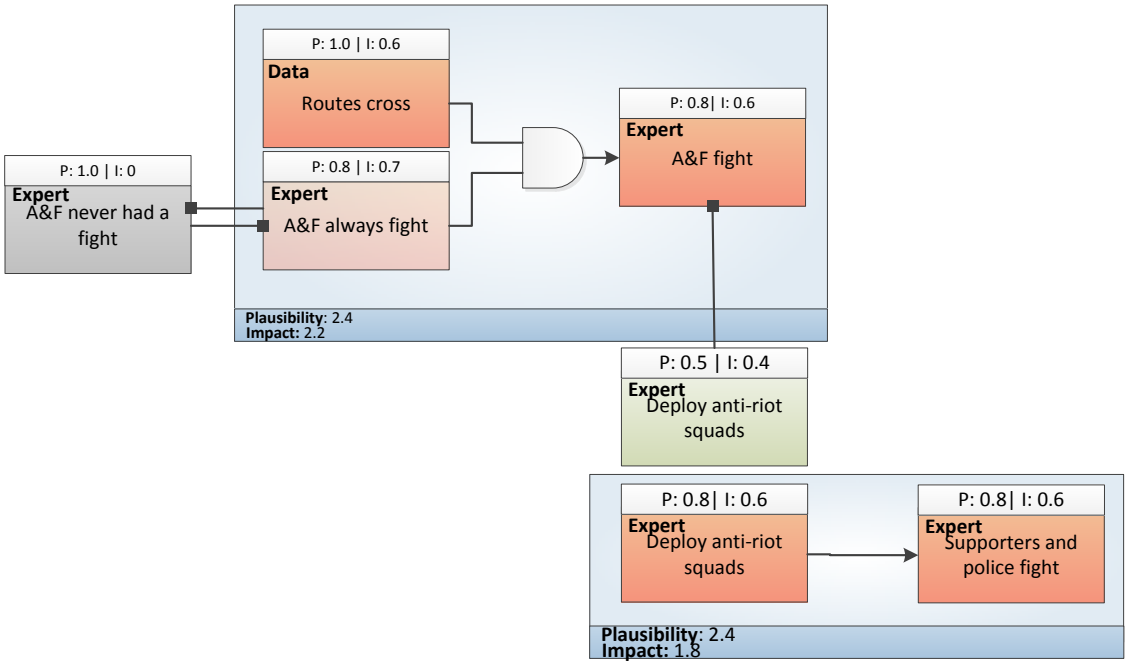

Figure 6.24: Inferring a risk scenario from a control

6.9 Assessing and comparing scenarios

Since multiple scenarios can be constructed, there should be a way to compare those scenarios to facilitate prioritization and improve decision-making. According to the hybrid theory, scenarios can be compared by how much evidential data supports each scenario. A rule of thumb is "the more evidential data that supports the story (scenario), the better the story or the less evidential gaps the better the story" (Bex, 2011, p.94). In our model the plausibility of a risk scenario is based on this rule of thumb, as will be explained later on in this section.

As discussed in Section 6.3 each piece of evidence, risk factor, control, claim, and scenario is assigned a plausibility (P) and impact (I) value. To determine the P and I values, the following rules can be used:

Propagation rules for determining the *P* and *I* values

Rule 1 A piece of evidence E propagates P to a direct conclusion C.

E.g E(P=0.8) that supports C, instantiates C as C(P=0.8).

Rule 2 A risk factor/claim X propagates P to a direct conclusion C.

E.g. X(P=1.0) that supports C, instantiates C as C(P=1.0).

Rule 3 If more than one premise (i.e. risk factor/claim, evidence) supports a conclusion C, then the premise with the highest P value is selected.

E.g. if we have some evidence E(P=0.8) and a risk factor X(P=1.0), we select X so we obtain C(P=1.0).

Rule 4 When using links through an AND function, the premise with the lowest P value is selected.

E.g. if we have a risk factor X(P=0.8) and a risk factor Y(P=1.0), we select X so we obtain C(P=0.8).

Rule 5 When using links through an OR/XOR function, the premise with the highest P value is selected.

E.g. if we have a risk factor X(P=0.8) and a risk factor Y(P=1.0), we select Y so we obtain C(P=1.0).

Rule 6 A premise X defeats a premise Y if and only if $P_X > P_Y$.

E.g. a claim X(P=1.0) that attacks a risk factor Y(P=0.8) defeats Y.

Rule 7 The I value is determined by selecting the highest I value of the arguments that are not defeated.

E.g. if we have arguments X(I=0.6), Y(I=1.0), and Z(I=0.8), we obtain C(I=1.0).

The plausibility value can be determined by the following scale:

Scale to determine the plausibility value

0.2 No substantial evidence available, the plausibility of the event occurring is small.

0.4 No substantial evidence available, the plausibility of the event occurring is medium.

0.6 Different claims and information from reliable evidence sources, the plausibility of the event occurring is medium.

0.8 Substantial evidence to support and confirm that the event might occur. The time and place are unknown. The plausibility of the event occurring is high.

1.0 Very strong evidence to support and confirm that the event might occur. The time and place are known. The plausibility of the event occurring is very high.

The impact value can be determined by means of the following scale:

Scale to determine the impact value

0.2 Negligible

0.4 Minor

0.6 Moderate

0.8 Significant

1.0 Severe

The plausibility scale is adapted from the probability scale as defined by Vagias (2006), while the impact scale is based on the common scale for impact as used in a qualitative risk matrix-based approach. However, the definition of the scales can be altered if needed, as will be illustrated in Section 7.2.

To explain the propagation of P and I values to a premise and conclusion, we start off with the risk scenario as visualized in Figure 6.25, where the arguments are expanded, showing the underlying evidence.

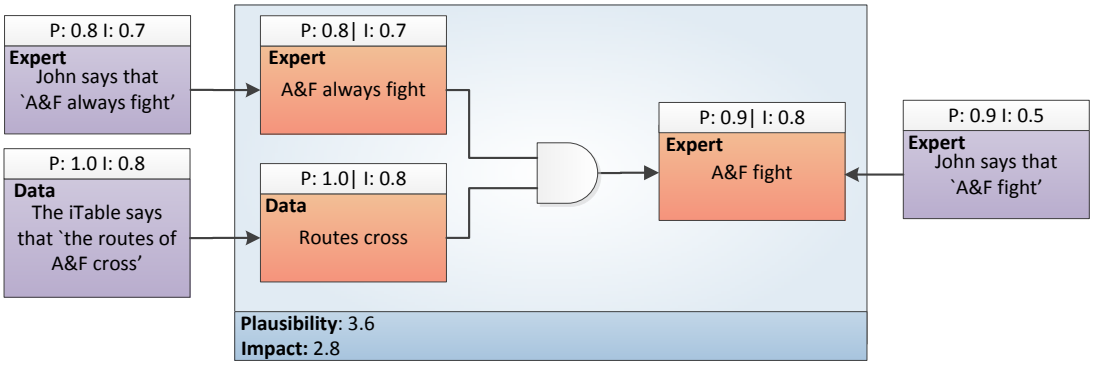

Figure 6.25: A risk scenario with P and I values

According to **Rule 1**, the P value of the risk factor 'A& fight' are based on the values assigned to the piece of evidence that directly supports the risk factor. However, the risk factor is also being supported by two other risk factors, which are connected through an AND gate. According to **Rule 4**, the premise with the lowest P value should be selected, that is 'A&F always fight'. Following **Rule 2**, the risk factor 'A&F always fight' propagates the P value to the conclusion 'A&F fight. Because multiple premises are supporting the risk factor 'A&F fight', we should select the premise with the highest P-value according to **Rule 3**, thus the P value of the evidence which states that John says that 'A&F fight'. To determine the I value of the risk factor 'A&F

fight' the highest I value of the arguments that support the risk factor and are not defeated is selected (**Rule 7**).

The P value of the risk scenario is calculated by taking the sum of the P values of the risk factors and evidence that directly support a conclusion, and which are not defeated. In the same sense, the I value is calculated by taking the sum of the impact values. We define a set of risk factors and evidence that directly support a conclusion, and which are not defeated, as a set DS.

How to determine *P* and *I* values of a risk scenario

$$P_{scenario} = \sum DS_{plausibility} \tag{6.9.1}$$

$$I_{scenario} = \sum DS_{impact} \tag{6.9.2}$$

In our example, this translates to the sum of 'A&F always fight', 'Routes cross', 'A&F fight', and the piece of evidence which directly supports the conclusion 'A&F fight'. Hence, the P value of 3.6 and the I value of 2.5.

Now, according to **Rule 6**, if we would attack and defeat the risk factor 'A&F always fight' by introducing a claim with a higher P value, the P (and I) values of the risk factor do not count anymore towards the plausibility and impact of the risk scenario (Figure 6.26). This would change the content of our set DS to $DS = \{\text{Routes cross}, \text{A\&F fight}, \text{John says that 'A\&F fight'}\}$. Because the risk factor 'Routes cross' now has the highest P value, its P value is assigned to the conclusion 'A&F fight' (**Rule 2 and 3**). In case there would have been multiple premises with a P value of 1, the risk analysts should determine which premise could actually have the highest risk.

By using the equations 6.9.1 and 6.9.2 defined above, we can derive $P(2.8)$ and $I(2.1)$.

Finally, a control 'Deploy anti-riot squads' is used to attack the risk factor 'A&F fight' (Figure 7.2 on page 90). However, since the P value of the control is lower than the P value of the risk factor, the risk factor is not defeated (**Rule 6**), so the P and I values of the risk factor are not being influenced.

In the example we used a simple combination of arguments to infer a risk scenario, however we could also construct more complex scenarios. In Figure 6.28 on page 81, such a complex scenario is rendered. When we apply our defined rules to this argument, **Rule 1** states that the P and I value of 'A&F fight' are inferred from the evidence directly connected to it. However, since there are multiple risk factors that support 'A&F fight' in addition to the direct evidence, **Rule 4** applies, which states that the minimum P value of the premises is the P value of the conclusion. Since two of the risk factors are defeated, the P value of the conclusion is inferred

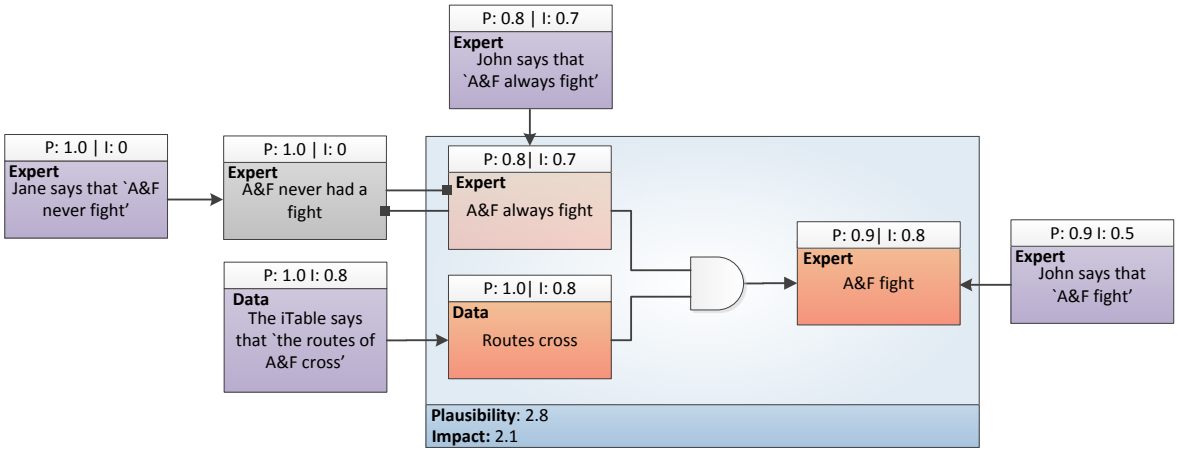

Figure 6.26: Attacking a risk factor to influence P and I values

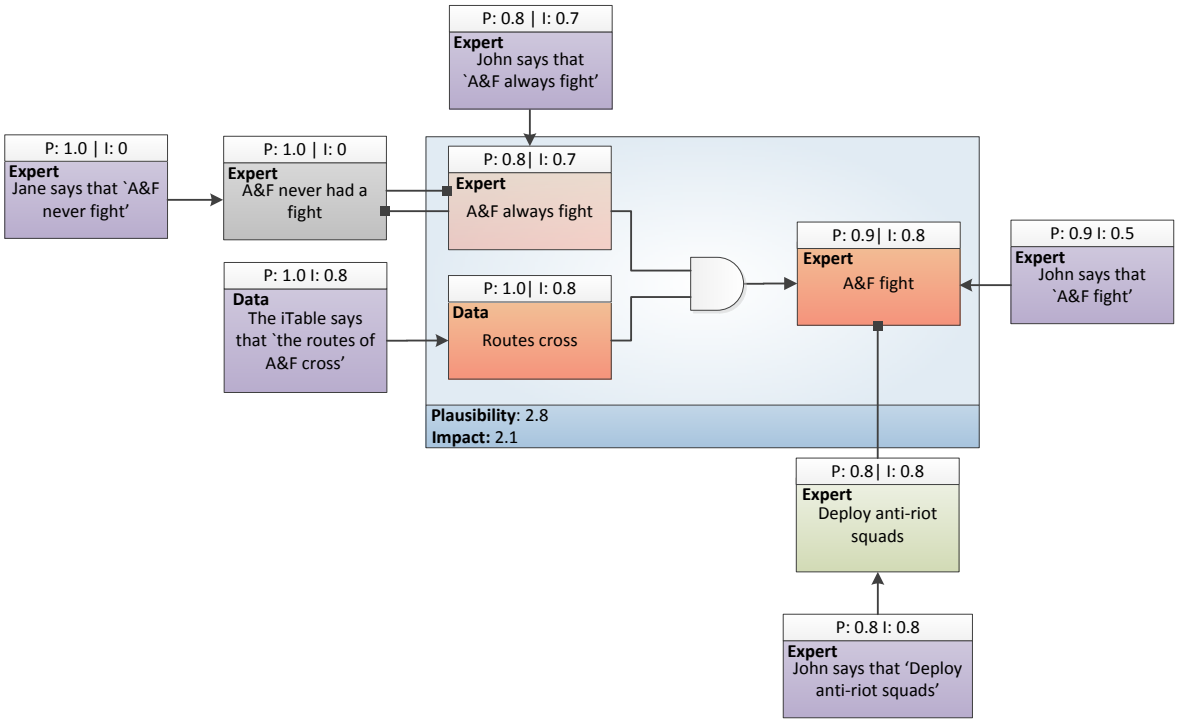

Figure 6.27: Introducing a control

from the risk factor with the lowest P value. Finally, equation 6.9.1 and 6.9.2 can be used to determine the P and I value of the risk scenario.

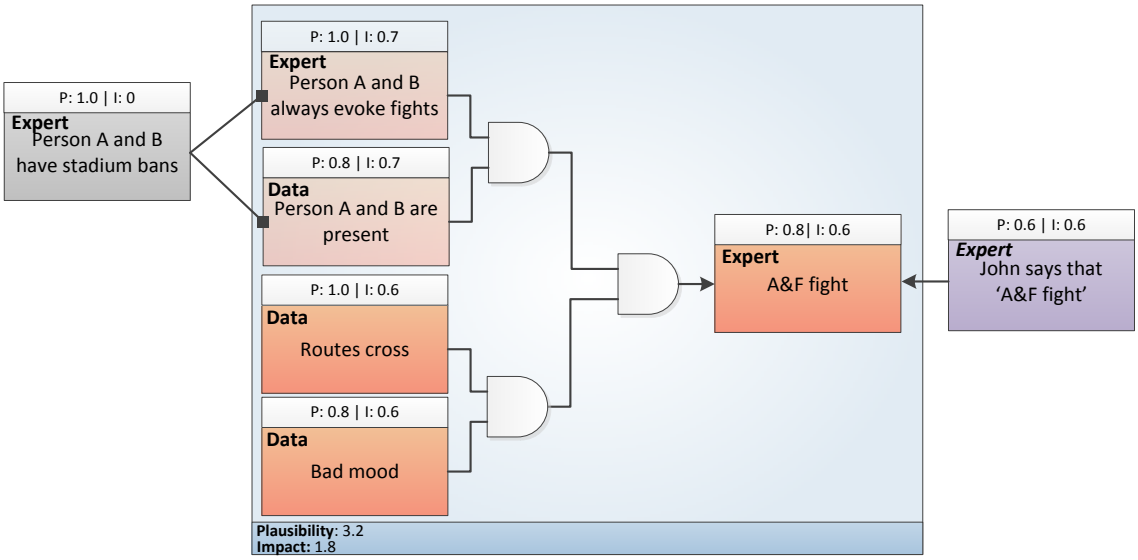

Figure 6.28: A complex scenario

We could of course have constructed multiple scenarios: S_3 which is being supported by 4 pieces of evidence with a total plausibility score of 3.5, and S_4 which is being supported by 10 pieces of evidence with a total plausibility score of 4.0. Let us assume that the impact value S_3 is 3.2 and the impact value of S_4 is 4.

According to the rule of thumb which states the best scenario is the scenario with the highest evidential support we could prioritize the scenarios as: S_4, S_3, S_2, and S_1. However, since we include an impact value we also want to be able to include this value in our comparison. To facilitate this comparison a risk matrix-approach can be adopted.

6.9.1 Basic Tool: Risk Matrix

Recall from Section 2.3.2, where we discussed different methods and tools for risk assessment that a risk matrix can facilitate the comparison of events and scenarios and is easily understood. Also, we discussed some characteristics and requirements for designing an effective risk matrix (e.g. easy to understand, not dependent on extensive understanding of qualitative risk analysis, depict tolerable and intolerable levels. To depict tolerable and intolerable risks, a risk matrix should at a minimum have clear blocks where the risk is tolerable or intolerable (Ozog & Perry, 2002). An example of a risk matrix is visualized in Figure 6.29.

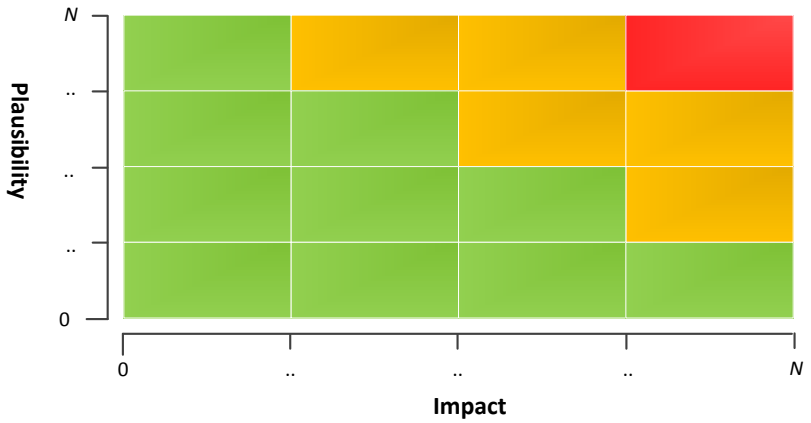

Figure 6.29: An empty risk matrix

The plausibility and impact ranges are defined by consequence ranges assigned by risk analysts. Since our example is aimed at football supporter flows, we can use the ranges as defined on the CIV matrix of the Dutch police force. Because our model provides us with quantitative values, we can use the approach as proposed by Ozog and Perry (2002), to assign P and I values to different criteria levels as defined in the scales below.

Scale to determine the plausibility value

Level 1 No substantial evidence available, the plausibility of the scenario occurring is small.

$P \leq 1$

Level 2 No substantial evidence available, the plausibility of the scenario occurring is medium.

$1 \leq P \leq 2$

Level 3 Different claims and information from reliable evidence sources, the plausibility of the scenario occurring is medium.

$2 \leq P \leq 3$

Level 4 Substantial evidence to support and confirm that the scenario might occur. The time and place are unknown. The plausibility of the scenario is high.

$3 \leq P \leq 4$

Level 5 Very strong evidence to support and confirm that the scenario might occur. The time and place are known. The plausibility of the scenario is very high.

$P \geq 5$

Scale to determine the impact value

Level 1 No additional danger compared to an event of the same size.

$I \leq 1$

Level 2 Chance of minor damage to people/goods.

$1 \leq I \leq 2$

Level 3 Possible threat caused by violence, rivalry or special circumstances that can result in reasonable damage to people/goods.

$2 \leq I \leq 3$

Level 4 Possible threat caused by the formation of different (organized) groups, which can result in high damage to people/goods.

$3 \leq I \leq 4$

Level 5 Increased possible threat caused by organized violence, rivalry or special circumstances that can result in a significant amount of damage to people/goods.

$I \geq 5$

Furthermore, a risk rank table can be defined, in which the levels of plausibility and impact can be categorized according to their risk level. The CIV risk matrix contains such a table, so we use those values in our example (Table 6.1).

Risk level	**Plausibility level**	**Impact level**
Low (green)	Between 0-2	Between 0-2
Medium (yellow)	Between 2-4	Between 3-4
High (red)	Between 4-5	Between 4-5

Table 6.1: Risk rank table

Subsequently a risk matrix, such as visualized in Figure 6.30 can be constructed, where we plotted the values for S_1, S_2, S_3 and S_4 on the risk matrix. This allows us to easily compare the different scenarios according to their plausibility (evidential support) and the impact. Furthermore, the risk matrix can be used as a quick reference tool, while specific risk scenarios that are depicted on the matrix can be examined in detail by zooming in on the argumentation structure underlying the risk scenario. This also enables to see how the plausibility and impact vales are derived.

From this matrix we can deduce the following prioritization: S_4, S_3, S_2, and S_1.

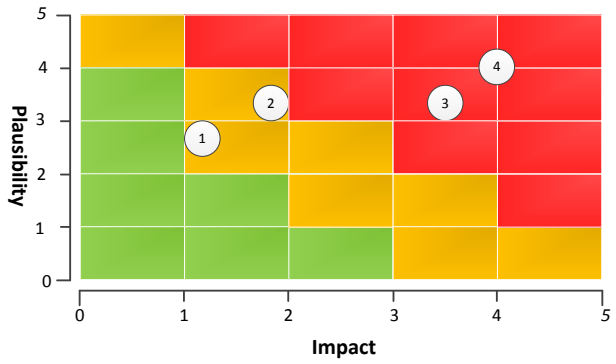

Figure 6.30: A risk matrix with plotted scenarios

6.10 Uncovering risk factors and controls

As explained above, the hybrid theory usually revolves around the analysis and explanation of evidence about what *has happened* in a case. But, since the core of risk assessment is to identify and analyze possible risks in the future, we want to explain what *could happen*, i.e. we want to predict possible effects and consequences.

So instead of solely assuming there is already some conclusion to explain (top-down), we are also building conclusions from available evidence (bottom-up). For example, if we want to develop scenarios around football supporter flows, we could let us say have a conclusion 'Ajax and Feyenoord supporters fight'. From there on we try to develop this scenario by searching for risks that could explain the different steps to what could cause the fight. However, we are also interested in uncovering new risks that could occur as a result of the fight, so we can apply a bottom-up approach. Doing so, enables the model to be used in an exploring as well an an explaining perspective. This approach means that we start off with some evidence, let us say 'An expert says that every fight someone is hospitalized' and by reasoning steps infer a conclusion, e.g. 'People will need emergency care'.

One of the dangers of predicting possible risks is that an extensive list could be created which is not specific enough to develop an understanding of possible risks. Our model can solve this problem, because risks are identified by means of arguments about possible risks. From these arguments the plausibility of the conclusion is inferred. Irrelevant risk factors are assigned a lower plausibility value. In this way, a risk analyst can construct a more specific overview of relevant risks.

7

Case study: Dutch police force

As discussed in Section 6.5, scenario schemes can aid risk assessors in quickly uncovering risk scenarios by offering possible risks and controls. In our case study we aim to capture different scenario schemes related to football supporters flows. The case study is an exploratory single-case study and is designed according to the guidelines by Yin (2013). The guidelines distinguish four phases: 1) case study design, 2) conduct case study, 3) collect data, and 4) analyze case study data. An important artifact in the case study design phase is the case study protocol which can increase the reliability of the case study by describing the steps to carry out the data collection. In this chapter, first the case study protocol is described to set out our guidelines for the execution of the case study. Subsequently, in Section 7.2 the case study is evaluated to uncover strengths and weaknesses of the case study. Furthermore, it is described how scenario schemes were extracted from experts. Finally, in Section 7.4 the implementation of the model in the iTable is discussed.

7.1 Case study design

The case study protocol usually consist of four sections: 1) an overview of the case study project, 2) field procedures, 3) case study questions, 4) a guide for the case study report. This section will give an overview of the most significant parts that should be included in our case study protocol, but will not go into detail on all of the four sections, because not all of the information is of added value to this section (e.g. agreements on time, date, etc.)

As mentioned above and as explained in Section 3.1, the Dutch police force is facing problems around football supporter flows. Currently, the Dutch police force uses a risk matrix to determine the likelihood and impact of a risk factor and scenario. This matrix can be used as guide during the case study execution, because it lists possible risk factors and gives a scale to base

the plausibility and impact values on (Appendix C). However, their current methods and tools are insufficient, so the police force decided to move on to a new solution in the form of an iTable application, which is developed by a team of bachelor Informatics students at Utrecht University as part of their graduation project. The application enables risk analysts to plot different elements on a map, such as routes, locations of football stadiums, information on hooligans and possible points of interest. Furthermore, thanks to Leiden University an algorithm has been developed which can connect different data sources to visualize specific types of relationships between people (involved in violence, friends, family, etc.). This data can help in uncovering possible risks regarding violence around football supporter flows by depicting specific high risk people and risk evoking situations.

To guide the data collection of our case study several questions were defined, which are used in semi-structured interview session. The interview is semi-structured to enable us to be more flexible, which can produce unexpected and interesting data. The setup of the case study consists of three experts in the field of football hooliganism and safety, an analyst of the police force, and a researcher who guides the execution of the case study.

The first three questions can help us in the search for possible scenario schemes and their accompanying possible plausibility and impacts values for each argument. Furthermore, questions 4 and 5 enable us to gain an understanding of how plausibility and impact values could be determined in the real world. Finally, we zoom in on the relations between arguments in question 6 by researching how arguments could complement each other.

Question 1: Considering the risk matrix and possible other sources, what are common clusters of risk factors?

Question 2: Considering the risk matrix and possible other sources, what are common controls?

Question 3: To fill in the matrix information on routes, supporters etc. is gathered. How can we somehow estimate the reliability of this information?

Question 4: How can we estimate to what degree a certain risk factor adds to the plausibility and impact of a risk scenario?

Question 5: How can we estimate to what degree a certain control decreases the plausibility or impact of a risk scenario?

Question 6: Not all of the controls will have the same effect on the plausibility and impact of a risk scenario. When and why do we, or do we not pick which control?

Question 7: Some risk factors can increase the plausibility and impact of other risk factors outweighing other risk factors. How can we cope with this?

7.2 Case study evaluation

To clarify how our model can be used in practice, an example is provided in this section, which explains how to construct scenarios, uncover risk and controls, and how to determine the plausibility and impact of arguments and scenarios. Furthermore, this example illustrates how our model is capable of supporting the risk assessment processes of the Risk management process framework (RMPF) by AIRMIC (2002) as described in Section 2.3. The RMPF states that a model for risk assessment should be capable of supporting several processes, i.e. risk identification, risk description, risk estimation and risk evaluation. Since our model is dynamic, in the sense that it enables overlap between the different processes, our example will not explicitly separate the different processes.

The first process (risk identification) of the example is described from both a top-down approach as well as bottom-up approach to illustrate how the different approaches can be used in risk assessment. The remaining processes do not differ in terms of how they are handled in the top-down or bottom-up approach. First an overview of the case is given in the following section.

7.2.1 Background

In six weeks there is a match between Ajax and Feyenoord in 'de Kuip', the home base of Feyenoord in the city of Rotterdam. To discuss the possible risks that can occur before and after the match a team of people with knowledge of security, safety, regulation and other relevant fields gather around an iTable (see Section 1.2). The iTable can be used to visualize and present data that can serve as evidence for the construction of scenarios, such as routes, possible risk evoking persons, et cetera. The final goal of the meeting is to construct possible scenarios about what could happen when the supporter groups from both football clubs move from and to the football stadium, and how the risks that might result from these flow of supporters can be mitigated.

7.2.2 Risk identification, description and estimation

In this phase, different possible risks are identified. As mentioned above, the team can start off with some scheme of risk factors and controls as in the top-down approach, or they can start off blank and infer possible risk factors and controls from the evidence at hand as in the bottom-up approach.

The **top-down approach** assumes there is already some scheme which list possible risk factors and controls. Since we defined some scenario schemes, we can select one of the schemes which could apply to our situation, e.g the scheme described below.

Scenario scheme: a fight due to crossing routes

- **Risk that the scheme explains:** a fight between group X and group Y
- **Central action of the scheme:** the routes of X and Y cross.
- **Relevant risk factors:** road construction.
- **Relevant controls:** change routes, advice preferred routes.
- **Relevant information:** group X and route Y, preferred routes.
- **Pattern of actions:** The routes of X and Y cross $\rightarrow$ group X and group Y get into a fight.

The risk factors that are defined in the scheme can be used to construct our scenario. Such scenario schemes can help in uncovering risk factors and controls by offering a template which can be filled in by replacing the variables with constants. This scenario scheme can be used during the construction of a scenario to check for possible risk factor that are not yet addressed.

The **bottom-up approach** assumes we start off blank, without the support of a scenario scheme. Whereas the team started with a pre-defined list of risk factors in the top-down approach, they now have to search for evidence from which the team can extract risk factors and controls. For instance, a document which describes the routes of both supporter groups from home to the stadium. After the team plots the routes on the iTable, they notice that the routes cross and mark this a possible risk factor. One of the experts mentions that crossing routes could result in a fight between Ajax and Feyenoord supporter groups. Furthermore, the expert knows that the supporter groups of Ajax and Feyenoord always fight.

To illustrate how scenario schemes can be applied, the example will elaborate on the **top-down approach**. So starting off with the scenario scheme, the team of risk analysts can check if the risk factors are also applicable for the match between Ajax and Feyenoord by searching for possible evidence and arguments.

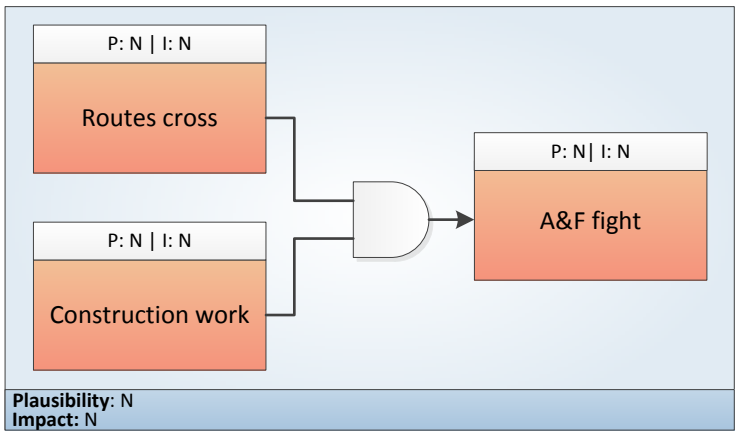

Figure 7.1: Scenario scheme of a routes cross - fight risk scenario

After some discussion, one of the experts concludes that there are different claims and information coming from reliable evidence sources which state that Ajax and Feyenoord might get into a fight (P=0.6). The expert's opinion supports the risk factor 'A&F fight'. The impact of the fight is estimated as possible to result in high damage to people/goods (I=0.8).

The risk analysts consult the iTable and see that the routes of Ajax and Feyenoord indeed cross. After some discussion about the plausibility and impact of the crossing routes on the risk scenario, the experts agree on that it is very plausible that crossing routes might result in a fight between Ajax and Feyenoord, because there is very strong evidence to support and confirm this (P=1.0). Furthermore, the time and place are known. The impact of the risk factor can be described as a possible threat caused by violence, rivalry or special circumstances that can result in reasonable damage to people/goods (I=0.6).

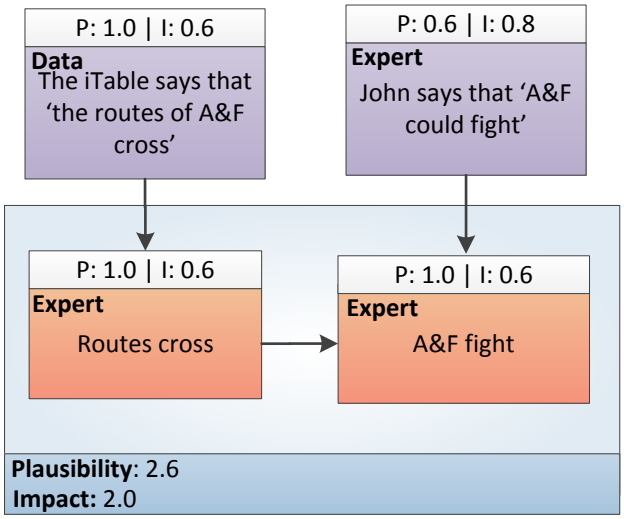

Figure 7.2: Inferring plausibility and impact values

However, the other risk factor that is proposed in the scenario scheme 'construction work' does not apply in this situation and can thus be removed from the risk scenario.

A scenario can be extended by introducing new arguments. For instance, from a database with incidents the team has analyzed some data which states that 'Ajax and Feyenoord supporters always fight'. In addition to the evidence on crossing routes, this data can be used to increase the evidential support of the scenario. So we can add this risk factor to the scenario by combining it with the other risk factor through an AND gate.

Let us assume that the risk factor has a P value of 0.8 and an I value of 0.8. As explained above, an AND gate selects the minimum between a set of values, so the values of 'A&F always fight' are selected. Since, in addition to the two risk factors, there is also some evidence that supports the risk factor 'A&F fight'. According to our rules as defined above, when there are multiple incoming links of the same type (i.e. support/attack), the premise with the highest P value should be selected. Because, the evidence has a lower P value than 'A&F always fight', the values of that risk factor are propagated to the risk factor it supports, i.e. 'A&F fight' (Figure 7.3).

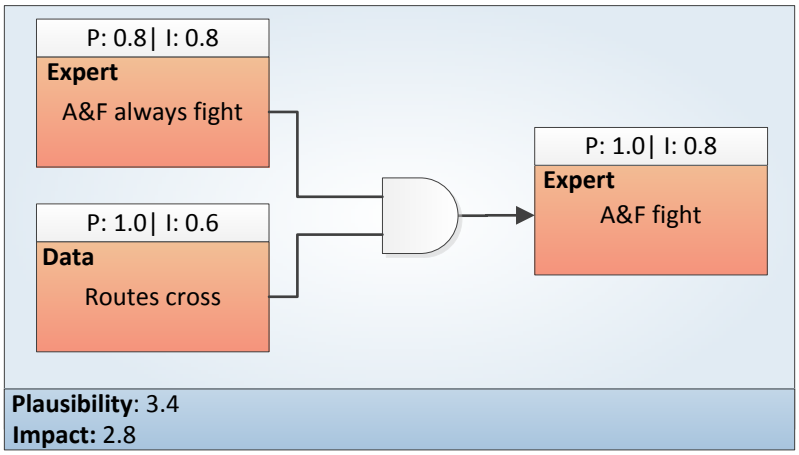

Figure 7.3: Adding a risk factor to the scenario

Suppose the risk analyst uncover more risk factors that could add risk to the risk scenario. For instance, one of the experts knows that the mood amongst the supporters is likely to be negative. Furthermore, another expert knows from experience that in some cases supporters are extremely intoxicated, while in other cases the supporters can still intoxicated, but less significantly less unpredictable. We can add these risk factors to our risk scenario through a combination of AND and XOR gates as visualized in Figure 7.4 on page 92.

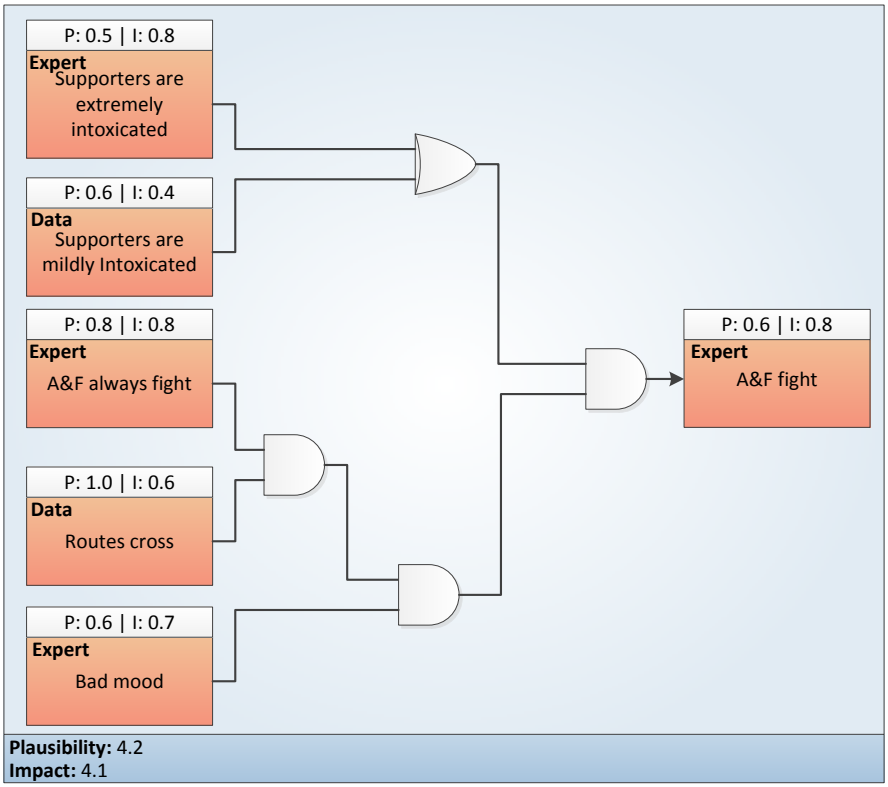

Figure 7.4: Adding risk factors through a combination of logic gates

The P and I values of the risk scenario are calculated according to equations 6.9.1 and 6.9.2. The propagation of plausibility and impact values through the support links and gates happens as follows:

- XOR gate: select the premise with the highest P value.
  In our example, this is 'supporters are mildly intoxicated'.
- AND gate: select the premise with the lowest P score.
  The first AND gate has as an output 'A&F always fight'. The second AND gate returns 'bad mood', and the third AND gate produces 'supporters are mildly intoxicated'.
- Multiple incoming links: select the premise with the highest P value
  In our example the evidence that directly supports the conclusion (risk factor) 'A&F fight' is left implicit, but however does still count towards the evidential support of the risk scenario. Because there are also some risk factors that support the conclusion, we can say that the conclusion has multiple incoming support links. According to our propagation rules described above, the premise with the highest P value is selected, i.e. the evidence that directly supports the conclusion.

Critical questions can be asked to expose sources of doubt in reasoning. Examples of such questions could be 'How credible is *e* as an expert source?' or 'Is *a* consistent with what other experts assert?', where *e* is the team member and *a* is the claim that the Ajax and Feyenoord always fight. Answers to these questions could result in the discovery of for instance new risk factors if source *e* cannot be seen as a reliable source or proposition *a* is doubtful. Let us assume the answer to this question is negative, so we assume that John who claims that 'A&F always fight' is unreliable or biased (P=1.0). As explained in Section 6.6.1, we can use this claim by undercutting the evidence from which the risk factor is inferred. Since the *P* value of the claim 'John is biased' is higher than the *P* value of the evidence which supports 'A&F always fight', the risk factor is defeated. Figure 7.5 is zoomed in on the risk factor and shows how the evidence is being undercut. Because the *P* value of the claim is higher than the *P* value of the risk factor and the risk factor is not supported by other arguments, it is defeated.

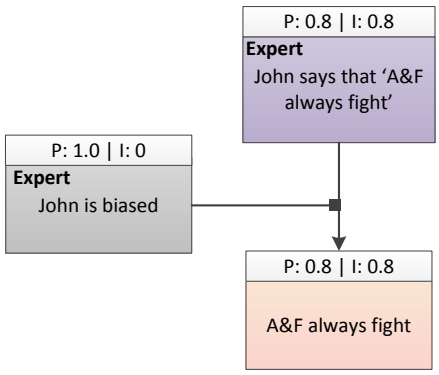

Figure 7.5: A claim inferred from critical questions undercutting evidence

Because a defeated argument is excluded from the risk scenario, the propagation of plausibility and impact values through the support links and gates happens as follows:

- XOR gate: select the premise with the highest *P* value.
  In our example, this is 'supporters are mildly intoxicated'.
- AND gate: select the premise with the lowest *P* score.
  The first AND gate has as an output 'Routes cross', because the other risk factor is defeated. The second AND gate produces 'supporters are mildly intoxicated'.
- Multiple incoming links: select the premise with the highest *P* value
  According to our propagation rules, the premise with the highest *P* value is selected, i.e. the risk factor 'Routes cross'.

Again, the *P* and *I* values of the risk scenario are calculated according to equations 6.9.1 and 6.9.2, which yield *P=3.4* and *I=3.3*.

For now we assume that these are all of the relevant risk factors that are identified by the risk analysts and added to a scenario S_1. Since we want to mitigate risk, the risk factors can be attacked and possibly defeated. Above, already an example was given of how evidence can be undercut and defeated by introducing a claim. However, our model also enables the use of controls to attack and mitigate the risk of a risk scenario. For instance, an expert mentions that deploying anti-riot squads can decrease the plausibility and impact of a fight between Ajax and Feyenoord.

However, as discussed above, a control can sometimes also function as a risk factor. In our example, an expert states that deploying anti-riot squads could likely result in a fight between supporter groups and the police, especially since the mood amongst supporters is bad. With this knowledge, a new risk scenario (S_2) can be constructed (Figure 7.6 on page 95).

Since our model enables the use of scenario schemes, we could construct scenario schemes out of risk scenarios if the risk analysts think that the scenario could be a possible reoccurring pattern of risk factors. The scenario scheme for the newly uncovered risk scenario based on 'Deployment of anti-riot squads', could be defined as follows:

Scenario scheme: a fight between supporters and the police due to the deployment of anti-riot squads

- **Risk that the scheme explains:** a fight between supporters and the police
- **Central action of the scheme:** deployment of anti-riot squads.
- **Relevant risk factors:** bad mood.
- **Relevant controls:** -
- **Relevant information:** number of (risk) supporters.
- **Pattern of actions:** deployment of anti-riot squads $\rightarrow$ supporters and police get into a fight.

For now, we assume these are all of the risks and controls the team can come up with. However, this process of supporting and attacking arguments by using other arguments based on some evidence to uncover new possible risks and controls can be continued until a satisfying level of detail is reached.

7.2.3 Risk evaluation

After analysis of the possible risks, a selection of most plausible and highest impact scenarios is made. Recall that we derived the following plausibility and impact values for our scenario:

$S_1(\text{p}) = 4.2$
$S_1(\text{i}) = 4.1$

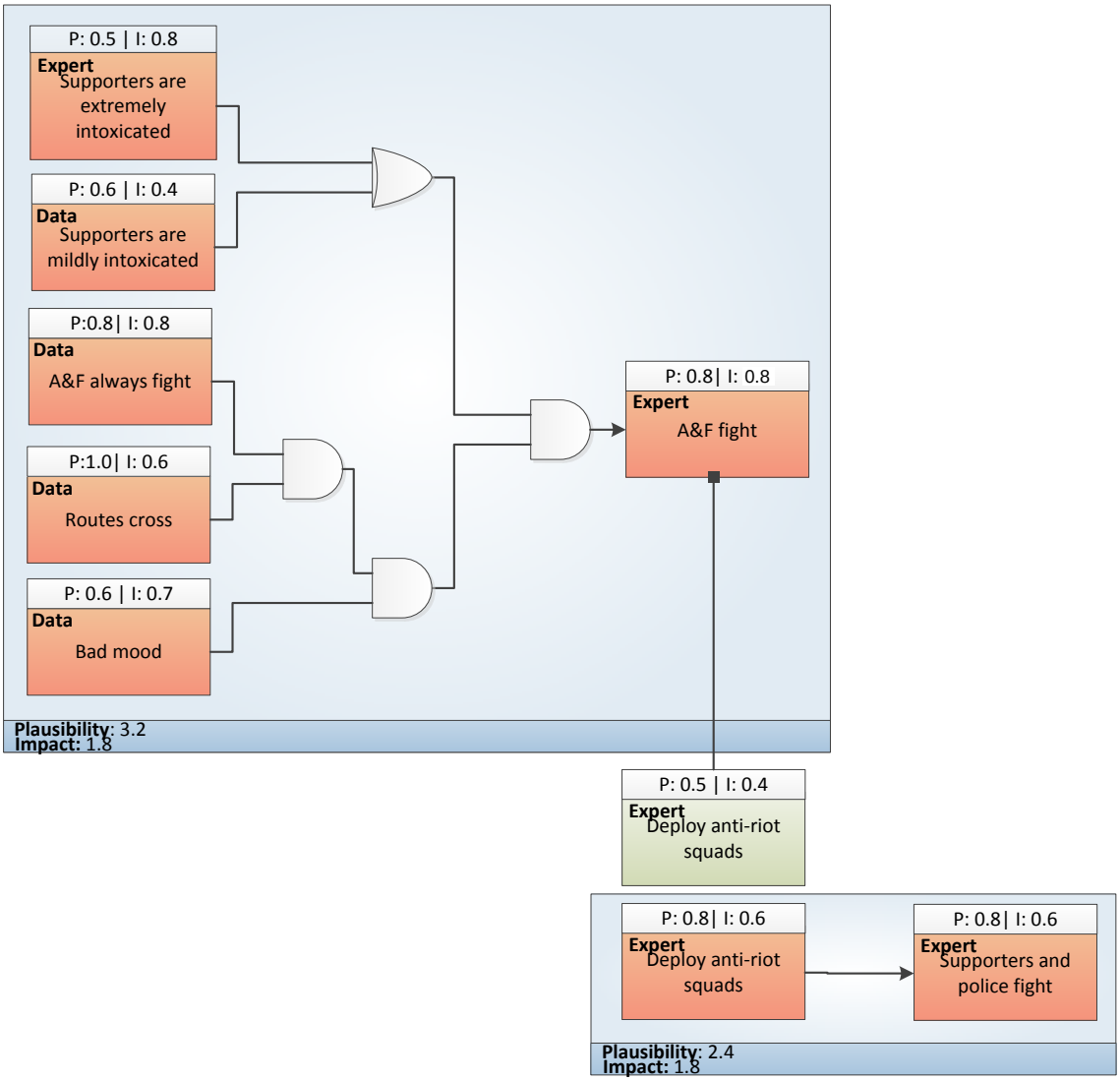

Figure 7.6: Inferring a new risk scenario

S_2(p) = 2.4
S_2(i) = 1.8

Assume we have constructed two more scenarios:

S_3(p) = 1.8
S_3(i) = 3.2

S_4(p) = 4.0

S_4(i) = 1.4

By using the risk matrix as a tool, the team can easily depict which scenario requires the most attention. How the tolerable and intolerable levels are determined was explained in Section 6.9.1. Assume we generate the matrix as visualized in Figure 7.7. By offering a visual comparison of risk scenarios it is easier to decide on which scenarios have a higher risk. Furthermore, the underlying risk factors and controls can be traced back by zooming in on a scenario.

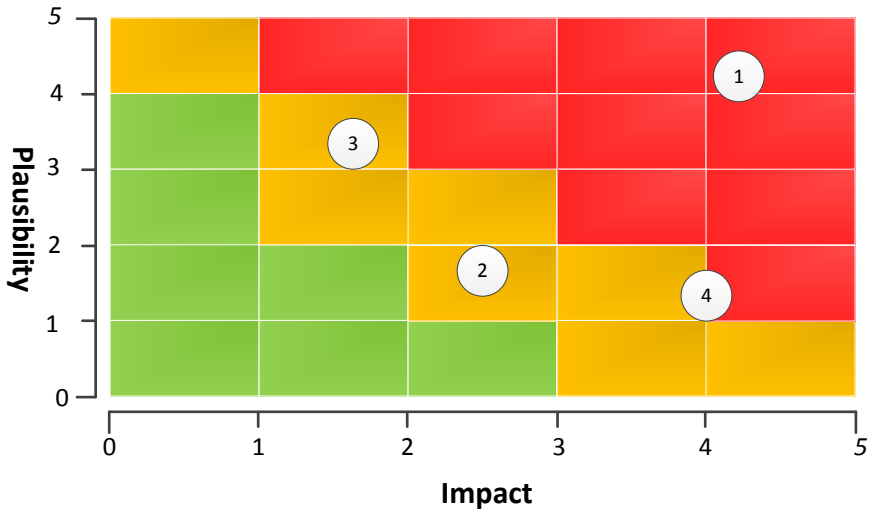

Figure 7.7: Case example risk matrix

Now it is not only easy to see which risk scenarios could possibly evoke the highest risk, but also why and how these scenarios evoke risk, by zooming in on the argumentation structure underlying a specific scenario.

7.3 Data analysis

In this section the data extracted from the interview is analyzed by answering each of the questions as described in the case study protocol. These answers were provided by a group of three experts in the field of football regulation, hooliganism and safety.

7.3.1 Scenario schemes

Because we want to construct possible scenario schemes, possible common clusters of risk factors should be determined. In addition to the risk factors that were extracted from the CIV

risk matrix, the experts pointed out some other relevant risk factors. Based on the experts' experiences and opinions several common combinations could be inferred. In addition to these risk factors, the experts mentioned some common controls which can be applied to several risk factors. The overview of possible risk factors and controls is provided in Appendix B.

The lists of risk factors and controls were used to form clusters of different risk factors and possible controls. In total, six different clusters could be formed (Table 7.3.1). In addition, from the interviews it was extracted which risk factors and control target which groups. Furthermore, the time frame in which the controls are being applied when preparing and monitoring a match were extracted. This information can be useful, because it enables to offer controls to the user which are relevant for the stage they are preparing/monitoring.

Risk	Control target group	Possible controls	Time
Cluster 1	Individual supporters		
Number of risk supporters		Regulation of ticket sales	>6 weeks before the match
Number of supporters with a stadium ban		Contact with individual supporters before match	>1 week before the match
Availability of tickets from alternative sources		Notification duty	Before/during the match
		Monitor ANPR	Before/during the game
Cluster 2	Supporter groups		
Relationship between home/away supporters		Make combi-regeling mandatory	>6 weeks before the match
Preparartion or organisation of violence and disturbance		Governmental: ban on meetings	>1 week before the match
Mood of the supporters		Governmental: ban/limit on alcohol	>1 week before the match
Organisation of a meeting		Surveillance car visibly present	Before/during the match
		Deploy helicopter	Before/during the match
		Contact with supporter (flows)	Before/during the match
Cluster 3	Club		

Rivalry (derby)		Governmental: ban/limit on alcohol	>1 week before the match
History of the match		Regulation of ticket sales	>6 weeks before the match
Position on ranklist		Deploy stewards/security	Before/during the match
Relationship between supporters/team		Opening hours stadium	>6 weeks before the match
Relationship between supporters/board of the club		Contact with individual supporters before match	>1 week before match
Cluster 4	Societal		
Political/racist statements/motives		Surveillance car visibly present	Before/during the match
Media attention		Deploy stewards/security	Before/during the match
Inference with other events		Governmental: change permits	>6 weeks before the match
Cluster 5	Stadium		
Location of home/away supporters		Entertainment in stadium	Before/during the match
Measures of the club (e.g. obligation of identification, etc.)			Before/during the match
House rules of the club			>6 weeks before the match
Infrastructure stadium (possibilities to separate groups)			>6 weeks before the match
Location stadium (crowded areas)			>6 weeks before the match
Cluster 6	Route		
Road construction		Change routes	Before/during the match
Crossing supporter flows		Advice preffered routes	>1 week before the match
Cluster 7	Route		
Number of buses			6 weeks before the match

Number of supporters		>6 weeks before the match
Infrastructure stadium		>1 week before the match
Cluster 8	Route	
Deployment of anti-riot squads		6 weeks before the match
Strictness and enforcement of rules		>6 weeks before the match
Number of risk supporters	Regulation of ticket sales	>6 week before the match

Table 7.1: Cluster of risk factors and controls

Each of these combinations of risk factors can form certain scenarios which are based on the possible consequences of the clusters. The experts defined the possible scenarios as listed in Table 7.2.

	Scenario description (consequence(s))
Cluster 1	Fights between supporters / vandalism
Cluster 2	Fights between supporters / vandalism
Cluster 3	Fights between supporters / vandalism / riots
Cluster 4	Fights between supporters / vandalism / riots
Cluster 5	Fights between supporters
Cluster 6	Fights between supporters
Cluster 7	Fights between supporters / vandalism
Cluster 8	Fights between supporters and police / vandalism / riots

Table 7.2: Possible risk scenarios inferred from clusters

The clusters of risk factors together with possible controls can be formed into scenario schemes. One of the scenario schemes, based on cluster 7, is depicted below. The risk that the scheme explains is based on the possible consequences as defined in Table 7.2. The remaining scenario schemes can be found in Appendix D.

Scenario scheme: a fight due to too many buses

- **Risk that the scheme explains:** a fight between group *X* and group *Y*
- **Central action of the scheme:** Too many buses with supporters.
- **Relevant risk factors:** Bad infrastructure (traffic jams, blocked access to stadium), high number of supporters.

- **Relevant controls:** Deploy double-deck buses.
- **Relevant information:** group X and route Y, number of supporters, number of buses, availability of double-deck buses.
- **Pattern of actions:** Too many buses $\rightarrow$ group X and group Y get into a fight.

7.3.2 Estimating the plausibility and impact of evidence

Since we are not only interested in deriving possible risk factors and controls, but also want to determine their effect in terms of plausibility and impact on a risk scenario, the experts were questioned about how they determine the reliability of evidence. By having an indication of the reliability of information, the plausibility can be determined, that is how plausible is it that the risk factor or control supports or attacks a risk scenario. Furthermore, having insight into the reliability of some evidence, can help us determine more accurately the impact of a risk factor or control on a risk scenario.

As discussed in Section 3.3, the Dutch police force mainly relies on a risk matrix-based approach to risk assessment. However, during the interview the experts mentioned that the risk matrix is often used as a guidance and in most cases the probability and impact values of each seperate risk factor are not estimated. The way in which the Dutch police force estimates the reliability of evidence is by checking the type of source. If some information is coming from the RVD (official information service of the police force), the information is deemed more reliable, and thus more plausible than the information coming from other sources (e.g. social media, rumours). Because most of the expert data is validated by the RVD, the experts pointed out that risk factors and controls inferred from expert opinions can be classified in general as substantial evidence (0.8). Of course not all risk factors and controls are necessarily inferred from expert opinions (or other sources) which have been verified by the RVD. In this case, the plausibility (and impact) are determined by experience and general knowledge.

Not all of the risk factors and controls have the same effect on the risk of a risk scenario. For instance, in the case of a risk factor 'routes cross', this risk factor might have a large effect in case of a match between Ajax and Feyenoord, but this does not mean that for every football club crossing routes can be considered a large risk. Because of that, general plausibility and impact values can be used as a guide to assess risk factors and controls, but the actual plausibility and impact of a risk factor/control should be based on the situation at hand.

As discussed in Section 6.8, the effect of a control on the risk of the situation that is being assessed can be two-fold: risk can be mitigated or risk can be triggered. In our study, the experts mentioned that they do consider the possible negative effects of applying certain controls to a risk scenario. However, the possible risk that could result from an intervention is not always assessed.

7.4 Risk assessment tools

In this section the application of our risk assessment model to develop risk assessments tools is explained. The tool that is being discussed is the iTable application that will be used by the Dutch police force.

7.4.1 iTable

As discussed above, the iTable application can be used to visualize information concerning football supporter flows. One of the main functions of the application is to provide information about hooligans and the relations between different (groups of) hooligans. An example is visualized in Figure 7.8 on page 101.

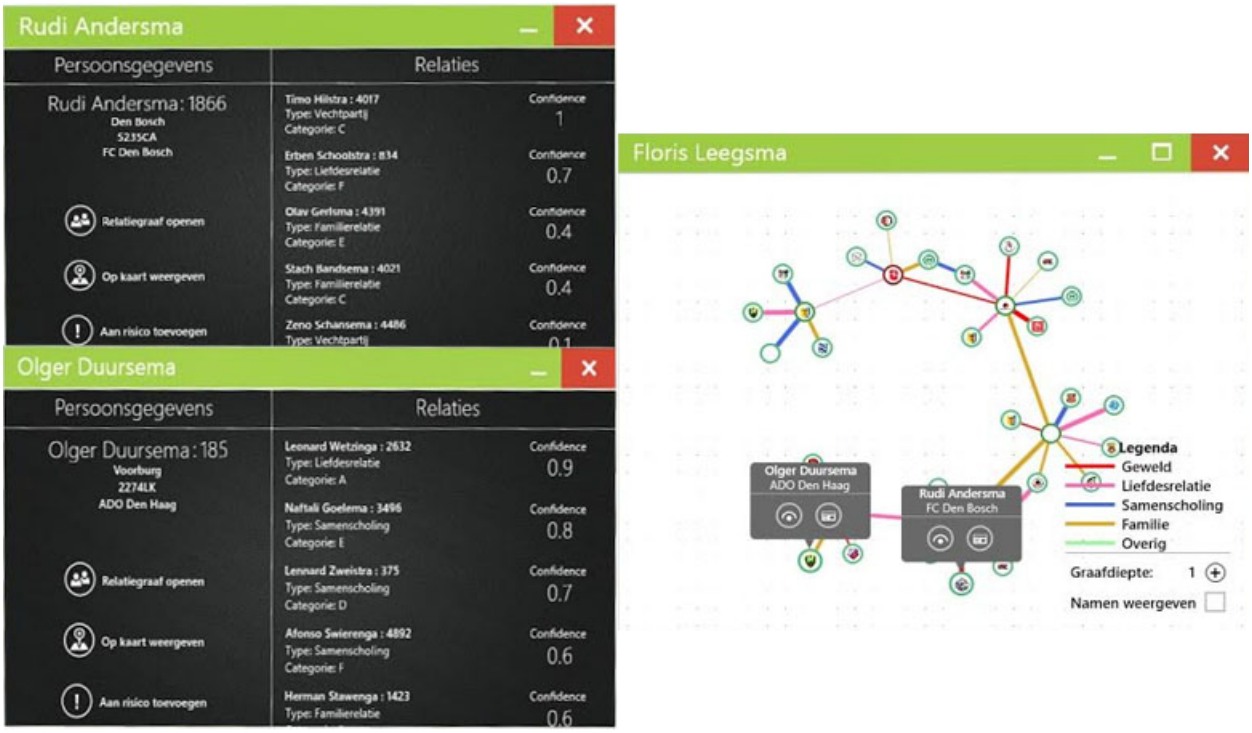

Figure 7.8: Visualization of relationships between people

Different risk factors can be constructed on the iTable from available evidence, such as the visualization of crossing routes. These risk factors can be added to a risk scenario. In addition, controls can be added to attack and defeat risk factors. In Figure 7.9, an example of the visualization of a risk scenario on the iTable is rendered.

Figure 7.9: A scenario on the iTable

The model on the iTable is a simplified version of the model described in this thesis, since it only allows a pattern of argument-counterargument, not more complex patterns, such as argument-counterargument-counter counterargument, etc. In terms of risk assessment this means we can only attacks risk factors with controls, and we cannot attack the controls.

To visualize the risk level of a scenario, an indicator is provided which can switch colors based on how many risk factors are attacked and defeated. The risk level is red if none of the risk factors are defeated, yellow if one of the risk factors is defeated, and green if all of the risk factors are defeated. In terms of plausibility and impact this means that a red indicator assigned to a risk scenario expresses a very plausible and high impact scenario, while yellow and green indicate medium or low plausibility and impact scenarios. Currently, the application does not yet support the input of plausibility and impact values tailored to each risk factors or control as defined in our risk assessment model.

The Dutch police force uses a risk matrix to determine the likelihood and impact of a risk factor and scenario. This matrix can be used as guide to determine the scales to base the plausibility and impact values on. The plausibility value in our model can be related to the 'waarschijnlijkheid' (probability) scale and the impact value can be related to the impact scale on the matrix. We can use the plausibility scale as defined in Section 6.9. Since the impact scale as described in the matrix is specific to the situation at the Dutch police force we can use that scale:

Scale to determine the impact value

0.2 No additional danger compared to an event of the same size.

0.4 Chance of minor damage to people/goods.

0.6 Possible threat caused by violence, rivalry or special circumstances that can result in reasonable damage to people/goods.

0.8 Possible threat caused by the formation of different (organized) groups, which can result in high damage to people/goods.

1.0 Increased possible threat caused by organized violence, rivalry or special circumstances that can result in a significant amount of damage to people/goods.

Our model enables the use of scenario schemes which can represent reoccurring patterns of possible risk factors. Since scenario schemes can support a risk analyst in uncovering risks, it would be useful to extract several scenario schemes from experts in the field of football hooliganism.

Data model

To implement the risk assessment model into the iTable, the following data model can be used (Figure 7.10). This data model shows that scenarios consist of arguments and can be assigned a scenario scheme. Furthermore, the arguments can be assigned an argumentation scheme, which can contain several critical questions.

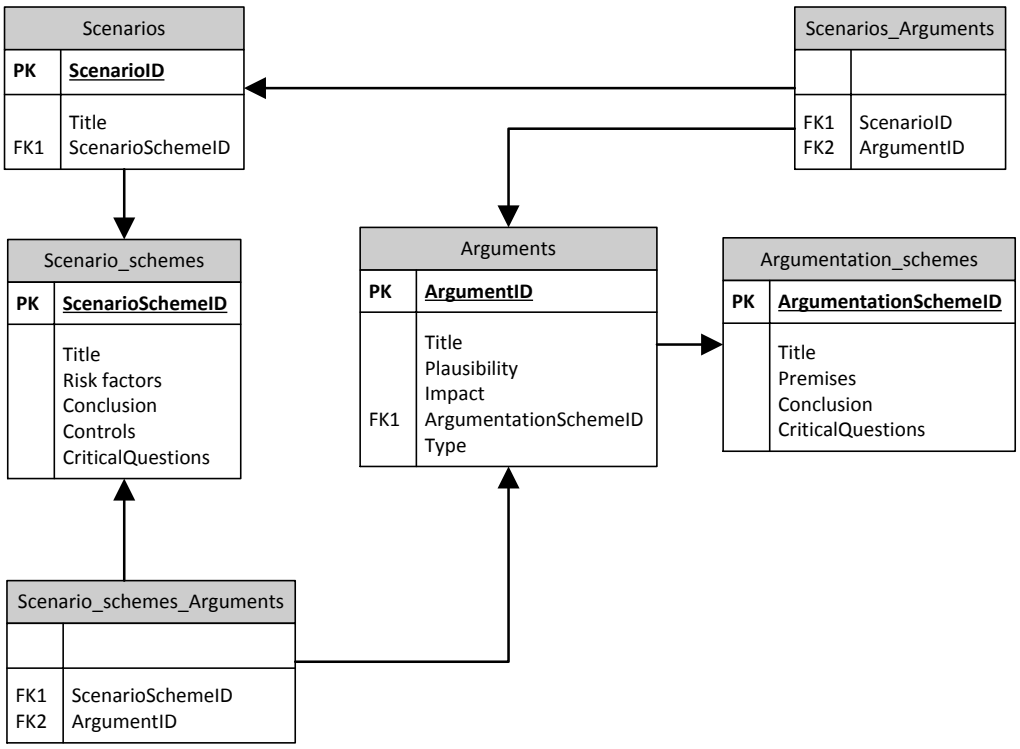

Figure 7.10: Data model for implementation in iTable

8

Conclusion

In this chapter an answer is given to our main research question:

How can a risk assessment model be developed which enables the identification and analysis of scenarios, risks and controls, while not requiring complex mathematical, statistical or formal knowledge?

Several sub-questions were defined to guide the research of the main research question. The conclusions of the sub-questions are provided in the following sub-sections, after which an answer is given to the main research question.

8.1 Conclusions of sub-questions

The conclusions of the first, second and third sub-question are derived from literature research in the field of risk management. Furthermore, the practice of risk management at the Dutch police force is taken into account to answer the third sub-question. The answer to the fourth sub-question is based on research into the hybrid theory and is combined with the knowledge extracted from the previous sub-questions. Finally, the results from the case study are used to answer question five.

8.1.1 Question one

Which methods and tools are available to support and perform risk assessment?

In Table 8.1 an overview is presented of the analyzed risk assessment methods and tools in this thesis. This list is not exhaustive, but based on the literature research, these methods and tools were extracted as the most common risk assessment methods and tools.

	Qualitative	Quantitative
Methods	SWIFT	ETA & FTA
	FMECA	Markov method
	HAZOP	
	RISA	
Tools	Risk matrix	Petri nets
	Cause and effect diagram	Bayesian network

Table 8.1: Analyzed risk assessment methods and tools

Not all of the methods and tools are exclusively qualitative or quantitative, but because there is a preferred approach to each method and tool, the methods and tools are presented as such in Table 8.1.

8.1.2 Question two

What are the drivers and requirements of using a method for risk assessment?

From the literature on risk management in general and topics related to risk management at the Dutch police force, a list of requirements for a risk assessment model was compiled.

- Scenarios
  Because risk scenarios can show how risk factors and controls are related, it is easier to comprehend how the risk of a scenario is inferred from the risk events (i.e. risk factors) that constitute a possible risk scenario. Furthermore, scenarios can expand one's thinking. First of all, because risk factors and controls that are relevant to one scenario could be input for other possible risk scenarios. Second of all, by developing a clear overview of how risk factors and controls are connected in a risk scenario, otherwise unknown possible risks can be uncovered by checking what could cause or be the effect of a risk factor or control.
- Accessible
  One of the main requirements of our risk assessment model states that the model should not be dependent on complex mathematical or formal knowledge. However, because quantitative risk assessment can give a more detailed view of risk, the model should enable quantitative analysis of risk. Since the common 'probability x impact' approach to

risk assessment requires understanding of probability values, our model implements a 'plausibility x impact' approach.

- Systematic
  To be able to consistently use the model, and to determine plausibility and impact values, a systemic approach is required. Our model has its roots in the hybrid theory, which proposes a structured approach to making sense of evidential data. In addition, a set of rules is defined to determine the plausibility and impact values of risk factors, claims, controls and scenarios.
- Dynamic
  A dynamic risk assessment model enables to easily construct or extend risk scenarios by adding risk factors and controls. Because our model is based on a systematic approach and a clear set of rules, it provides a convenient solution to the uncovering of risk factors and controls

8.1.3 Question three

What are the limitations of current risk assessment methods and tools?

Literature research and expert opinions of the Dutch police force were used to identify limitations (Appendix A). In sum, first of all, the requirement of complex mathematical or formal knowledge can form a constraint on the applicability of a risk assessment model, if that specific knowledge is not available. For instance, complex tools, such as a Bayesian network requires (complex) probability value estimations. However, more simple methods and tools, such as a risk matrix, cause and effect diagram, SWIFT, FMECA, and HAZOP, do not facilitate a comprehensive view of risk factors and controls in relation to each other. A clear view on risks is necessary to improve the risk assessment process, because risks that make sense enable to adequately act upon risks.

8.1.4 Question four

How can the hybrid theory be applied to risk assessment?

To answer this sub-question, three underlying questions were defined.

a) How can the concepts of the hybrid theory be translated to risk assessment?

The hybrid theory can be applied to risk assessment by viewing risk scenarios as a set of connected risk events which can be supported and attacked by other risk factors, claims and controls.

To depict and structure reoccurring patterns of risk events, scenario schemes can be constructed. In the hybrid theory it is mentioned that such schemes can aid an analyst in quickly developing and analyzing scenarios by offering templates which can be referred to. In the same way, our model enables the use of scenario schemes to quickly uncover risks and control, Furthermore, such schemes can be used to check for possible gaps in reasoning about a certain risk scenario. Several scenario schemes were extracted from an interview with experts of the Dutch police force. To uncover possible doubts in reasoning about the risk scenario, critical questions can be asked. The answers to these questions can result in the identification of new risks and controls.

Like with scenario schemes, argumentation schemes can depict and structure reoccurring patterns. However, in contrast to scenario schemes, which are more complex structures used to act as general background for a scenario, argumentation schemes only apply to a single inference. Such schemes can also be assigned critical questions to uncover possible doubts in risk factors, controls and claims.

b) How can risk assessment be supported by stories and arguments?

Risk scenarios in the context of risk assessment can be related to stories as defined in the hybrid theory, because in both contexts a scenario is constructed from events which are and can be supported by other arguments. However, the hybrid theory is focused on explaining past events, while risk assessment is aimed at predicting possible events. The difference here is that in risk assessment one cannot assume that there is some explanandum, because it is not possible to judge a possible event in the future as an undeniable fact.

The risk events in risk scenario are the conclusions of arguments about these risk events. The concept of arguments from the hybrid theory translates to risk factors and controls as known in risk management, in addition to the new concept of claims. Risk factors can be added to a risk scenario and are considered the risk events that should be mitigated. Controls can then be used to mitigate risks by attacking and defeating arguments that support a risk scenario. Finally, claims can support and attack risk factors, controls and other claims.

c) How can coherent scenarios be defined?

According to the hybrid theory, there are three criteria for determining the coherence of a scenario: 1) the scenario has to conform to a plausible scenario scheme, 2) the events should be plausible, and 3) the scenario should not contain contradictions. The plausibility of a risk scenario is the extent to which the risk events are supported by arguments and can be determined by taking the sum of the risk events and evidence that directly support a conclusion and which are not defeated. Since each risk scenario can have a different impact on the situation at hand, it is also interesting to take this parameter into account. Also the impact of a risk scenario is based on the risk events and evidence that directly supports the conclusion.

To increase the plausibility and impact of a risk scenario, risk factors can be added to the sce-

nario. These risk factors are essentially the risk events and can be supported and attacked by evidence and claims based on evidence. Increasing the support of a scenario by adding (arguments based on) evidence increases the evidential support of the scenario. Likewise, the evidential contradiction of a scenario can be influenced by attacking and defeating risk factors/claims that support the scenario. In Section 6.9, we defined a set of rules for the propagation of plausibility and impact values through arguments.

By providing scenario schemes to a risk analyst, relevant risk scenarios can be quickly uncovered, because such schemes represent templates of reoccurring patterns of risk factors and possible relevant controls. Furthermore, scenario schemes can be used to check for doubts in reasoning about a risk scenario, by checking the scheme for common (combinations of) risk factors and controls. The scenario schemes that were constructed as a result of the case study are based on expert knowledge and experience and can thus serve as plausible scenario schemes.

8.1.5 Question five

What is the added value of risk assessment based on the hybrid theory?

Implementing our model enables to make sense of data and can improve the construction of scenarios, because it provides an accessible, systematic and dynamic way of inferring risks and controls from (a combination of) different evidence sources and scenario schemes. Furthermore, because the model can be understood without requiring complex knowledge, it can be easily implemented in methods and tools. An example of such a tool has been developed at the Utrecht University by a group of informatics students.

As part of their bachelor thesis, the students developed an iTable application, which can implement a simplified version of our risk assessment model. The added value of the iTable application is the possibility to visualize and uncover risks that could be relevant for a certain match, by offering information on routes, football stadiums, clubs, and other points of interest. Furthermore, an in-depth analysis of relationships between groups of person and individual persons can be conducted, by analyzing visualizations of social networks. An underlying risk assessment model can help to make sense of available evidence extracted from data, to create a meaningful view on risk.

However, to be able to give a definite answer to this question, the model should be evaluated by observing in practice to what extent the model enables the construction and analysis of risk scenarios. The evaluation can give insight in what the possible strengths and weaknesses of the model are by checking if more relevant risks are identified and acted upon in comparison to the current situation.

8.2 Conclusion of main question

The main research question is answered by the sub-questions. To develop a risk assessment model which *enables the identification and analysis of scenarios, risks and controls, while not requiring complex mathematical, statistical or formal knowledge*, the concepts and ideas as proposed in the hybrid theory by Bex (2011) were applied to risk assessment and combined in a model, which exists of four concepts (Figure 8.1)

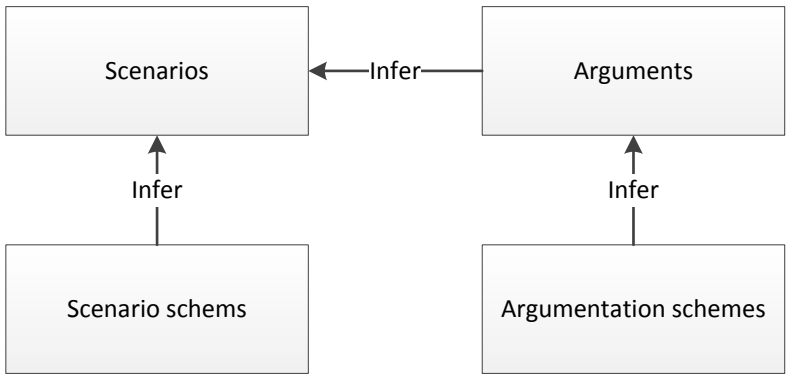

Figure 8.1: Structure of the risk assessment model

Arguments can be inferred from argumentation schemes, whereas scenarios can be inferred from scenario schemes. Arguments can be used to support or attack a risk scenario, so the risk scenario is inferred from different arguments.

In our case study we examined an organization which assesses risk according to a matrix-based approach. As pointed out by one of the experts during the interview, a risk matrix is often used as guideline, not as an actual tool to assess risk. This can be explained by two factors. First of all, the experts find the process of filling in the probability and impact values quite consuming. Second of all, the risk matrix is not always sufficiently extensive, in the sense that it does not give proper directions to relevant risk factors. Our hybrid-argumentative risk assessment model could provide a solution to these two limitations, because it enables to make sense of risk by determining the plausibility and impact values through everyday concepts of scenarios (stories) and arguments. Furthermore, arguments about risk can uncover new risks and possible controls.

In sum, our model enables to make sense of risks, because risk analysts can identify and analyze risk scenarios in a natural way based on intuitive concepts of scenarios and arguments. As a result, the model can be used to assess and compare risk scenarios without the requirement of complex mathematical or formal knowledge. Furthermore, the concepts and ideas in the model can be used to develop risk assessment methods and tools. An example, as described earlier on

in this thesis, is the iTable application, which supports risk analysts at the Dutch police force in identifying and acting upon possible risks around football supporter flows.

9

Discussion

The research process has resulted in several limitations to the development of the risk assessment model. In Section 9.1 the limitations of the case study will be grouped as threats to construct validity, internal validity, external validity and reliability. In Section 9.2 suggestions for improvements for future research are presented.

9.1 Limitations

A general limitation of this research is concerned with the mostly theoretical foundation of this research. Even though the model adapts the concepts and ideas as defined in the hybrid theory, we cannot conclude the possible benefits of our model, because multiple studies of actual cases are required to do so.

In the following sub-sections an explanation is given of the different types of threats that were raised during the execution of our study. The definitions of the different threats to validity are based on the work by Wohlin et al. (2012).

9.1.1 Construct validity

This validity measure reflects to what extent the study represent what the researcher has in mind and what is investigated according to the research questions. Since we were not able to evaluate the model, the case study focused on identifying possible risk scenarios. With the questions asked during the case study some scenario schemes could be defined and validated by experts.

The implementation of the model in an actual case setup was not evaluated. However, a case example was provided to describe and explain how the model can be used in practice. Nevertheless, to draw conclusions on the added value of the model for an actual risk assessment case, the results in terms of the ability to actually increase the identification and mitigation of risks should be assessed. In order to compare the results of a risk assessment with and without applying the model, a treatment and control group should both conduct a risk assessment on the same case. By analyzing if the treatment groups performs better than the control group, conclusions can be drawn on the added value (or possible limitations) of the risk assessment model as proposed in this thesis.

9.1.2 Internal validity

This aspect is of concern when causal relations are examined. In our case, this means that the results of a possible application of our model are addressed to the model and no other factors. However, since we only evaluated our model by means of a theoretical case and the results were not controlled with a control group, it is difficult to draw strong conclusions on the results of risk assessment based on our model.

9.1.3 External validity

This aspect of validity is concerned with to what extent it is possible to generalize the findings. The outcome of the questions we defined to uncover risk scenarios can be used to identify common risk and controls when asked in a different setup. Our model is not bound to one specific field of application and provides abstract concepts which can be used to develop risk assessment methods and tools. However, since the model has not yet been evaluated in practice, but a case example is provided based on a possible real life scenario, the external validity is poor. Furthermore, multiple case studies should be conducted to validate and generalize the results from our study.

9.1.4 Reliability

The reliability refers to the consistency and repeatability of the study and is concerned with to what extent the data and analysis are dependent on the specific researchers. The process of constructing possible scenario schemes has been elaborately described to make the study repeatable. Furthermore, a comprehensive example was given in the case study evaluation, which explains how the different concepts of the model can be applied and how plausibility and impact values can be determined.

9.2 Future research

The research as discussed in this thesis has triggered some possibilities for future research.

First of all, since the model has not yet been evaluated in practice, case studies should be conducted to assess the strengths and weaknesses of applying the risk assessment model in practice. These case studies should compare to what extent the model enables the construction of risk scenarios and what are the improvements made to the risk assessment process compared to other (previously used) models. A risk assessment process can be judged as improved if more relevant risks can be uncovered, in addition to more effective ways of mitigating these risks.

Second of all, scenario schemes can be of great support when developing risk scenarios due to their generic nature and suggestions for possible risk factors and controls. It would be interesting to investigate how scenario schemes can be automatically uncovered. For instance, if there are multiple records in a database from which can be inferred that Person X always gets arrested at match Y because of vandalism, this knowledge can be added to a scenario scheme. Also, relevant risk factors can be uncovered by checking which reoccurring relations with other risk factors in the scenario exist.

Finally, the model could be extended by allowing to reason about the generalizations that connect the different risk events in a risk scenario. Currently, these generalizations are only used to infer conclusions from premises. However, the generalizations could also be supported and attacked by arguments to make sense of how the events are connected. One of the difficulties of supporting and attacking generalizations is the propagation of plausibility and impact values through links and arguments. For instance, if 'Ajax and Feyenoord always fight' supports 'Ajax and Feyenoord fight', the generalization between the events could be something like 'If Ajax and Feyenoord always fight, then Ajax and Feyenoord fight'. If we support this generalization and increase the plausibility value, does this mean that the plausibility value of 'Ajax and Feyenoord fight' is increased, or are we saying that the effect of both events on the risk scenario is increased? And how is this reflected in the propagation of plausibility and impact values?

References

Adang, O. (2007). Openbare ordehandhaving. In C. Fijnaut, E. Muller, U. Rosenthal, & E. van der Torre (Eds.), (p. 803). Deventer: Kluwer.

Adang, O. (2010). Initiation and escalation of collective violence: A comparative observational study of protest and football events. *Preventing Crowd Violence*, 47-68.

Adang, O., & Brown, E. (2008). Policing football in europe: Experiences from peer review evaluation teams. *Apeldoorn: Police Academy of the Netherlands*.

AIRMIC, I., ALARM. (2002). A risk management standard.

Atkinson, R., & Flint, J. (2001). Accessing hidden and hard-to-reach populations: Snowball research strategies. *Social research update*, *33*(1), 1-4.

Aven, T. (2007). On the ethical justification for the use of risk acceptance criteria. *Risk Analysis*, *27*(2), 303-312.

Aven, T., & Vinnem, J. E. (2005). On the use of risk acceptance criteria in the offshore oil and gas industry. *Reliability Engineering & System Safety*, *90*(1), 15-24.

Berg, H.-P. (2010). Risk management: Procedures, methods and experiences. *Risk Management*, *1*.

Bergmans, H., van der Hors, J., Janssen, L., Pruyt, E., Veldheer, V., Wijnmalen, D., … van de Leur, J. (2009). *Working with scenarios, risk assessment and capabilities in the national safety and security strategy of the netherlands* (Tech. Rep.).

Bex, F. J. (2009). Analysing stories using schemes. *Legal Evidence and Proof: Statistics, Stories, Logic*, 93-116.

Bex, F. J. (2011). *Arguments, stories and criminal evidence: A formal hybrid theory* (Vol. 92). Springer.

Bex, F. J., Prakken, H., Reed, C., & Walton, D. (2003). Towards a formal account of reasoning about evidence: argumentation schemes and generalisations. *Artificial Intelligence and Law*, *11*(2-3), 125-165.

Bex, F. J., Prakken, H., & Verheij, B. (2007). Formalising argumentative story-based analysis of evidence. In *Proceedings of the 11th international conference on artificial intelligence and law* (p. 1-10). ACM.

Bex, F. J., Van Koppen, P. J., Prakken, H., & Verheij, B. (2010). A hybrid formal theory of arguments, stories and criminal evidence. *Artificial Intelligence and Law*, *18*(2), 123-152.

Card, A. J., Ward, J. R., & Clarkson, P. J. (2012). Beyond fmea: The structured what-if technique (swift). *Journal of Healthcare Risk Management*, *31*(4), 23-29.

CIV. (2013). *Jaaroverzicht seizoen 2012 / 2013; veiligheid en openbare ordebeheersing rondom het nederlands betaald voetbal* (Tech. Rep.). Centraal Informatiepunt Voetbalvandalisme 2013.

CIV. (2014). *Jaaroverzicht seizoen 2013 / 2014; veiligheid en openbare ordebeheersing rondom het nederlands betaald voetbal* (Tech. Rep.). Centraal Informatiepunt Voetbalvandalisme 2014.

Cope, N. (2004). 'intelligence led policing or policing led intelligence?'integrating volume crime analysis into policing. *British Journal of Criminology*, *44*(2), 188-203.

Cox, L. A. (2008). What's wrong with risk matrices? *Risk analysis*, *28*(2), 497-512.

Cox, L. A. (2009). Limitations of risk assessment using risk matrices. In (p. 101-124). Springer.

den Hengst, M., Rovers, B., & Regterschot, H. (2014). *Intelligence bij evenementen: Een inventarisatie van risicomanagementpraktijken bij de politie.* (1st ed.). Den Haag: Boom Lemma.

Dhillon, B. S. (2006). *Maintainability, maintenance, and reliability for engineers.* CRC Press.

Dung, P. M. (1995). On the acceptability of arguments and its fundamental role in nonmonotonic reasoning, logic programming and n-person games. *Artificial Intelligence*, *77*(2), 321-357.

Fenton, N., & Neil, M. (2005). Visualising your risks.

Fenton, N., & Neil, M. (2011). The use of bayes and causal modelling in decision making, uncertainty and risk. *CEPIS Upgrade 12 (5)*, 10-21.

Fenton, N., & Neil, M. (2012). *Risk assessment and decision analysis with bayesian networks.* CRC Press.

Ferwerda, H., & Adang, O. (2005). Hooligans in beeld: van veel blauw naar slim blauw. *Tijdschrift voor de Politie*, *12*, 18-20.

Franqueira, V. N., Tun, T. T., Yu, Y., Wieringa, R., & Nuseibeh, B. (2011). Risk and argument: a risk-based argumentation method for practical security. In *Requirements engineering conference (re), 2011 19th ieee international* (p. 239-248). IEEE.

Gomes, A., Mota, A., Sampaio, A., Ferri, F., & Buzzi, J. (2010). Systematic model-based safety assessment via probabilistic model checking. In (p. 625-639). Springer.

Haley, C. B., Laney, R., Moffett, J. D., & Nuseibeh, B. (2008). Security requirements engineering: A framework for representation and analysis. *Software Engineering, IEEE Transactions on*, *34*(1), 133-153.

Helbing, D., & Mukerji, P. (2012). Crowd disasters as systemic failures: analysis of the love parade disaster. *EPJ Data Science*, *1*(1), 1-40.

Hopkin, P. (2012). *Fundamentals of risk management: understanding, evaluating and implementing effective risk management.* Kogan Page Publishers.

HSE. (1992). The tolerability of risk from nuclear power stations.

Jaeger, C. (2010). Risk, rationality, and resilience. *International Journal of Disaster Risk Science*, *1*(1), 10-16.

Krause, P., Fox, J., & Judson, P. (1993). An argumentation-based approach to risk assesment. *IMA Journal of Management Mathematics*, *5*(1), 249-263.

Muller, E. R., Zannoni, M., Ammerlaan, K., Schaap, S., Uildriks, N., & van der Varst, L. (2010). *Ordeverstoringen en groepsgeweld bij evenementen en grootschalige gebeurtenissen* (Tech. Rep.).

Ostrom, L. T., & Wilhelmsen, C. A. (2012). *Risk assessment: tools, techniques, and their applica-*

tions. John Wiley & Sons.

Ozog, H., & Perry, J. (2002). Designing an effective risk matrix. *Mosaic Corp.White Paper.Salem*.

Prakken, H., Ionita, D., & Wieringa, R. (2013). Risk assessment as an argumentation game. In (p. 357-373). Springer.

Prakken, H., & Vreeswijk, G. (2002). Logics for defeasible argumentation. In (p. 14-15). Springer.

Radu, L.-D. (2009). Qualitative, semi-quantitative and, quantitative methods for risk assessment: Case of the financial audit. *Analele Stiintifice ale Universitatii" Alexandru Ioan Cuza" din Iasi-Stiinte Economice*, *56*, 643-657.

Rausand, M. (2011). *Risk assessment: Theory, methods, and applications* (Vol. 115). John Wiley & Sons.

Rosenberg, J. V., & Schuermann, T. (2006). A general approach to integrated risk management with skewed, fat-tailed risks. *Journal of Financial Economics*, *79*(3), 569-614.

Roxburgh, C. (2009). The use and abuse of scenarios. *McKinsey Quarterly*, *1*(10), 1-10.

Spaaij, R. (2013). Risk, security and technology: governing football supporters in the twenty-first century. *Sport in Society*, *16*(2), 167-183.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *Nist special publication*, *800*(30), 800-830.

Stott, C., & Reicher, S. (1998). Crowd action as intergroup process: Introducing the police perspective. *European Journal of Social Psychology*, *28*(4), 509-529.

Streeton, R., Cooke, M., & Campbell, J. (2004). Researching the researchers: Using a snowballing technique. *Nurse Researcher*, *12*(1), 35-46.

Vagias, W. M. (2006). Likert-type scale response anchors. *Clemson International Institute for Tourism & Research Development, Department of Parks, Recreation and Tourism Management*.

Van den Braak, S. W. (2010). Sensemaking software for crime analysis.

van de Weerd, I., & Brinkkemper, S. (2008). Meta-modeling for situational analysis and design methods. *Handbook of research on modern systems analysis and design technologies and applications*, *35*.

Verschuren, P., Doorewaard, H., & Mellion, M. (2010). *Designing a research project*. Eleven International Publishing.

von Alan, R. H., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, *28*(1), 75-105.

Walton, D. (1996). *Argumentation schemes for presumptive reasoning*. Lawrence Erlbaum Associates.

Walton, D., Reed, C., & Macagno, F. (2008). *Argumentation schemes*. Cambridge University Press.

WHO. (2009). Risk characterization of microbiological hazards in food. *Microbiological Risk Assessment Series.*.

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). *Experimentation in software engineering*. Springer Science & Business Media.

Xu, H., & Bechta Dugan, J. (2004). Combining dynamic fault trees and event trees for probabilistic risk assessment. In *Reliability and maintainability, 2004 annual symposium-rams* (p. 214-219). IEEE.

Yin, R. K. (2013). *Case study research: Design and methods*. Sage publications.

A

Limitations overview of risk assessment methods and tools

Type	Method/tool	Limitations
Qualitative	Risk matrix	- Do not always provide qualitatively useful information for setting,risk priorities and for identifying risks that are high enough to worry, about and risks that are low enough to be neglected (Cox, 2009). - Assigning probability and impact values is difficult and can result in poor decision making. - Does not provide a means to construct causal sequences i.e. scenarios.
	SWIFT	- Not thorough, in the sense that identification of risks and controls is limited (Rausand, 2011). - Highly dependent on checklists prepared in advance, and on the experience of the leader and available knowledge within the team (Rausand, 2011).
	FMECA	- Cause and effect diagrams do not rank the causes in an "if-then" manner (Rausand, 2011). - Success depends on the experience of the analysts (Rausand, 2011). - Does not consider risks caused by a combinations of events (Rausand, 2011), therefore providing no clear overview of causal relationships within a scenario. -
	HAZOP	- Success depends on the knowledge of the team (Rausand, 2011). - Produces lengthy documentation (Rausand, 2011).

Type	Method/tool	Limitations
Quantitative	Bayesian network	- Require the use of a computer application even for very small systems (Rausand, 2011). - Not easily understood by people without a statistical/mathematical background (Fenton & Neil, 2012).
	ETA & FTA	- Not easily understood by people without a statistical/mathematical background (Rausand, 2011). - Not very useful when working in dynamic environments (Rausand, 2011). - Can become too rigid in its requirements (Rausand, 2011).
	Markov method	- Not suitable for the identification of (sequences of) causes and risk events (Rausand, 2011).
	Petri nets	- Not suitable for the identification of (sequences of) causes and risk events (Rausand, 2011).

B

Risk factors football supporter

Risk factors extracted from the matrix
Number of “not” risk supporters
Number of risk supporters
Number of stadium bans
Level of activity
Mood (positive/negative)
Signs of organizing a gathering
Match history of the past three years
History of the current season
Rivalry between playing clubs
Risk factors extracted from experts
Availability of “Kruidvat kaartje” (free traveling train ticket for a fixed lowered price”)
If a match is assigned level A (see Section 3.1), increased risk due to unregulated traveling.
Inconsistent frisking of risk supporters
Time of the match (and other possible matches)
A long bus/train drive to/from the stadium and no planned break
Deployment of anti-riot squads
An exceeding amount of bus lines traveling from and to the stadium.
Strictness and enforcement of rules
Weather conditions

Table B.1: Overiew of risk factors related to football supporter flows

Controls extracted from the matrix
Make use of the 'combi-regeling' mandatory
Change transportation options
Regulate ticket sales
Change the opening hours of the stadium.
Ban/limit the sales of alcohol
Deploy stewards/security
Ban on meetings
Controls extracted from experts
Separate supporter groups in buses
A reliable, timely and clear information supply towards the supporters before the match
Use 'spotters' dressed as civilians to monitor the supporter groups
Time of the match (and other possible matches)
Proper traffic regulation to prevent traffic jams
Deployment of anti-riot squads
Deploy double-deck buses
Monitor ANPR
Make video surveillance visibly present
Deploy helicopter
Contact with supporter (flows)
Change permits
Change routes
Advice preferred routes

Table B.2: Overview of possible controls related to football supporter flows

C

CIV risk matrix

Risicoanalyse Matrix THUIS

Wedstrijd : **Datum :** **Tijdstip :**	**Risiconiveau**					***Namen betrokkenen vooroverleg:***.....	
Thuis supporters	**1**	**2**	**3**	**4**	**5**	**Waarschijnlijkheid/ betrouwbaarheid**	
1. Aantal "geen" risicosupporters: ..... Welk risiconiveau brengt dit aantal op het totaal binnen het betreffende stadion+omgeving en centrum met zich mee?						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
2. Aantal risicosupporters: ..... Welk risiconiveau brengt dit aantal op het totaal binnen het betreffende stadion+omgeving en centrum met zich mee?						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	*(Mate van gebruik alcohol, drugs, wapens, geweld.)*
3. Aantal stadionverboden: .....: Hoeveel supporters met stadionverbod zullen naar de wedstrijd proberen te komen en welk risico brengt dit met zich mee?						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
4. Mate van activiteit: Zijn er signalen dat de supporters zich aan het organiseren zijn rond de wedstrijd die duiden op geweld of verstoring van o.o.: Ja/Nee						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
5. Gemoedstoestand: pos/neg a. Voor welk risico vormt de huidige gemoedstoestand zorgen?						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
b. Welk risico vormt de stand op de ranglijst voor de gemoedstoestand? c.						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
6. Signalen van het zich organiseren op een verzamelplaats: Ja/ Nee Hoeveel risico vormt het bij elkaar komen in cafés e.a. plaatsen? Tijdstip van aankomst in speelstad of omgeving:						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
7. Geschiedenis wedstrijd van de afgelopen drie jaar: Denk aan aantal incidenten, rivaliteit en nieuwe informatie die dit bevestigd.						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
8. Geschiedenis van het lopende seizoen: Denk aan aantal incidenten en nieuwe informatie die risicogedrag op bevestigen.						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	

9. Rivaliteit spelende clubs: Derby: Ja / Nee						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
10. Politiek/racistische motieven: Welk risico is aanwezig politieke en racistische standpunten worden uitgedragen die kunnen leiden tot geweld?						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
11. Plaats van risicosupporters in eigen stadion: Welk risico brengt de plaats van het uitvak t.a.v. de plaats van eigen risicosupporters met zich mee?						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
12. Interne maatregelen club: Welke risico's brengen deze maatregelen met zich mee; denk aan extra toegangscontrole/ legitimatieplicht, verandering van bestuur?						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
13. Handhavingsbeleid club (huisregels): Welk risico brengt het beleid met zich mee?						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
14. Kaarten vanuit het alternatieve circuit: Is dit aanwezig en welk risico geeft dit?						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
Algemeen	**1**	**2**	**3**	**4**	**5**		
1. Bijzonderheden stad/route Denk aan wegopbreking, of route langs café. Kruisende supportersstromen.						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
2. Infrastructuur rond stadion Denk aan belemmeringen voor supp scheiding. Kruisende supportersstromen.						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
3. Ligging stadion Denk aan woonwijk of andere evenement.						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
4. Media uitingen Beladenheid wedstrijd en media aandacht.						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
5. Entertainment in stadion Het niet/ wel inzetten geeft risico's.						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	

Het patroon wat ontstaat bij het aankruizen duidt op een:

A wedstrijd *laag risico*	*B wedstrijd* *midden risico*	*C wedstrijd* *hoog risico*
☐ **alle risico's worden ingeschat op voornamelijk 1 en hoogstens 2 risiconiveau.**	☐ **risico's worden ingeschat op voornamelijk risiconiveau 3** ☐ **ondanks het patroon een A-categorie aangeeft, zijn één of twee risico's die van niveau 3 of 4 zijn doorslaggevend om over te gaan op een B-categorisering.**	☐ **alle risico's worden ingeschat op voornamelijk 5 en tenminste een 4 risiconiveau.** ☐ **ondanks het patroon een lagere wedstrijd categorie aangeeft, zijn één of twee risico's van risiconiveau 5 doorslaggevend om over te gaan op een C-categorisering**

Definities:

Ingeschat Risiconiveau *Niveau 1:* geen extra gevaar dan bij een ander evenement van dergelijke omvang. *Niveau 2:* kans op geringe schade aan een persoon en/of goed. *Niveau 3:* Gering gevaar door baldadigheid, enige rivaliteit of bijzondere omstandigheden dat kan leiden tot een redelijke omvang van schade aan mensen en/of goederen. *Niveau 4:* Gevaar door (enige organisatie) van een groep personen wat kan leiden tot behoorlijke schade aan mensen en goederen. *Niveau 5:* Extra gevaar dat door (georganiseerd) geweld, rivaliteit of bijzondere omstandigheden kan leiden tot veel van schade aan mensen en/of goederen.	***Waarschijnlijkheid dat het risico zal optreden/ betrouwbaarheid van de info:*** I. *Zeer laag:* Geen concrete en bevestigde informatie aanwezig en de gebeurtenis wordt evenmin voorstelbaar geacht. II. *Laag:* Geen concrete aanwijzingen, maar de gebeurtenis wordt nog enigszins voorstelbaar geacht. III. *Gemiddeld:* Verschillende aanwijzingen en informatie vanuit betrouwbare bronnen met betrekking tot een gebeurtenis en de gebeurtenis is voorstelbaar. IV. *Hoog:* Concrete aanwijzingen en bevestigde* informatie dat een gebeurtenis zich zal voordoen, alleen plaats en tijd zijn niet bekend. En/ of een gebeurtenis wordt zeer voorstelbaar geacht. V. *Zeer hoog:* Concrete aanwijzingen (feiten en omstandigheden) en bevestigde informatie dat een gebeurtenis geëffectueerd zal worden: bekendheid van plaats en tijd.

* bevestigde informatie is informatie die door de RID als zodanig gekwalificeerd is dan wel zelf waargenomen feiten en omstandigheden door voetbalcoördinator (hieronder valt geen informatie 'van horen zeggen')

Afspraken en maatregelen:

a.	**Combiregeling verplichting: Ja/Nee**	
b.	**Andere vervoerswijze:**	
c.	**Ticketing**	**Start:** **Einde:** **Kaartverkoop op wedstrijddag:** **Uitgesloten clubkaarten:**
d.	**Opening stadion:**	
e.	**Alcoholverkoop: Nee/ Ja, wel of geen verlaagd percentage**	

f.	**Afwijkende geplande inzet:**
g.	**...**
h.	**...**

Evaluatie :

1. Was de inschatting van de risico-elementen juist?	**1. Ja/Nee, want.....**
2. Was de inschatting A/B/C goed?	**2. Ja/Nee, want.....**
	3. Ja/Nee, want.....
3. Zijn de afspraken en maatregelen zoals afgesproken uitgevoerd?	**4. Ja/Nee, want.....**
4. Waren de afspraken en maatregelen doeltreffend?	**5. .....**
5. Bijzonderheden:	**.....**

Risicoanalyse Matrix UIT

Wedstrijd : **Datum :** **Tijdstip :**	**Risiconiveau**					***Namen betrokkenen vooroverleg:***.....	
Uit supporters	**1**	**2**	**3**	**4**	**5**	**Waarschijnlijkheid/ betrouwbaarheid**	
15. Aantal "geen" risicosupporters: ..... Welk risiconiveau brengt dit aantal op het totaal binnen het betreffende stadion+omgeving en centrum met zich mee?						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
16. Aantal risicosupporters: ..... Welk risiconiveau brengt dit aantal op het totaal binnen het betreffende stadion+omgeving en centrum met zich mee?						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	*(Mate van gebruik alcohol, drugs, wapens, geweld.)*
17. Aantal stadionverboden: ..... Hoeveel supporters met stadionverbod zullen naar de wedstrijd proberen te komen en welk risico brengt dit met zich mee?						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
18. Mate van activiteit Zijn er signalen dat de supporters zich aan het organiseren zijn rond de wedstrijd die duiden op geweld of verstoring van o.o.: Ja/Nee						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
19. Gemoedstoestand pos/neg Voor welk risico vormt de huidige gemoedstoestand zorgen?						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
20. Welk risico vormt de stand op de ranglijst voor de gemoedstoestand?						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
21. Signalen van het zich organiseren op een verzamelplaats: Ja/ Nee Hoeveel risico vormt het vooraf bij elkaar komen in cafés e a. plaatsen, gezien het verleden en nieuwe informatie?						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
22. Geschiedenis wedstrijd van de afgelopen drie jaar Denk aan aantal incidenten, rivaliteit en nieuwe informatie die dit bevestigd.						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	
23. Geschiedenis van het lopende seizoen Denk aan aantal incidenten en nieuwe informatie die risicogedrag op bevestigen.						I. ☐ II. ☐ III. ☐ IV. ☐ V. ☐	

24. Rivaliteit spelende clubs Derby: Ja / Nee						I. ☐ II. ☐ III. ☐ IV ☐ V ☐	
25. Politiek/racistische motieven Welk risico is aanwezig politieke en racistische standpunten worden uitgedragen die kunnen leiden tot geweld?						I. ☐ II. ☐ III. ☐ IV ☐ V ☐	
Uit supporters vervolg	**1**	**2**	**3**	**4**	**5**		
26. Plaats van risicosupporters in eigen stadion Welk risico brengt de plaats van het uitvak t.a.v. de plaats van eigen risicosupporters met zich mee?						I. ☐ II. ☐ III. ☐ IV ☐ V ☐	
27. Interne maatregelen club Welke risico's brengen deze maatregelen met zich mee; denk aan extra toegangscontrole/ legitimatieplicht, verandering van bestuur?						I. ☐ II. ☐ III. ☐ IV ☐ V ☐	
28. Handhavingsbeleid club (huisregels) Welk risico brengt het beleid met zich mee?						I. ☐ II. ☐ III. ☐ IV ☐ V ☐	
29. Kaarten vanuit het alternatieve circuit Is dit aanwezig en welk risico geeft dit?						I. ☐ II. ☐ III. ☐ IV ☐ V ☐	
30. Weerstand tegen combi regeling Wel risico brengt weerstand met zich mee, acties, boycot, kaarten voor andere vakken e.d.?						I. ☐ II. ☐ III. ☐ IV ☐ V ☐	

Definities:

Ingeschat Risiconiveau	*Waarschijnlijkheid dat het risico zal optreden/ betrouwbaarheid van de info:*
Niveau 1: geen extra gevaar dan bij een ander evenement van dergelijke omvang. *Niveau 2:* kans op geringe schade aan een persoon en/of goed. *Niveau 3:* Gering gevaar door baldadigheid, enige rivaliteit of bijzondere omstandigheden dat kan leiden tot een redelijke omvang van schade aan mensen en/of goederen. *Niveau 4:* Gevaar door (enige organisatie) van een groep personen wat kan leiden tot behoorlijke schade aan mensen en goederen. *Niveau 5:* Extra gevaar dat door (georganiseerd) geweld, rivaliteit of bijzondere omstandigheden kan leiden tot veel van schade aan mensen en/of goederen.	I. *Zeer laag:* Geen concrete en bevestigde informatie aanwezig en de gebeurtenis wordt evenmin voorstelbaar geacht. II. *Laag:* Geen concrete aanwijzingen, maar de gebeurtenis wordt nog enigszins voorstelbaar geacht. III. *Gemiddeld:* Verschillende aanwijzingen en informatie vanuit betrouwbare bronnen met betrekking tot een gebeurtenis en de gebeurtenis is voorstelbaar. IV. *Hoog:* Concrete aanwijzingen en bevestigde* informatie dat een gebeurtenis zich zal voordoen, alleen plaats en tijd zijn niet bekend. En/ of een gebeurtenis wordt zeer voorstelbaar geacht. V. *Zeer hoog:* Concrete aanwijzingen (feiten en omstandigheden) en bevestigde informatie dat een gebeurtenis geëffectueerd zal worden: bekendheid van plaats en tijd.

* bevestigde informatie is informatie die door de RID als zodanig gekwalificeerd is dan wel zelf waargenomen feiten en omstandigheden door voetbalcoördinator (hieronder valt geen informatie 'van horen zeggen')

D

Case study: scenario schemes

Scenario scheme: risk due to a high number of supporters

- **Risk that the scheme explains:** a conflict amongst supporters.
- **Central action of the scheme:** high number of supporters.
- **Relevant risk factors:** high number of supporters with a stadium ban, availability of tickets from alternative sources.
- **Relevant controls:** regulation of ticket sales, contact with individual supporters before match, notification duty, Monitor ANPR.
- **Relevant information:** number of supporters.
- **Pattern of actions:** a high number of supporters → a conflict amongst supporters.

Scenario scheme: risk due to a high number of buses

- **Risk that the scheme explains:** a fight between group *X* and group *Y*.
- **Central action of the scheme:** too many buses with supporters.
- **Relevant risk factors:** bad infrastructure (traffic jams, blocked access to stadium).

- **Relevant controls:** deploy double-deck buses.

- **Relevant information:** group *X* and route *Y*, number of buses, availability of double-deck buses.
- **Pattern of actions:** Too many buses → group *X* and group *Y* get into a fight.

Scenario scheme: risk due to a bad relationship between home/away supporters

- **Risk that the scheme explains:** a fight between group *X* and group *Y*.

- **Central action of the scheme:** bad relationship between group *X* and group *Y*.

- **Relevant risk factors:** preparation or organisation of violence and disturbance, mood of supporters, organisation of a meeting.

- **Relevant controls:** make combi-regeling mandatory, governmental: ban on meetings, governmental: ban/limit on alcohol, Surveillance car visibly present, deploy helicopter, contact with supporter (flows).

- **Relevant information:** group *X* and group *Y*.
- **Pattern of actions:** bad relationship between group *X* and group *Y* → group *X* and group *Y* get into a fight.

Scenario scheme: risk due to rivalry

- **Risk that the scheme explains:** a fight between group *X* and group *Y*.

- **Central action of the scheme:** rivalry between group *X* and group *Y*.

- **Relevant risk factors:** history of the match, position on ranklist, relationship between supporters/team, relationship between supporters/board of the club.

- **Relevant controls:** governmental: ban/limit on alcohol, regulation of ticket sales, deploy stewards/security, change opening hours stadium, contact with individual supporters before match.

- **Relevant information:** group *X* and group *Y*.

- **Pattern of actions:** rivalry between group X and group $Y \rightarrow$ group X and group Y get into a fight.

Scenario scheme: risk due to societal influences

- **Risk that the scheme explains:** a fight between group X and group Y/vandalism/etc.
- **Central action of the scheme:** inference with other events.
- **Relevant risk factors:** political/racist statements/motives, media attention.
- **Relevant controls:** surveillance car visibly present, deploy stewards/security, governmental: change permits.
- **Relevant information:** group X and group Y.
- **Pattern of actions:** inference with other events $\rightarrow$ fights/vandalism.

Scenario scheme: risk due to routes

- **Risk that the scheme explains:** a fight between group X and group Y/vandalism/etc.
- **Central action of the scheme:** crossing routes.
- **Relevant risk factors:** road construction.
- **Relevant controls:** change routes.
- **Relevant information:** group X and group Y, routes of group X and group Y.
- **Pattern of actions:** crossing routes $\rightarrow$ fights/vandalism.

Scenario scheme: risk due to anti-riot squads

- **Risk that the scheme explains:** a fight between supporters and police/vandalism/etc.
- **Central action of the scheme:** deployment of anti-riot squads.

- **Relevant risk factors:** strictness and enforcement of rules, number of risk supporters .
- **Relevant controls:** regulation of ticket sales.
- **Relevant information:** group *X* and group *Y*.
- **Pattern of actions:** deployment of anti-riot squads $\rightarrow$ fight between supporters and police/vandalism.