Rijkswaterstaat
*Ministry of Infrastructure and Water Management*

# Guidelines on Performance-based Risk Analyses (PRA)

## Enabling asset management based on system performance

Water. Wegen. Werken. Rijkswaterstaat.

# Guidelines on Performance-based Risk Analyses (PRA)

**Enabling asset management based on system performance**

## Colofon


| | |
|---|---|
| Published by | ProBo Support Desk |
| Information | Arjen van Maaren |
| E-mail | probo@rws.nl |
| Copy-editing, design and production | Infram, BCP |
| Date | 8 March 2018 |
| Status | Final |
| Version number | 1.0.1 |
| Number | 5333 |
| Network | HWN, HVWN, HWS |
| Field of knowledge | Asset management |

# Contents

# Executive Summary

Policy objectives, legislation and regulations, and administrative agreements are the terms of reference for the performance of the primary infrastructure networks built and maintained by Rijkswaterstaat. In order to demonstrably meet this set of requirements, Rijkswaterstaat enables asset design, construction and maintenance processes in terms of performance of these networks. Performance-based risk analysis is an important tool in this respect.
The Executive Board of Rijkswaterstaat decided in 2013 that performance-based asset management would be the basis of construction and maintenance activities [1]. Performance-based risk analyses must be used during construction of and/or maintenance work on viaducts, bridges, waterways, roads, levees, dams and dunes. These Guidelines on Performance-based Risk Analyses (PRA) explain how the 'performance-based risk analysis' works and how it can be used in practice.

The PRA guidelines describe how a series of criteria, commonly referred to as RAMSSHE€P aspects, determines system performance. These aspects are *reliability, availability, maintainability, safety, security, health, environment, economics and politics*, and each of them is subject to what are known as 'aspect requirements'. The guidelines address the concept of aspect requirements and the way in which certain aspects, such as availability and reliability, determine the performance of the primary networks.

Failure to comply with the aspect requirements presents risks to our networks. The guidelines outline the process that Rijkswaterstaat completes in order to chart the (often related) risks based on a qualitative and/or quantitative risk analysis. Rijkswaterstaat distinguishes three types of risk analysis, which provide input for three differently styled maintenance plans.

At the heart of a (qualitative) maintenance plan (MP) is a qualitative risk analysis, or *failure mode, effect and criticality analysis* (FMECA). This risk analysis provides insight into the system's risk of failure by estimating the probability and severity categories in terms of the RAMSSHE€P aspects. This estimate is based on expert judgement. The analysis suffices for the major, non-critical part of Rijkswaterstaat's infrastructure (over 6,000 objects). Qualitative risk analysis results in a set of measures to reduce the risks to such an extent that the probability of system failure is acceptably low. These measures are incorporated into the maintenance plan for the relevant part of the network.

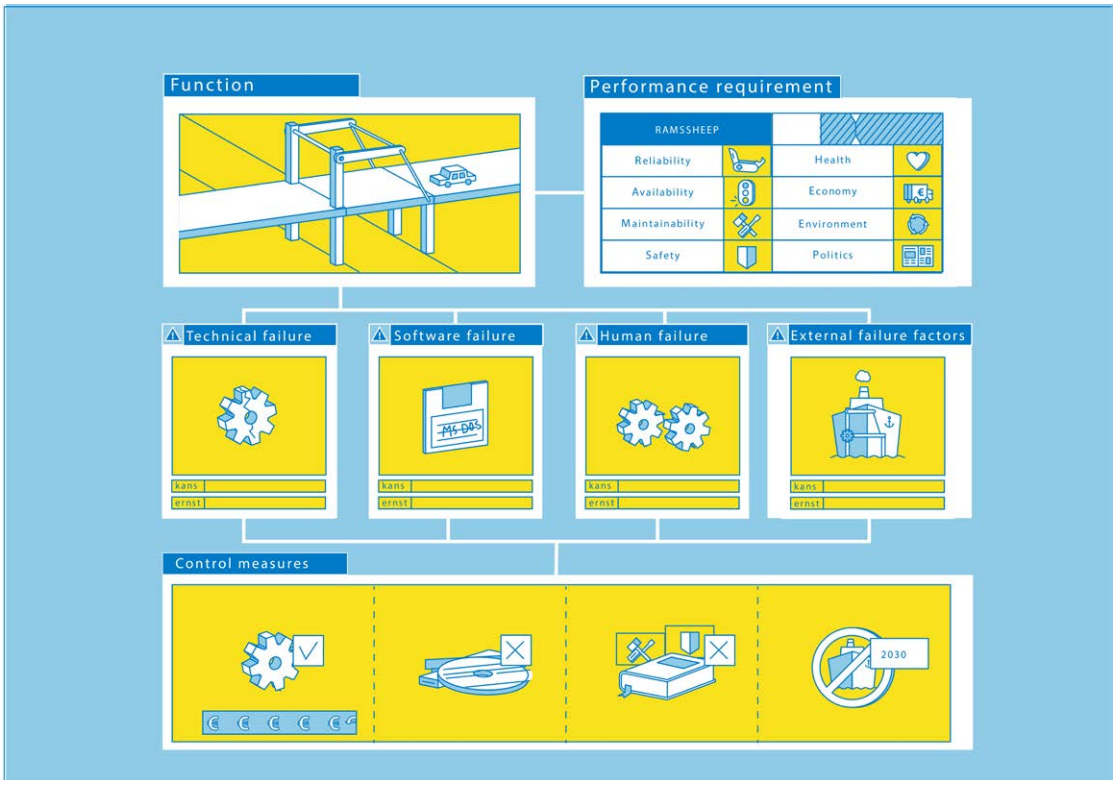
The foundation of a performance-based maintenance plan (p-MP) is a quantitative risk analysis. This is a mathematical calculation or modelling of the probability of system failure. This variant therefore focuses exclusively on 'reliability' and 'availability' and not on the other RAMSSHE€P aspects. Performance of a quantitative risk analysis is indicated by the requirements set for the object concerned. For Rijkswaterstaat these are certain quantitative requirements, e.g. requirements set for flood defences set out in the Water Act. A total of six objects (all storm surge barriers) are managed on the basis of the maintenance plan stemming from the most comprehensive quantitative risk analysis adopted by Rijkswaterstaat. In these, fault tree analysis is used to determine the exact performance and maintenance requirements. A quantitative risk analysis could also be desirable where no (statutory) requirements have been set for the reliability or availability of an object. This is the case for all objects that make a critical contribution to the functionality of the networks. A total of 119 objects have been appointed by Rijkswaterstaat in this category.

The quantitative approach used in this category (based on RCM Cost models) also results in a set of measures. These entail demonstrable fulfilment of the performance requirements. In the case of object construction, for example, the quantitative risk analysis provides confidence in sufficient reliability and availability. During the operational stage, this variant establishes a relationship between maintenance costs and the associated expected performance. In addition to demonstrating that the requisite performance has been delivered, the quantitative risk analysis also enables maintenance costs to be optimized in line with the RCM method. In 2016, the Executive Board of Rijkswaterstaat designated 119 complexes for which a p-MP is to be drafted.

The results of the risk analysis are an important source for the maintenance plans, which in turn guarantee that measures to be implemented will actually be implemented. These results are included in the p-MP. Consequently, performance-based risk analyses and the resulting p-MPs are of inestimable value for optimal planning of availability and reducing unplanned non-availability of objects. The PRA guidelines set out which elements of the risk analysis need to be incorporated into the maintenance plan. Finally, the guidelines indicate how to use performance-based risk analyses in contracts with contractors.

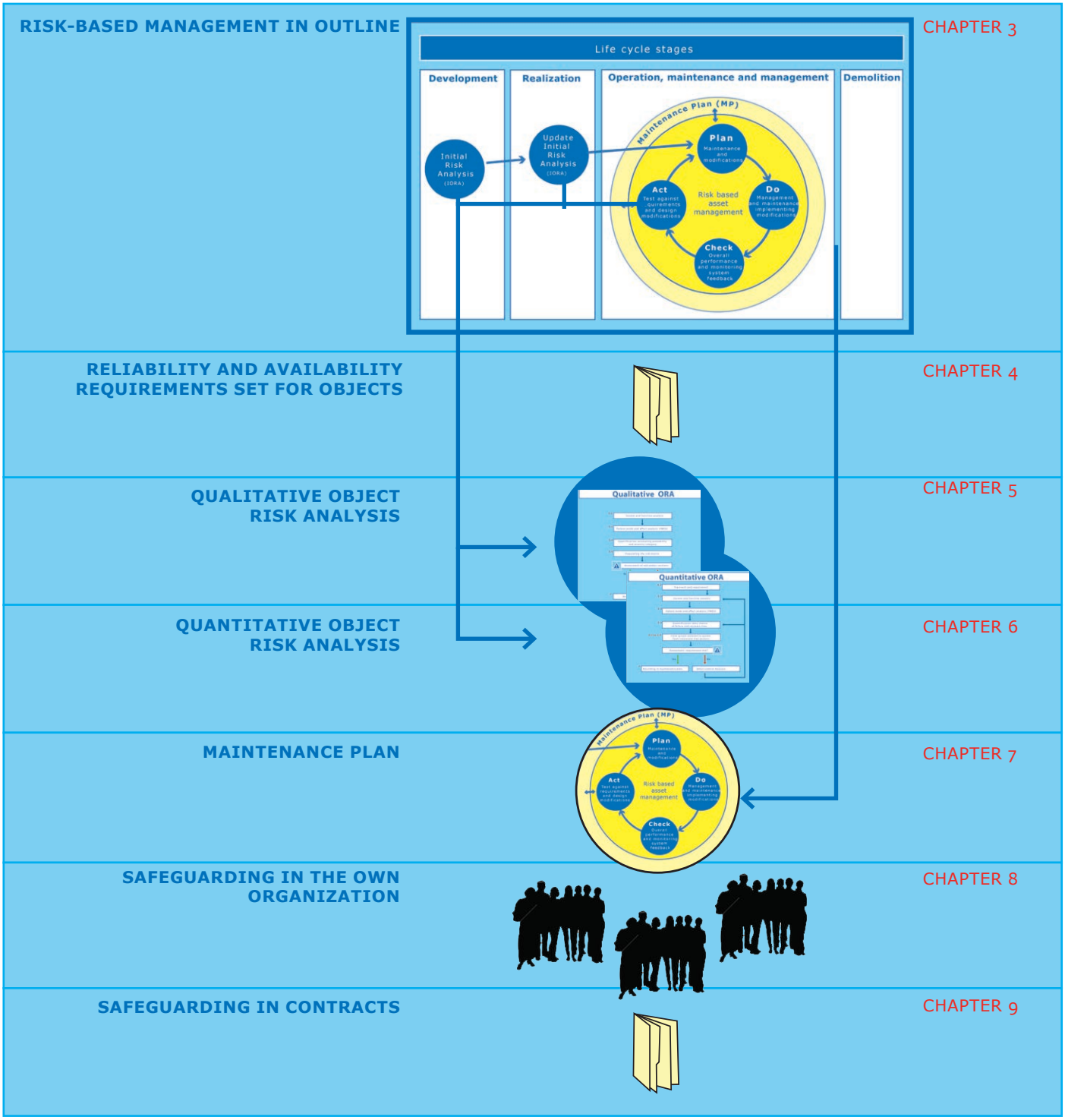
An MP drafted using ProBO is based on a special form of quantitative risk analysis. This comprises a comprehensive quantitative approach for critical assets, with strict requirements being the benchmark (fault tree method). An MP based on ProBO will be drafted for the five storm surge barriers being managed by Rijkswaterstaat (six from 2018 onward).

The infographic on the PRA process steps below forms part of the animation and brochure that accompany these guidelines.



# How to use this document

These guidelines describe the process of performance-based risk analysis and the tools needed for them. It has an umbrella role  for the methods and tools used in the details of this process. Specific methods and tools are not discussed in the guidelines, but they are referenced. They are managed by Rijkswaterstaat and can be requested from the ProBo support desk.



*Chapter 1* describes the most important characteristics of risk-based asset management: What is it? Why is it useful? What is the need? What relationships does risk-based asset management have within the broader context of policy, implementation and management?

*Chapter 2* examines the huge significance of performance-based risk analyses for policy. Definitions and terminology from the field of systems engineering are used to outline the management model. For readers who are not yet (or not yet fully) familiar with the terms and concepts associated with risk-based asset management, this chapter also provides an explanation of the most common terminology.

*Chapter 3* outlines actual risk-based management, performance of the initial risk analysis and its use during the operational stage. It also extensively discusses what is the right approach for what context:

- a comprehensive quantitative approach for critical assets, with strict requirements being the benchmark (fault tree method, resulting in an MP based on ProBO);
- a less extensive quantitative approach for assets that play a crucial role in network performance (RCM method, resulting in a p-MP);
- and finally, a semi-quantitative (qualitative) approach which Rijkswaterstaat uses to manage and maintain the vast majority of its assets (FMECA, resulting in a (qualitative) MP).

*Chapter 4* considers various options of formulating requirements for objects, network links or networks. Ultimately the wish of the Minister for Infrastructure and Water Management will play a decisive role.

*Chapter 5* describes the qualitative approach and the standards applied in that regard. This chapter seeks to provide a framework by presenting an unambiguous record of how Rijkswaterstaat performs risk-based asset management by way of inspections.

*Chapter 6* has the same structure as chapter 5, but discusses the quantitative approach and the standards applied in that regard. The quantitative approach explicitly results in an expected degree of reliability and/or availability. This chapter can be regarded as a framework for how Rijkswaterstaat calculates expected reliability and availability.

*Chapter 7* discusses how the results of the risk analyses can be incorporated into a maintenance plan. It indicates how this plan constitutes a foundation for the maintenance work to be carried out, and also provides preconditions enabling delivery of the performance promised. The form and content of the maintenance plan itself are beyond the scope of the guidelines, but they are also managed by Rijkswaterstaat and can be requested via the ProBo support desk.

*Chapter 8* considers the organization required to guarantee that the performance promised will also actually be delivered during the operational stage. This will be done on the basis of the well-known plan-do-check-act (PDCA) cycle.

Finally, *chapter 9* shows the consequences risk-based management has for the various contractual forms Rijkswaterstaat works with.

# 1 Risk-based asset management

## 1.1 Introduction

The *Guidelines on Performance-based Risk Analyses* (PRA) have been drawn up to render risk-based approaches practicable for the infrastructural assets managed by Rijkswaterstaat. The organization regards risk-based asset management as an indispensable component of asset management. The guidelines support the development phase, the realization phase and the operational phase of assets throughout the infrastructure system, from gear box to network and from client to supplier. The guidelines integrate and supersede the *RAMS Guidelines* and the *Risk-based Management and Maintenance Guidelines.*

The current political and social move towards a smaller government also entails a challenge. Rijkswaterstaat is less directly engaged in construction and maintenance of infrastructure than it used to be and is primarily concentrating on a directing role. Accordingly, the role of the market is changing too. This changed division of roles puts managing performance centre stage and depends on effective communication and clear agreements. The *Guidelines on Performance-based Risk Analyses contribute* to this by documenting the methodology of and agreements on managing performance.

## 1.2 What is risk-based asset management?

Risk-based asset management entails a methodology based on an expectation (calculated or estimated by expert judgement) that objects will satisfy set requirements in terms of performance. The risk-based methodology also enables the continuous demonstration of compliance with performance requirements in the different stages of the life cycle of infrastructure assets.

These guidelines set out a methodology, including a set of methods with which to carry out performance-based risk analyses. The risk-based approach thus ensures that performance (or potential performance) can be charted coherently and also be recorded in such way that it remains fully traceable. Furthermore, it allows mitigation of risks in terms of performance, identification of weak spots in an object, implementation of targeted measures and comparison of alternatives, with the possibility of cost optimization emerging as a result.

## 1.3 Usefulness and need of risk-based asset management

Practical experience learns that, in the conventional method of asset management, there is no transparent relationship between the selected designs, investments and implementation of management and maintenance activities, on the one hand, and the implicit or explicit performance requirements for an object's function, on the other.

As such, the question of whether or not the performance requirements are being satisfied is not straightforward to answer in practice. As a result, an object may over- or underperform and budget allocation could be suboptimal.

The risk-based approach and the underlying methods are intended to make the

relationship between performance requirements and performance levels in a certain area transparent and traceable. Full and successful implementation of the risk-based approach enables area managers to:

- remain consistently in control of the area, without major surprises in terms of maintenance costs or performance risks
- demonstrably comply with legislation, regulations and Service Level Agreements (SLAs)
- have an unequivocal model for communication with the contractor (and, indirectly, the user), to render the contractor's performance transparent
- optimize maintenance costs/yields at object and network level.

As a result of these qualities, the risk-based approach is an effective application of *public-oriented network management*, one of Rijkswaterstaat's key focus areas. After all, the risk-based approach ensures an optimal balance between investment of public funds and the performance levels of infrastructure. Furthermore, direct stakeholders can be informed on and involved in decisions on infrastructure specifications on objective and rational grounds.

## 1.4 Context of risk-based asset management

The transition to risk-based asset management occurs within a context of policymaking, implementational methods and procedures, the relationship with the operational manager, various integrated project management roles in major projects, existing legislation and regulations and relationships with market parties. Consequently, this section examines what performance-based risk analysis can signify for the most important entities in this context.

### Relationship with policy

The Minister of Infrastructure and Water Management establishes policy objectives for the networks managed by Rijkswaterstaat. The risk-based approach is extremely valuable when it comes to fulfilling policy wishes and renders the associated costs transparent.

Policy topics for accessibility, safety and quality of life particularly affect the construction programme and the Replacement and Renovation programme, as described in the *Multi-year Programme for Infrastructure, Space and Transport*.

Agreements on management and maintenance are made in service level agreements (SLAs). In these agreements, the Secretary General of the Ministry of Infrastructure and Water Management and the Director General of Rijkswaterstaat set out the performance Rijkswaterstaat must provide and the related costs. Risk-based asset management plays a crucial role in honouring the agreements. In the case of construction projects, no agreements are made (yet) on the expected performance in terms of reliability and availability. One of the reasons for this is that the performance of infrastructure networks not only depends on construction, management and maintenance, but also on traffic management, water management and incident management. These guidelines pertain solely to construction, management and maintenance.

### Relationship with asset management

Asset management ensures optimum utilization of the Rijkswaterstaat networks, for which striking the right balance between performance and costs is essential. Risk-based asset management is part of asset management. It hones understanding of the contribution that each individual object makes to performance and workings of the overall network. Hence there is a link between

various levels of maintenance and their consequences for the performance of the network. What will happen to that performance if no maintenance work is carried out over the next four or ten years? What will the consequences be if different maintenance levels are chosen? What degree of availability should the bridge have? Will this availability have the desired effect on the network? These kinds of questions illustrate just how inextricably intertwined performance-based risk analysis is with asset management.

The risk-based approach can be used in any phase of the life cycle of a certain portion of the network. When applied in combination with *life cycle costing* (LCC), Rijkswaterstaat knows exactly when concrete risks will arise for the performance of the relevant network. Combined with knowledge of the construction and maintenance costs, this insight makes it possible to strike an optimum balance between the performance level of the area and the costs for maintaining or improving it, where necessary. This means that the risk-based approach connects operational decisions on construction, management and maintenance to the organization's tactical and strategic objectives. As such, it is an important pillar of asset management [2].

### Relationship with systems engineering

Systems engineering (SE) is a structured method for constructing systems that perform well. Adequate performance depends on such factors as the system's reliability and availability. The *System Engineering Guidelines* discuss these aspects in comprehensive detail [3]. These guidelines are to be regarded as the specification of certain analytical methods, as specified in the *Systems Engineering Guidelines*, thereby also enabling validation and verification of performance.

### Relationship with life cycle costing

Risk-based asset management concerns opinions on future developments: how is the system expected to function and perform in view of the method of construction and/or maintenance? The direct connection between method of construction and/or maintenance and the performance expected also provides a lead for charting future costs. The risk-based approach is indispensable for life cycle costing as well.

### Relationship with legislation and regulations

Inherent to the risk-based approach is the fact that performance requirements are set for functions. These are primarily based on legislation and regulations. Two well-known examples of such legislation are the *Water Act* and the *Safety of Road Tunnels (Supplementary Regulations) Act.*

Incidentally, the *Buildings Decree* has for decades been predicated on standards that assume a quantitative performance requirement. The Eurocodes, which the *Buildings Decree* mandates must be used when designing structures, require maximum permissible probability of failure for each reference period.

### Relationship with the operational manager

Rijkswaterstaat's regional organizational units draw up performance-based and risk-based maintenance plans on the basis of location-specific and object-specific information. They draw on risk analyses of the objects, which are composed and updated using the system described in these guidelines. The maintenance plans form the basis of the management and maintenance work to be carried out. They safeguard the agreements on the performance the objects are to achieve and the investments necessary for this. (See chapter 7 for further information on the role of the maintenance plan and chapter 8 for the organizational aspects that the operational manager in particular is faced with.)

### Relationship with the (technical) manager

Rijkswaterstaat carries out construction and major renovation projects with a team set up in accordance with the Integrated Project Management model (IPM). If the object to be built or renovated is subject to reliability and/or availability requirements, the IPM team will have to formulate these requirements, ensure they are stipulated in the contract and test whether or not the requirements will be fulfilled in accordance with expectations. The technical manager must have adequate knowledge to supervise these activities.

### Relationship with the contractor

If the risk analysis for a construction or maintenance project has been outsourced, the contractor will have to be capable of carrying out an object risk analysis (ORA) and updating it. The object risk analysis is part of the object and becomes/remains the property of Rijkswaterstaat. As such, it should be available, utilizable and accessible to Rijkswaterstaat. The contractor has a contractual obligation to perform such analyses in a standardized fashion, and will also be able to use these guidelines as a resource and source of information.

# 2 From policy to construction and maintenance

Rijkswaterstaat  develops, manages and maintains three main infrastructure networks in the Netherlands:

- the main road network (HWN)
- the main waterways network (HVWN) and
- the main water system (HWS).

Management of the performance of these networks requires a risk-based approach at all levels within the organization. In conjunction with prevailing legislation and administrative agreements, policy formulated at the highest, strategic level is decisive for construction, management and maintenance.

For management at a tactical level, policy preferences for a primary system or network are translated to objects. This concerns the function(s) that the various objects fulfil and the associated performance requirements. It goes without saying that during this translation the aggregate performance of objects and subsystems should continue to fulfil the policy objectives for the system as well as legislation and regulations.

Construction, management and maintenance are specified at operational level, in such a way that the agreed performance is actually delivered and there is clarity on the associated costs.

An example of the way in which performance requirements, policy objectives and legislation and regulations are mutually coordinated can be found in the Water Act. The Water Act stipulates a safety standard for every levee. The policy objective is to protect the hinterland from flooding. Under the administrative agreements, the water boards manage the levees and have a duty of care in terms of ensuring compliance with the safety standard, while the provincial authorities and the Ministry of Infrastructure and Water Management monitor the safety levels achieved. The requirement for infrastructure is that it must be capable of retaining a water level that has a small probability of occurring each year. This is a reliability requirement.

Another example: the problem of a road having insufficient capacity can be remedied by widening the road, which will increase its capacity. The primary process ‘construction’ contributes to achieving the policy objectives. Traffic management can also provide solutions, such as through ramp metering, speed limits or diversions. Requirements for reliability and availability affect the quality of the new parts of the network.

Planned work on roads and waterways (known about in advance) and unplanned work (not anticipated) are a necessary evil. The quantity of work and thus non-availability can be influenced by smarter types of maintenance, more use of sustainable materials, shorter recovery times, etc.

This way, smart performance of maintenance work contributes to network performance. Consequences of non-availability can be reduced by means of traffic management: announcing the maintenance work along with diversions, as well as working at night rather than during the day.

The final example is incident management. Better incident management ensures that the road is free and fully available more quickly, resulting in fewer traffic jams. Hence incident management contributes to one of the Ministry's policy objectives.

## 2.1 Policy objectives

Examples of policy objectives for the three networks managed by Rijkswaterstaat:

**Main road network:**
- The average journey time on motorways between cities during rush hours should be no more than one and a half times as long as outside of rush hours.
- The average journey time on motorways around cities and on non-motorways that are part of the main road network during rush hours should be no more than twice as long as outside of rush hours.

**Main waterways network:**
- Transport over the waterways must be as reliable, efficient, safe and sustainable as possible. The Ministry of Infrastructure and Water Management sets this objective at strategic level. 'As possible' indicates that the four aspects cited are never feasible in an absolute sense.
- This aim as set out in the objective trickles down to the tactical and operational levels. Rijkswaterstaat aspires to unequivocal, transparent and (in nautical and technical terms) efficient waterway management. Spearheads include: journey times that are as reliable as possible, good accessibility, and continuation of the high degree of safety of waterborne transport.

**Main water system:**
- *Water safety.* The land behind the sea wall and the primary flood defences have has to be protected from flooding. At tactical and operational levels this policy objective makes itself felt in maintaining the coastline, taking care of flood defences along the rivers and lakes, and ensuring the discharge and storage capacity of the main water system.
- *Fresh water.* Fresh water must be available in sufficient supply for all functions, including nature. During dry spells, the fresh water available in the main water system has to be evenly distributed, with priority being given to the most vital functions.
- *Water quality.* The water from the main water system must be clean and healthy enough for all designated uses, but particularly for drinking water consumption, recreation and ecological functions.

The Ministry of Infrastructure and Water Management tasks Rijkswaterstaat with managing and maintaining the networks. In other words (in asset management jargon): the Ministry of Infrastructure and Water Management is the 'asset owner' and Rijkswaterstaat is the 'asset manager'.

Rijkswaterstaat agrees on a *service level agreement* (SLA) with the Ministry of Infrastructure and Water Management for management, maintenance and development, and for traffic and water management. The SLA contains various types of agreement, including:

- agreements related to the availability of functions in the infrastructure system
- agreements related to the reliability with which the functions are fulfilled.

There is a relationship between performance, risks and costs: the lower the risks and the better the performance, the higher the costs. Policymakers must decide what risks are acceptable and what levels of performance and accompanying costs are desirable. The Minister for Infrastructure and Water Management makes budget available and Rijkswaterstaat ensures optimal utilization of this budget for performance of its assets.

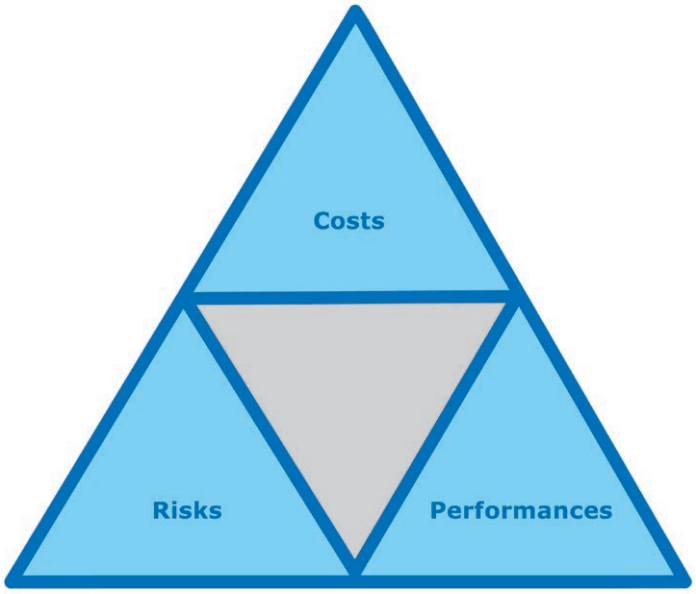



*Figure 2.1. Relationship between risks, performance and costs*

## 2.2 Systems, functions and requirements

For a sound understanding of what these guidelines encompass it is important to provide a brief explanation of a few key terms. A number of terms essential to these guidelines are derived from the domain of systems engineering [3].

**System**

A system is a coherent aggregate of (physical) parts intended to fulfil a certain function. The three networks maintained by Rijkswaterstaat have the status of 'primary system'. The components that make up the main systems, such as the connection between A and B, are referred to as subsystems or system elements. Subsystems in turn consist of even smaller system elements, such as road sections, junctions and bridges.

All system elements collectively determine whether or not a system functions properly as a whole. 'Collectively' here not only means 'the sum of the parts' but also expressly implies 'conjunctively'. Furthermore, the quality of each of the system elements individually also has a direct influence on the quality of the networks of which they form part.

Rijkswaterstaat uses the following classification, in line with the NEN 2767 [4] standard. Rijkswaterstaat designates the three networks it maintains as *primary systems.* The components that make up the primary systems are referred to as systems, such as Rijksweg 1 (national trunk road 1) in the main road network. The systems in turn consist of *system parts*, such as the connection between A and B. The system parts comprise management objects, such as roads, canals, locks and bridges. The components of these are called elements and these are in turn subdivided into *structural units.* This structured breakdown is essential within the risk analysis. The breakdown can also be incorporated into the operational manager's maintenance plans.

### Function

A function refers to the function (or intended function) and/or actions of a system and/or a task that is being performed. Systems exist because they perform functions. Thus (in simple terms) the main road network has the function of 'making it possible to get from A to B by vehicle'. A lock has the function of transporting a ship across a water level differential. A battery has the function of storing electrical energy and delivering it back in a controlled manner, etc.

Functions usually have a hierarchical structure (depicted as function trees). Within such a hierarchy functions are subdivided into subfunctions. For example, managing traffic is a subfunction of Rijkswaterstaat's transport networks (main roads and main waterways).

### System requirements

'System requirements' is the collective term for all requirements set for the system. Rijkswaterstaat refers to the aggregate of functional requirements, aspect requirements and interface requirements as 'the requirements'. For the sake of clarity, we have opted for the distinguishing term 'system requirements' in these guidelines.

### Functional requirement

The functional requirement is a primary requirement set for the function. It encompasses what the system needs to be capable of doing. A functional requirement often pertains to the capacity a system is required to provide when it comes to fulfilling the function. Examples include the volume of traffic that the main road network has to be capable of coping with, or the size of the ships that a lock has to be capable of accommodating, or the height of the water level differential across which the ships passing through the lock have to be transported, or the amount of electricity a battery has to store.

### Aspect requirement

An aspect requirement describes the precondition(s) subject to which the system is to fulfil its functions. Examples include: availability, reliability, maintainability, safety, sustainability, health. In short, requirements in terms of RAMSSHE€P (for this acronym see section 2.3). A lock can be sufficient in size and capable of spanning a water level differential, but if it does not satisfy the precondition 'availability' (e.g. due to a technical fault) then its functional quality will be zero at that juncture and possibly less than anticipated on an annual basis.

### Interface requirement

This type of requirement set for a system is the result of an interface analysis. Such an analysis inventories the requirements that the system's environment sets for the system.

### Failure

Failure can be said to occur when a system is no longer capable of fulfilling its function as a result of an event or a collection of events. The system is then no

longer fulfilling the functional requirements. This is a crucial point, as the notion of 'failure' is often linked to systems. In such cases we say that 'the system is failing', but in fact it is important that the function that the system performs is no longer being fulfilled.

The reasons a system might no longer be capable of fulfilling its function are several and various. Only a limited proportion of causes can be influenced by construction, management or maintenance. For example, if a system is not fulfilling its function due to lack of capacity, this cannot be termed a failure. In this case, the system is being used in a way it was not designed for.

### Failure definition

There is a clear need for a failure definition, an agreement on when something can be termed a failure. A failure definition establishes the relationship between the failure of (the function of) a subsystem and the consequences this has for the system. If, for example, a safety system (subsystem) fails, the safety of the system will no longer be adequately safeguarded. The failure definition establishes the necessary measures, which do not always encompass halting the primary function. Usually it is evident when something can be termed a failure. If the doors of a lock no longer open or close, the function 'passing through a lock' will have failed.

Failure of subsystems does not necessarily have to result in overall failure of the primary function. If the primary function is not completely lost, the failure of a subsystem will usually cause a limitation in terms of the system's function. For example, if one or more cameras fail whilst being controlled remotely, the failure definition indicates how many and which cameras are allowed to fail before the function 'adequate view' can be deemed to have failed. If more or specific cameras fail, the function 'adequate view' can be deemed to have failed. The process (performance of the function) will then have to be halted.

## Examples of the relationship between policy objectives and the requirements set for functions

### The main road network

The wish of the Ministry of Infrastructure and Water Management is for the average journey time on motorways between cities during rush hours to be no more than one and a half times as long as outside of rush hours. This wish pertains to the function 'managing road traffic'. The functional requirement of the road section could be: 'in the event of a volume of traffic less than or equal to the design capacity, a minimum of 4,500 vehicles per hour must be able to pass through at a speed of 100 kph (62 mph)'.

An accompanying aspect requirement could be: 'availability must be at least 99%'. What this means is that 4,500 vehicles are able to pass through at a speed of 100 kph (62 mph) at least 99% of the time. If, for instance, fewer than 4,500 vehicles per hour are able to pass through at a speed of 100 kph (62 mph) due to a hole in the road, then this would count as a failure.

### The main waterways network

The Ministry of Infrastructure and Water Management wants transport over the waterways to be smooth, reliable, efficient, safe and sustainable. The accompanying function is 'managing shipping traffic'.

A related functional requirement is that a lock in the network has to be capable of transporting a ship across a water level differential of 6m. A precondition for this functionality could be: 'availability (aspect requirement) must be at least 99%'. What this means is that the lock must be capable of transporting a ship across a water level differential of 6m at least 99% of the time.

**The main water system**
Policy requires that during extremely dry spells sufficient fresh water is available for drinking water, shipping and industry. The function here is 'supplying fresh water'. A functional requirement of the weir at Driel, which regulates water distribution on the River IJssel and the River Lek, could be: 'the water discharge through the River IJssel must be at least 55 $m^3/s$'. An accompanying aspect requirement for the weir would then be: 'availability of the weir must be at least 99.5%'. Consequently, the minimum flow rate of the River IJssel will be present 99.5% of the time. The system will have failed if the flow rate is less than 55 $m^3/s$. If water discharge from the Rhine is less than 1,000 $m^3/s$ in dry spells, for example, the weir at Driel will not be capable of draining the requisite 55 $m^3/s$. The system is not designed to perform its function under these conditions. Hence this cannot be deemed a failure.

## 2.3 RAMSSHE€P

RAMSSHE€P is an acronym for *reliability, availability, maintainability, safety, security, health, environment, economics* (€) and *politics*. These are all aspects of the system.

The aspects reliability and availability are indicators of expected system performance. Section 2.4 discusses this in more detail. The other aspects manifest themselves as (usually undesirable) side effects or possible consequences. Requirements set for these aspects serve as preconditions for the functioning of the system. The aspects are briefly described below, resurfacing in chapter 5 on qualitative object risk analysis.

**Maintainability (M)**
This aspect is usually defined as the probability that a system (or system element) can be repaired, inspected or subjected to preventive maintenance within a specific period of time and under certain conditions. The conditional stipulation 'specific period of time' (read: recovery time or inspection time) is also an important component of the aspect availability.

According to this definition, maintainability is (as yet) rarely used in practice, particularly at Rijkswaterstaat. Rijkswaterstaat often interprets maintainability as a precondition for the accessibility of system elements, or for having sufficient and appropriate tools, etc. These are factors that shorten the recovery time, replacement time or inspection time, resulting in a higher degree of availability.

### Safety (S)
This aspect pertains to the probability that a system does not cause human casualties (injuries, fatalities) over a particular period of time and under certain conditions. This definition is the same as that for reliability (see section 2.4), with the difference being that for the aspect 'safety' the consequences are expressed in terms of potential victims, whereas for the aspect 'reliability' they are expressed in terms of potential 'damage'. Rijkswaterstaat conceives as potential victims the users of the system, the staff operating and maintaining the objects, and the local residents. This also encompasses the term 'occupational safety'. To get a picture of how the aspect 'safety' works, consider a bridge. The degree of safety is dependent on such factors as the probability that the bridge will collapse. Provided they are used properly, the regulations applied by Rijkswaterstaat will ensure that the probability of a bridge collapsing will be no higher than 0.0001 per 50-year period, rendering the system (the bridge) sufficiently safe.

### Security (S)
The aspect security pertains to the security of a system with regard to deliberate unsafe human actions, such as vandalism, terrorism and cybercrime. Rijkswaterstaat uses the term 'integrated security'.

### Health (H)
The health aspect can be described as physical, mental and/or social well-being, without involvement of acute risks to safety or system failure. This well-being pertains to users of the infrastructure, to people working on the infrastructure and (where applicable) to the infrastructure itself. Consider in this regard the effects arising from ergonomics or dangerous substances. The difference between the aspects health and safety can be rather arbitrary. Healthy working is also encompassed by occupational safety, for instance.

### Environment (E)
This aspect pertains to the relationship with the physical environment. It could relate to adaptation of infrastructure to and the influence or potential influence of infrastructure on the physical environment. Consider in this regard the effects on environmental quality and their impact on flora, fauna and pollution (noise, particulate matter). The distinction between health and environment can also be rather arbitrary.

### Economics (€ )
The aspect 'economics' encompasses the aggregate of financial consequences, such as the costs of construction and maintenance activities as well as claims and fines. The cost aspect is inextricably intertwined with the other RAMSSHE€P aspects, because enhancing or reducing performance in terms of those aspects always entails consequences in terms of costs. This pattern applies to all stages of the life cycle of systems and is explicit in the life cycle cost (LCC) [5] approach. Risk-based asset management provides a transparent relationship between costs and the other RAMSSHE€P aspects. Enhancing or reducing RAMSSHE€P performance is commonly expressed in terms of costs to society.

### Politics (P)
The aspect 'politics' expresses political-administrative and social consequences. These include effects on the image of the management organization or consequences for the reputation of the parties with political-administrative responsibility.

The MSSHE€P aspects (i.e. excluding the aspects reliability and availability) are often formulated as hard preconditions set for the function, such as:

- the precondition pertaining to noise levels in the case of a road (e.g. installing a noise barrier)

- the precondition pertaining to particulate matter (installing noise barriers or screening off tunnel portals)
- the security requirements on sites (putting up fencing).

For some MSSHE€P aspects requirements can be set at a high level of abstraction, such as the maximum level of noise permissible along a road. Other MSSHE€P aspects have to be stipulated instrumentally, such as a security concept.

**Example**

From the perspective of the aspect 'health', a requirement is set specifying that the noise pollution next to a road section must be limited. Consequently, noise barriers are to be installed. These ensure that the function for the subfunction 'limiting noise transmission' is fulfilled. Functional requirements can be set for this subfunction, such as: 'maximum x dBA on the façade behind'. Requirements can also be set in terms of availability or reliability for the quality with which this subfunction is being fulfilled, e.g. '2% of the time the noise level may exceed x dBA on the façade behind'. This is an availability requirement set for the noise barrier, whereas the noise barrier itself stems from an aspect requirement set for the overarching system (the road section).

This example indicates that requirements pertaining to reliability and availability could also be linked to MSSHE€P aspects.

## 2.4 The aspects reliability and availability

Rijkswaterstaat uses the terms R (*reliability*) and A (*availability*) to express the performance of networks. These determine the level of functioning of the system.

Setting requirements for these R and A aspects enables Rijkswaterstaat to limit the probability of system failure, thereby safeguarding the extent to which the functions are fulfilled. Such a requirement could be: 'the function may not fail more than 4 times a year on average', or 'in the event of failure, the function is to be restored within 4 hours'. These requirements indicate (from the perspective of reliability) how many instances of failure will be deemed acceptable and (from the perspective of availability) for how long a function may be disrupted.

The total extent to which a function is fulfilled is referred to as the **performance** of the network or of the system (or subsystem). As network operator, Rijkswaterstaat is keen to know what performance the systems are required to deliver and at what price. To this end, it is necessary to know:

- what functional requirements are being set for a system and what performance requirements are applicable in that respect
- what performance is currently being delivered, in view of the state of maintenance and the prevailing maintenance agreements
- what is necessary to deliver the requested performance, when and at what costs.

The terms reliability and availability can be directly expressed numerically, in contrast to other aspects, such as health. The definition of **reliability** is:

*Reliability is the probability that a system fulfils its function without failure, over a particular period of time and under certain conditions.*

In practice, the complement of reliability is almost always used: unreliability, or the probability of a system failing over a particular period of time and under certain conditions. Reliability is dimensionless per unit of time [-/unit of time ]. A probability per unit of time is, in fact, a frequency, with a relationship between the probability per unit of time and the number of instances per unit of time. Section 6.3 discusses this in more detail.

For an example of the aspect (un)reliability, consider the probability in a year of a traffic management failure, with no human casualties being expected, and the only damage being traffic jams longer than usual. If human casualties are conceivable, the failure will be part of the aspect safety. (See also section 2.3, safety)
Another example is the probability of a weir failing. Here, too, this probability is linked to a period of time (e.g. one year). When this happens, the result will 'merely' be damage.

Reliability therefore pertains to systems that are working (functioning) continuously, with damage as the result of system failure.

The definition of **availability** is:

*1) Availability pertains to the expected fraction of the total time over which a system is functioning, under certain conditions.*
*2) Availability (also) pertains to the probability of a system functioning, under certain conditions, when it is put to use at a random juncture.*

At first glance, these appear to be two entirely different definitions of availability. Upon closer inspection, however, they turn out to be two manifestations of the same principle. After all, the ratio between the intervals in which a system is working over a particular unit of time (first definition) and the intervals in which the system is not working (is failing) is equal to the probability that the system will be available when it is needed (second definition).

Figure 2.2 illustrates the difference between reliability and availability.

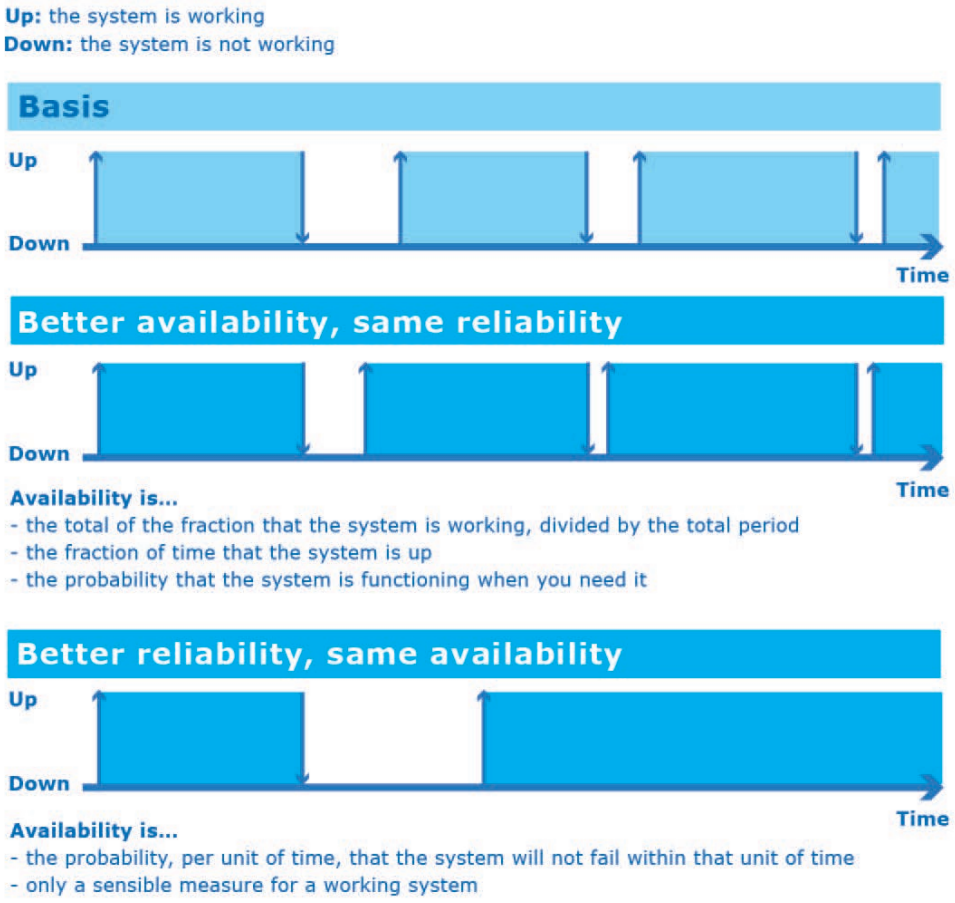



*Figure 2.2. Reliability and availability*

A time bar presents the (measured or expected) functioning of a system (see figure 2.2). The number of downtimes is 4 in the case of the top two time bars and 2 in the case of the bottom one. The surface area is similar in all cases, although the bottom time bar exhibits fewer instances of failure. In the event of consistent reliability and increasing availability, the number of instances of failure will stay the same, but the total recovery time will decrease (comparison upper time bar with middle time bar). If reliability increases and availability stays the same, the number of instances of failure will decrease, but the total recovery time will stay the same (comparison upper and lower time bar).

For an example of availability consider the fraction of the time that a road section or a tunnel is in use. Rijkswaterstaat often stipulates that contractors are to ensure that their objects are obstructed for no more than a certain period of time, e.g. a maximum of 45 hours a year. This would entail an availability requirement of 8,760 hours {=number of hours in 1 year} - 45 hours) / 8,760 hours ≈ 99.5%. This means that the non-availability of the system may not exceed 0.5% as a maximum.

Another example of non-availability: the probability that the Maeslantkering (storm surge barrier) fails to close in the event of a storm surge may not exceed 0.01, i.e. 1%. This requirement stems from the Water Act. Hence a non-availability requirement of 0.01 must be satisfied.

What is essential in this regard is that the term 'probability' is used for both the R and the A aspects. The concept of probability enables calculation of the expected reliability and expected availability of a system. Rijkswaterstaat can set requirements for this reliability and availability to get a measure of control regarding the quality of the requested functions of a system. Section 6.3 addresses the term probability in more detail.

For the aspect availability, too, its complement is often used. The non-availability of a system is the fraction of the time that the system is down or the probability of the system not working when it is needed. The term availability is dimensionless. Availability is often expressed as a percentage, occasionally as a number of hours a year. In common parlance the terms availability and reliability are often used interchangeably. Thus it is common to hear a tunnel-related safety system or an object such as the Maeslantkering being referred to as 'reliable', whereas in actual fact it is a matter of availability, namely the probability that the systems will be working as required at the time they are required to function.

## 2.5 Planned versus unplanned non-availability

In the previous section, non-availability was defined as the fraction of time during which a system is not functioning, or the probability of a system not functioning if the system is put to use at a random juncture. The reason for the system not functioning does not form part of the definition, although it is of considerable practical importance.

Unplanned non-availability resulting from a breakdown or malfunction is perceived to be far more serious than planned non-availability. Also, unexpected obstructions have a far greater (adverse) effect on Rijkswaterstaat's image than planned obstructions. For non-availability that is planned and announced in advance, mitigating measures can be taken, such as opting for non-availability during off-peak times, informing users about taking an alternative route or adjusting transport plans. The (monetary) damage caused by the non-availability will therefore be less serious in the event of planned non-availability than it would be if the non-functioning occurs by surprise. Hence differentiation in terms of the requirements will be necessary.

Planned non-availability is divided into two categories:

- planned non-availability due to inspections or preventive maintenance
- planned non-availability due to the object not being operated. This of course only applies to objects that are operated, such as movable bridges and locks.

Unplanned non-availability has two causes as well:

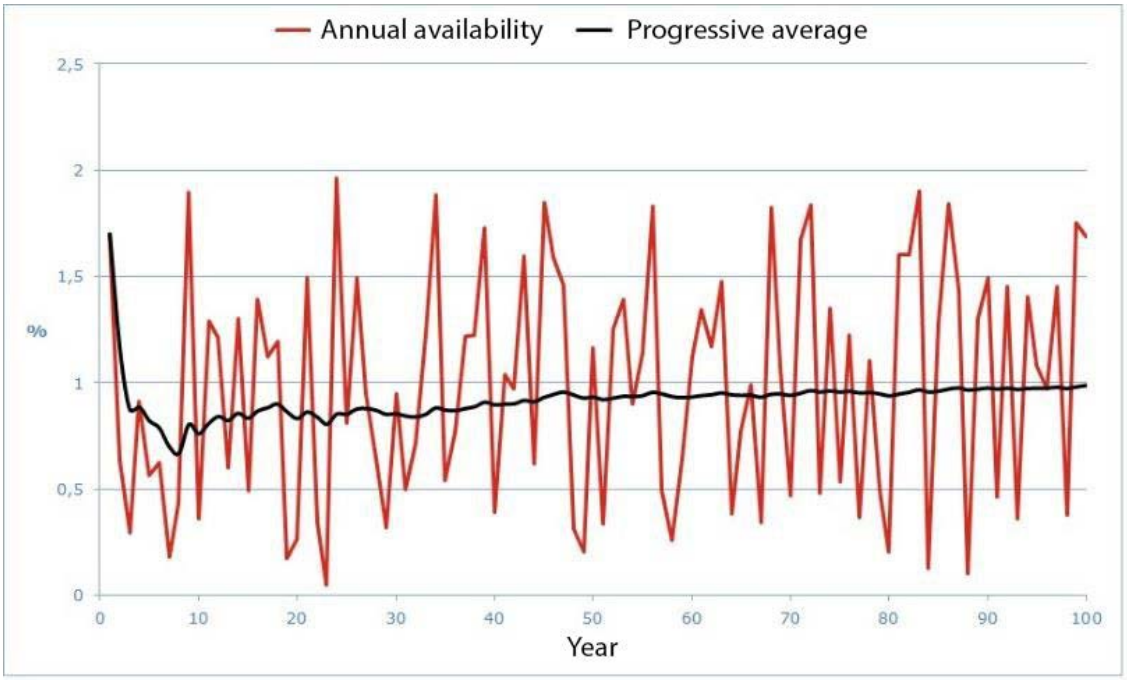
- unplanned non-availability due to breakdown or malfunction and/or failure of the object, subsequent to which (corrective) maintenance is required
- unplanned non-availability arising as a result of natural circumstances, such as high and low water levels, ice, wind or fog.

In the event of unplanned non-availability, no reasonable requirement can be set for the maximum permissible non-availability. After all, the probability of faults with protracted recovery times cannot be ruled out entirely (i.e. with a probability of 0). However, a requirement can be set for the *average* unplanned non-availability. The figure below (2.3) shows one possible course of unplanned non-availability, given an expectation of 1%.

## Retrospective measurement

In some cases the performance of functions can be measured retrospectively. For the aspect (un)reliability this can be done by counting how often a system has failed within a particular period of time. For the aspect availability this can be done by measuring the fraction of the total time that a system has functioned, or counting the number of times that a system has functioned when it was put to use at a random juncture. Based on these measurements, it is possible to verify the assumptions made in the model that calculates reliability and availability.

Measuring will only be possible if a system or function actually fails, such as in case of non-availability of a lock. If the probability of failure is very low, however, such as the probability of the Maeslantkering not closing in the event of a storm surge or the probability of the Van Brienenoordbrug bridge collapsing, statistically relevant measurements are not possible. In such cases, the starting point will have to be the model calculating the expected reliability or availability. Naturally, subsystems can often be measured, enabling improvement of the model.




*Figuur 2.3. Figure 2.3. Example of current, annual unplanned non-availability (red) and its moving average (black). Uniformly distributed non-availability with limits 0 and 2 (%) has been assumed. The average is therefore 1%.*

## 2.6 Life cycle of a system

Five stages in the life cycle of infrastructure are distinguished [3]:
1) Identification of needs
2) Development and design
3) Realization
4) Operation, Maintenance and Management (this also includes replacement and renovation (RandR)
5) Demolition

Figure 2.4 constitutes an adaptation of the V model from the *Systems Engineering Guidelines.* On the left are the stages Development and Realization in the life cycle. The PDCA cycle indicates the management and maintenance stages up to the point of demolition.

During the system's development stage, a risk analysis is built from the outset. This means that the required reliability and availability are taken into account from as early as the design stage. If the realization stage deviates from the design, this will be adopted accordingly in the risk analysis, ensuring that expectations in terms of reliability and availability are based on the correct data.

The realization stage is followed by the operational stage, during which the operational manager operates and maintains the system. System performance is monitored wherever possible.

Rijkswaterstaat endeavours to follow the PDCA cycle for all its objects during the operational stage and to continuously monitor the performance of the objects in terms of RAMSSHE€P. Maintenance work on or replacement of subsystems enable the operational manager to keep the performance of objects at a satisfactory level. If the system's function is no longer required, the system should be demolished.

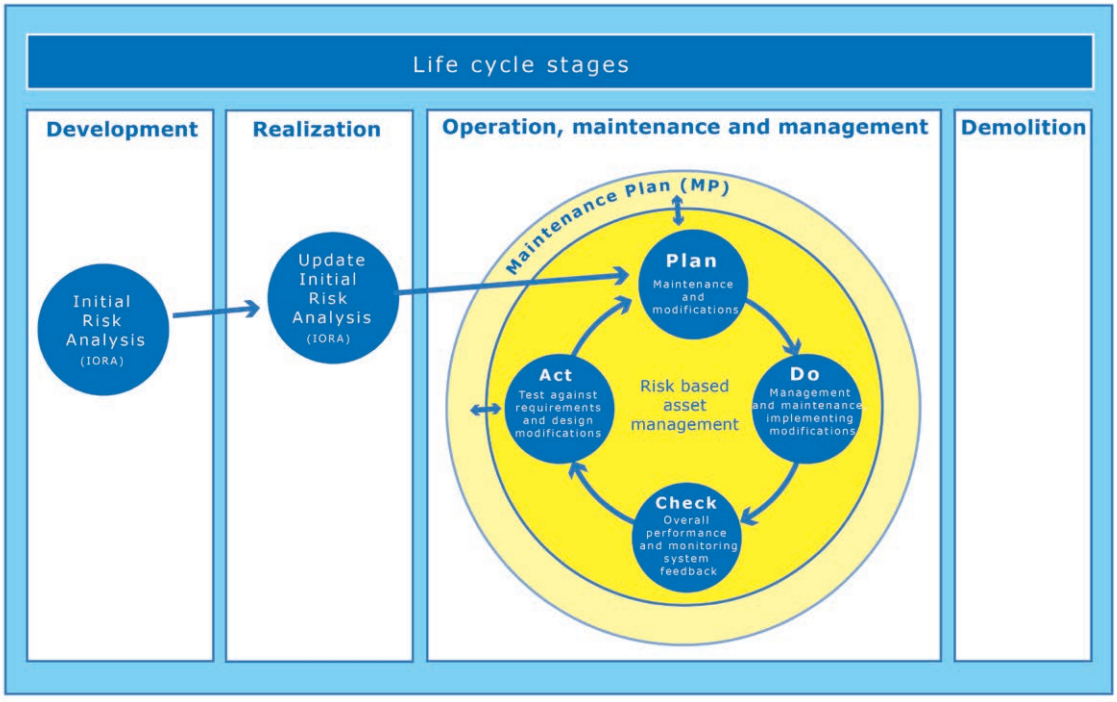



*Figure 2.4. Safeguarding performance throughout the life cycle*

# 3 An outline of risk-based management

## 3.1 Introduction

Risk-based management based on performance requirements set for an object is done on the basis of a risk analysis. The object and the requirements determine the nature and depth of the analysis. This risk analysis is termed an Object Risk Analysis (ORA). Project risks, such as those managed at Rijkswaterstaat by way of Risk Management, are beyond the scope of these guidelines.

Rijkswaterstaat carries out the ORA for all objects, starting with the qualitative part and, where necessary, expanding this to include a quantitative part. The qualitative variant considers both unexpected faults that have a significant effect on performance of the networks and the measures required to maintain the networks in the longer term. This variant is not limited to the aspects reliability and availability but focuses explicitly on all RAMSSHE€P aspects of the object. Furthermore, the qualitative ORA also considers risks that are negligible in the short term, but could be extremely costly in the long run if no standard operational maintenance (SOM) is performed. This standard operational maintenance encompasses such measures as conserving, restoring soil protection and fixing leaks.

One essential difference between the qualitative and the quantitative ORAs is that the qualitative ORA does not provide information on the expected performance in terms of the object's reliability and availability. Consequently, the qualitative approach will only suffice for objects for which the aspects reliability and availability (unplanned or otherwise) have a negligible effect on the network. This is the case for a large number of components in the networks, such as line objects (road sections and waterway basins), as well as for fixed bridges, viaducts and suchlike. These kinds of objects have a small risk of unplanned non-availability. Only a limited group of objects has a decisive influence on performance of the network, which is why the quantitative variant is used for these objects (more on these objects in section 3.4). The qualitative ORA will be examined in more detail in chapter 5.

The quantitative part of the ORA focuses specifically on the aspects reliability and/or availability. It can be performed to varying levels of detail. The level of detail is determined by the criticality and nature of the objects. The most detailed quantitative approach is also known by the obsolete names 'ProBO comprehensive' or 'ProBO advanced'. Such a way of working proves to be necessary to ensure, for example, that storm surge barriers or tunnels are in compliance with statutory requirements. For less critical objects a less detailed analysis can be performed. The risk analysis produces a conservative estimate of an object's actual performance.

Because – depending on the nature of the objects – the possible simplifications are many and diverse, these guidelines omit the separate nomenclature for different levels of accuracy of quantitative risk analyses. Only a fundamental difference between the qualitative and quantitative risk analysis remains. The quantitative ORA will be examined in more detail in chapter 6.

In daily practice, Rijkswaterstaat uses three different types of risk analysis:

- MP: In these guidelines, this corresponds to the quantitative risk analysis. This uses the FMECA tool and is applied primarily for permanent structures and line objects.
- p-MP: This approach is called quantitative risk analysis in these guidelines and is based on the RCM method. This type of risk analysis is mostly used for management and maintenance of critical, movable objects and tunnels.
- MP based on ProBo: This is the most comprehensive form of quantitative risk analysis, used for storm surge barriers and construction of tunnels and water-retaining objects. This approach uses fault trees.

As the p-MP and MP based on ProBO have a large overlap in terms of content, these guidelines address these two variants as quantitative risk analysis.

Rijkswaterstaat uses the quantitative risk analysis during the construction stage of an object. It makes it possible to generate sufficient trust in the quality of the design with which the relevant function will be fulfilled. It is a way of setting and managing requirements for the quality of the components being designed by the contractor, without curbing freedom in terms of the design. In principle, a contractor is free to design as they see fit. Rijkswaterstaat no longer engages in design activities itself, but must demonstrate that the system will be reliable and/or sufficiently available and (therefore) consists of hard-wearing components. Hence the ORA sets the direction in the design stage.

Performing an ORA at too early a stage (conceptual stage) of a design is not worthwhile, because the uncertainty of the results will be too high at that juncture. However, it is possible to generate results at an early stage regarding the differences in reliability or availability among a range of alternative designs. Here it is not the absolute accuracy but the relative accuracy that is important. A quantitative ORA at the end of the design stage will provide an understanding of the performance of the design in terms of the reliability and availability to be expected.

During the operational stage, the ORA is adapted to the current status at specified intervals. Components age, conditions (such as the extent of loads) change, renovation work is carried out, etc. These events can affect the object's reliability and/or availability and therefore the network's performance. The qualitative ORA provides an answer to the question of the extent to which the object is still fulfilling the set RAMSSHE€P requirements, whereas the quantitative ORA indicates whether the object is still sufficiently reliable and/or available. If the system is no longer performing (reasonably) well, both parts of the ORAs will identify the weak spots in the system and areas where efficient improvements are possible, ensuring that the system lives up to the performance promised once more. Hence the ORA sets the direction in the operational stage too.

NB: The quantitative risk analysis calculates an expectation of unplanned non-availability. For the purposes of calculating these expectations, assumptions need to be made with regard to maintenance. The fulfilment of these assumptions therefore partly determine the planned non-availability.

Conclusion: The ORA is the pivot within risk-based management. Use of the risk analysis for the purposes of asset management will be outlined in the next few sections.

## 3.2 Risk analysis for the purposes of asset management

The ORA objectively and transparently clarifies what risks and what elements (components) jeopardize the functioning of the system and in what situations.

**The qualitative risk analysis** of risk-based asset management always features the following steps (see figure 3.1):
- system and functional analysis
- failure mode and effect analysis
- estimating probability and severity categories
- documentation via the risk matrix
- formulating measures (depending on the previous step).

**The quantitative risk analysis** calculates the reliability and/or the planned/ unplanned non-availability and consists of the following steps (see figure 3.1):
- calculating the top event and establishing the requirement set for the function
- system and functional analysis
- failure mode and effect analysis
- calculating failure data
- modelling the system
- comparing result with the requirement.

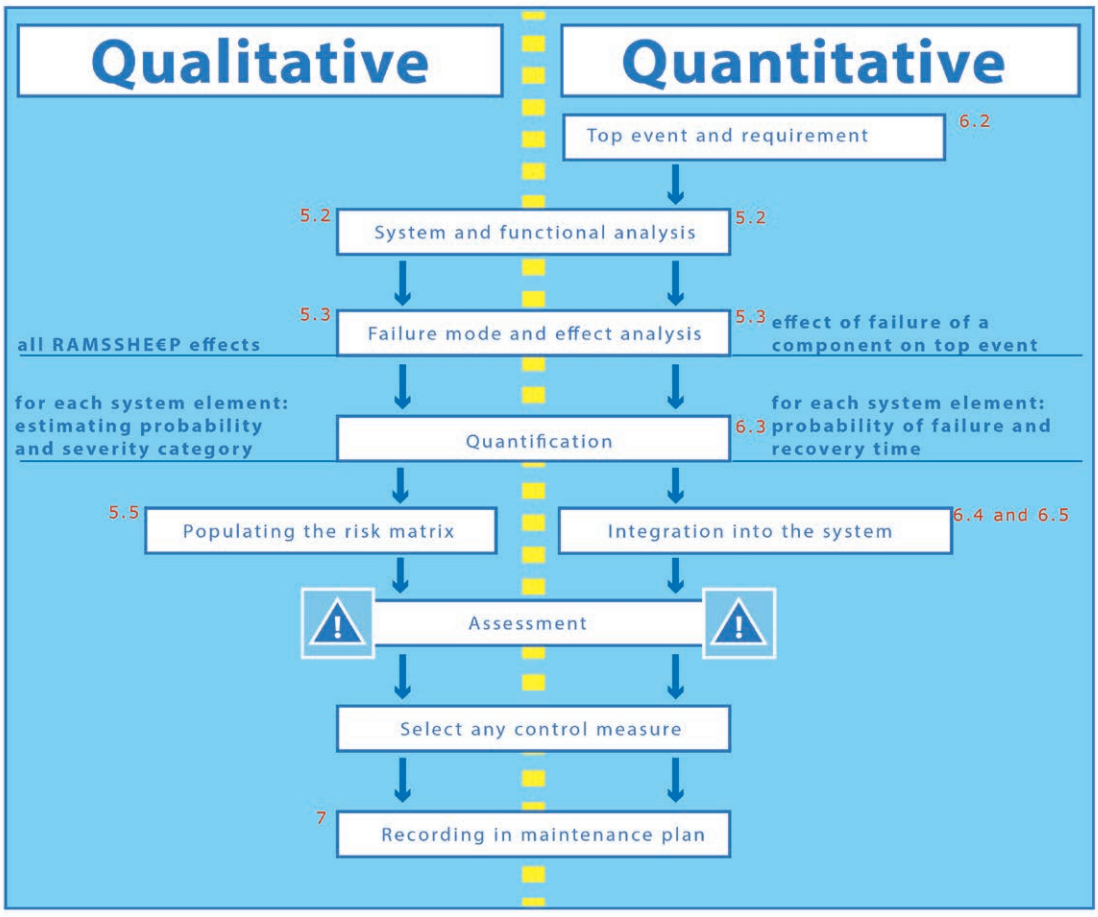



*Figure 3.1. The steps in a qualitative and quantitative ORA. The numbers refer to the sections where these steps are discussed in more detail.*

The steps 'system and functional analysis' and 'failure mode and effect analysis' (FMEA) are the same in both risk analyses. However, the tools for the FMEA (standardized spreadsheets) differ, as the next step, (semi-)quantification, is also part of the spreadsheets. The other components vary. Both analyses result in a test that establishes whether the system is sufficient or whether additional measures will be required.


### *3.2.1 Calculating the top event*

The quantitative variant of the ORA starts by ascertaining the functions for which the risk analysis is to be performed. This is necessary because a quantitative risk analysis always pertains to a single function. Sometimes infrastructure objects only have a single function, e.g. retaining high water (storm surge barriers), enabling a water level differential to be spanned (lock), or pumping up water (pumping station). Objects may also have multiple functions. Aside from the function 'span water level differential', a lock can also have the function 'withstand high water'. The reliability or availability of each individual function is calculated and tested against the requirement applying to that single function. If an object is fulfilling two important functions, with two requirements applying, two risk analyses will be necessary. The failure of the function is termed the top event and the ORA essentially calculates the probability of the top event.

This first step is not necessary for the qualitative variant of the ORA. This variant considers all elements of the system, irrespective of the function to which they are contributing. By also considering all aspects of RAMSSHE€P, the qualitative variant looks not only at the failure of the system's primary function but also at the effects (the consequences) of failure of the system (or elements thereof).


### *3.2.2 System and functional analysis*

The aim of the system and functional analysis is to provide a description of what the system (object) is and what subfunction(s) the system's subsystems will need to be capable of fulfilling. In this respect, the following questions are relevant:

- How is the system functioning?
- What subsystems are playing a role in this?
- What are the functions of the relevant subsystems?

The products of the system assessment are:

- a system description
- the physical breakdown
- sometimes a functional breakdown.

The system must be considered from a broad perspective. All elements contributing to the system's function(s) must be charted. These include hardware, software, human actions, external events and relevant processes.

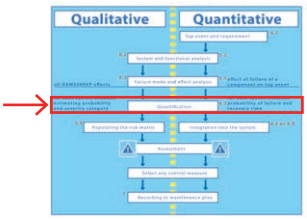
This is one of the reasons why it is important to carefully determine, weigh up and record the system limits.


### *3.2.3 Failure mode and effect analysis*

The *failure mode and effect analysis* (FMEA) is a technique to identify all possible anomalies in terms of the functioning of system elements and simultaneously record the consequences of failure of those elements for the system. This is done in a standardized way, based on the results from the previous step.

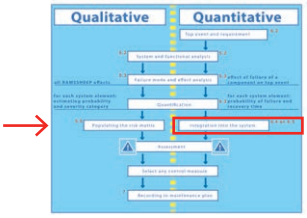
The quantitative analysis looks only at the effect of a component's failure on the top event (failure of the function under consideration), whereas the qualitative analysis estimates all RAMSSHE€P effects. Even the term 'component' needs to be interpreted in a broad sense: software and human actions are also components

of the system, in addition to hardware. This stage also entails an inventory of those external events whose cause is extrinsic to the system, yet could cause the system to fail. Typical examples in this regard include collision and lightning strike.




### 3.2.4 Quantification: calculating failure data and estimating probability and severity

In the case of a quantitative analysis, an estimate is made for each of the system's elements of the probability of failure (sometimes as a function of time) and recovery time. In the case of a qualitative analysis, an estimate is made – likewise for each element – of the probability of failure in a *probability category* and of the consequence in a *severity category*. If external events are declared applicable during the screening, these will be included in this step too.




### 3.2.5 From element to system

The results of a quantitative analysis of all individual elements are compiled to form a single picture of the reliability and/or availability of the required system function. Because a probability of failure that does not vary over time is used, this approach produces the expected reliability and/or availability in the short term.

For more complicated forms the fault tree technique can be used, sometimes in combination with the event tree technique.

In the simpler variants of the analysis (e.g. in *Reliability Centred Maintenance*, RCM) the compilation consists of an addition sum.

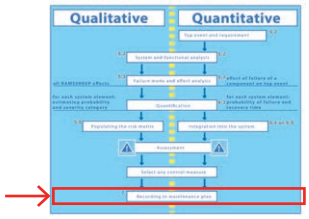

### 3.2.6 Documentation via the risk matrix

In the case of the qualitative analysis, the results from the previous step (the quantification) are entered into a risk matrix (see figure 3.2). Measures for improvement will depend on the position in the risk matrix. The fundamental principle is that risks in the red area must be addressed by means of measures immediately. For risks in the amber area, the speed with which they will need to be addressed will have to be looked at (this being dependent on the nature and criticality of the object), and risks in the green area are acceptable.

In the case of a quantitative analysis, the calculated reliability and/or availability are tested against the set requirement. If the score turns out to be inadequate, the system will have to be improved. The ORA provides an overview of the weak spots: the elements of the system making a significant contribution to the unreliability or non-availability.

| RISK MATRIX | | CONSEQUENCE | | | |
|---|---|---|---|---|---|
| | | 1: NEGLIGIBLE | 2: LIMITED | 3: MAJOR | 4: SEVERE |
| PROBABILITY | 1: NEGLIGIBLE | Acceptable | Acceptable | Acceptable | Acceptable |
| | 2: LOW | Acceptable | Acceptable | Undesirable | Undesirable |
| | 3: MODERATE | Acceptable | Undesirable | Undesirable | Undesirable |
| | 4: HIGH | Acceptable | Undesirable | Undesirable | Unacceptable |
| | 5: CERTAIN | Undesirable | Undesirable | Unacceptable | Unacceptable |

*Figure 3.2. Risk matrix*




### 3.2.7 *Recording in the maintenance plan*

In addition to measures that could be taken, the ORA will result in a number of preconditions considering necessary maintenance activities. These assumptions must be demonstrably safeguarded. Only then will the risk analysis be valid and the expected performance correct. Ensuring that this maintenance work is actually carried out in practice is done by recording the preconditions and the follow-up in the maintenance plan. The preconditions resulting from the qualitative analysis are documented in a (qualitative) MP, the preconditions resulting from the quantitative analysis are recorded in the p-MP, and the preconditions from the most accurate quantitative analysis are laid down in an MP based on ProBo. The preventive maintenance required to guarantee the system elements' performance may result in planned non-availability. Hence the unplanned non-availability and a proportion of the planned non-availability both stem from the ORA.

## 3.3 Updating the risk analysis

Enabling management on the basis of an object's performance is key. What this means is not only that the expected performance must be known at the time of completion of an object, but also that at any given juncture it demonstrably forms part of the decisions regarding the management of the object.

Rijkswaterstaat carries out risk-based asset management in line with the PDCA cycle (Plan, Do, Check, Act). As described in the introduction to this chapter, an initial risk analysis is required for each object. From the perspective of the ORA, actions are formulated that are included in the maintenance plan (Plan). Performing the activities specified in the maintenance plan (Do) will ensure that the object satisfies the pre-determined performance. In terms of usage, the actual performance of both the object and the measures implemented are to be measured (Check). The results are then incorporated into the ORA (Act), after which the maintenance plan is adjusted and the PDCA cycle is repeated. This process is illustrated in figure 3.3. Chapter 8 will examine this PDCA cycle in more detail.

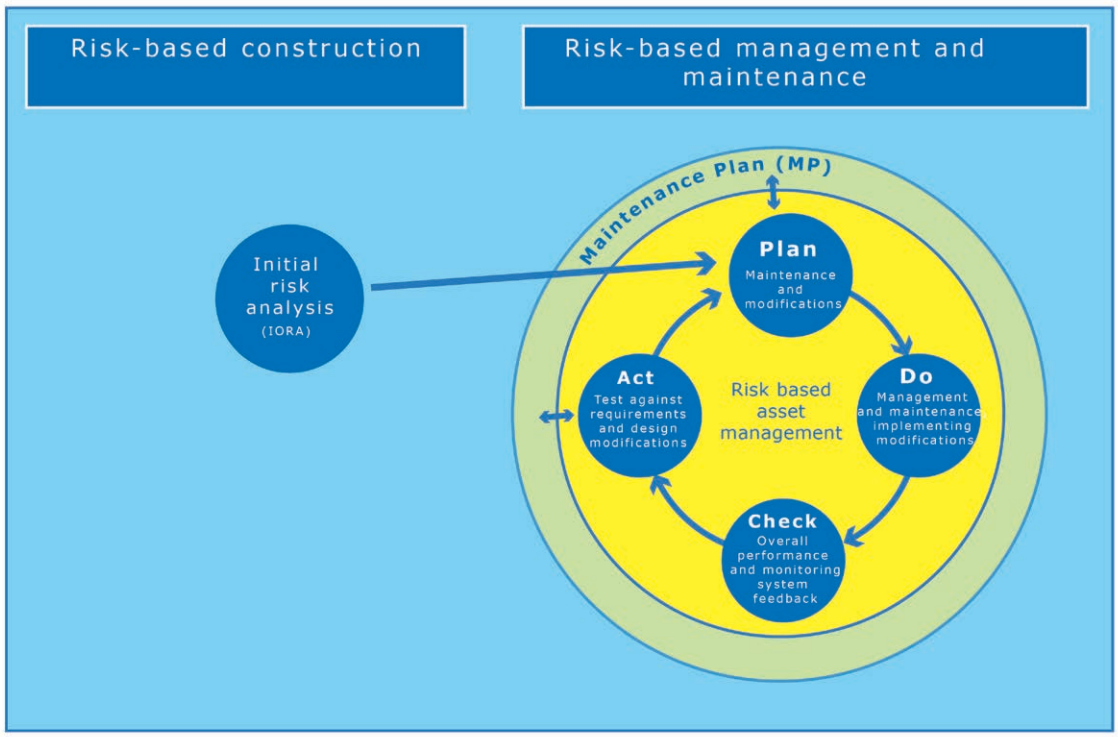



*Figure 3.3. The initial ORA during construction and the PDCA cycle during management and maintenance*

## 3.4 When to perform a quantitative risk assessment?

The above touched on the fact that Rijkswaterstaat uses two different object risk analyses, the quantitative variant and the qualitative (semi-quantitative) variant.

A qualitative risk analysis should be performed for all objects. Occasionally it is necessary to perform a quantitative risk analysis to supplement this.

Opting for the quantitative risk analysis will depend on the requirements set for the relevant object. If the requirement is quantitative, a quantitative risk analysis will be necessary. Examples are requirements set for flood defences stemming from the *Water Act.* However, a quantitative risk analysis could also be desirable where no (statutory) requirements are set for the reliability or availability of an object. This will be the case for all objects making a critical contribution to the functionality of the networks. This encompasses virtually all objects that fail with a relatively high degree of frequency and whose failure has a considerable impact on the functioning of the infrastructure as a whole. These include the large movable bridges in the main road network, the locks in the main waterways network and the tunnels managed by Rijkswaterstaat. These objects function due to a complex interplay of mechanical, hydraulic and electrical and software-related subsystems, combined with human actions.

Purely static objects, such as a fixed bridge or viaduct, riverbanks, waterway beds and noise control barriers, almost never fail unexpectedly. A qualitative ORA will suffice for such objects, with a relatively straightforward specification of probability and consequences of risks and based on generic fundamental principles and inspections.

Taking this idea as a starting point, the Executive Board of Rijkswaterstaat has established which objects have to be managed and maintained on the basis of a quantitative ORA [1] by means of a p-MP or MP based on ProBO. Hence an assessment based on an assessment framework will no longer be necessary.

# 4 Performance requirements for objects

## 4.1 Introduction

Chapter 2 stated that the Minister for Infrastructure and Water Management makes agreements with Rijkswaterstaat on the performance of the three networks in the form of SLAs. The extent to which the networks perform depends on such factors as the reliability and availability of the components of these networks. However, a network's performance is not readily expressed solely through the reliability and availability of the components. The quality of traffic and water management, incident management and capacity play an important role too. The recording of *labelled vehicle and vessel hours lost* (VHL) perhaps offers more opportunities to quantify the effect of traffic and water management, incident management and shortage of capacity.

If a component (object) in a network is unavailable, the effect of this on the network's performance will depend on the importance of the object within the network. This importance is determined by the number and type of vessels or vehicles using the object, by the availability of alternative routes, as well as by the redundancy in the network. Rijkswaterstaat distinguishes between main and normal transport axes, between routes along which dangerous substances are or are not allowed to be transported, and suchlike. These are examples taken from both transport networks, although Rijkswaterstaat also makes such a distinction for the main water system, albeit in a slightly different form.

Because the availability and reliability of an object only partly determine the overall network's performance, it is (at this point) impossible to directly translate the agreements in the SLAs into the requirements for the reliability or availability of objects. Whether or not this would be possible by means of a method based on vehicle and vessel hours lost is currently being investigated. If anything, the significance of the object for the network will be expressed more clearly.

## 4.2 Methods for requirements

As long as a direct, quantitative relationship with the SLAs cannot be made, other methods will have to be adopted to do justice to the spirit of the SLAs: stringent requirements for important objects and less stringent requirements for less important objects. A number of methods are available for the purpose of drawing up this reliability or availability (R/A) requirement.

### *4.2.1 Economic optimization*

The most rational way of establishing an R/A requirement is to use a social cost-benefit analysis (SCBA) to look for equilibrium between the damage sustained as a result of the non-availability of the object and the (life cycle) costs it requires to achieve the desired degree of availability. Damage (failure costs) comprises the direct costs of the repair actions and the damage to society. In the event of failure on the part of the transport networks of Rijkswaterstaat, this could include capitalizing vehicle and vessel hours lost. This theory is illustrated in figure 4.1.

As (expected) availability increases, the failure costs decrease, to € 0 in the hypothetical but impossible scenario of 100% availability. However, the costs of achieving this degree of availability increase exponentially. The total costs (which, incidentally, do not have to be borne by a single party) are the sum of both. The fact that each cost item increases as the other decreases means that a minimum can always be found for the total costs. Usually this is a flat minimum, between 96.5% and 98% in the example.

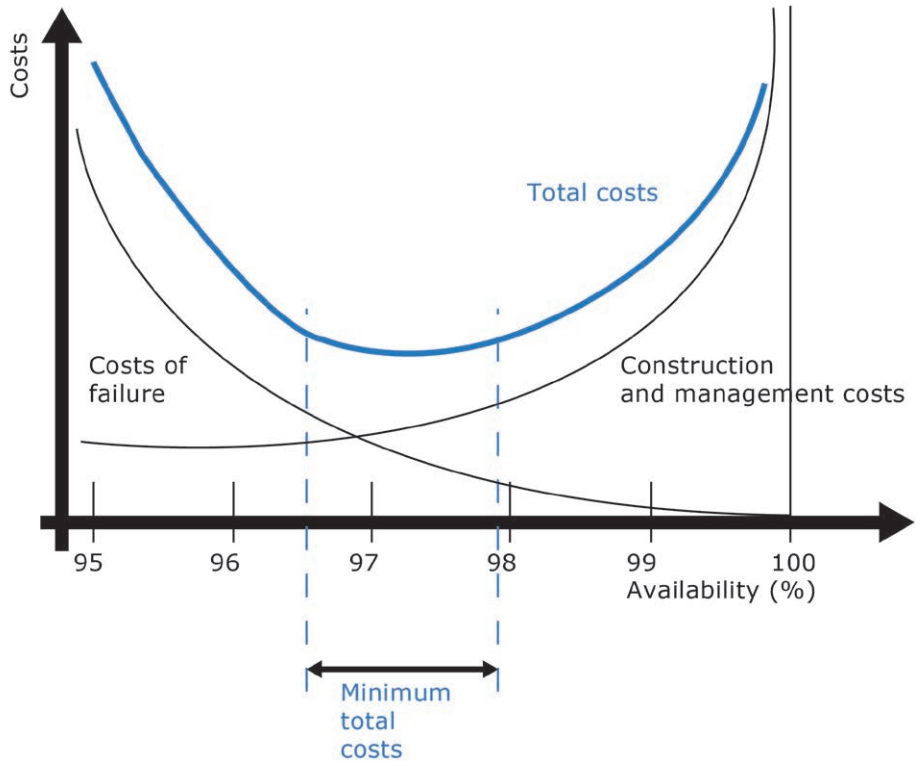



*Figure 4.1 Economic optimization*

The procedure of economic optimization provides a basis for the requirement for the object (the system element of the network). This procedure is illustrative and transparent, as well as expensive and specific to the relevant object. Neither can the result be generalized adequately to similar objects, because the failure costs depend on the significance of the object for the network.

This approach is described in more detail for the function 'passing through a lock' in [6]. The accompanying realistic case study established that a requirement of (no more than) 1-1.5% unplanned non-availability was economically optimal for the function 'passing through a lock'.

### *4.2.2 Requirements stemming from legislation and regulations*

Things are much more straightforward when the R/A requirements stem from legislation or regulations. This is the case, for instance, for civil engineering structures in (primary) flood defences, for which the Water Act dictates requirements for the function 'retaining high water'.

There are more statutory frameworks that constitute a source of requirements set for objects. For example, the Housing Act stipulates, by way of the Buildings Decree and the Eurocodes, reliability requirements for structures in relation to the function 'withstanding loads' (i.e. requirements in terms of strength). And the *National Tunnel Standard* [7] sets out explicit requirements for the reliability and availability of Rijkswaterstaat's tunnel systems. For the function 'full traffic flow', for instance, this standard sets an availability requirement of 93%. The tunnel is allowed to be available to a limited extent (limited traffic flow) 5% of the time and the other 2% the tunnel may be out of use (no traffic flow). This means that the tunnel is available to the road user 98% of the time (on average), with limited traffic flow making up a maximum of 5% of this. The National Tunnel Standard also sets requirements for the frequencies of disruptions (unplanned maintenance). For example, an entire tunnel may only be obstructed as a result of a disruption once a year on average (based on the prevailing version of the National Tunnel Standard 2016).

### *4.2.3 Requirements stemming from the past*

Past performance of objects can form a basis for drawing up requirements in the event of major renovations or for requirements to be set for similar objects to be newly built. The same applies to past performance that was not deemed satisfactory. This can assist in formulating a more stringent requirement.

It should be noted, however, that the perception of the reliability and availability of an existing object will usually differ in a positive sense from the actual reliability and availability and, to an even greater extent, from the calculated reliability and/or availability. Minor disruptions sometimes are deemed insignificant (particularly in the main waterways network and the main water system) and major disruptions only occur very sporadically, causing a skewed perception of actual reliability/availability. Nevertheless, both types of disruption do form part of the risk analysis.

### *4.2.4 Requirements stemming from a reference design*

If a reference design is prepared for a tendering process, a risk analysis of that design will provide realistic requirements for the object to be built. In such a case, it will also be possible to study what additional costs more stringent requirements will entail and how much can be saved by setting less stringent requirements. Economic optimization, as described in section 4.2.1, will then be within reach. As a variant of this, existing similar objects could be considered. What requirements have been set for them? And are they transferable?

## 4.3 Concluding remarks

In general, increasing planned non-availability results in a decrease in unplanned non-availability, and vice versa. If a stringent requirement is set for the unplanned non-availability, a more relaxed requirement for planned non-availability would be appropriate. Nevertheless, such a situation will also be more expensive than its opposite: little planned maintenance and a lot of unplanned non-availability, at least if the failure costs are not charged. It is, therefore, advisable to draft uniform specifications.

Sometimes it is worthwhile setting a requirement for both reliability and availability. This prevents scenarios in which systems that do not fail frequently come with protracted recovery times. Or conversely, systems that fail frequently come with short recovery times. The second option is desirable in situations where queues can build, such as at tunnels or movable bridges. The aggregate of multiple brief disruptions is not as serious as one extremely long disruption, as waiting times increase quadratically in the event of a long disruption.

Requirements set for functions and systems must be realistic. If these requirements have not yet been recorded properly, this will have to be done in the maintenance plan for that object. The systems design requirements must be feasible and maintainable. As already stated in section 4.2.3, perception, statistics and calculations differ. If the requirement is to be verified by way of calculation (i.e. it is a quantitative requirement), this should be taken into consideration. A requirement set for unplanned maintenance must also be grounded in realism. For example, it will not be possible to set a requirement in terms of maximum duration. Indeed, the risk analysis calculates the average non-availability, but the precise juncture and how long the repair work will take cannot be predicted.

# 5 Qualitative object risk analysis

## 5.1 Introduction

The previous chapters outlined the characteristics and uses of the qualitative and quantitative variants of the object risk analysis (ORA). This chapter will examine the **qualitative object risk analysis** in more detail. In the figure below, the numbers accompanying the successive process steps refer to the sections in which they are discussed.

This chapter uses the FMECA format of simplified object risk analysis, version 2.1.1., from WW RWS number 1560. **For the most recent version, including the manual, see WW RWS.**

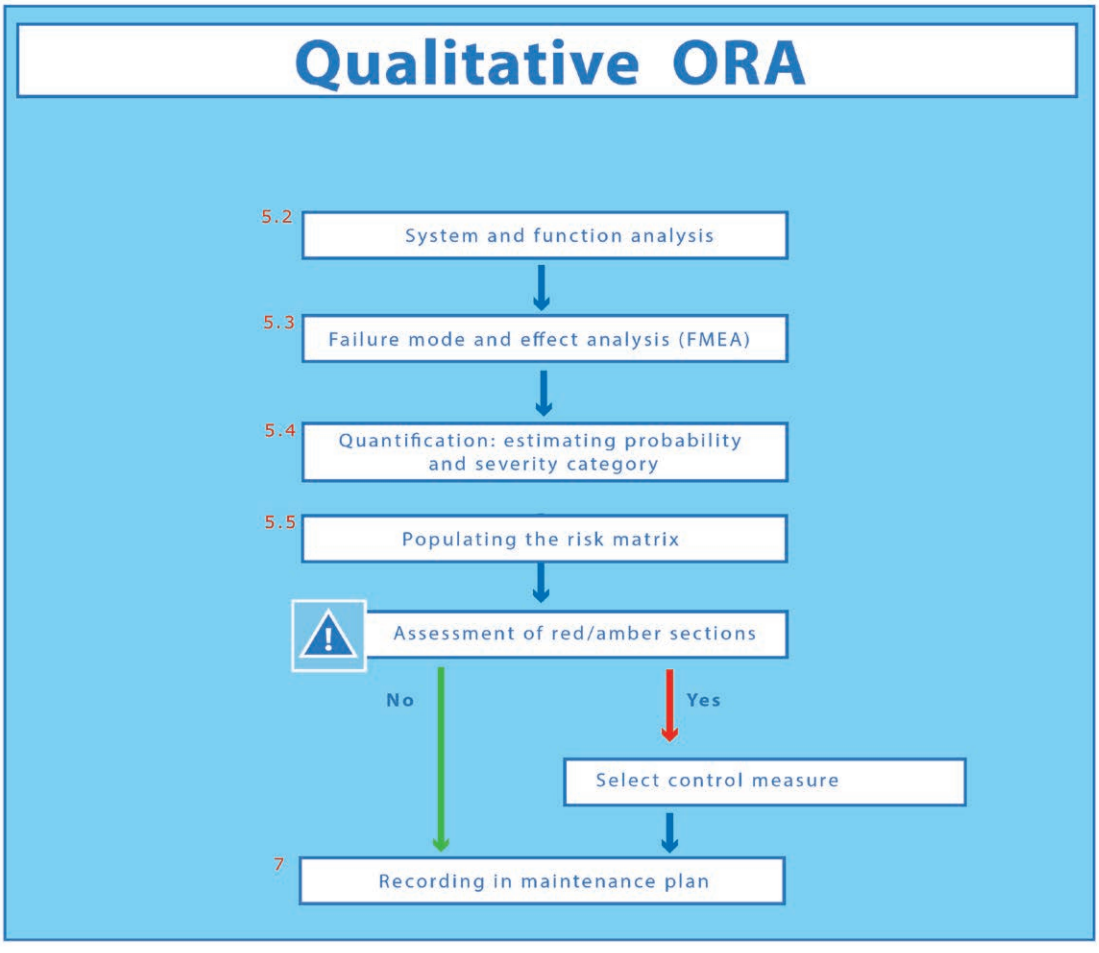



*Figure 5.1. Steps in the qualitative ORA*

The descriptions below illustrate the successive steps using a movable bridge. This movable bridge will serve as an example for the next few chapters.

## Example: a drawbridge

In this example of a movable bridge the focus is on the aspect non-availability. Reliability is determined in a similar way.

The movable bridge is of the type 'drawbridge', comprising a roadway (the movable bridge deck), an operating mechanism (with only the electromotor being considered for the sake of simplicity), an operator's cabin with an operator, a computer with operating system, and two sensors that both indicate whether the bridge deck is at rest again after the bridge has been open. See figure 5.2.

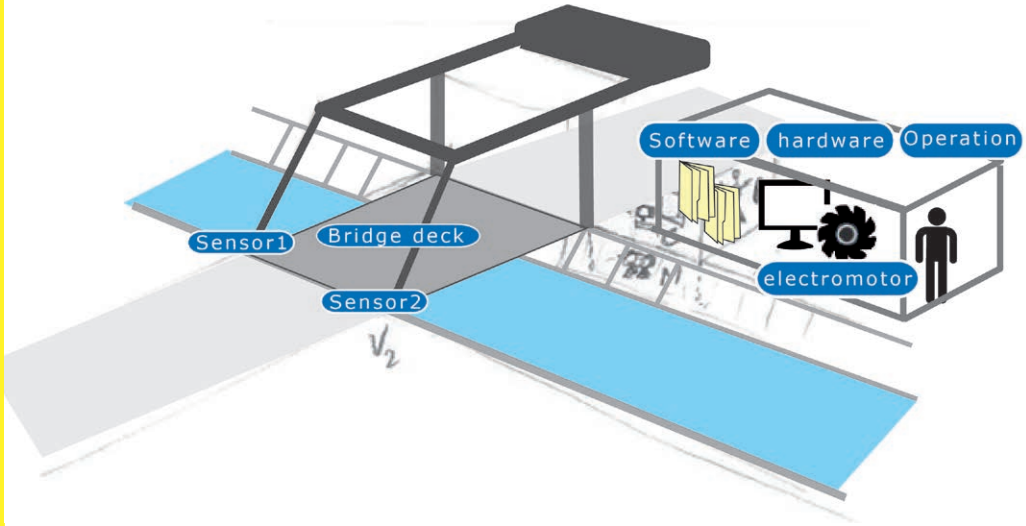
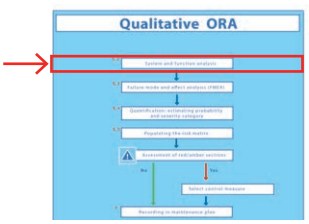



*Figure 5.2: Drawbridge*

The bridge is part of a motorway and spans a local waterway. At rest, the bridge enables traffic on land to pass across it; when open, it lets through waterborne traffic that is too tall to pass through when the bridge is at rest. When the bridge has to be opened, the operator sees to it that the bridge is free from traffic in accordance with a prescribed procedure. Next he sets the operating mechanism in motion, usually by means of hardware (computer) and special software (operating system). The operating mechanism opens the bridge. When closing the bridge, the operating system uses both sensors to test whether the bridge deck is back in the required position. The mechanism is redundant: if one sensor fails, the other sensor can be relied on. Only once the operating system indicates that the bridge deck is in the correct position will the operator be able to open the motorway again.




## 5.2 Process step: system and functional analysis

Risk-based asset management calls for a functional approach, with performance requirements being set on the basis of RAMSSHE€P terms in addition to functional requirements. Prior to carrying out the initial ORA, the object must first be properly described in terms of systems engineering. This system and functional description is important for documenting how the system works. For complex objects, a functional breakdown is recommended, which provides definitions of various component functionalities.

Every object has one or more primary functions. A storm surge barrier, for instance, protects inland areas against flooding. If the storm surge barrier is movable, a second primary function could be allowing vessels to pass through. The primary function of a weir is to control the water level in a river. A tunnel allows people to get from A to B and therefore facilitates the flow of road traffic. A corridor of weirs and locks in a waterway combines a primary function for water management with the function 'flow of water traffic'.

In addition to primary function(s), objects usually also have several secondary functions, such as creating an ecological link at a storm surge barrier by allowing fauna to pass through. To accurately determine the desired performance of an object, it may be necessary to break down the primary functions into subfunctions. The primary function of a moveable storm surge barrier, for example, can be subdivided into shutting off and stemming the flow of water. Opening a barrier is an important function for restoring the function of the waterway (shipping and/or draining water).

Finally, a quick note on the term safety, which is often regarded as a primary function. This is correct if it relates to a movable storm surge barrier whose primary function is to ensure safety. As regards most other objects, safety may well be important, but it does not constitute a function. A tunnel, for example, does not have the function of fostering safety. In systems engineering terminology, safety is called an aspect requirement. Applied to a tunnel, this means that road traffic flows through in a safe manner. The primary function of a tunnel is to facilitate traffic flow subject to the precondition (aspect requirement) that this occurs safely. In such cases, the safety aspect places additional requirements on a system.

### System and functional description

A system and functional description provides a clear overview of:

- how the system works;
- which subsystems play a role;
- what the functions of the subsystems are.

The preferred method for creating a system and functional description for existing objects is by using available design and as-built information. As a rule, this description will consist of texts and diagrams that clearly illustrate the structure of the system. For objects that do not (or do not yet) exist, the design documents are used. See also [3] and [8].

The system description must be composed in such a way that it provides full documentation of how the system works and of the functionality of its elements. Elements could be hardware components, software modules and human actions. In these guidelines, the term 'components' pertains to hardware components.

In order to be able to perform a risk analysis, it is imperative that the system limits of the object are clearly recorded. It is also important for administrators to know the object's purpose in relation to other objects. In line with the systems engineering approach, the description of the system must provide objective, comprehensive information on the system's function(s). After all, it is important to know (for example) whether lowering a weir should require 1 or 4 hours. The system and functional description must formulate the success criteria in such a way that they are quantifiable. At the end of the day, these criteria are related to the failure criteria, which in turn are linked to the performance requirements.

## System breakdown

Breaking down objects and functions and linking them as individual elements creates visible relationships between the functions and the physical components of the object. These relationships are essential for the risk analysis, as the relationships between the failure of elements must be translated into the possible failure of the object's function.

Breaking down the object is based on a system breakdown structure (SBS) with the aid of the NEN 2767-4 standard. Crucial in this regard is an unambiguous representation of the physical correlation of the components that make up the object. The function of each SBS element must be defined. The functional cohesion between the various SBS elements must be illustrated using block diagrams, which must also outline how the elements work and combine. The input and output of the various blocks must be clear, with particular attention for the links between various block diagrams (the system interfaces).

Particularly when more complex systems are concerned, it is important to properly identify the relationships between parts of the system and functions. This will result in a matrix with the breakdown into system parts (down to system element level) on one axis, and the breakdown into component functions on the other. The breakdown is not an end in itself, but rather a tool and a solid basis on which to produce a risk analysis and an integrated consideration of the entire maintenance process.

## Breakdown level

The general response to the question as to what level of detail a breakdown has to be carried out is: to the level of the system element (structural part) – and in this case the hardware component – that is subjected to maintenance, replacement or reconditioning as a separate unit.

In anticipation of the quantitative analysis (chapter 6), it is also important for the breakdown level that the failure frequency and recovery time are calculated. A pump, for instance, will be fully replaced when it fails. A more detailed breakdown into parts is therefore not necessary or desirable. The frequency of failure of a pump can be retrieved from data books. This is different for a complete power supply unit. This has to be broken down into constituent parts, each of which will have its own failure frequency, such as the emergency power unit, the mains supply and the connecting components.

In the case of software system elements, the breakdown will reach module level (see section 6.3.2). Human actions are broken down to the level at which the OPSCHEP model can be used (see section 6.3.3).

## NEN 2767-4

The guidelines that are binding for system breakdown are set out in NEN 2767-4. Application of the standard will ensure that similar objects are described in a uniform manner. Furthermore, it will enable efficient use of any available libraries of failure modes and failure definitions and best practices of previously described and analysed objects. Using the coding adopted in the standard enables better comparison and assessment of similar objects.

The lowest level that the NEN 2767-4 uses is the level of structural or plant component. In many cases the requisite breakdown will probably go beyond that level. For those lower levels no nomenclature and coding are prescribed, but it would seem obvious to do so in line with the NEN standard.

## Example: the drawbridge

The scope of the analysis is determined by the system described in the previous section. This means, for example, that the outer harbour with its mooring sites is beyond the scope of the analysis and hence does not have to feature in it.

In the example of the drawbridge, the scope was intentionally limited and the breakdown simplified to the system elements:

- bridge deck
- operating mechanism
- computer (hardware)
- sensors (2)
- operator
- operating system (software)

In reality, the system elements 'operating mechanism' and 'computer' will be broken down further. After all, it is not possible to establish the probability of failure for 'an' operating mechanism, as there are too many different types of such a composite part. Additionally, maintenance work is carried out on parts of the operating mechanism.

A simplified breakdown for movable bridges in accordance with NEN 2767-4 will comprise:

- 1461 Main supporting structure (bridge deck)
- 1182 Drive unit and operating mechanism, electromotor
- 1431 Operating and control equipment, PLC (computer, hardware)
- 1490 Measuring equipment, sensor.

Operation by the operator and the software are not classified by the NEN-2767 standard.

Even the functional analysis is straightforward in this simple example. The bridge has two functions: allowing road traffic to pass through and allowing vessels to pass through. Figure 5.3 presents the relationship between functions, system elements and subfunctions.

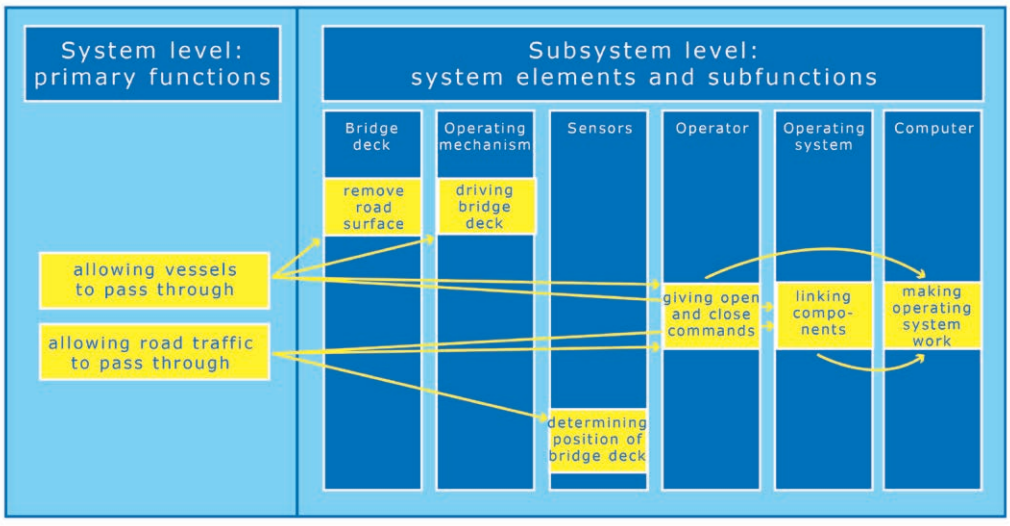
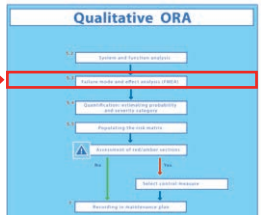



*Figure 5.3. Functional analysis and allocation*




## 5.3 Process step: FMEA

*The failure mode and effect analysis* (FMEA) is a technique used to identify all possible anomalies in terms of the functioning of a system element and to record the consequences of that failure for the system. The technique has been standardized [9].

How the system is structured and how it works are set out in the system analysis (see 5.2). The system is broken down into an object tree, in line with NEN 2767-4 [4], and possibly a function tree, in line with the SE approach [3, 8].

For each system element it will subsequently be determined, in a setting with experts on the system, how the system element could fail (failure modes) and what the consequences of failure would be (effect). This is done in a structured manner based on a list of (standard) guide words. See table 5.1.

The results of this analysis are recorded in a table or spreadsheet. Rijkswaterstaat uses a standardized Excel template for this [10].

| GUIDE WORD | APPLICATION |
|---|---|
| NONE or NOT | The intended function is missing entirely. |
| MORE or HIGHER or LATER or FASTER | There is a quantitative increase in the intended function. Depending on the nature of the deviation, the most suitable guide word will be chosen. |
| LESS or LOWER or SOONER or SLOWER | There is a quantitative decrease in the intended function. Depending on the nature of the deviation, the most suitable guide word will be chosen. |
| UNSATISFACTORY | The intended function is being unsatisfactorily fulfilled. |
| INCORRECT | An incorrect function is being fulfilled rather than the intended function. |
| PARTIAL | The intended function is only partially being fulfilled. |
| IRREGULAR | The intended function is being fulfilled irregularly. |
| AS WELL AS | The intended function is satisfactory, though an additional effect is occurring. |
| WRONG | The intended function is being fulfilled in the correct way, but wrongly because this function was not supposed to be fulfilled. |
| REVERSE | The intended function is not being fulfilled and, in fact, the opposite effect or direction is occurring. |
| OTHER THAN or WHERE DIFFERENT | The intended function is not being fulfilled at all. Something completely different is happening, possibly even at another location. |

*Table 5.1. The most common guide words with their application for the purposes of an FMEA*

## Example: the drawbridge

The breakdown from section 5.2 forms the basis of the FMEA. For each system element it will be systematically investigated, with the aid of guide words, whether non-functioning will entail consequences for the system. In this stage we limit ourselves to the different failure modes and the impact of failure on the function. Figure 5.4 summarizes the result of the FMEA.

**Object risk analysis (ORA)**

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Management object code** | | | | | | **Date:** | 20-11-2015 | **Drawn up b** | S.E. van Manen | | | | |
| **Name according to DISK:** | | Example movable bridge | | | | **Version:** | 1.0.0 | **Consultanc** | RWS | | | | |
| **Name other (optional):** | | | | | | **DISK cluster code:** | | **Contract c** | | | | | |
| | **Stage 1: Desk-based study: process steps information transfer and I-ORA** | | | | | | | | | | | | |
| **Element/structural part** | | **Code element/ structural part** | **Function of the part** | **Functional failure** | **Failure mode** | **Code failure mode** | **Failure mechanism** | **Cause of failure** | **Source of failure** | **Consequence of failure** | **Immediately measurable?** | **Allowing road traffic to pass** | **Allowing vessels to pass** |
| **Main supporting structure** | | | | | | | | | | | | | |
| 1461 | Bridge deck | V | Supporting road traffic | Is not capable of supporting road traffic | Collapse | B | Falling down | Fatigue crack | Incorrect details in design | Possible casualties and fatalities, expensive repair and protracted recovery time | Yes | Yes | Yes |
| **Drive unit and operating mechani** | | | | | | | | | | | | | |
| 1182 | Electromotor | EM | Setting the bridge deck in motion | Bridge deck cannot be lifted | Motor will not start | SN | Ageing, vibration, wear, friction | External influence | Maintenance | Vessels cannot pass through | No | No | Yes |
| | | | | | Motor stops prematurely | SV | Ageing, overheating, wear | Overload | NA | Neither vessels nor road traffic can pass through | Yes | Yes | Yes |
| **Operating and control equipment** | | | | | | | | | | | | | |
| 1431 | PLC | BB | Controlling the various components | The bridge cannot be lifted | Stops working | SV | Vibration, degradation | External influence | NA | Vessels cannot pass through | Yes | No | Yes |
| **Measuring equipment** | | | | | | | | | | | | | |
| 1490 | Sensor no 1 | S | Determine whether the bridge deck is in the right place | The bridge cannot be opened to road traffic | Stops working | SV | Degradation, contamination, wear | External influence | NA | Bridge remains closed to road traffic | No | Yes | No |
| 1490 | Sensor no 2 | S | Determine whether the bridge deck is in the right place | The bridge cannot be opened to road traffic | Stops working | SV | Degradation, contamination, wear | External influence | NA | Bridge remains closed to road traffic | No | Yes | No |

*Figure 5.4. FMEA drawbridge*

Formally speaking, all guide words from table 5.1 need to be applied to the function of all components. For the function of the bridge deck, then, 'none', 'insufficient' or 'partial' apply. The other anomalies of the function are not applicable as they are, in fact, inconceivable. The 'support road traffic more', or 'support road traffic more slowly', do not make sense.

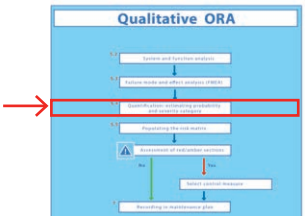
'None', 'insufficient' or 'partial' can all be included separately as failure mechanisms. 'None' can mean collapsing, 'insufficient' could stand for unsafe (the bridge deck is still functioning, but the strength is inadequate to the task of supporting large traffic loads), and 'partial' might imply partially collapsing. For the sake of simplicity, only the failure mode 'cannot support road traffic' will be used in the example from here on, meaning that the bridge has collapsed.

In the case of the electromotor there are two possible failure modes: the motor does not start (guide word 'none') or it stalls halfway (guide

word 'later'). Naturally expansion is possible, using terms such as 'irregular', etc. Thus the following failure mechanisms are identified for the drawbridge:

| SYSTEM ELEMENT | GUIDE WORD | FAILURE MECHANISM |
|---|---|---|
| BRIDGE DECK | None | Collapse |
| ELECTROMOTOR | Not | Does not start |
| ELECTROMOTOR | Later | Stops prematurely |
| PLC | Not, incorrect | Stops working |
| SENSORS (2) | Not, wrong | Stops working |

Note that the operator, with the function 'operate', and the operating system, with the function 'control the components', do not feature in the FMEA. They do feature in the quantitative analysis, however.




## 5.4 Process step: estimating probability and severity categories

When using the qualitative variant of object risk analysis, the FMEA is extended to include probability and severity categories. As such, the qualitative variant is in effect a semi-quantitative variant; after all, the range within which the probability of failure lies is estimated and expressed as a numerical relationship. The severity categories are also quantitative, wherever possible. In essence, the FMEA is expanded to become an FMECA (*failure mode, effect and criticality analysis).* The FMECA results in measures to reduce the observed risks. This variant is not explicitly used during the realization stage, because the fundamental principle is that the risks are already being managed by means of appropriate measures that have largely been incorporated into the customer requirement specification.

For all failure modes of all system elements from the FMEA (section 5.3), an estimate is made of the probability of occurrence and the consequences. The scale of the risk can be calculated based on the total of these estimates.

### *5.4.1 The probability score*

Estimating probability is based on the current standard of operational maintenance.

The probability of a certain failure mode occurring for an element of a system is entered based on expert opinion and occasionally supplier information. The source of this estimation needs to be stated as well (e.g. 'Rijkswaterstaat Reference Framework Management and Maintenance' [11], supplier information or expert opinion). The indicator used in this respect is 'lifespan', or mean time to failure (MTTF). The MTTF generally becomes shorter the older the system is. If the technical lifespan of a component is up (or nearly up), the probability of failure will be greater than it will be for a new component. In particular cases a system will barely age and the failure rate will remain constant.

The MTTF is then classed in a probability category. The limits of the probability categories (the time windows) were chosen on the basis of a 6-year maintenance inspection.

The following probability scores apply to ageing in the model-risk matrix (here *t* denotes the point in time at which the next failure is anticipated).
*1. Negligible (20 yr < t)*
The failure is not expected to occur within the next 20 years.
*2. Low (6 yr < t ≤ 20 yr)*
The failure is expected to occur within 6 to 20 years from the current point in time.
*3. Moderate (2 yr < t ≤ 6 yr)*
The failure is expected to occur within 2 to 6 years from the current point in time.
*4. High (½ yr < t ≤ 2 yr)*
The failure is expected to occur within 6 months to 2 years from the current point in time.
*5. Certain (t ≤ ½ yr)*
The failure has already happened or is expected to occur within the next 6 months.

If the probability of failure remains constant over time, the probability scores given should be regarded as average frequencies:
*1. Negligible*
On average, the failure occurs less than once every 20 years.
*2. Low (6 yr < t ≤ 20 yr)*
On average, the failure occurs once every 20 years or more often, but less than once every 6 years.
*3. Moderate (2 yr < t ≤ 6 yr)*
On average, the failure occurs once every 6 years or more often, but less than once every 2 years.
*4. High (½ yr < t ≤ 2 yr)*
On average, the failure occurs once every 2 years or more often, but less than once every ½ year.
*5. Certain (t ≤ ½ yr)*
On average, the failure occurs once every ½ year or more often.

### *5.4.2 The severity score*

The qualitative risk analysis considers the consequences for all RAMSSHE€P aspects. The aspect reliability (R) represents the probability, which is classified in probability categories in this process step, and is therefore not included in the consequence analysis. For the other aspects the severity score is calculated for each aspect with the aid of the table below (table 5.2). For each failure mode, the highest severity score over all aspects applies for the purposes of calculating the total risk score.

Rijkswaterstaat has elected to group the undesirable consequences into four categories:
1. Negligible
2. Limited
3. Major
4. Serious

Furthermore, severity score 0 is allocated if there is no consequence for an aspect. The severity score corresponds to the desired performance level of the relevant object. In the case of availability, or hindrance (A), a predetermined upper and lower limit are used. Hindrance shorter in duration than the lower limit is assigned the severity score 'Limited' (2). Hindrance longer in duration than the upper limit is assigned the severity score 'Serious' (4). Hindrance between the upper and lower limits is assigned the severity score 'Major' (3). Table 5.2 indicates what is meant by 'Negligible', 'Limited', 'Major' and 'Serious' for the other RAMSSHE€P aspects.

| | | CONSEQUENCE | | | |
|---|---|---|---|---|---|
| | | **1: NEGLIGIBLE** | **2: LIMITED** | **3: MAJOR** | **4: SEVERE** |
| **RAMSSHE€P** | **A** | Extremely brief hindrance for primary object functions; no hindrance for network | Hindrance for network is shorter in duration than the lower limit for all function categories:<br>1. road traffic<br>2. shipping<br>3. water management | Hindrance for network is shorter in duration than the upper limit in all function categories, but exceeds the lower limit in one or more of the function categories:<br>1. road traffic<br>2. shipping<br>3. water management | Hindrance for network exceeds the upper limit in one or more of the function categories:<br>1. road traffic<br>2. shipping<br>3. water management |
| | **M** | Local repair, easily done | Repair involving extra effort (e.g. due to special tool, or waiting for spare parts) | Repair involving considerable effort (e.g. due to forcing access for the purposes of carrying out maintenance work or waiting for permits or spare parts that need to be specially made) | Repair is no longer viable in view of the economic lifespan of the object; other types of measures will be necessary (e.g. large-scale replacement) |
| | **S** | The failure leads directly or indirectly to accidents involving non-permanent injury to one or more people without resulting in absence | The failure leads directly or indirectly to accidents involving non-permanent injury to one or more people with medical assistance/hospital admission being required | The failure leads directly or indirectly to accidents involving permanent injury to one person | The failure leads directly or indirectly to accidents involving:<br>- permanent injury to multiple people, or<br>- fatal injury to one or more people |
| | **SE** | Undesirable human actions possibly with minor consequences such as graffiti | Undesirable human actions possibly with limited consequences such as access to an unimportant space | Undesirable human actions possibly with major consequences such as digital/physical access to confidential information | Undesirable human actions possibly with serious consequences such as digital/physical access to the object's (emergency) controls |
| | **H** | In time, adverse health effect in one or more people | In time, temporary damage to health of one or more people | In time, permanent damage to health of one person | In time:<br>- permanent damage to health of more people<br>- fatal damage to health of one or more people |
| | **E** | Negligible consequences for flora and fauna | Limited consequences for flora and/or fauna; no measure necessary, will rectify itself | Major consequences for flora and/or fauna; measures necessary to prevent becoming more serious | Serious, long-term consequences for flora and fauna; large-scale measures necessary |
| | **€** | Consequential costs between €100 and €10,000 | Consequential costs between €10,000 and €100,000 | Consequential costs between €100,000 and €500,000 | Consequential costs > €500,000 |
| | **P** | Complaints | Loss of image local | Loss of image regional | Loss of image nationwide |

*Tabel 5.2. De classification of possible consequences*

## Example: the drawbridge

For qualitative risk analysis, the FMEA is extended to form an FMECA. The initial desk-based study entails an estimate of the probability category and the severity category for each failure mode identified.

The drawbridge was built in 1995. A failure of the bridge deck will be immediately evident and will entail consequences for both road traffic and shipping traffic. For the primary function 'allowing road traffic to pass through' (LPW), the lower limit set for disruption is 1 day and the upper limit set for disruption is 1 week. For the function 'allowing vessels to pass through' (LPS), the lower limit set is 2 days and the upper limit set is 1 month.

The bridge deck is estimated to have an average lifespan equal to the planned lifespan: 100 years. This is a pessimistic estimate. This estimate places the bridge deck in probability category 1 (see table 5.2).

With these assumptions, the consequences of the bridge deck's failure for the RAMSSHE€P aspects (minus reliability) are:

| ASPECT | CONSEQUENCE | SEVERITY CATEGORY |
|---|---|---|
| AVAILABILITY (HINDRANCE) | Severe, greater than 1 month | 4 |
| MAINTAINABILITY | None | 0 |
| SAFETY | Severe | 4 |
| SECURITY | None | 0 |
| HEALTH | None | 0 |
| ENVIRONMENT | None | 0 |
| COSTS | Severe, more than €500,000 | 4 |
| IMAGE | Nationwide loss of image | 4 |

Information on the electromotor's failure frequency is in a database. For the purposes of this example it has been assumed that the motor fails relatively frequently, namely once a year, putting it in probability category 4. This, too, is a pessimistic estimate, as in practice, the electromotor fails (much) less often. The electromotor can be repaired within one day (approx. 12 hours). With this assumption, the consequences will be:

| ASPECT | CONSEQUENCE | SEVERITY CATEGORY |
|---|---|---|
| AVAILABILITY (HINDRANCE) | Shorter than the lower limit | 2 |
| COSTS | Between €100 and €10,000 | 1 |
| IMAGE | Complaints | 1 |

The other consequences are not applicable, and should therefore be reported as such.

The PLC fails once every 5 years on average, as listed in a database. This puts it just in probability category 3. Failure can be remedied within a day. The consequences for this assumption are as follows:

| ASPECT | CONSEQUENCE | SEVERITY CATEGORY |
|---|---|---|
| AVAILABILITY (HINDRANCE) | Shorter than the lower limit | 2 |
| COSTS | Between €100 and €10,000 | 1 |
| IMAGE | Complaints | 1 |

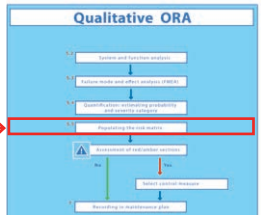
On average, a sensor fails once every 10 years. This corresponds to probability category 2. The failure is not noticeable before the bridge deck is lowered again. The recovery time is (only) 4 hours because the second sensor is the backup enabling the bridge to continue working. The repair work will not affect availability. The consequences for these assumptions are as follows:

| ASPECT | CONSEQUENCE | SEVERITY CATEGORY |
|---|---|---|
| AVAILABILITY (HINDRANCE) | Negligible | 1 |
| COSTS | Between €100 and €10,000 | 1 |
| SECURITY | Undesirable human actions possible, vandalism | 1 |
| IMAGO | Complaints | 1 |

All assumptions and identified values from the 'drawbridge' example are summarized in figure 5.5.

| Element/structural part | | Year of build/installatio | MTTF [years] | Probability score | Hindrance | M | S | Se | H | E | € | P | Maximum severity score | Risk score | Risk level | Explanation, source |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Main supporting structure** | | | | | | | | | | | | | | | | |
| 1461 | Bridge deck | 1995 | 100 | 1 | 4 | 0 | 4 | 0 | 0 | 0 | 4 | 4 | 4 | 4 | Acceptable | Design documents, Eurocode |
| **Drive unit and operating mechani** | | | | | | | | | | | | | | | | |
| 1182 | Electromotor | 1995 | 1 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 2 | 8 | Undesirable | Rijkswaterstaat Database for contractors |
| | | | 1 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 2 | 8 | Undesirable | Rijkswaterstaat Database for contractors |
| **Operating and control equipment** | | | | | | | | | | | | | | | | |
| 1431 | PLC | 2005 | 5 | 3 | 2 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 2 | 6 | Undesirable | Rijkswaterstaat Database for contractors |
| **Measuring equipment** | | | | | | | | | | | | | | | | |
| 1490 | Sensor no 1 | 2005 | 10 | 2 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 2 | Acceptable | Rijkswaterstaat Database for contractors – sensor position counter |
| 1490 | Sensor no 2 | 2005 | 10 | 2 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 2 | Acceptable | Rijkswaterstaat Database for contractors – sensor position counter |

*Figure 5.5. Estimate probability and severity categories in the initial analysis, the desk-based study*




## 5.5 Process step: populating the risk matrix

The risk matrix provides an immediate overview of the necessity of a control for a given failure mode with a probability category and a severity category. The matrix works with a colour code for three levels: red, amber or green.

1. Red = unacceptable
A measure must be taken to manage the risk. There may also be grounds to review regular maintenance or to propose a variable maintenance measure or even redesign.

2. Amber = undesirable
Either a measure must be implemented to manage the risk or the reason(s) why this is not feasible/necessary will need to be demonstrated. It may also be necessary to review standard operational maintenance or to add a variable maintenance measure.

3. Green = acceptable
No measures have to be taken to manage the risk. If the failure mode presents itself, the usual actions are taken to effect repair (or recovery of function). It should be noted that a low risk could still give grounds for reviewing standard operational maintenance, but in this case because fewer activities are necessary.

| RISK MATRIX | | CONSEQUENCE | | | |
|---|---|---|---|---|---|
| | | 1: NEGLIGIBLE | 2: LIMITED | 3: MAJOR | 4: SEVERE |
| PROBABILITY | 1: NEGLIGIBLE | Acceptable | Acceptable | Acceptable | Acceptable |
| | 2: LOW | Acceptable | Acceptable | Undesirable | Undesirable |
| | 3: MODERATE | Acceptable | Undesirable | Undesirable | Undesirable |
| | 4: HIGH | Acceptable | Undesirable | Undesirable | Unacceptable |
| | 5: CERTAIN | Undesirable | Undesirable | Unacceptable | Unacceptable |

*Table 5.3. Risk matrix*

### Risk profile of the system

The risk matrix presents the probability categories, severity categories and their interrelationships. Subsequently, the total of all failure modes for all system elements can be expressed in a risk profile. To this end, the risk matrix is populated with the number of risks for each individual probability-severity combination in the relevant object.

As with the quantitative variant, the qualitative variant of the object risk analysis is of a cyclical plan-do-check-act nature. The initial desk-based study as described in this chapter is followed by an inspection (check). Deviations from the initial analysis are recorded in the same way (act). Based on this, maintenance advice (plan) will be issued, containing the measures to be taken (do). Even the anticipated effect of these measures is expressed through the risk matrix. The ultimate goal is for all risks to be within the 'green' zone.

This will also be incorporated into the maintenance plan for that object.

## Example: the drawbridge

The probability and severity estimates, as made in the previous section, are plotted in the risk matrix. This produces the risk profile - see figure 5.6.

*Risk profile per stage: number of risks in the ORA for each probability/severity combination*

*(manually refresh* ***for each risk profile*** *after* ***each ORA adjustment****. Right-click on a cell in the risk*

| *Risk profile stage 1* | Maximum severity sco | | | | |
|---|---|---|---|---|---|
| Probability score | 0 | 1 | 2 | 3 | 4 | End total |
| 1 | | | | | 1 | 1 |
| 2 | | 2 | | | | 2 |
| 3 | | | 1 | | | 1 |
| 4 | | | 2 | | | 2 |
| 5 | | | | | | |
| End total | | 2 | 3 | | 1 | 6 |

*Figure 5.6. Risk matrix following desk-based study*

There are three possible events that do not require any care, as well as three events that are undesirable. These concern the electromotor and the PLC. As already stated, the probability of these components failing has been estimated pessimistically. As long as frequent failure does not manifest itself in practice, specific measures will not yet be necessary.

During an inspection of all components, large longitudinal cracks are observed in the road surface. The probability of the bridge deck failing has become significant and now falls within category 4. No peculiarities are observed for the other components. The FMECA is adjusted and yields the picture presented in figure 5.7.

| | | Stage 2: Inspection (adjusted ORA) | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Element/structural part | | Inspection finding | MTTF | Probability score | Hindrance | MS | Se | H | E | € | P | Maximum severity score | Risk score | Risk level |
| **Main supporting structure** | | | | | | | | | | | | | | |
| 1461 | Bridge deck | Longitudinal crack (2 metres) | 2 | 4 | 4 | 0 | 4 | 0 | 0 | 0 | 4 | 4 | 4 | 16 | Unacceptable |
| **Drive unit and operating mechani** | | | | | | | | | | | | | | |
| 1182 | Electromotor | No peculiarities | 1 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 2 | 8 | Undesirable |
| | | Ditto | 1 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 2 | 8 | Undesirable |
| **Operating and control equipment** | | | | | | | | | | | | | | |
| 1431 | PLC | No peculiarities | 5 | 3 | 2 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 2 | 6 | Undesirable |
| **Measuring equipment** | | | | | | | | | | | | | | |
| 1490 | Sensor no 1 | Just replaced | 10 | 2 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 2 | Acceptable |
| 1490 | Sensor no 2 | Just replaced | 10 | 2 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 2 | Acceptable |

*Figure 5.7. Estimate of probability and severity categories following inspection*

The consequences are unchanged, as a result of which the risk 'Bridge deck collapsing' is now unacceptably high. Immediate action must be taken. Figure 5.8 gives the risk profile following inspection.

**Risk profile per stage: number of risks in the ORA for each probability/severity combination**

*(manually refresh **for each risk profile** after **each ORA adjustment**. Right-click on a cell in the risk*

| Risk profile stage 1 | Maximum severity sco | | | | |
|---|---|---|---|---|---|
| Probability score | 0 | 1 | 2 | 3 | 4 | End total |
| 1 | | | | | 1 | 1 |
| 2 | | 2 | | | | 2 |
| 3 | | | 1 | | | 1 |
| 4 | | | 2 | | | 2 |
| 5 | | | | | | |
| End total | | 2 | 3 | | 1 | 6 |

| Risk profile stage 2 | Maximum severity sco | | | | |
|---|---|---|---|---|---|
| Probability score | 0 | 1 | 2 | 3 | 4 | End total |
| 1 | | | | | | |
| 2 | | 2 | | | | 2 |
| 3 | | | 1 | | | 1 |
| 4 | | | 2 | | 1 | 3 |
| 5 | | | | | | |
| End total | | 2 | 3 | | 1 | 6 |

*Figure 5.8. Risk profile following inspection*

The bridge deck is now in the red and measures must be taken immediately. These consist of removing (heavy) traffic, removing the road surfacing, reparing the cracks, possibly welding on an extra plate and applying new road surfacing. Once the measures have been taken, the FMECA looks as follows (figure 5.9):

| | | Stage 3: Risk management: process step maintenance advice and report | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Element/structural part | | Control measure | Costs | Probability score after | A | MS | $ e | H | E | € | P | Severity score after control | Risk score after control | Risk level after control measure | Prioritization | Necessary due to statutory requirements | Explanation |
| **Main supporting structure** | | | | | | | | | | | | | | | | | |
| 1461 | Bridge deck | Getting traffic off the bridge, removing the road surfacing, welding the cracks shut, welding on an extra plate, applying new road surfacing | 50.000 | 3 | 4 | 0 | 4 | 0 | 0 | 4 | 4 | 4 | 12 | Undesirable | High | Yes | Increase frequency of inspection after repair |
| **Drive unit and operating mechanism** | | | | | | | | | | | | | | | | | |
| 1182 | Electromotor | None | | 4 | 2 | 0 | 0 | 0 | 0 | 1 | 1 | 2 | 8 | Undesirable | | | |
| | | None | | 4 | 2 | 0 | 0 | 0 | 0 | 1 | 1 | 2 | 8 | Undesirable | | | |
| **Operating and control equipment** | | | | | | | | | | | | | | | | | |
| 1431 | PLC | None | | 3 | 2 | 0 | 0 | 0 | 0 | 1 | 1 | 2 | 6 | Undesirable | | | |
| **Measuring equipment** | | | | | | | | | | | | | | | | | |
| 1490 | Sensor no 1 | None | | 2 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 2 | Acceptable | | | |
| 1490 | Sensor no 2 | None | | 2 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 2 | Acceptable | | | |

*Figure 5.9. Estimate of probability and severity categories following repair of the bridge deck*

The risk has been mitigated, but remains undesirable. One possible measure would be to increase the frequency of inspection. Figure 5.10 gives the remaining risk profile.

***Risk profile per stage: number of risks in the ORA for each probability/severity combination***

*(manually refresh **for each risk profile** after **each ORA adjustment**. Right-click on a cell in the risk*

| *Risk profile stage 1* | Maximum severity sc | | | | | |
|---|---|---|---|---|---|---|
| Probability score | 0 | 1 | 2 | 3 | 4 | End total |
| 1 | | | | | 1 | 1 |
| 2 | | 2 | | | | 2 |
| 3 | | | 1 | | | 1 |
| 4 | | | 2 | | | 2 |
| 5 | | | | | | |
| End total | | 2 | 3 | | 1 | 6 |

| *Risk profile stage 2* | Maximum severity sc | | | | | |
|---|---|---|---|---|---|---|
| Probability score | 0 | 1 | 2 | 3 | 4 | End total |
| 1 | | | | | | |
| 2 | | 2 | | | | 2 |
| 3 | | | 1 | | | 1 |
| 4 | | | 2 | | 1 | 3 |
| 5 | | | | | | |
| End total | | 2 | 3 | | 1 | 6 |

| *Risk profile stage 3* | Maximum severity score after control measure | | | | | |
|---|---|---|---|---|---|---|
| Probability score after control measure | 0 | 1 | 2 | 3 | 4 | End total |
| 1 | | | | | | |
| 2 | | 2 | | | | 2 |
| 3 | | | 1 | | 1 | 2 |
| 4 | | | 2 | | | 2 |
| 5 | | | | | | |
| End total | | 2 | 3 | | 1 | 6 |

*Figure 5.10. The remaining risk profile*

# 6 Quantitative object risk analysis

## 6.1 Introduction

This chapter describes quantitative object risk analysis (ORA) in detail. In the figure below, the numbers accompanying the successive process steps refer to the sections in which they are discussed. Because 'system and functional analysis' and 'FMEA' are the same as they are for the qualitative risk analysis, these steps in the figure refer to sections 5.2 and 5.3.

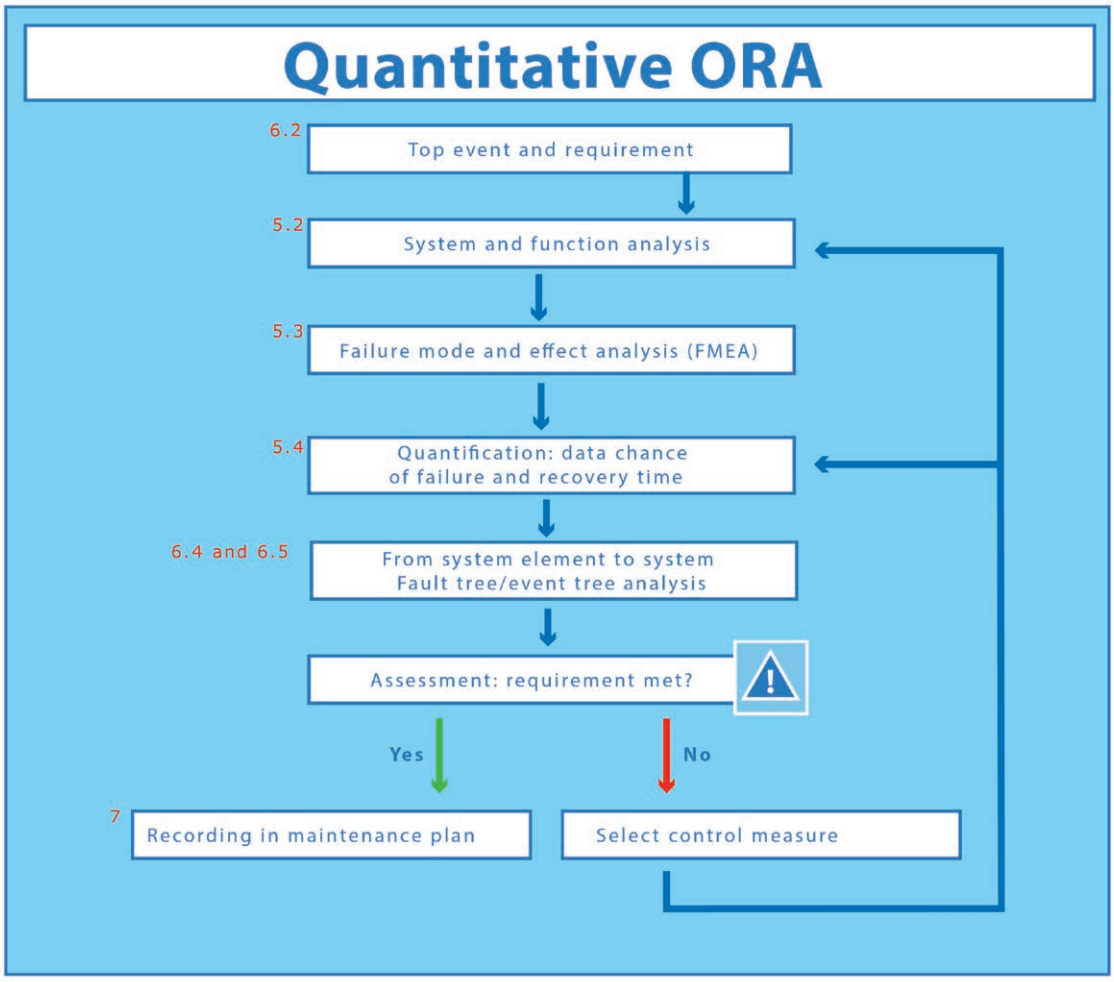
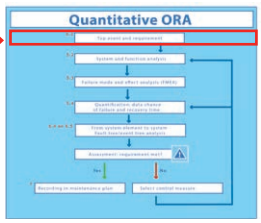



*Figure 6.1. Steps in the quantitative ORA*




## 6.2 Process step: top event and requirement

Occasionally an object has multiple top events. In the case of a movable bridge, for instance, one top event could be failure of the function 'allowing vessels to pass through' and another could be failure of the function 'allowing road traffic to pass through'. It is also conceivable for the top event to express the extent of failure. In the case of a discharge sluice complex featuring two gullies, three top events could be important: gully 1 fails, gully 2 fails and both gullies fail. Or, even more problematically, in the case of a tunnel with two lanes for each tunnel tube,

one tunnel tube might be unavailable (both lanes), or a speed restriction might have been imposed on one lane. These are three different top events, each of which can be caused by different system elements failing and each of which could have its own reliability or availability requirement.

It goes without saying that a requirement should be set for each top event: acceptable non-availability or acceptable unreliability. However, even without a requirement a quantitative ORA would be worthwhile - it would indicate what might be expected of the object in terms of reliability and availability and, with regard to these aspects, where the weaknesses as well as the potential optimizations are in the system. Furthermore, if a requirement is set, worthwhile measures can be formulated in case the requirement is not fulfilled.

## Example: the drawbridge

The drawbridge has two primary functions: allowing road traffic to pass through and allowing vessels to pass through. The top events can be induced from these directly:

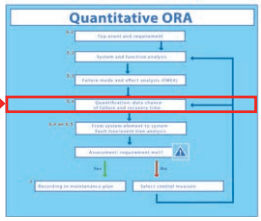
1. The drawbridge will not open (allowing vessels to pass through fails).
2. The drawbridge will not close (allowing road traffic to pass through fails).

Both primary functions must satisfy the Rijkswaterstaat mission of smooth, safe traffic flow.

Smooth traffic flow can be achieved by setting a requirement for availability. Suppose that it has been agreed, in accordance with the agreements entered into with the Minister for Infrastructure and Water Management in the SLA, that the unplanned non-availability of the bridge may total 1% on average for the function 'allowing vessels to pass through'. This boils down to around 90 hours per year (IPM teams and operational managers prefer to think in terms of hours per year).

Hence the following requirement can be included in the scope:

| ID | AVERAGE UNPLANNED NON-AVAILABILITY LPS | HIGHER | LOWER |
|---|---|---|---|
| REQUIREMENT Z | Rijkswaterstaat infrastructure should fulfil the function 'allowing vessels to pass through' with an unplanned non-availability not exceeding (an average of) 90 hours a year, calculated over the lifespan. | Requirement W | |
| **VERIFICATION STAGE** | **VERIFICATION METHOD** | **DESCRIPTION OF VERIFICATION METHOD** | |
| DESIGN AND BUILD | Verification method Reliability and Availability, 18 June 2015, version 1.0.4 | A quantitative availability analysis is requested, with it being conceivable that some risks will be borne by Rijkswaterstaat. In such a case, the contractor will not have to charge for them. | |




## 6.3 Processtap: dataverzameling

In the quantitative variant of the object risk analysis, the FMEA is extended with calculation of probability of failure and recovery times. Figure 6.2 provides an overview of this variant.

Qualitative modelling, described in sections 3 and 5.3, is followed by quantitative modelling. All system elements that could entail consequences for the top event are included in the quantitative analysis.

1. **hardware**, e.g. an engine, the electricity grid or a hydraulic cylinder
2. **software**, e.g. that of the operating system or the software used for communication between operator and system
3. **human actions**, e.g. operator errors resulting in faults, maintenance errors resulting in latent failure, or (im)proper repairs to failure during operation
4. **external events**, causes of system failure that have arisen beyond the compass of the system's normal functioning. These include fire, lightning, flooding, power cuts and ship collision. This could also include non-availability due to natural conditions (ice, excessively strong wind, excessively high water).

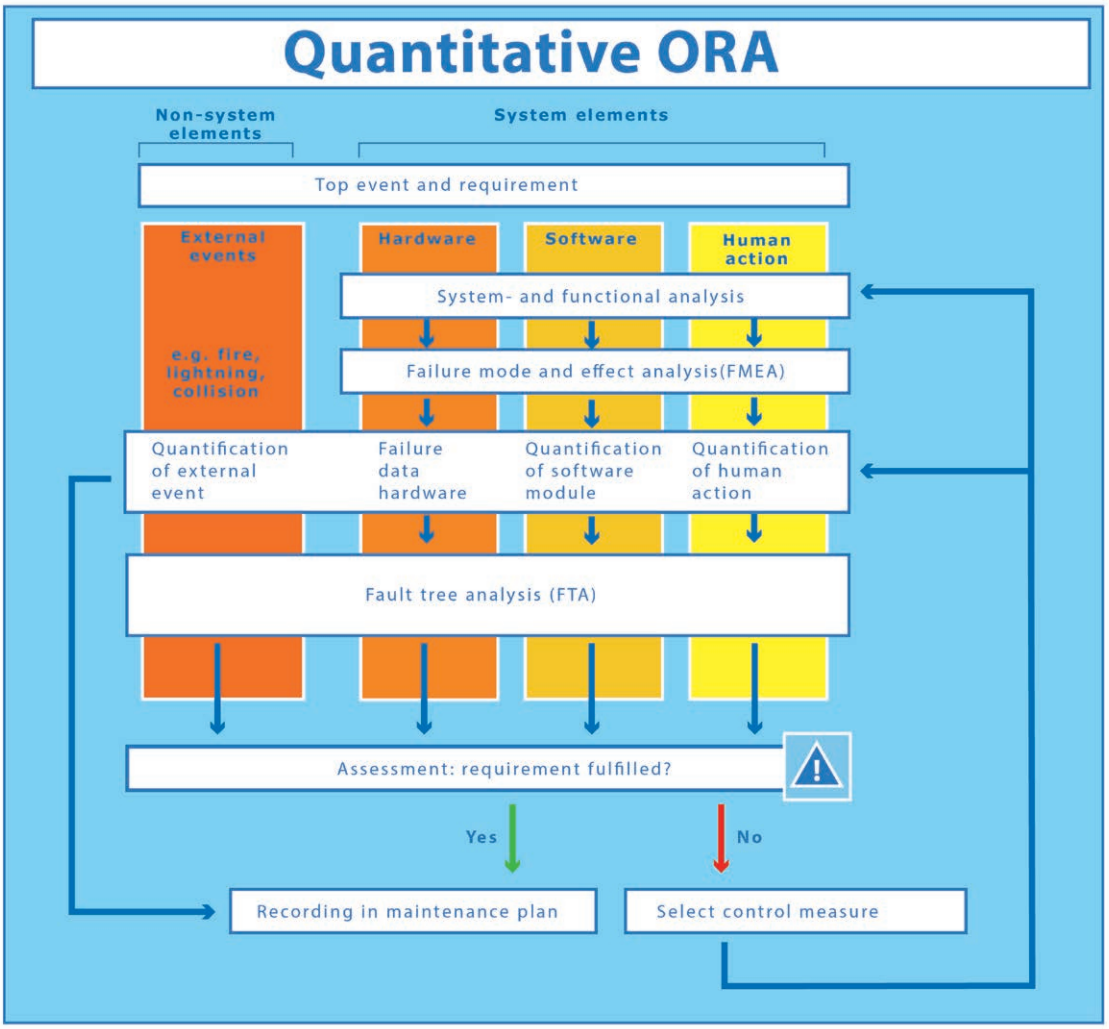



*Figure 6.2. The steps and data flows in the quantitative ORA*

As they all contribute towards possible system failure, they are elements of the risk analysis. Two characteristics need to be ascertained for these elements: the probability of failure and, in the case of hardware, software and external causes, the recovery time. Both terms are explained in more detail below.

### The concept of probability

A great deal has been said about probability and frequencies above, but a clear definition has not been offered. The concept of probability is a standardized measure of the likelihood of results of experiments, termed events. The concept of probability, as currently conceived, was first used in experiments that, from the perspective of symmetry, gave statistically predictable results. Examples include tossing a coin, or rolling a dice, or randomly picking a card from a deck of cards. It was already assumed that the sum of the probabilities of all possible outcomes of the experiment would be 1 and that the probability of an impossible outcome is 0. These assumptions constitute an important axiom: $0 \leq p \leq 1$.

A probability is always between 0 and 1. This makes it immediately possible to state that the probability of getting heads when tossing a coin is ½ and that the probability of picking the ace of clubs from a deck of 52 cards is 1/52.

If this experiment is actually carried out, e.g. tossing a coin 10,000 times, the relative frequency of getting heads or tails will be almost exactly ½: 5,000 times heads and 5,000 times tails.

And so the frequentistical notion of probability is self-evident: $p=n/M$, where n is the number of events for which the probability is being calculated and M is the total number of experiments.

Using this definition as a foundation, the concept of probability can also express someone's feeling of probability regarding an event, even if it does not involve any symmetry and repeated experiments are not possible. Statements such as 'the probability that it will not rain tomorrow is 0.8 (80%)' fall within this category. All the information acquired in the past makes such a statement possible. In that case, probability is a property not only of the system but also of the person making the judgement. This subjective concept of probability is called the Bayesian concept of probability. It is used when solving virtually all practical problems, including the concept of probability that enables us to carry out risk-based asset management.

### Probability versus frequency

These guidelines often use the term frequency as the probability of an event over a period of time. Unreliability, as defined in section 2.4, is an example of this, namely the probability of failure over a particular period of time. If the probability in such a unit of time is significant, it will also be likely that the event will occur multiple times. In such a scenario, it will be more practical to switch from 'probability of failure' to the notion 'number of failure events in a period of time'.

The relationship is simple and can be proven by making the period of time (infinitely) small: $p=1-e-\lambda$, where p is the probability that the event will occur 1 or more times and $\lambda$ is the expected number of events, both in the same period of time. Point of departure in this formula is that $\lambda$ is constant.

### Recovery time

For hardware system elements and for external events, the failure frequency is not sufficient for the purposes of calculating unplanned non-availability of the component, and thus of the system. After all, non-availability is a probability per demand which, in the case of systems in continuous operation, comprises the product of failure frequency and recovery time. Recovery times are therefore required for the purposes of an availability analysis.

The recovery time is the total time needed to get the system element up and running again. Hence it is the period of time between the point at which a fault is noticed and the point at which the repaired component is given the all-clear for use. In general, this period of time far exceeds the repair time, as order time, time to reach the scene, testing time, etc. are part of the recovery time as well.

Within the scope of the analysis it is assumed that the repaired or replaced component will have the same characteristics as the original element: as good as new. Nevertheless, it is always possible to assume a larger or smaller failure frequency following replacement or repair.

## *6.3.1 Hardware failure*

Components function in two fundamentally different ways:

- continuously, such as the energy supply through the main power grid
- in standby mode, such as an emergency power supply, e.g. the emergency diesel generator.

In the first case, failure is noticed immediately, in the second case it is not. The failure of the component on standby will only be noticed once the component is put into use: it does not start. Hence in the case of a component in standby mode there is a probability of failure for each demand. A functional test will be required in order to detect this imperceptible failure at an earlier point in time. The more often functional testing is performed, the smaller the probability of undetected failure of the component. As such, the availability of the system element is increased, assuming that the inspection itself does not result in any (planned) non-availability. The time interval for functional testing is based on economic optimization and the result of the test is adopted in the ORA.
It will be self-evident that such a testing interval will also have to feature in the maintenance plan and that the tests will actually have to be performed.

The failure behaviour of components in continuous operation is calculated by means of the failure frequency ($\lambda$) [-/time]. The time unit commonly used is hour, though very occasionally it is year. Mean time between failures (MTBF) is also used, a parameter equal to $1/\lambda$, with it being implicitly assumed that failure frequency does not increase over time.

The failure behaviour of standby components is calculated by means of the failure frequency ($\lambda$), the recovery time ($\theta$) and the testing interval ($\tau$) [time]. The failure frequency relates to the undetected failure during the standby period. The longer this standby period is, the greater the probability of the component not working by the time it is needed. Periodic testing (and repair or replacement, if need be) will reduce the probability of component failure when it is put into use.

Circumspection is required, however: as soon as a component that is normally in standby mode starts working, the probability of failure will change, and so too will the failure frequency. This is virtually always greater than it is in standby mode. Such a component will therefore have two failure frequencies: one during standby and another during operation.

## Maintenance analysis

Because different periods of use entail different causes of failure, the failure frequency of a component will not be constant during use. The failure frequency can broadly be divided into three distinct periods. Figure 6.3 shows the typical characteristic of the failure frequency in the successive periods. This characteristic is known as the 'bathtub curve'.

*Period I: Failure due to teething problems.*
If a component is new to the market and faults occur shortly after it is put into use, these are often regarded as teething problems. Usually these pertain to design, factory or installation errors. The older a component gets, the lower the probability of such faults occurring.

*Period II: Constant rate of failure.*
Following the teething problems period and prior to the component being prone to age-related deterioration, there is a period in which age is less relevant to the frequency of failure. Faults that do occur tend to do so more or less at random times and often have nothing to do with the component's condition or age.

*Period III: Failure due to age.*
After a certain amount of time the age of a component exerts greater influence over failure behaviour. During this period, the probability of faults occurring increases as the component gets older. A component's degradation then becomes the dominant cause of failure.

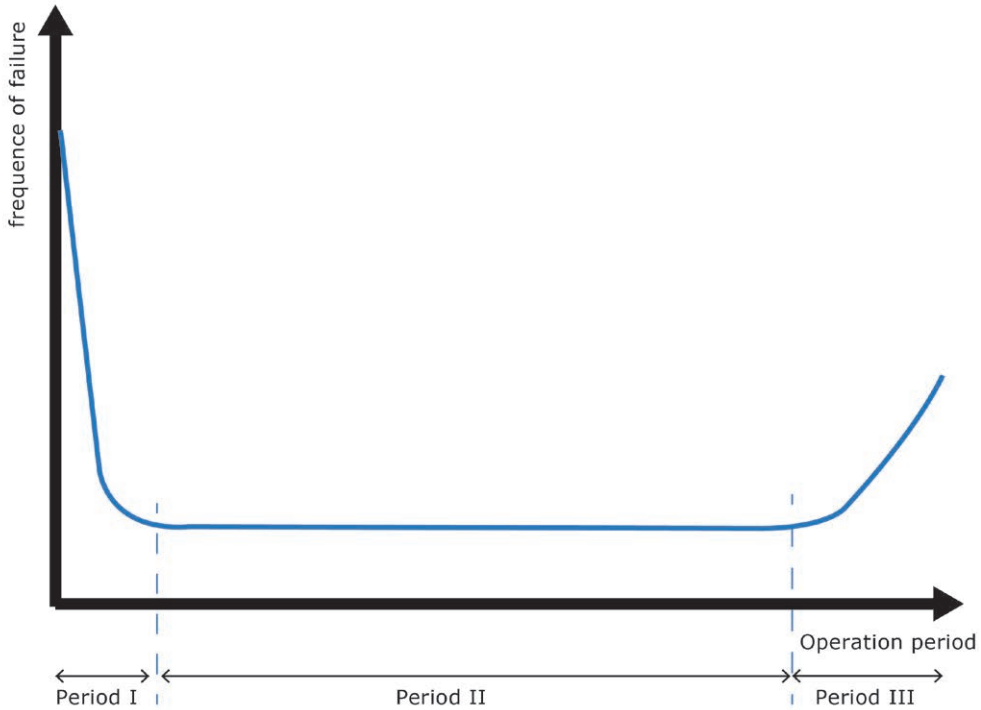



*Figure 6.3: Simplified depiction of failure frequency over time*

Whether or not components go through all periods and what the duration will be for each period depend on a variety of factors. The constant frequency of failure, which is assumed in *short-term quantitative risk analyses*, is the failure rate accompanying period II. Hence at the end of period II the component will have to be reconditioned or replaced, or the risk analysis adapted.

An effective maintenance strategy is drawn up with the aid of a detailed maintenance analysis, which also takes phases I and II into account. For a proper understanding of the use of this strategy in the successive periods of use, an explanation will first be provided of the nature and possibilities of the 'maintenance strategy'.

There are three maintenance strategies: corrective maintenance (CM), preventive maintenance (PM) and condition-based maintenance (CBM). A maintenance strategy is applied to an element (component) of the system, i.e. a system element of the objects.

Corrective maintenance (CM) entails waiting until the system element fails. At that juncture, or at the point at which it becomes evident that the system failed at an earlier juncture (in standby mode), the system element is replaced or reconditioned.
Preventive maintenance (PM) entails the component being replaced or reconditioned after a certain period of time, or after a certain period of use, or after a given number of times being put into use. Usage therefore determines replacement.
Condition-based maintenance (CBM) entails measurements revealing the component's condition and the component being replaced or reconditioned should the measured parameter — termed condition threshold — exceed a certain limit.

The choice of maintenance type will be made on the basis of cost and technical possibilities. Costs encompass the direct costs of maintenance and the anticipated failure costs to society. Technical possibilities include the measurability of condition parameters – if the condition cannot be monitored condition-based maintenance is not an option.

What this means is that **corrective maintenance** (CM) will be opted for in case of low costs of failure and/or poor predictability (a constant frequency of failure). A good example of CM is maintaining car lights. This is not done until they (the components) fail. In the case of components on standby, that failure will go undetected, as they are not in use.

**Preventive maintenance** (PM) is used for components where the point at which they will enter period III (see figure 6.3) is readily predictable based on usage, whereas the costs of failure are high. Taking the car as an example again, replacement of the cam belt in a car's engine based on mileage is a good example of PM. Predicting the deterioration in quality is perfectly possible on the basis of usage, and the costs of failure are (extremely) high, namely irreparable damage to the entire engine block. PM only entails replacement or reconditioning. This is periodic and preservative, or conservative, maintenance. The interval to be chosen is based on economic optimization.

Incidentally, the component may still fail prematurely. This probability is (occasionally) referred to as 'residual probability'. The reliability and/or availability of a component is therefore never 100%. In the case of PM, too, the replacement interval must be included in the maintenance plan and be implemented. After all, the assumption regarding the component's probability of failure is based on this interval.

**Condition-based maintenance** (CBM) is possible if there is something to measure that renders the start of period III (see figure 6.3) (more) predictable and if the process of measuring this will be relatively inexpensive. Taking the car as an example, tyre wear is a good example of CBM. Tread depth can be measured accurately and inexpensively, and the threshold limit (number

of millimetres of tread) is prescribed. In the case of the PM example above (replacing the cam belt), the quality of the belt can also be measured, but the measuring process is extremely expensive, meaning that in this case PM will be cheaper than CBM.

While with CBM inspection is primary, the inspection does not give a full guarantee of flawless functioning. Apart from the impossibility of guaranteeing 100% availability, the chance of detection and the accuracy of the measurement also play a role. The inspection interval and the limit at which the component will be declared unfit are based on economic optimization and are used in the ORA. As such, these parameters also constitute the points of departure included in the maintenance plan.

### Optimization

Economic optimization at component level proves to be the basis of the parameters to be used: testing intervals, replacement intervals and inspection intervals. This optimization will also provide the accompanying failure frequency of the component.

There are various tools for economic optimization, e.g. Rijkswaterstaat's LVO model [12] or Isograph's RCM-Cost [13]. These tools enable comparisons on the basis of minimum life cycle costs (LCC). They result in the most inexpensive strategy, including the accompanying parameters and, therefore, the failure frequency. It is also possible when using RCM-Cost to assume a given performance requirement for the system. For example, a failure frequency is required that is smaller than the cheapest strategy at system level indicates. If this requirement is satisfied by means of suboptimization at element level, then by extension the model will produce a smaller inspection interval or replacement interval.

The tools needed to ascertain the optimum maintenance strategy use an approximation of the failure rate as a function of time, as shown in figure 6.3.

Two situations are important in this regard: components that have a constant failure rate and components prone to ageing. For the first group, the failure rate ($\lambda$) has to be estimated. For the second group, an estimate of the lifespan (MTBF) and an estimate of the distribution around this are required. A distribution of probability will be compiled on the basis of this, usually a Weibull distribution, but occasionally a normal distribution as well. Usually, the first arm of the bathtub curve, the 'teething problems', is not modelled.

### Calculating failure frequency

There are three ways in which the failure frequency ($\lambda$), or the probability of failure on demand (Q), can be calculated for a hardware component's failure mechanism:

1. statistics
2. expert opinion
3. calculation.

*1. Statistics*
The failure context of hardware, i.e. physical elements such as a pump or an electromotor, is recorded and converted into probabilities of failure.
Generic databases are used to record failure frequencies and the probability of failure on demand. An especially large amount of failure data has been amassed in the offshore industry and the nuclear power-related sectors, meaning that reliable data on many hardware components is available. A supplier can provide data on the frequency of failure or probability of failure, as well as on recovery time, testing intervals, replacement intervals and inspection intervals.

Rijkswaterstaat manages a database containing conservative (high) failure figures [14]. These high failure figures may be used straightforwardly for Rijkswaterstaat's systems. If a contractor uses components that are more reliable and the contractor therefore wishes to incorporate lower failure figures into their analysis, they will have to substantiate this 'better' reliability. Incidentally, the data in the Rijkswaterstaat database is based on generic databases. It is conceivable that Rijkswaterstaat will adapt failure figures in due course based on its own experience.

It is always prudent to check whether the component in question is sufficiently similar to the component in the generic database from which the data is being derived and whether it is to be used in the same way as this component. Even the choice of the aforementioned maintenance strategies will play a role. If PM is being used, the probability of failure will depend on the replacement interval. In practice, the supplier's instructions are usually followed; however, clustering maintenance or other specific influences may allow replacement or renovation a little further down the line. However, in this case it will be necessary to consider and document that the component's probability of failure will increase. Something similar occurs when stretching out the inspection intervals in CBM. The LVO model and RCM-Cost tools will support calculation of the probability of failure.

*2. Expert opinion*
If there are no statistics to hand, for example because an entirely new component is being used or the generic data available does not apply to the situation concerned, expert opinion will be sought. Experience with similar components in similar situations will enable an expert to make a judgement on the probability or frequency of failure. When the opinions of multiple experts are combined, assessment of the experts (calibration) may have as a result that the opinion of a good expert is given greater weighting than the opinion of one that is not so good. This is discussed extensively [15].

*3. Calculation*
Finally, it is sometimes possible to calculate a component's probability of failure proceeding from a model of the component's functioning and random input from the data in that model. This structural analysis is primarily used for components that collapse due to degradation or (excessive) loads. In the Netherlands, this form of probabilistic method is termed 'Probabilistic Design'.

## Example: the drawbridge

The drawbridge has the following hardware components:

- bridge deck
- operating mechanism (electromotor)
- computer (PLC)
- sensors (2).

The first three hardware components play a crucial role in the primary function 'allowing vessels to pass through' (LPS). The sensors determine whether or not road traffic can pass over the bridge, and have no effect on not being able to open the bridge. They play a role in 'allowing road traffic to pass through' (LPW). See also figure 5.4.

The bridge deck is a component with a very small probability of failure that gradually increases over time, on the proviso that it is well maintained. CBM is the appropriate maintenance strategy for this component, with a detectable crack being the condition threshold. Without crack detection, the probability of the bridge deck failing can be derived from the instructions in the Eurocode, which were used during the design process. The Eurocode, designated by the *Housing Act* and the *Buildings Decree*, requires that structural components have a probability of failure not exceeding $8.5 \times 10^{-6}$ for each planned lifespan. In the case of the drawbridge the lifespan is 100 years. If the Eurocode's design and construction procedures are followed, it may be assumed that this requirement is being satisfied. This means a failure rate of approx. $1.10^{-11}$ per hour. The recovery time of a collapsed bridge deck is protracted at six months. A conservative assumption is 1 year.

The electromotor fails within the planned lifespan. The failure rate is constant and can be found in existing databases. The maintenance strategy is PM. Parts are replaced or reconditioned at set times, according to the manufacturer's specifications. In this example, the Rijkswaterstaat Failure Database contractors' version has been used [14] to calculate the failure rate of the electromotor. This database establishes that the motor on standby has a failure rate of: $\lambda = 1.1 \cdot 10^{-4}$ per hour. In operation the failure rate is also $\lambda = 1.1 \cdot 10^{-4}$ per hour. Evidently, in this situation no significant difference in failure rates has been found between the operational and non-operational stages. Recovery time of the motor is assumed to be 12 hours (including waiting, repair, testing and call-out time), which in turn is stipulated in contracts with maintenance firms.

The computer's maintenance strategy - which, for the sake of simplicity, is presumed to be a single PLC - is CM. No special maintenance actions are anticipated and the PLC will be replaced if it fails. According to [14], the failure rate is $\lambda = 2.08 \cdot 10^{-5}$ per hour. The failure is immediately noticeable and repair takes less than 8 hours.

Even the sensors are maintained by means of CM. The failure rate is $\lambda = 1.13 \cdot 10^{-5}$ per hour, once again derived from [14]. It is assumed that a sensor failure will go unnoticed, but will be observed immediately as the bridge deck is being lowered again. The recovery time is estimated at 24 hours.

A summary of the results is presented in figure 6.4.

| | Element/structural part | Consequence for *allowing vessels to pass through?* Yes/no | -evident -not evident -failure per demand -failure whilst in operation - falen tijdens | Frequency of failure λ [-/uur] | Probability of failure per demand Q [-] | Substantiation λ, Q [source/reference] | Repair times θ [hours] | Testing interval [uur] | Selected maintenance strategy | Common Cause Failure (CCF) Group | Common Cause Failure (CCF) Model | Common Cause Failure (CCF) Parameters | Remarks |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Main supporting structure** | | | | | | | | | | | | | |
| 1461 | Bridge deck | Yes | Evident, failure whilst in operation | 1,00E-11 | - | Eurocode | 8760 | NA | FDM | NA | NA | NA | |
| **Drive unit and operating mechanism** | | | | | | | | | | | | | |
| 1182 | Electro motor | Yes | Not evident | 1,10E-04 | - | Rijkswaterstaat Failure Database Contractors' Version | 12 | NA | FDM | NA | NA | NA | |
| | | Yes | Evident, failure whilst in operation | 1,10E-04 | - | Rijkswaterstaat Failure Database Contractors' Version | 12 | NA | FDM | NA | NA | NA | |
| **Operating and control equipment** | | Yes | | | | | | | | | | | |
| 1431 | PLC | Yes | Not evident | 2,08E-05 | - | Rijkswaterstaat Failure Database Contractors' Version | 8 | NA | FDM | NA | NA | NA | |
| **Measuring equipment** | | | | | | | | | | | | | |
| 1490 | Sensor no. 1 | No | Not evident | 1,13E-05 | - | Rijkswaterstaat Failure Database Contractors' Version | 0 | NA | FDM | Group 1 | Beta | 0,1 | Joint failure, recovery time 24 hours |
| 1490 | Sensor no. 2 | No | Not evident | 1,13E-05 | - | Rijkswaterstaat Failure Database Contractors' Version | 0 | NA | FDM | Group 1 | Beta | 0,1 | Joint failure, recovery time 24 hours |

*Figure 6.4. Data for the quantitative analysis*

## Bayesian updates

If data is, or could become, readily available for a specific component itself, it will be worthwhile to also include this in the risk analysis. Updating old data with new data could yield a new, improved estimate of the failure figures. One important method of updating is the Bayesian method. See [16] for a comprehensive discussion of this approach.

## Common Cause Failure (CCF) and redundancy

*Common Cause Failur*e (CCF) is the occurrence of two or more events that are not independent of one another. In such cases, the product rule for independent events does not hold true:

$$\Pr\{A \cap B\} \neq \Pr\{A\} \cdot \Pr\{B\}$$

where Pr {A} is the probability of event A and Pr{A ∩ B} is the probability of events A and B. Dependency renders the probability of A and B larger than the product.

The phenomenon of common cause failure plays an essential role in redundancy. Redundant design means the use of multiple system components to ensure that the system continues to function properly if one or more components fail. This is a good way of enhancing the reliability of the system, provided that the factor dependency is taken into consideration. Simply multiplying yields an overly favourable result. If the factor dependency plays a role, actual reliability will be lower. Furthermore, dependency almost always plays a role when installing more than one of the same component. In a failure probability analysis, it is therefore crucial to identify and analyse possible dependencies and to incorporate them into the analysis in a quantitatively accurate manner.

There are different sources of dependency:

1. **A shared component**, such as a power supply.

2. **Physical interaction**, e.g. in the event of failure as a result of high temperature. If the relevant components are both located in the same room, they will both fail if the room temperature gets too high.

3. **A shared production line.** Errors in the design or during manufacturing and assembly that were not previously detected will occur in all components from this production line. If one component fails as a result, it will become highly likely that the adjoining manufactured component will fail as well.

4. **Shared maintenance.** If maintenance is carried out by a single company, errors during maintenance work, e.g. due to lack of knowledge on the part of the maintenance engineer, or in the maintenance instructions, or the use of incorrect maintenance materials, will have the same effect on all similar components. The first source can be modelled using the fault tree method. Failure of the shared component will mean failure of the system. In the case of the other sources this is trickier, as the exact cause cannot be specified and quantified explicitly. What this means in practice is that CCF is calculated on the basis of statistics and expert opinion.

Rijkswaterstaat uses two models to calculate CCF. The best-known is the β factor model. This model assumes that there is only one cause of failure for all dependent components, as a result of which all components fail immediately if this cause of failure manifests itself.

The model therefore does not describe the joint failure of a subset of the dependent components. A single component fails or all components fail.

Hence part of a component's probability of failure is determined by a symptom common to all components. Essentially this is no different than explicitly modelling a separate 'virtual' component, which is a common element of all components in the group. This virtual component can be modelled as a separate, explicit contribution in a fault tree. The 'fault tree' (see figure 6.5) and the 'fault tree analysis' are more fully described in section 6.5.

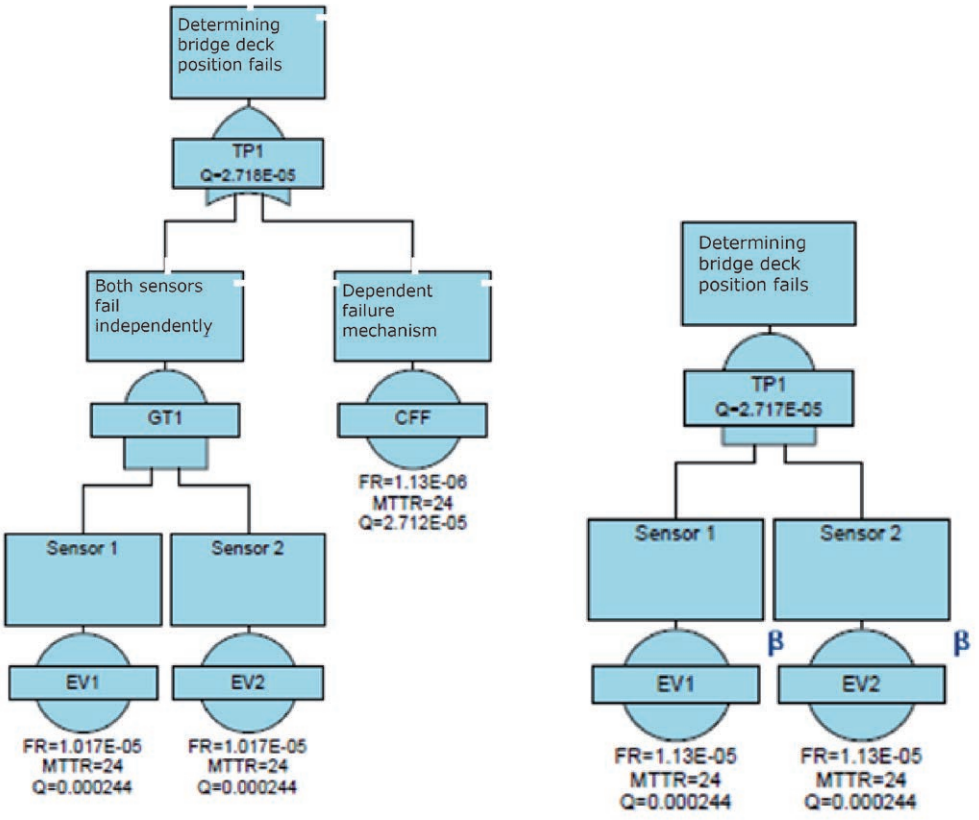



*Figure 6.5. Explicit (left) and implicit (right) modelling of CCF (read more in section 6.5)*

The 'dependent' part of the probability of failure, or the failure frequency in the case of continuously functioning components, is the fraction β. This virtual component's failure frequency is:

$\lambda_{c,d}=\beta\cdot\lambda_c$

where:

$\beta$ = the fraction of dependent failure,
$\lambda_c$ = the failure rate of a component, usually available in databases, and
$\lambda_{c,d}$ = the dependent portion of a component's failure rate.

In many cases the value β=0.1 is chosen for the CCF fraction. This means that 10% of the component's frequency of failure is a failure mode in which all components fail.

The second model used by Rijkswaterstaat is the *Binomial Failure Rate* model (BFR). This model assumes that each component has an independent probability p of failing as a result of an event occurring with a frequency of μ. When such an event occurs it is expected that the entire group of components will fail, although it is highly likely that they will not all fail. This event is called a *non-lethal shock*. Moreover, a second event is assumed, occurring with a frequency of ω and entailing all components failing simultaneously. This event is called a *lethal shock*.

Generic values often used for the parameters $p$, $\mu$ en $\omega$ are:

$p$ = 1/3
$\mu$ = $0{,}4\cdot\lambda_c$
$\omega$ = $0{,}005\cdot\lambda_c$

The simple $\beta$ factor model regards a CCF group as a single entity: all components are guaranteed to fail as soon as the common cause event occurs. In cases involving dependency on the part of more than two components, this model leads to a pessimistic assessment of the probability of failure. The BFR model provides a more likely picture of the probability and is capable of calculating the probability of failure of individual components rather than all components. This is why the $\beta$ factor model is used for one or at most two components that are the same, and why the BFR model is used if more than two components are deemed to be dependent.

An example of use of the $\beta$ factor model is the hydraulic operating mechanism in the lock at Heumen. The redundancy here is fully single, with the dependency of both systems having been modelled with the aid of the $\beta$ factor model. In this regard, $\beta$=0.1 has been maintained.

One example of using the BFR model pertains to the valves and pumps in the Maeslantkering (storm surge barrier). There, it is extremely important that only a few of the total number of components can fail. While this slows the barrier's functioning, it does not necessarily result in the failure of the barrier as a whole. The aforementioned values for the parameters $p$, $\mu$ and $\omega$ were used in the analysis for the Maeslantkering.

## Example: the drawbridge

The sensors that determine that the bridge deck is in the correct position are backups for one another; they are redundant. In such a case, possible common cause failure must be considered. In the present example both sensors are the same, are from the same manufacturer, probably from the same production batch, and are being maintained simultaneously by a single company. This creates dependency.

In the example, a sensor's probability of failure is: $\lambda_c$=1.13·10-5 per hour. If it is assumed that the dependent part is 10% of the total probability of failure ($\beta$=0.1), we get:

$\lambda_{c,d}=\beta\cdot\lambda_c=1{,}13\cdot10^{-6}$ per hour
$\lambda_{c,i}=(1-\beta)\cdot\lambda_c=1{,}017\cdot10^{-5}$ per hour.

24 hours was assumed as the recovery time. Non-availability of the sensor due to the dependent part then is:

$Q_d=\lambda_{c,d}\cdot\theta=2{,}712\cdot10^{-5}$ per demand

and for the independent part:

$Q_i=\lambda_{c,i}\cdot\theta=2{,}441\cdot10^{-4}$ per demand.

The probability of the system failing can now be calculated by means of the formula:

$Q_{system}=Q_d+Q_i\cdot Q_i=2{,}718\cdot10^{-5}$ per demand.

This is the probability of both sensors proving to be defective when the operator lowers the bridge again. At that juncture the bridge would become non-available, a state that would persist until the sensors have been reconditioned or replaced. The example above has also been calculated with the aid of FaultTree+ and the result is presented in figure 6.5.

### *6.3.2 Software failure*

The probability of failure of software is estimated using the TOPAAS method. The acronym TOPAAS stands for Task-oriented probability of abnormalities analysis for software. The method is carried out by independent experts who determine the scores based on information provided by the supplier. This method looks at the development process, the product, the degree of traceability and verification, the extent of product testing, and the environment in which the product operates. The method broadly consists of specifying the various software modules and calculating their probability of failure. For a more detailed account, please see [17].

## Example: the drawbridge

The drawbridge's components communicate with each other via an operating system consisting of hardware and software. The hardware (PLC) has already been discussed. For the purposes of this example it is assumed that the operating system comprises a single module. Table 6.1 provides a realistic depiction of the communication process. The second column contains the questions, the third gives the answers provided, and the fourth column shows the allocated rating for the answers provided. An answer rated red will increase the probability of failure, answers rated green will lower the probability of failure and answers rated white paint a neutral picture of the software's quality.

| | | | |
|---|---|---|---|
| **DEVELOPMENT PROCESS** | | | |
| 1 | The development process satisfies one of the SIL levels in IEC 61508 | Unknown | 0 |
| 2 | Use of inspections | Inspections performed in terms of designs and code | 0 |
| 3 | Number of changes compared to original design/package of requirements | Extremely frequent or a few fundamental changes | 2/3 |
| 4 | Culture and cooperation | Autodidactic organization | -1/2 |
| 5 | Developers' experience and level of education/training | Excellent knowledge of and ample experience with system development for the specific domain (unconsciously competent) | -1/2 |
| 6 | Cooperation with client | Client with sufficient knowledge closely involved, with open dialogue and a systems engineering approach | -1/2 |
| **PRODUCT** | | | |
| **7** | Complexity of decision logic | Decision logic and fault detection are exceedingly simple, MacCabe Index smaller than 10 | -1/2 |
| **8** | Scale of software module (Lines of code) | Less than 1,000 | -1/2 |
| **9** | Clarity of architectural concepts used | There is a clearly defined separation of roles and responsibilities for components, respecting the principle of 'maximum cohesion and minimum coupling', and this is being actively monitored during the development process | -1/2 |
| **10** | Use of a certified compiler | Use of a compiler with which the team have extensive experience | 0 |
| **REQUIREMENTS TRACEABILITY/VERIFIABILITY** | | | |
| **11** | Traceability of requirements throughout the process | Traceable to architecture and testing | -1/3 |

| | | | |
|---|---|---|---|
| **TESTING** | | | |
| **12** | Testing technologies and coverage | Tests have been documented, no formal testing technologies are being used; coverage unknown | -1/3 |
| **EXECUTION ENVIRONMENT/USAGE** | | | |
| **13** | Multiprocess environment | Dedicated CPU and memory on no, trivial or Proven OS | -1/3 |
| **14** | Availability of representative field data whilst in operation | Limited data available from own period in operation | 0 |
| **15** | Monitoring | Long-term monitoring, but infrequent use in operation | -1/3 |
| | | SUMMATION | **-3 2/3** |

*Table 6.1. Results of a TOPAAS analysis*

The probability of failure for the software is 10 to the power of the summation of the answers. The present case provides:

$Q_s = 1 \cdot 10^{-3,667} = 2,15 \cdot 10^{-4}$ per demand

The software initially has a significant share in the probability of failure. In the case of the operating system of a drawbridge, the input from the software will stabilize after a few months. The software virtually always follows the same process. Any faults within that process have been remedied, reducing the probability of failure. TOPAAS is (therefore) particularly good at predicting the probability of failure of little used software, such as security software.

Generally speaking, repair work to the software will take a fairly long time. The improvement protocol will have to be run through meticulously and all tests will have to be repeated. It is assumed that it will be possible to operate the bridge again after 24 hours, albeit in special circumstances.

### *6.3.3 Failure due to human actions*

The so-called OPSCHEP model has been developed to calculate failure probabilities resulting from human actions. 'OPSCHEP' stands for 'Ontwikkeling keringen Europoort  Project software for the calculation of human error probabilities'. The title refers to the Europort Barrier (Europoortkering) as it was the project for which the model was first developed. The OPSCHEP model is geared towards the quantification of human errors, or the contribution made by people to the non-availability of a system or sub-system.

The OPSCHEP model is managed by Rijkswaterstaat. A more detailed account can be found in [18].

## Example: the drawbridge

The drawbridge is operated by an operator, meaning there is potential for human error. Such an error could jeopardize safety as well as the availability of one or both of the primary functions. A 'process FMEA', also known as a HAZOP (*Hazard and Operability Analysis*), is imperative to formally investigate the errors that could be made by the operator and their consequences. This simple example will be limited to exploring one error: accidentally pressing the emergency stop. The consequences will be that both of the bridge's primary functions are jammed and that the operator will have to wait for an authorized engineer to arrive to release the emergency lock. The recovery time is estimated somewhat pessimistically at 4 hours.

The probability of an operator accidentally pressing the emergency stop is calculated by the OPSCHEP model that Rijkswaterstaat developed specifically for its objects. In the present example, the error made is an 'execution error', termed P3 in the OPSCHEP model. Various factors influence this error - see figure 6.6.

**Factor P3 (wrong choice)**

| Aspect | Assessment | Factor |
|---|---|---|
| Use/no use of work instructions | Work instructions are not important for the task | 1,00E+00 |
| Proximity/no proximity of components | Other component in immediate vicinity but is not similar | 2,00E+00 |
| Component labelling | Proper labelling | 1,00E+00 |
| Option of setting or adjusting a component in multiple positions | Only one position possible | 1,00E+00 |
| Complexity | (Exceedingly) easy task | 3,33E-01 |
| Working/not working in an uncomfortable working position | Normal working position | 1,00E+00 |
| Time pressure | No time pressure | 1,00E+00 |
| Extent of knowledge and skills | Sufficient knowledge and experience | 1,00E+00 |
| Having to/not having to repeat actions | Having to repeat actions, thereby reducing focus | 3,00E+00 |
| Interdependence of human actions | No dependence | 1,00E+00 |
| Motivation: circumstances when operating bridge | | |

| | |
|---|---|
| Basic value | 3,00E-04 |
| Correction factor | 2,00E+00 |
| Result P3 | **6,00E-04** |

*Figure 6.6. Quantification of an incorrect choice by the OPSCHEP model*

The result, i.e. the probability of the operator pressing the emergency stop, is therefore $Q_m = 6 \cdot 10^{-4}$ per demand. The bridge opens 4 times a day, roughly 1,500 times a year. What this means is that according to the model the emergency stop is pressed accidentally nearly once a year on average. Clearly this is too often, as in practice the emergency stop gets pressed accidentally no more than once in the bridge's lifespan. Based on the proven practical situation, the calculated probability must be reduced by a factor 100: $Q_m = 6 \cdot 10^{-6}$ per demand. The OPSCHEP model is overly pessimistic here, explicitly inviting us to check our answers.

### *6.3.4 Failure due to external events*

A separate analysis is required to acquire an overview of external events that constitute a threat to, or have a direct impact on, an object's performance. An external event is defined as an undesired event that occurs beyond the compass of the normal functioning of the system under consideration, but which could still result in failure of the system. Examples of external events include fire, lightning strike, collision and flooding.

Using an exhaustive list of potentially threatening external events, a screening process is carried out to determine which specific events constitute a threat to the object's functioning. [19] Submethods are available for analysis of the impact of various external events, such as for the risk of lightning [20], fire [21] and collision [22].

## Example: the drawbridge

The *external events screening process* was developed to ascertain which external events have to be analysed in more detail. This screening assesses whether external events that are potentially threatening to the drawbridge genuinely constitute a threat. The screening tool contains a fixed set of external, potentially threatening events.

For the drawbridge in the example, the screening process reveals that the following events will need to be analysed in more detail:

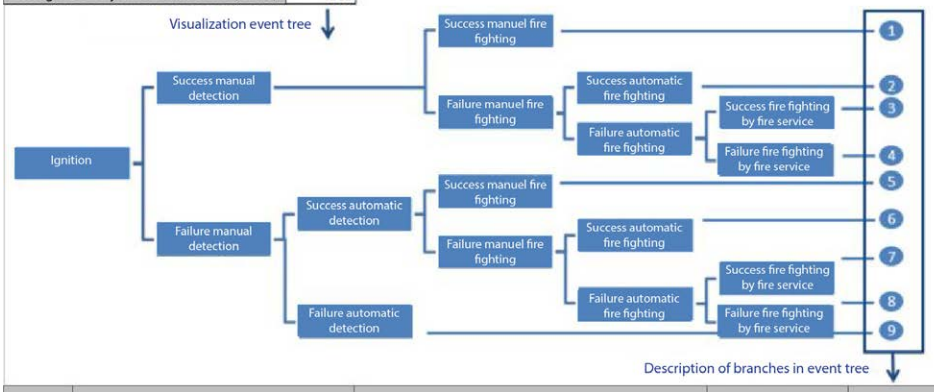
- lightning strike
- fire
- collision with pillars, bridge deck and roadway
- collision with barriers
- incident involving poisonous gases or chemicals as a result of a transport accident
- power cut.

The fire analysis has been worked out in more detail for this bridge. Rijkswaterstaat has developed the 'fire risk model' for the external event fire. The input required for this model includes the spaces and partition walls in the object and the flammable contents of the spaces. Standard probabilities of ignition are used to calculate the probability of fire in each space. The possibility of the fire spreading is determined by the detection and fire extinguishing systems as well as by the fire resistance of the partition walls. For each space in which there is a source of ignition, the model calculates the frequency of ignition and, on the basis of the recovery times specified by the user, provides the non-availability.

Figure 6.7 gives the results for the bridge's control room. The non-availability caused by fire is expected to be $Q_b=2.24\cdot10^{-4}$. Due to the fact that the machine room also contributes (not shown here), $Q_b=2.29\cdot10^{-4}$ will be used during the remainder of this example.

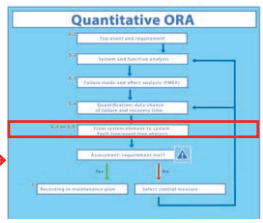
Results

| | |
|---|---|
| Average non-availability as a result of fire in bridge control room | 2,24E-04 |
| Frequency of ignition (-/hours) | 3,37E-07 |
| Average recovery time in case of fire (hours) | 663 |




| Branch # | Description of situation | Description of consequence | Probability (%) of branch, given ignition | Recovery time (hours) |
|---|---|---|---|---|
| 1 | Successful manual detection and manual fire fighting | Fire restricted to component | 1,9% | 41 |
| 2 | Successful manual detection and successful automatic fire fighting | Fire restricted to component. Any additional damage by extinguishing system | 0,0% | 41 |
| 3 | Successful manual detection and successful professional fire fighting | Fire limited to room, or to building, depending on fire service strategy | 13,1% | 730 |
| 4 | Successful manual detection but all attempts at extinguishing fail | Fire not actively managed | 1,5% | 730 |
| 5 | Successful automatic detection and successful manual fire fighting | Fire restricted to component | 7,8% | 41 |
| 6 | Successful automatic detection and fire fighting | Fire restricted to component. Any additional damage by extinguishing system | 0,0% | 41 |
| 7 | Successful automatic detection and successful professional fire fighting | Fire restricted to room, or to building, depending on fire service strategy | 53,1% | 730 |
| 8 | Successful automatic detection but all attempts at extinguishing fail. | Fire not actively managed | 5,9% | 730 |
| 9 | All detection options fail, i.e. no attempts at extinguishing | Fire not actively managed | 16,7% | 730 |

*Figure 6.7. Results of fire analysis*




## 6.4 Process step: from system element to system

The previous sections described the factors that determine the reliability and availability at the level of a system's elements.

This description at system element level still does not produce a picture of the performance of the system as a whole. Sometimes it will suffice, but often a picture of the expected reliability and availability of the overall system is required, e.g. to satisfy statutory requirements or fulfil agreements made with the Ministry of Infrastructure and Water Management (see chapter 2). Hence another step is required from the R and A characteristics of the elements to the reliability and/or availability of the system as a whole.

However, an important interim step is first required, namely the combination of optimum maintenance scenarios to form work packages. In this regard, the work is planned in such a way that the costs of performing tests and measurements are optimized. This usually has as a result that inspection and test intervals deviate somewhat from the optimum situation at component level and that probability and failure frequency increase. The changes will have to be calculated in the R and A characteristics of the system elements. Nonetheless, combining the work is virtually always more cost efficient.

Addition is the simplest way of combining the R and A characteristics of the system elements to produce the system's reliability and availability aspects.

If the frequencies of failure of the system elements that could cause the object to fail are added up, this will provide a conservative result for failure frequency λ of the system, or the system's reliability. Expressed as a formula:

$$\lambda_{system} \approx \Sigma \lambda_{systemelement}$$

The same goes for availability U: the sum of the products of the failure frequency and recovery time of the system elements is a conservative estimate of the system's non-availability:

$$U_{system} = \Sigma \lambda_{systemelement} \cdot \theta_{systemelement}$$

in which θ is the recovery time, i.e. the time between detecting the fault and the system element being restored to normal functioning.

The approximation is conservative because redundancy and dependency are disregarded and the calculation itself is conservative. After all, addition is not the exact way of calculating a system's probability of failure:

$$p_{system} = p_A + p_B - p_A \cdot p_B$$

During addition, the term $p_A \cdot p^B$ is disregarded.

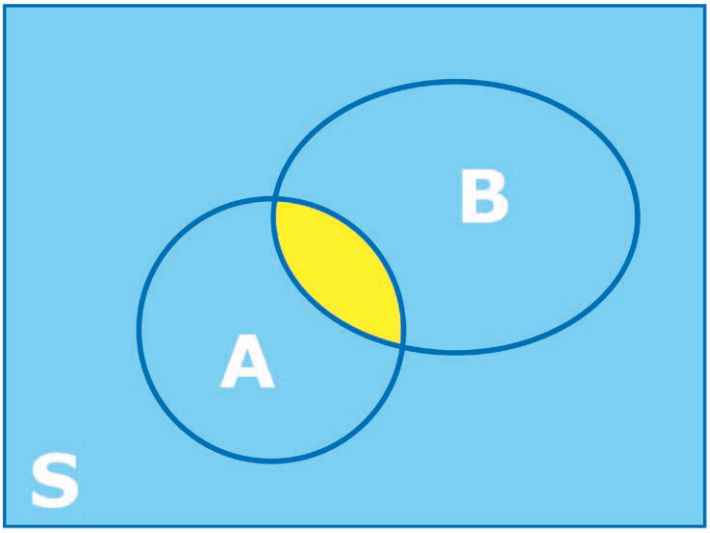



*Figure 6.8 Venn diagram of probability of system failure, in which A is an event from S (system) with characteristic A, and B is an event from S with characteristic B, within the aggregate of possible events. The yellow section is counted double and therefore has to be deducted from the probability of failure.*

These conservative results are eliminated with the aid of a fault tree analysis (FTA) (see section 6.5).

## Example: the drawbridge

All of the drawbridge's system elements were quantified above. In summary:

- bridge deck
- electromotor
- computer (hardware)
- sensors (2)
- operator
- operating system (software)
- fire

Paragraph 6.3.1 established that the bridge deck has a probability of failure of approx. $1.10^{-11}$ per hour and a recovery time of one year (8,760 hours). Although in practice vessels could get moving again fairly swiftly (the collapsed bridge deck will be removed and a temporarily solution will be constructed), this example assumes that failure of both the 'allowing road traffic to pass through' (LPW) and 'allowing vessels to pass through' (LPS) functions will last for a full year.

In this simple example, the operating mechanism is the electromotor, which can fail in standby and operational mode with the same failure frequency of $1.1.10^{-4}$ per hour. Failure whilst in operation means failure of both the LPW and LPS functions. Failure in standby only means failure of the LPS function; after all, the bridge can no longer be opened. Due to the fact that the operational time is short compared to the standby time, failure whilst in operation is being disregarded for the purposes of this simple example.

The PLC has a frequency of failure of $2.08.10^{-5}$ per hour and the recovery time is 8 hours. Failure of the PLC means failure of the LPS function.

Both sensors have a failure frequency of $1.13.10^{-5}$ per hour and a recovery time of 24 hours. If both sensors fail, it cannot be ascertained whether or not the bridge has closed properly, which means failure of the function 'allowing road traffic to pass through' (LPW).

The software fails with a probability of $2.15.10^{-4}$ per demand (see section 6.3.2). If the bridge is opened four times a day, this means:

$\lambda = 4 \cdot 2.15 \cdot 10^{-4}$ in 24 hours $= (4 \cdot 2{,}15 \cdot 10^{-4})/24 = 3.58 \cdot 10^{-5}$ per hour
As noted earlier, this is a conservative value if the bridge has been in use for some time (and any faults in the programmed routine have already been remedied). Repairing the software takes 24 hours and failure will only entail consequences for the LPS function.

An operational error will also be modelled by way of a probability per demand. It has been deduced in paragraph 6.3.3 that this will be roughly $6.10^{-6}$ per demand. 4 Hours was assumed for the recovery time. The fault will have consequences for both LPW and LPS.

Finally, the effect of fire was calculated (section 6.3.4). The result was already expressed in terms of non-availability straight away: $2.29.10^{-4}$.

Table 6.2 (on the next page) summarizes this overview once more.

| CAUSE OF FAILURE | PROBABILITY PER DEMAND | NUMBER OF DEMANDS PER HOUR | FRACTION OF THE TIME | FREQUENCY PER HOUR | RECOVERY TIME (HOURS) | NON AVAILABILITY LPS | NON AVAILABILITY LPW | LPW WITH REDUNDANCY |
|---|---|---|---|---|---|---|---|---|
| ROADWAY COLLAPSES | | | | 1,00E-11 | 8760 | 8,760E-08 | 8,76E-08 | 8,76E-08 |
| ELECTROMOTOR WILL NOT START | | | 9,58E-01 | 1,10E-04 | 12 | 1,265E-03 | | |
| ELECTROMOTOR STOPS PREMATURELY | | | 4,17E-02 | 1,10E-04 | 12 | 5,500E-05 | 5,500E-05 | 5,500E-05 |
| PLC FAILS | | | | 2,08E-05 | 8 | 1,664E-04 | | |
| SENSOR 1 FAILS | | | | 1,13E-05 | 24 | | 2,71E-04 | 2,72E-05 |
| SENSOR 2 FAILS | | | | 1,13E-05 | 24 | | 2,71E-04 | |
| SOFTWARE FAILS | 2,15E-04 | 0,167 | | 3,58E-05 | 24 | 8,600E-04 | | |
| OPERATING ERROR | 6,00E-06 | 0,167 | | 1,00E-06 | 4 | 4,000E-06 | 4,00E-06 | 4,00E-06 |
| FIRE | | | | | | 2,290E-04 | 2,29E-04 | 2,29E-04 |
| | | | | | | | | |
| | | | | | **TOTAL** | 0,00258 | 0,00083 | 0,00032 |
| | | | | | **PERCENTAGE** | 0,26% | 0,08% | 0,03% |
| | | | | | **HOURS PER ANNUM** | 22,6 | 7,3 | 2,8 |

*Table 6.2. Simple addition of non-availability of movable bridge component*

This produces a non-availability of 0.26%, or 22.6 hours a year, for the function 'allowing vessels to pass through' (LPS). This means the requirement, as formulated in section 6.2, of 1%, or 90 hours a year, is easily achieved, and that a more accurate analysis is unnecessary.

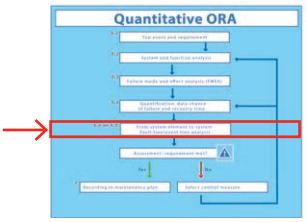
Non-availability for road traffic is 0.08%, corresponding to an average of 7.3 hours a year. However, the probability of failure of both sensors has been added here, whereas in reality they would be each other's backup, as a result of which 'redundancy (and any common cause failure)' must be taken into consideration. The correct method of modelling is done using an FTA.

For the purposes of comparison, the result of this analysis for the object 'drawbridge' has been calculated with the aid of the program RCM-Cost from Isograph [13]. This program uses simulation to calculate reliability and availability (section 6.5). The number of simulations is a measure of the reliability of the result. Table 6.3 (on the next page) compares the results above with the results from RCM-Cost for 10,000 and 10,000,000 simulations.

| CAUSE OF FAILURE | NON-AVAILABILITY LPS | NON-AVAILABILITY LPW | RCM-COST LPS | RCM-COST LPW | RCM-COST LPS | RCM-COST LPW |
|---|---|---|---|---|---|---|
| NUMBER OF SIMULATIONS | Analytical | | 10.000 | | 10.000.000 | |
| BRIDGE DECK COLLAPSES | 8,760E-08 | 8,76E-08 | 0 | 0 | 3,78E-08 | 3,78E-08 |
| ELECTROMOTOR WILL NOT START | 1,265E-03 | | 1,28E-03 | | 1,26E-03 | |
| ELECTROMOTOR STOPS PREMATURELY | 5,500E-05 | 5,500E-05 | 5,25E-05 | 5,25E-05 | 5,49E-05 | 5,49E-05 |
| PLC FAILS | 1,664E-04 | | 1,66E-04 | | 1,67E-04 | |
| SENSOR 1 FAILS | | 2,71E-04 | | 2,72E-04 | | 2,71E-04 |
| SENSOR 2 FAILS | | 2,71E-04 | | 2,72E-04 | | 2,71E-04 |
| SOFTWARE FAILS | 8,600E-04 | | 8,52E-04 | | 8,55E-04 | |
| OPERATING ERROR | 4,000E-06 | 4,00E-06 | 4,43E-06 | 4,43E-06 | 4,00E-06 | 4,00E-06 |
| FIRE | 2,290E-04 | 2,29E-04 | 2,46E-04 | 2,46E-04 | 2,26E-04 | 2,26E-04 |
| | | | | | | |
| **TOTAL** | 0,00258 | 0,00083 | 0,00260 | 0,00085 | 0,00257 | 0,00083 |
| **PERCENTAGE** | 0,26% | 0,08% | 0,26% | 0,08% | 0,26% | 0,08% |
| **HOURS PER ANNUM** | 22,60 | 7,28 | 22,75 | 7,42 | 22,50 | 7,24 |

*Table 6.3. Comparison of non-availability of the movable bridge system*

Note that the 10,000 simulations approximate to the values based on the analytical calculation.




## 6.5 Process step: fault tree analysis

A *fault tree analysis* (FTA) is an analysis calculating a system's probability of failure (the probability of the top event) by combining the probabilities of failure of the individual system elements in a model. The difference with the method 'addition', which was described in the previous section, is that the FTA correctly uses probability calculation and correctly regards redundancy and dependency. This produces a less conservative result than addition of the system elements' data alone. The FTA also provides better insight into a system's weak spots than is possible with the 'addition' method.

An FTA is characterized by the 'fault tree', a graphic representation showing the correspondence between the failure of the different system elements which could result in the top event.

A fault tree consists of a single 'top' event located above various basic events. Basic events describe the failure of system elements. This could be the failure of a physical system element, but it could also be that of a software module, a fault in terms of human actions, or an external event. A basic event or combination of basic events necessary and sufficient to cause the top event is called a 'cut set'. A cut set with a single basic event is termed a '*single point of failure*'. A cut set in which two basic events have to occur in order to cause the top event is termed a $2_{nd}$-order cut set, etc.

Calculating and adding the probability of each cut set produces a value for the probability of the top event. Depending on the type of analysis, this results in a probability or frequency of failure. If the recovery times are included, the analysis will result in the unplanned non-availability of the system, which is also the probability of failure per demand, as explained in section 6.3.1.

The basic events are linked to the top event by way of logical '*gates*'. A range of gates is possible, but the most important are:

- *AND gates*: for the purposes of linking underlying events that will only cause the (sub)top event if they **all** occur.
- *OR gates*: for the purposes of linking underlying events that will cause the (sub)top event if **at least one** of them occurs.
- *K-out-of-N gates* (Voting OR gates): for the purposes of linking underlying events that will cause the (sub)top event if **at least K out of N** of the events occur. This gate is in fact a composite of AND and OR gates.

For the purposes of constructing a fault tree, a number of rules apply.

- The top event is always the non-fulfilment of a functional requirement or the failure of a system. No 'positive' events occur in a fault tree.
- A fault tree is constructed from top to bottom, presenting the process flow from end to beginning. The top event is broken down via intermediate steps until the level of the basic events is reached.

Basic events are quantified using the results from the process step 'data collection' (section 6.3). An FTA assumes a constant failure rate, or the flat section of the 'bathtub curve' (see figure 6.3). This simplification means that the result of the calculation of the expected reliability and/or availability will hold for the short term, namely until the point at which the rising arm of the curve in figure 6.3 is reached.

Calculating a system's probability or frequency of failure is usually a complex affair. Even graphic representation of the system is not straightforward without

tools. Consequently, Rijkswaterstaat requires that an FTA is done with the aid of an (inter)nationally recognized program. In doing so, the interconnection between the system elements will have to be entered along with the relevant failure data for each system element. The program will subsequently process the data entered to form the cut sets and the probabilities, the probability of the top event and the graphic representation of the fault tree.

Once the fault tree has been quantified, a few checks should be performed. The most significant errors that might be made when modelling will quickly be revealed by reviewing and understanding the cut sets with the highest probability of occurrence.

### Sensitivity analysis

Failure data used for the system elements are always an estimate. Carrying out a sensitivity analysis will give an impression of the importance of the parameters determining the system's reliability and availability. This will enable some optimization improvements to be made. For example, if the testing interval significantly affects the final result, a shorter testing interval will significantly increase the reliability and availability of the system. If a component's testing interval exerts only minimal influence, the testing interval could be increased without significantly affecting the final outcome.

The software used features an option to automatically carry out this sensitivity analysis, and there are a number of indices that indicate the importance of the system elements in the system. The best-known indices are the *Birnbaum importance measure* and the *Fussell-Vesely importance measure*.

The *Birnbaum importance measure* presents the sensitivity of the system's reliability or availability for a system element, or $(\partial Q_{sys})/(\partial q_i)$. This is the derivative to the system element. In the formula, Qsys stands for the probability of failure of the system as a whole as a function of time, or for the non-availability of the system as a whole, whereas qi represents the probability of failure or non-availability of the system element. The *Fussell-Vesely importance measure* gives the effect on the reliability or availability of the system if a system element is assumed to be perfect: $Q_{sys}$ if $q_i=0$.

### Simulation technology

An interesting development is the prediction of reliability and availability in combination with predicting the costs with the aid of simulations. The expected reliability and availability and the expected costs are calculated by taking the average of multiple 'realizations'. This entails the lifespan of a system being 're-enacted'. The more simulations are considered, the higher the accuracy of the averages calculated.

This simulation technology also makes it possible to look further ahead. The result of a fault tree analysis applies for the short term, until the point at which the failure frequency of one or more components starts to increase. However, the method of simulation also makes it possible to disregard the increase in the probability of failure as a function of time. In combination with the costs entailed by inspections, repair work and replacements, a realistic picture of the expected performance as well as the expected costs can be obtained for the near future.

The RCM-Cost program from Isograph [13] facilitates such a calculation. The quantity of requisite data should not be underestimated, however.

## Example: the drawbridge

Figures 6.8 and 6.9 show the result of fault tree modelling for both LPW and LPS. The figures and the result of the calculation were obtained using a FaultTree+ calculation. FR stands for failure frequency, MTTR for mean time to recovery and Q for non-availability.

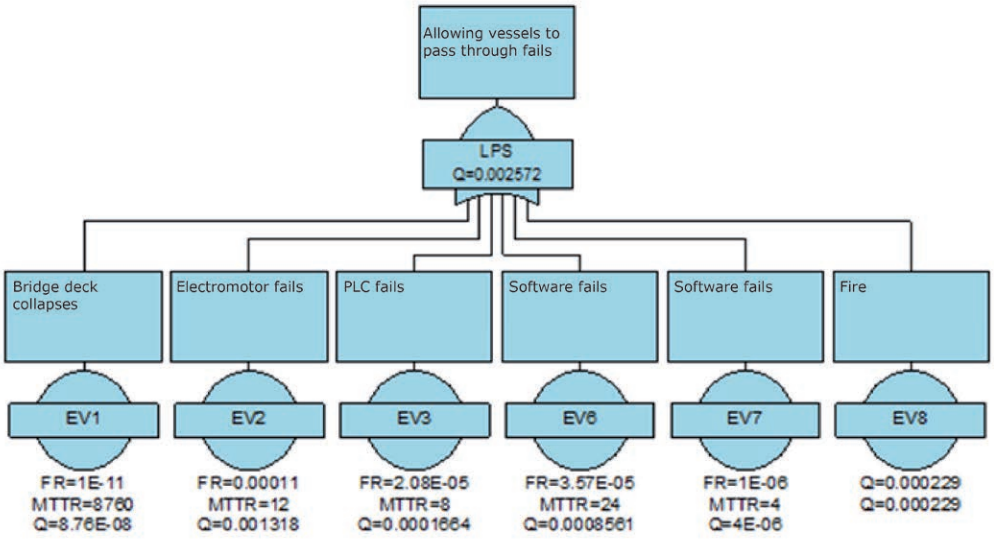



*Figure 6.9. Fault tree 'allowing vessels to pass through' (LPS)*

Figure 6.9 presents the fault tree containing the results for 'allowing vessels to pass through'. The sensors do not play a role and the failure of all other system elements will mean immediate failure of the system. They have been modelled using an 'OR gate'. The result is a non-availability of the system of 0.002572, in line with the result from the previous section.

Figure 6.10 presents the fault tree containing the results for 'allowing road traffic to pass through'. Both sensors are modelled using an 'AND gate'; after all, they both have to fail in order to cause failure of the system that records the position of the bridge deck. They constitute a second-order cut set. The dependency between both sensors has been modelled using the $\beta$-factor model, with $\beta = 0.1$. All other system elements are independently capable of causing the top event. They are modelled in the fault tree using an 'OR gate'.

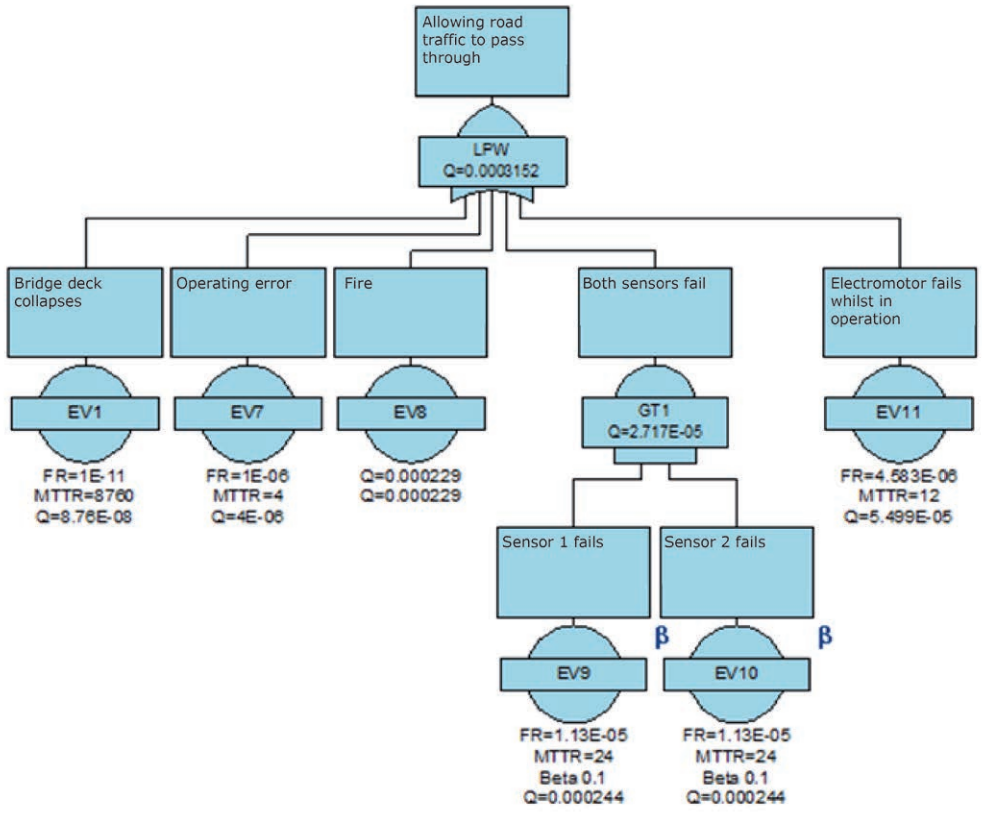



*Figure 6.10. Fault tree 'allowing road traffic to pass through' (LPS)*

The result for LPW is a non-availability of 0.0003152. This is considerably better than the 0.00083 from the previous section. The cause of this difference lies in the modelling of the redundant sensors. This has been done correctly in the fault tree. The *Fussell-Vesely importance measure* is presented in table 6.4, both in analytical terms and as a result of FaultTree+.

| CAUSE OF FAILURE | FUSSELL-VESELY LPS | FUSSELL-VESELY LPS FAULTTREE+ | FUSSELL-VESELY LPW | FUSSELL-VESELY LPW FAULTTREE+ |
|---|---|---|---|---|
| BRIDGE DECK COLLAPSES | 3,40E-05 | 3,40E-05 | 2,78E-04 | 2,78E-04 |
| ELECTROMOTOR WILL NOT START | 0,4904 | | | |
| ELECTROMOTOR STOPS PREMATURELY | 0,0213 | | 0,1745 | 0,1744 |
| PLC FAILS | 0,0645 | 0,0646 | | |
| SENSOR 1 FAILS | | | 0,0862 | 0,0862 |
| SENSOR 2 FAILS | | | | |
| SOFTWARE FAILS | 0,3334 | 0,3326 | | |
| OPERATING ERROR | 0,0016 | 0,0016 | 0,0127 | 0,0127 |
| FIRE | 0,0888 | 0,0890 | 0,7264 | 0,7264 |
| **TOTAL** | 1,0000 | | 1,0000 | |

*Table 6.4. Fussell-Vesely Importance*

In the case of the top event for the function 'allowing vessels to pass through' (LPS), the electromotor, the software and the PLC are the most significant causes of failure expected. In the case of 'allowing road traffic to pass through' (LPW), fire is the cause of failure most expected.

## 6.6 Process step: event tree analysis

The preceding sections all discussed a single relationship between an event and its consequence for a system element or the failure of an object. In reality, a certain (initiating) event is followed by multiple other events which, by way of a scenario, end up producing the ultimate effect on the functioning of the object. An event tree analysis (ETA) can chart and calculate the probability of different consequences as a result of a given (initiating) event.

As with a fault tree, presenting an event tree graphically is particularly illustrative, rendering transparent possible scenarios that could occur after a given (usually undesired) initiating event. As with a fault tree, the probability of these scenarios can be added to an event tree.

An event tree always starts with an initiating event. Events that follow on from the initiating event are called intermediate events.

An event tree offers a number of significant benefits:

- It clearly organizes all scenarios that can result from one specific event.
- It makes the situation transparent, as a result of which it can also be used as a means of communication. As soon as the initiating event has been determined, anyone can see and understand why certain intermediate events take place, and likewise why other (combinations of) events do not.
- The different scenarios render the probability of the event occurring transparent and traceable and show how this can be influenced.

Proceeding from an initiating event, an event tree is constructed by first gathering all relevant intermediate events. These must then be arranged in the correct order. Often this order is chronological, corresponding with the activation of various (safety) systems or physical processes that could occur after the initiating event. Proceeding from the initiating event, scenarios can be developed by means of branches for each relevant intermediate event. In many cases, a sizeable number of different scenarios are possible, but in practice these will merely result in a limited number of different consequences (see figure 6.10).

Once qualitative modelling has been completed and all scenarios have been identified, each intermediate event can be assigned a conditional probability of occurrence. The condition is that the previous event has occurred. The probability of each scenario is calculated by multiplying the probabilities of occurrence of the intermediate events that together determine the scenario. Because all scenarios are described and the initiating event is a fact with a probability equal to 1, the sum of the probabilities of the various scenarios will also be 1 at any point in time. This fact is an important control tool during quantification.

Paragraph 6.3 specifies possible sources for these conditional probabilities.
In some cases it will be necessary to establish probability using an FTA. This produces a combination of an FTA (to calculate the probability of a top event) and an event tree analysis (to calculate the probabilities of the consequences). The most unique manifestation of this is the bow-tie model, with the initial event of the event tree also being the top event from the fault tree.

## Example: the drawbridge

Figure 6.11 gives the result of event tree modelling for the primary function 'allowing vessels to pass through' (LPS).

| A SHIP IS ARRIVING | BRIDGE HAS FAILED | CONTROL BUILDING HAS BURNED DOWN | PLC HAS FAILED | SOFTWARE FAILS | EMERGENCY STOP PRESSED ACCIDENTALLY | ELECTRO-MOTOR FAILS | CONSEQUENCE | FREQUENCY |
|---|---|---|---|---|---|---|---|---|
| W=1 | Q = 8.76E-08 | Q=0.000229 | Q= 0.0001664 | Q=0.00086 | Q=4E-06 | Q= 0.00132 | | 1 |
| | | | | | | | SHIPPING IS POSSIBLE | 0.9974 |
| | | | | | | | SHIPPING HALTED | 0.001318 |
| A SHIP IS ARRIVING | | | | | | | SHIPPING HALTED | 3.995E-06 |
| | | | | | | | SHIPPING HALTED | 0.0008597 |
| | | | | | | | SHIPPING HALTED | 0.0001664 |
| | | | | | | | SHIPPING HALTED | 0.000229 |
| | | | | | | | SHIPPING HALTED | 8.76E-08 |

*Figure 6.11. Event tree 'allowing vessels to pass through' (LPS)*

The initiating event is that a ship is approaching. The intermediate events are arranged somewhat in chronological order, but this is, in this example, rather forced. Non-availability has been conceived of as probability here, e.g. the probability that the operator's cabin has burned down.

Each branch constitutes a scenario. The probability that it will occur is specified in the right-hand column. The sum of the probabilities of the scenarios that result in 'shipping halted' is $2.577.10^{-3}$. This is the complement of the probability of the branch 'shipping possible': 0.9974. See also figure 6.12, part of a report from FaultTree+.

RWB V12.0

Consequence Confidence Re

Allowing vessels to pass through

| ID | Description | Mean frequency |
|---|---|---|
| CQ1 | Shipping halted | 2.577e-3 |
| CQ2 | Shipping is possible | 9.974e-1 |

*Figure 6.12. The results of the events tree 'allowing vessels to pass through'*

## 6.7 Process step: additional control measures

### *6.7.1 Remedial action in the event of failure due to human error*

One of the possibilities for improving the performance calculated is the introduction of recovery actions. In contrast to the use of redundancy or human failure, this concerns a human action explicitly being included as a recovery measure.

The idea is that if a part of the system fails, remedial actions can be carried out that will ensure continued performance of the function. Examples include manually flicking a switch when an automatic low-voltage distributor fails or the winch at the Maeslantkering is cut through. Such remedial action cannot usually be modelled directly in the fault tree, as it involves multiple system parts and the action may well be time-dependent.

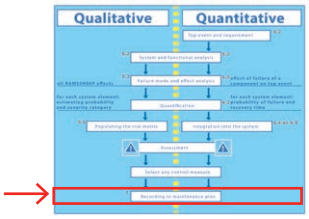
The procedure first entails calculation of the fault tree without recovery actions, after which a correction factor is indicated for each cut set, which reduces the contribution of that cut set to the overall probability of failure. To this end, a recovery database and MS Access application have been set up for the Maeslantkering, linking the cut sets and taking factors such as feasibility and probability of success into consideration. It goes without saying that the proposed recovery actions must be set, practicable and rehearsed.

### *6.7.2 Spare parts*

Another possibility for improving calculated performance is the use of spare parts. This prevents a protracted recovery time if the component is not in stock, not even at the supplier's business. Hence it could be worthwhile purchasing a spare part, or even multiple spare parts, and keeping these on standby. Particularly in a system with several components that are the same, this spare part may be used for a component that has failed previously. If so, it will still be possible to find that the part is out of stock, with a protracted recovery time as a result. It can also be cost-efficient to have one or more spare parts in stock.

There is an (analytical) connection between finding that a component is out of stock, the length of the stock replenishment time, the number of components in the system and the number of spare parts present. On the basis of this a judgement can be made on the minimum number of spare parts needed. This analysis is described in the 'Guidelines for Basic Model for Spare Parts' [23].

# 7 The relationship of object risk analysis to the maintenance plan




## 7.1 Introduction

This chapter sets out how the results of the ORA are recorded in the maintenance plan (MP). This step is essential because the assumptions and preconditions used in the ORA must be embedded in the risk-based asset management process. Without this step the determined or calculated performance will not be accurate nor guaranteed in the future. Within the Plan-Do-Check-Act cycle (see section 3.3) this pertains to the transition from 'act' (adjusting the ORA) to 'plan' (planning and scheduling the requisite maintenance work). Following construction, the contractor will be required to deliver the assumptions and fundamental principles from the initial risk analysis in the maintenance plan, with the red arrows being the actions in the PDCA cycle, indicating a relationship between the ORA and the MP. See figure 7.1.

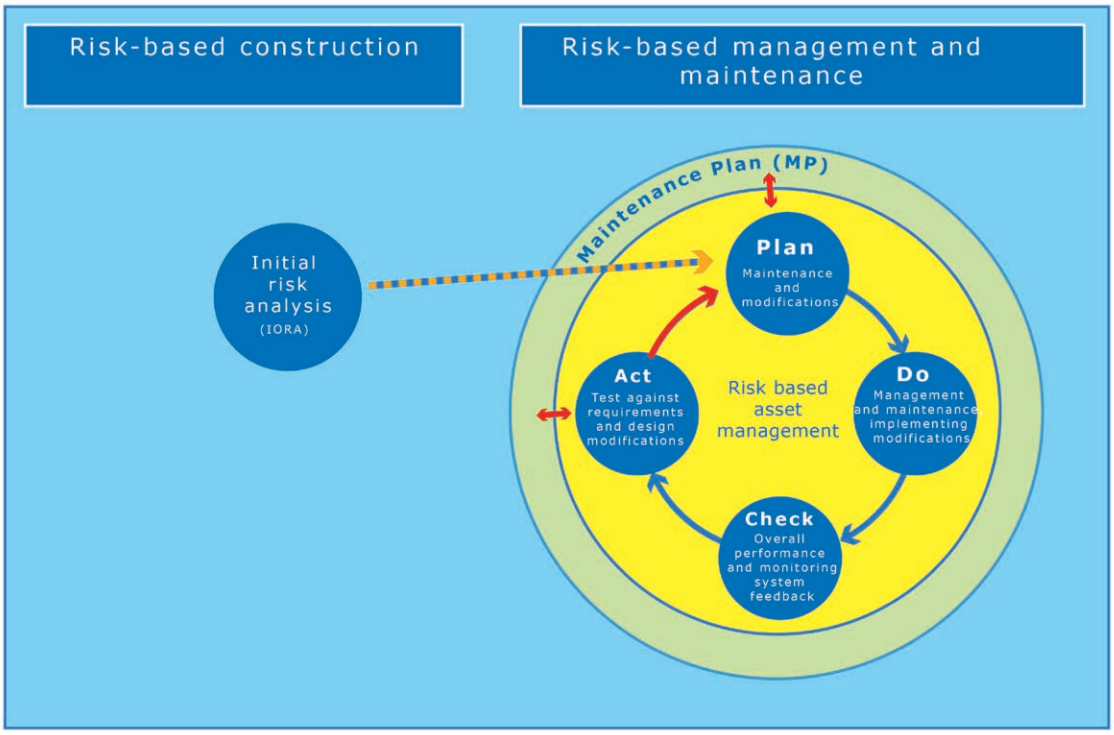



*Figure 7.1. The information from ORA to MP*

This chapter discusses the focus points associated with the maintenance plan. First a brief account of the function of an MP will be presented, followed by a description of the way in which the qualitative and quantitative ORA provide input for the maintenance plans. Finally, a few focus points regarding safeguarding the MP will be looked at.

## 7.2 The maintenance plan

A maintenance plan (MP) is a dynamic document drawn up and periodically updated by or on behalf of the operational manager. The MP describes such general matters as object data, applicable performance requirements and functions based on prevailing legislation and regulations, but also important environmental aspects and the performance that the object is expected to deliver in line with the management and maintenance measures also included in the MP. As such, the MP serves multiple purposes and the ORA is one of the sources. The other subjects included in the MP are beyond the scope of these guidelines as they are not risk-based. Information on how to draw up an MP is available from the ProBo support desk.

The ORA can be performed both qualitatively and quantitatively (chapter 3). In both cases, the risk analysis results in a set of management and maintenance measures whose implementation should be guaranteed by the MP. The two variants of the ORA result in various types of measures. After periodical inspection, a qualitative ORA will result in a set of maintenance measures that will have to be implemented in the subsequent period. An MP based on a qualitative ORA is referred to as a **(qualitative) MP.**

Besides these immediate maintenance measures, a quantitative ORA will also culminate in pointers for targeted interim inspections and tests to be performed. Possibly, condition-based thresholds will have to be monitored. Furthermore, the recovery time assumed in the ORA can be recorded in the MP. An MP based on a quantitative ORA is referred to as a **p-MP (performance-based MP) or MP based on ProBO.**

### 7.2.1 The qualitative ORA and MP

The qualitative ORA establishes, on the basis of an inspection, the condition of the structural units and subsequently provides an indication of the risks that an operational manager is running in terms of all RAMSSHE€P aspects. In risk sessions, risks can be entered into the risk matrix using a combination of probability and severity categories. Based on the scores, management and/or maintenance measures will be formulated. For a more detailed account, see section 5.5.

These measures are weighed up in more detail in the MP, for which subjects like economizing, prioritization and/or administrative agreements can serve as additional sources.

Preconditions in that regard are that transparency is maintained in terms of what the risks to the object are and that the absence of measures will lead to an increase in risk and should therefore be incorporated into the ORA.

The management and maintenance measures are recorded in the MP and assigned costs. This presents what is known as the *maintenance requirement* of the object, which will satisfy the requirements and standards set by Rijkswaterstaat.

### 7.2.2 The quantitative ORA and MP

A quantitative ORA provides an object's expected performance in terms of reliability and availability, assuming that the standard operational maintenance work is performed in line with the maintenance analysis that was used as input for the ORA (see chapter 6). These are preconditions from the hardware analysis in the ORA, such as task-setting recovery times, testing and inspection intervals and the failure frequency of system elements in a certain stage of their life cycle.

The software analysis can also generate preconditions, as will the human factor analysis. In the case of the analysis of human actions, these preconditions will concern level of education/training, frequency of training, presence, use and quality of work instructions and so on.

The analysis of external events can generate preconditions in terms of monitoring frequency, presence of a certified firefighting system, certified fire compartmentalization, certified lightning protection equipment, upkeep of surrounding greenery and suchlike. If the maintenance work stemming from the ORA is not being scheduled and incorporated into the MP, the risk analysis will need to be adjusted, just as it would be with the qualitative ORA. In such cases, the object will be expected to perform differently. Hence this new expectation in terms of performance will have to be incorporated into the expectations for the relevant network and tested against the agreements in the SLA (see chapter 2).

Here, too, the maintenance requirement of an object can be ascertained. The management and maintenance measures are set down in an MP.

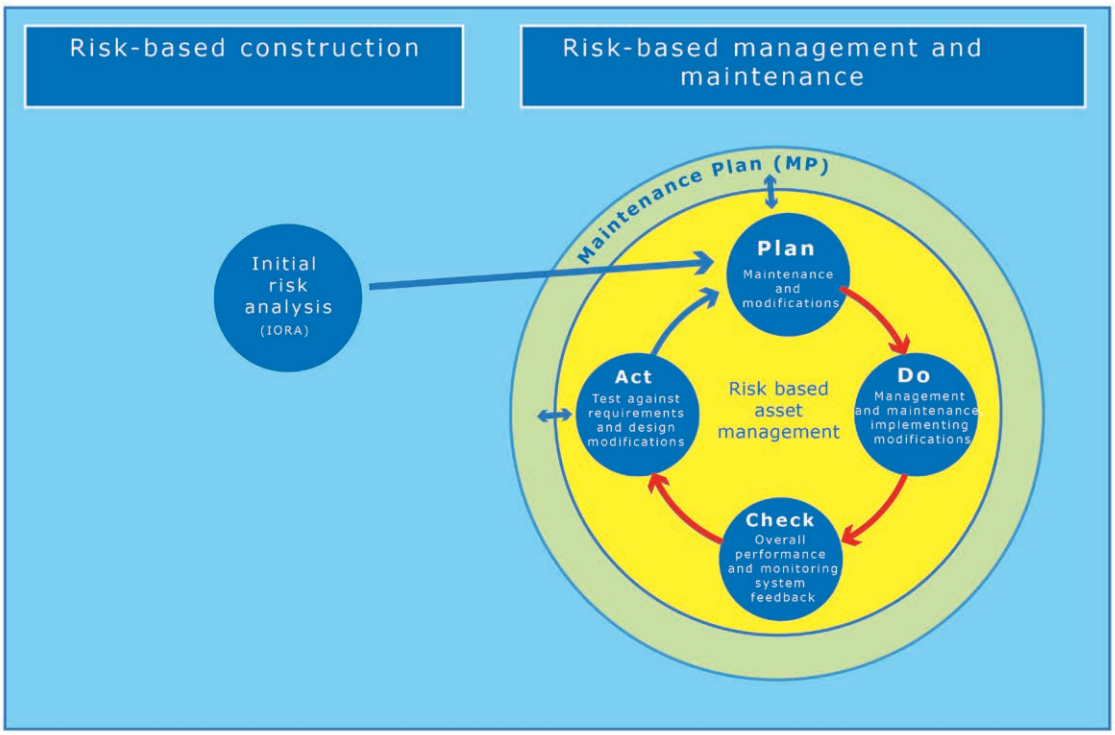



*Figure 7.2. Adjusting the ORA in response to changes to the maintenance work desired*

## 7.3 Focus points for safeguarding management and maintenance measures in the MP

The management and maintenance measures resulting from the ORA must be embedded in the maintenance plan. If it is decided not to include the measures in the MP, this will have to be stated explicitly in the MP, citing the reasons for this decision, the risk arising as a result of the decision and substantiation as to why that risk is nevertheless acceptable. This way, both the measure not implemented, the risk taken and the reasoning are documented and available when updating the ORA.

In contrast to the qualitative ORA, not adopting management and maintenance measures from the quantitative ORA has a direct effect on the object's expected performance. Here, too, the MP must state the reasons why the decision was reached and what the subsequent consequences and risks will be for that object.

Monitoring of the object (the 'check' element in the PDCA cycle) is often more comprehensive in the quantitative variant, because a greater number of aspects have to be measured. The method of monitoring these aspects is set down in the MP.

The quantitative ORA includes a (quantitative) maintenance analysis. With the system in mind, an optimal balance is established between maintenance efforts and the performance expected of the object. The maintenance efforts are task-setting (mandatory, otherwise the object's expected performance will no longer be delivered) and encompass such things as:

- maintenance intervals
- task-setting recovery time in the event of faults
- testing intervals
- inspection intervals
- condition-based monitoring thresholds
- replacement intervals.

The intervals specified may be smaller than but not greater than those resulting from the ORA. They are maximum intervals. The same goes for the expected recovery time in the event of faults. It is not (yet) customary, but it commonly proves to be necessary to explicitly specify the recovery time in the contracts and regularly check whether the contractual recovery times are actually being achieved as well.

Even the measure that has to be taken when a condition threshold is exceeded must be included in the MP. If, for example, it is decided that a crack in a bridge deck will be repaired if it exceeds 10 cm, this principle must be included in the MP and will play a role in the ORA for determining the failure probability of the bridge deck.

# 8 Safeguarding risk-based asset management in the organization

## 8.1 Introduction

Like strength analysis, risk analysis is a design tool for achieving the desired objective, in this case sufficient reliability and/or availability. An initial risk assessment is drawn up during construction of or major renovation work on an object. This must be kept up to date during the design and construction process and will retrospectively serve as verification of the design. This will provide an 'as is' ORA upon completion of the object: a risk analysis that optimally models reality.

The initial risk analysis marks the beginning of a continuous cycle for managing the object's performance level. The requisite management and maintenance activities stemming from the risk analysis (act) are safeguarded in the MP (plan), implemented (do) and measured (check). Next, the difference between requirements and measured performance is established and the ORA is updated (act). Where necessary, improvement actions and possible optimizations ensue (plan), repeating the PDCA cycle (see figure 8.1).

If no initial risk analysis has been performed for an existing object, this should still be done. This will result in the actual performance level. Management or maintenance measures are often specified and incorporated into the ORA as well, ensuring that the potential performance of the object is transparent. The ORA can also be used to effect improvements in the existing design. In both cases this ORA is the point of departure for management and maintenance during the operational stage.

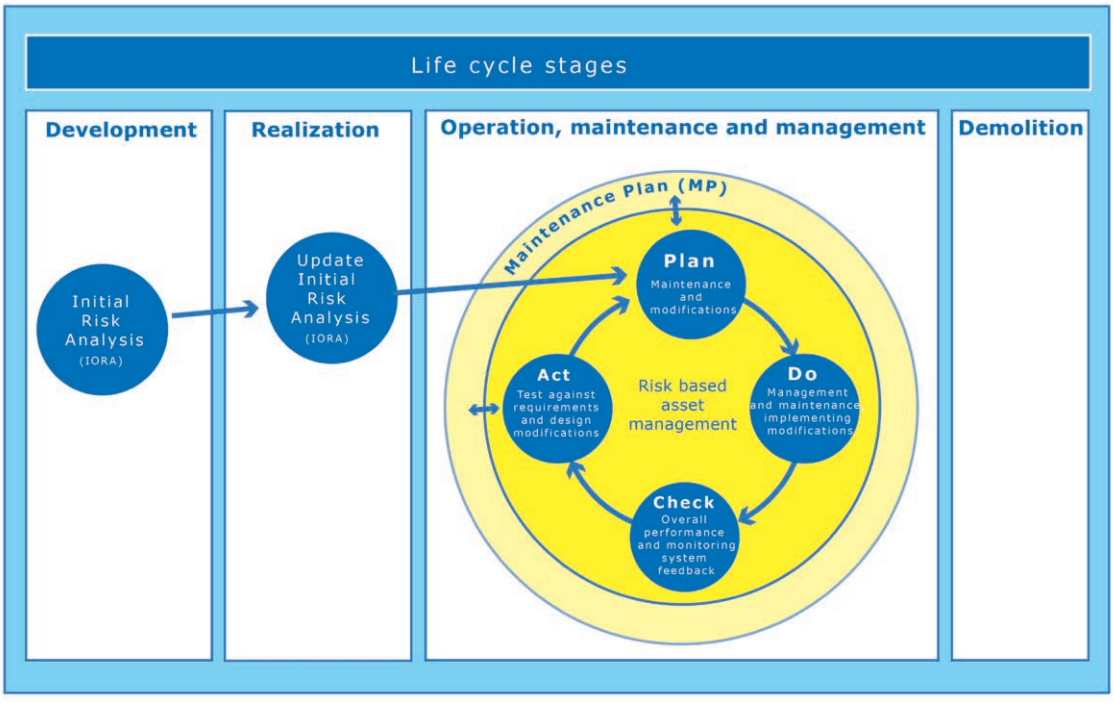



*Figure 8.1. PDCA cycle following the initial object risk analysis*

During that management and maintenance stage, the ORA is an indispensable element for continuously managing the object's performance, and thus for embedding in the organization that the object will continue to fulfil performance requirements. If the prevailing performance requirements are met, maintenance costs can be minimized over the life cycle. If an organization masters this process, and it can be demonstrated at any point in time that the performance requirements are being satisfied, the organization will be in control of performance of its assets and the requisite investments to this end.

In practice, it is not self-evident for this 'in control' status to remain up to date following the initial implementation of the risk-based approach. Under the influence of work pressure, reorganizations and staff turnover, attention to transparent and systematic working and demonstrably recording results (or partial results) wanes. This does not have to mean that the organization is no longer capable of maintaining the object's performance level, but it does mean that this is no longer demonstrable. To maintain the 'in control' status, the processes should be permanently evaluated in the PDCA cycle.

This chapter discusses the preconditions for organizing risk-based asset management. In a number of cases this approach has already been implemented in the organization. For example, the National Tunnel Standard [7], drawn up by the Rijkswaterstaat Board as the standard for its tunnels, also sets requirements for the processes and the management organization of a tunnel. Allocating these roles will contribute to safeguarding the quality of the maintenance process. It would be prudent to combine the roles required for the risk-based approach sensibly with the roles deemed necessary by the *National Tunnel Standard.*

## 8.2 Safeguarding risk-based construction

During the construction of or major renovation work on an object, Rijkswaterstaat utilizes the integrated project management model (IPM model). The quality of the initial risk analysis is initially determined using the contractor's quality system. The Technical Manager tests the contractor's work with the aid of Systems-based Contract Management (SCM). This can differ from what is important for management and/or maintenance. It is therefore advisable to coordinate with the operational manager at as early a stage as possible. Depending on the specific nature and scope of the analysis, the help of consultants will be enlisted.

In some cases the technical manager may have specific wishes (such as external reviews) with regard to safeguarding the quality of the initial risk analysis. This will always be set down in advance in the product quality plan, in dialogue with the consultant involved.

## 8.3 Safeguarding risk-based management and maintenance

Aside from the technology, a suitable organization is also required during the management and maintenance stage to keep management and maintenance activities at a controlled level. Demonstrably being in control (the essence of risk-based asset management) requires a process-oriented approach, with the ORA being the core of the risk-based management. The processes required to this end may include:

- the organizational set-up (structure, tasks, responsibilities and authorizations, lines of control),
- knowledge and experience (job profiles, training courses, personal development) and
- culture (behaviour, relevant competencies).

Three processes directly influence the object's performance level: the maintenance process, the operational process and the management process, as visualized in figure 8.2.


*Figure 8.2. Processes that influence the risk-based approach*

### *8.3.1 The maintenance process*

Rijkswaterstaat's objects are subject to ageing, wear and tear and changing circumstances. Maintenance, renovation and replacement or extension are essential in order to ensure ongoing fulfilment of the performance requirements. The risk-based maintenance process provides for this in line with a PDCA cycle.

**Plan stage**

The 'plan' stage is characterized by the conversion of management and maintenance activities (adopted in the ORA) or measures (stemming from the qualitative ORA) into concrete plans. In summary, the concrete plans are added to and/or inserted in the maintenance plan. This step encompasses all maintenance activities (strategy, duration, frequency, numbers, quality, costs) and the practices applied for use of the object (procedures, work instructions).

The activities in the maintenance plan must be made implementable by the organization (tasks, authorizations, responsibilities, insourcing and outsourcing/ contracting). The concrete plans are organized into a schedule and implemented during the 'do' stage. This occasionally implies non-availability of the object.

The products from the 'plan' stage are:
- an (updated) maintenance plan
- modified contracts, in line with the (updated) MP.

**Do stage**

The 'do' stage is characterized by the actual implementation of work and measures defined in the 'plan' stage and set down in the maintenance plan. These activities are task-setting. They *must* be performed in order to guarantee the object's desired performance. Procedures and work instructions are used to enable this. To the extent that activities stem from the quantitative ORA, performance requirements set for system elements, frequencies, turnaround times for inspection, testing and maintenance work and fault recovery times also play a

role. These parameters may also be task-setting outcomes of the ORA. They guarantee the reliability and availability of the object's functions.

Possible products from the 'do' stage are:
- applied inspection planning, including the actual inspection intervals
- inspection reports, including the development of condition parameters
- applied test planning, including the actual testing intervals
- test reports, including the number of defects or rejections following a test
- fault database, including statement of actual recovery times
- root cause analyses for major or recurring faults
- statement of actual availability, including representation of non-availabilities categorized into the causes of:
    - planned maintenance
    - inspections
    - testing
    - faults (unplanned maintenance)
- signed-off procedures and work instructions.

### Check stage

The 'check' stage is intended to monitor and evaluate the data and information from the 'do' stage. It is essential that the information relevant to this end is properly ordered and recorded by the operational manager during the 'do' stage. In essence, the monitoring process focuses on flagging up deviations from both the process and plans and the technical condition of an object as well as on turning this into useful information.

Parameters that could deviate include:
- the malfunction frequency and failure mechanisms
- recovery times, test results and inspection results
- unexpected trends or readings in condition thresholds (see chapter 6)
- visual abnormalities of the object
- anomalies in terms of spare parts management
- unexpected human actions
- unexpected software responses
- anomalies in terms of staff's level of training/education.

Possible products from of the 'check' stage are:
- analyses of anomalies
- reporting of changes

### Act-fase

During the 'act' stage the data and proposals from the 'check' stage are converted into concrete maintenance measures, including possible system changes. Measures and any system changes are incorporated into the ORA, establishing a new performance level. The performance requirements are also evaluated and, if need be, adjusted. This presents an opportunity for optimization.

Products from of the 'act' stage are:
- if changed: an adjusted system description
- if changed: an adjusted physical breakdown
- an adjusted ORA
- adjusted performance

### *8.3.2 The operational process*

The operational process is crucial for the proper functioning of (part of) the area and is therefore essential for the fulfilment of the performance requirements. Poor organization of operations can affect the performance level. In some cases the performance requirement can only be fulfilled if specific requirements are set for the operational process, such as training, motivation, tools and suchlike. Consequently, a clear description of the operational process will have to be provided in a handbook, including the structure of the operational organization [24].

### *8.3.3 The management process*

An element deserving particular attention when implementing and assuring risk-based asset management is the role of management. This includes control, direction and final responsibility regarding the proper functioning of the objects. By supporting the organization, management enables the realization and long-term assurance of the desired situation (i.e. meeting the performance requirements in a cost efficient manner). Management also has the task of matching needs in terms of budget, capacity and suchlike with the organizational requirements. This requires communication with the budget providers, the Board (potentially being relayed into the political sphere) as well as with local residents and the media. This applies to both the regional operational manager and Rijkswaterstaat's nationwide services.

Management and maintenance activities are carried out at various levels within Rijkswaterstaat. Any organizational description of management and maintenance must therefore be divided up into each of those levels.

**Strategic**

At strategic level, consideration is given to budget, capacity and the performance to be delivered using these. Advantages and disadvantages must be clear to decision-makers, so that they can make well-considered and properly justified decisions. All information required to this end will have to be available.

**Tactical**

Decisions at strategic level are cascaded down to the regional organizational units which, as a product of their scheduling process, will make proposals for clustering maintenance network-wide. Another activity at this level is procurement of maintenance services.

**Operational**

The regional organizational units, particularly the districts, are charged with the responsibility for day-to-day management and maintenance of the objects. It is of great importance to the successful implementation of risk-based asset management that this responsibility be properly fulfilled: the work has a significant influence on the ultimate performance level. The regional organizational units control the ORAs drawn up, record the assumptions and results of risk analyses along with the calculated costs in maintenance plans and see to it that the measures specified in these plans are implemented. Moreover, operational control of the objects is performed by the nationwide organizational unit Traffic and Water Management.

The regional maintenance organization and the operational organization play an important role when it comes to delivering the desired network performance levels. An important concept in the introduction of risk-based asset management is separation of the responsibilities of the asset manager and the performance manager. The asset manager is responsible for the day-to-day management and

maintenance of the object; the performance manager periodically assesses the object's performance, independently of the asset manager. Rijkswaterstaat does not consider it to be desirable to combine these responsibilities. After all, the scope of the asset manager is far broader than asset performance alone. Political, economic and environmental concerns could conflict with the desired performance level. The asset manager weighs these factors up. Naturally it is essential to ensure proper cooperation and information sharing between the two managers.

## 8.4 Preconditions for the management and maintenance organization

In order to be able to carry out risk-based asset management, the aforementioned processes must satisfy a number of preconditions. The level of depth and detail of these preconditions varies for the different types of object and depends on the complexity of the object. Generic preconditions can be categorized into:

- people
- methods
- resources

### *8.4.1 People*

One consequence of the risk-based approach is that it must be continuously guaranteed that the requisite competences and skills are available to a sufficient extent. Aspects affecting the performance level that must be considered as minimal and evaluated periodically are:

- the availability of staff with the right knowledge, competences and skills, with the strategic HRM plan as an important tool for assurance
- clear and transparent recording of staff tasks, responsibilities and authorizations, for which the RASCI method is an important tool
- the knowledge and experience of staff, for which the HRM and training plans are important tools
- a description of the training and education for current and new employees.

### *8.4.2 Methods*

The ORA incorporates fundamental principles on how maintenance and operations are to be carried out. Staff must act in line with these fundamental principles to ensure the validity of the object risk analysis.

This requires the following:

- methods to measure and record performance
- inspection and testing protocols
- procedures and/or work instructions for maintenance and recovery actions
- scheduling inspections, testing and maintenance
- recording methods for evaluating the maintenance process
- handbooks for the operational stage
- procedures and/or work instructions for operational actions
- recording methods for evaluating the operational process.

### *8.4.3 Resources*

In the ORA, assumptions are also made with regard to the available resources. If these resources are lacking, this will result in failure to fully achieve set recovery times, recovery options, etc. Resources include:

- sufficient budget to implement the measures arising from the ORA
- ancillary systems for the ORA, such as templates to support the FMECA and computer software for RCM or fault trees
- the ancillary systems for maintenance, including keeping records, such as a

maintenance management system (MMS)
- the necessary measuring equipment for maintenance activities
- the necessary spare parts and tools for maintenance and recovery
- the requisite safety equipment for maintenance and recovery activities
- the ancillary systems for operations, such as decision-making protocols
- the ancillary information systems for operations and maintenance
- the availability of a quality system
- the presence of an evaluation structure, stating what has to be evaluated and reported and when.

## 8.5 Quality assurance

The precise organizational set-up to create or maintain a controlled and guaranteed maintenance process is largely beyond the scope of these guidelines. However, criteria and preconditions can be derived from generally accepted and available ISO standards for quality assurance that provide an idea of the extent to which the organization is capable of carrying out the desired process at a satisfactory level.

Just as technical failure cannot be fully prevented, errors cannot be ruled out within an organization. The quality system is designed to minimize these mistakes and, wherever possible and worthwhile, to rectify them in a timely manner, bringing the probability of poor quality down to an acceptably low level.

It is important that the organization has faith in the satisfactory performance of the quality system. If it emerges in practice that 'surprises' regularly occur, the quality system is not yet embedded into the quality culture. It goes without saying that the quality system too will have to be periodically assessed and, if need be, adjusted.

An internationally drawn up and accepted standard for quality management is the NEN-EN-ISO 9000 [25] or a standard derived from this, such as the ISO 55000 for asset management [26], formerly PAS55. These standards offer sufficient starting points for setting up a quality system for the management and maintenance organization or for the operational organization. For the purposes of quality management, the standards prescribe such aspects as:
- the recording of products, processes, roles and responsibilities
- the periodic evaluation of the products, processes, roles and responsibilities
- the integration of risk management into the processes.

The substantive aspects that, from the perspective of risk-based work, must be guaranteed in the various processes have been described in more detail and explained generically in the section above. A tool has been developed at Rijkswaterstaat that assesses the processes in terms of these aspects, thereby validating the risk analysis: the 'Compass'. At the present juncture, the Compass has only been specified for the quantitative risk analysis for storm surge barriers.

In principle, such a tool could also be used for other types of objects and for the qualitative ORA, although a few aspects would have to be adapted.

# 9 Safeguarding risk-based asset management in contracts

## 9.1 What fundamental principles have to be safeguarded?

The risk-based asset management philosophy must not only be embedded in the organization, but must also be enshrined in the contracts. It does not really matter how tasks, responsibilities and authorizations are divided in a contract, as long as the chains surrounding the risk analysis, the maintenance plan, and the management of both remain intact. To this end, the fundamental principles of risk-based asset management must be set out as preconditions in the contracts. In that regard, specific attention must be paid to:

- creating, managing, configuring and updating the risk analysis (ORA, chapters 5 and 6)
- drawing up and updating the maintenance plan (MP, chapter 7)
- implementing and providing feedback on (parts of) the maintenance plan
- evaluating the results.

The scope of outsourcing of activities will have a major influence on the way in which Rijkswaterstaat's own management organization is set up. This organization must be in a position to exert control over contracts, processes and activities, as well as test the outsourced activities or have them tested by an external party. As such, both the contractor and Rijkswaterstaat must have the right competences and the right knowledge and expertise.

### *9.1.1 Object risk analysis in contracts*

All contracts must be based on a risk analysis with the right level of depth and quality. This risk analysis will be drawn up by the operational manager, or by a contractor working for or on behalf of the operational manager. The document *Verification Method Reliability and Availability* [27] addresses requests for performing the quantitative part of the ORA and summarizes the requirements that Rijkswaterstaat sets for an ORA.

### *9.1.2 The maintenance plan in contracts*

The object risk analysis and the maintenance plan offer the object manager the option of contracting out the maintenance work that is required. It is crucial that requirements are set for the maintenance process and in particular for feedback during the process. Requirements set for the maintenance process pertain to the testing, replacement and inspection intervals and to the recovery times to be achieved. The feedback enables the operational manager to keep the object risk analysis, the maintenance plan and the maintenance management system up to date.

Consequently, the object manager will have to specify in the contract that the right information is being amassed and recorded, e.g. test and inspection results, failed components, including the affected mechanisms, etc. The summary below shows a few of the parameters that are important for a maintenance plan that is based in part on a quantitative ORA.

**Operational parameters:**
- records of operating hours
- number of operations.

**Fault data:**
- date/time of fault message
- registration of structural part/element/component, in line with the FMEA
- description of failure mode and cause of failure
- number of faults that have occurred for each component
- waiting time between fault message and proceeding to actual restoration of functionality
- the recovery time from waiting time to restoration of functionality
- recovery time (sum of both of the times above)
- date/time of fault deregistration.

**Maintenance data:**
- date/time of carrying out systematic maintenance activities
- the duration of testing for each component
- the duration of inspection (condition-dependent inspections) for each component
- the condition thresholds measured
- the duration of the maintenance work for each component
- number of spare parts for component in stock (if applicable).

The contracts should include clear agreements on how the contractor will comply with these parameters. This maintenance information must be recorded in Rijkswaterstaat data systems for future use.

### *9.1.3 Implementing (parts of) the maintenance plan*
The preconditions from the ORA must be safeguarded. If, for example, the ORA assumes an on-hand stock of at least two components or a recovery time of no more than 24 hours, these assumptions must be included as requirements in the contract with the contractor.

### *9.1.4 Evaluating the results*
The data amassed during the object's use, part of which has been set out above, must be interpreted and converted into feedback, as described in section 9.1.2., to complete the PDCA loop.

## 9.2 Safeguarding in Rijkswaterstaat's contractual forms

Rijkswaterstaat has a variety of contractual forms with contractors. In these contracts, Rijkswaterstaat sets out functional requirements, describing what functions have to be achieved rather than how exactly those functions are to be provided or created.

This can be done successfully if the scope for solutions (the variation in terms of possible specifics of the requested function) is considerable, but will become more difficult the more preconditions apply. The latter point is particularly relevant to maintenance: the existing situation limits the *scope for solutions*. An approach based on system elements, as in systems engineering and as proposed in the present document, means that components can be replaced or reconditioned. In such situations it may even be required to purchase a product of a specific brand, leaving no freedom whatsoever in terms of solutions. Neither will there be much in the way of functional freedom for the contractor when it comes to reconditioning an existing component.

This means that the various contractual forms differ quite a bit. If there is a lot of freedom in terms of solutions, specifications will be functional and it will be important to set performance requirements. If there is little to no scope in terms of solutions, the reliability and/or availability achieved will be more of a result than a requirement specified in advance. In such cases, the ORA for the system will need to be adjusted using the R/A characteristics achieved by the component.

Rijkswaterstaat works with the following contractual forms in the groundwork, road and hydraulic engineering sector:

**Engineering & construct (E&C)**
The contractor performs work with a minimal proportion of detailed engineering (predominantly variable maintenance work).

**Design & construct (D&C)**
The contractor is responsible for the design and its implementation. This pertains primarily to construction or renovation activities.

**Performance contracts**
The contractor is responsible for maintaining part of the network for several years.

**Design, build, finance & maintain (DBFM)**
The contractor is responsible not only for the design and construction work entailed by the project, but also for financing and overall maintenance.

**Partnership agreement engineering services**
Agreed conditions for putting services out to tender among a select group of engineering firms.

**Marketplace model for project and technical staff**
Method to select the most suitable candidate for hiring project and technical staff.

The last two contractual forms do not pertain to contracts in which (sub)systems are supplied and will not be discussed further here.

### 9.2.1 E&C-contract

Engineering & construct (E&C) contracts are generally used for construction projects and variable maintenance projects that entail little or no design work. The design work will be limited to a minimal proportion of detailed engineering. An example of an E&C contract is the application of new coatings of asphalt on existing road surfaces.

Rijkswaterstaat endeavours to draw up tendering documents that are as specific as possible in functional terms. Because the scope for design is limited, the functional requirements are generally at a low level of abstraction. Ascertaining what work the contractor will have to perform in order to deliver what has been requested will remain the contractor's responsibility.

As the contractor is working on only part of the object, i.e. a subsystem, only RAMSSHE€P requirements can be set for this part. Requirements set for reliability or availability must therefore apply to the subsystem and not the entire object. The object's ORA can be used to ascertain the subsystem's previous level of reliability and availability. This can then be used to formulate worthwhile R/A requirements for the subsystem to be maintained, replaced, or reconditioned.

Occasionally, the freedom in terms of design is so limited that one has to accept that the new subsystem will have a certain level of reliability, or availability, and will not be able to satisfy stricter requirements. If that is the case, the object's ORA will have to be adjusted before having to revisit the question of whether the object still satisfies the requirements set. This is part of updating the ORA, as described in section 3.3.

### 9.2.2 D&C-contract

Under Design & Construct contracts (D&C), the contractor is responsible for designing the infrastructure and implementing its construction. Rijkswaterstaat will draw up a call for tenders with clear functional specifications. The contractor will be given freedom to include innovations in the design and implementation. These two stages will have to be closely coordinated.

D&C contracts exist primarily for projects in the construction sector and for major renovation work. Examples include the Delft-Schiedam road section on the A4 (construction) and the repair of dam walls along the Amsterdam-Rhine Canal (maintenance).

D&C contracts are particularly suited to working with clear functional specifications: requesting delivery of a function rather than a system. The quality of the function supplied is stipulated by the RAMSSHE€P aspect requirements. The requirements set for the extent to which the function has to be fulfilled are expressed in quantitative requirements for the reliability and availability of the function. Because the contractor's responsibility ceases upon delivery of the system, it is imperative in the case of D&C to show with the aid of an ORA that the object will satisfy the set requirements after completion. If this pertains to a bridge's reliability, the contractor will do so by adhering to the (international) design requirements and documenting this. When it comes to the availability of a lock, this is guaranteed by performing a quantitative risk analysis, in line with the instructions of Rijkswaterstaat [24].

### *9.2.3 Performance contract*

Rijkswaterstaat uses performance contracts for long-term maintenance work. Under such contracts, the contractor is responsible for maintaining an object. The object must satisfy all preset requirements throughout the contractual term. The emphasis in the performance contract's terms of reference is chiefly on maintaining the 'day-to-day functionality and performance' of the area and managing the risks in the area, in addition to 'maintaining the condition'.

The contractor supplies the data for the ORA and the MP. The contractor will be asked to maintain and monitor the object (the area) for several years and keep the client informed on its condition. In doing so, the contractor focuses on performance and quality rather than concrete activities, although specific activities are not ruled out. In general, the contractor will update the necessary parts of the ORA and the corresponding parts of the MP.

In practice, contractors only have limited experience with the risk-based approach. The requisite maintenance work requested will be task-setting. In such a case, it will be important to ensure that the request is in step with the ORA, evidencing that the underlying performance requirements are being satisfied. Subsequently, whilst periodically running through their management cycle, the operational manager will have to test whether the contractor is indeed satisfying the preconditions from the risk analysis. This can be done by checking mandatory feedback from the contractor (e.g. recovery times achieved), or by testing the contractor's processes (e.g. the staff training process).

### *9.2.4 DBFM contract*

Under design, build, finance and maintain (DBFM) contracts, the contractor is responsible both for the design and the construction of the project and for its financing and overall maintenance for a set number of years. It is therefore an integrated contractual form, offering the contractor maximum freedom to use their knowledge and creativity in the design, build and maintenance phases of the contract. This last stage is lacking in D&C contracts. The theory is that the contractor will consider the object's life cycle during the construction process: they will optimize the sum of construction costs and maintenance costs. Depending on the contract, the contractor will be responsible for maintenance for another 20 or 30 years following the realization stage.

Another fundamental principle in DBFM contracts is that risks and responsibilities are vested in the party most capable of managing and bearing them. The contractor is paid periodically following the construction work, based on services rendered. If the agreed services are not supplied, penalty clauses will come into effect. The profit objective of the consortium and the private financiers will ensure that the sum of penalties incurred and the costs are kept to a minimum.

Rijkswaterstaat uses D&C contracts to purchase a product, such as a dual carriageway. In the case of a DBFM contract, however, the client is buying a service: an available dual carriageway. One of the earliest examples of a DBFM project is the Second Coen Tunnel (put out to tender in 2005).

Stipulating performance requirements is essential in this contractual form too, resulting in an object that will satisfy requirements (statutory or otherwise).

An example pertains to the requirements in the Water Act. In general, the function 'retaining high water' has a strict reliability requirement, whereas the system is only required to fulfil the function occasionally. This is why it is not possible to ascertain by means of measurements whether the required performance is being achieved for the function 'retaining high water' and why Rijkswaterstaat elects to demonstrate the required performance with the aid of a risk analysis. This ORA will have to be regularly adapted to changes in the system to demonstrate fulfilment of the requirements during the course of the operational stage as well.

However, even if it is possible to measure the quality of the function being supplied in the operational stage, the contractor will seek an economic optimum in view of the imposition of fines (accountability). This does not necessarily need to concur with the requirements that are desirable from society's perspective. It is, of course, possible to achieve the desired effect by choosing the right penalty regime, but the contractor will then need to have a clear picture of the costs involved to attain the required performance level.

What this means in practice is that Rijkwaterstaat sets RAMSSHE€P requirements for the primary functions and that upon completion (availability date) the contractor will use an ORA and the resulting MP to make a reasonable case for the fact that the object will satisfy the requirements. For those functions whose characteristics are not measurable during the operational stage, the contractor will regularly have to update the ORA in line with section 3.3. For those functions whose characteristics are measurable – such as the function 'allowing road traffic to pass through' at a tunnel - an appropriate penalty regime will enable quality assurance.

# 10 References

[1] Struik, P.
*Business case risk-based maintenance, appendix 1*
Rijkswaterstaat Board Memo, Number RWS-2013/33552, 27 June 2013
Approved Rijkswaterstaat Management Meeting no. 18, 5 July 2013

[2] Velde, Jenne van der and Henrik Hooimeijer
*Asset Management within Rijkswaterstaat, A general introduction*
Rijkswaterstaat, November 2010

[3] Working party systems engineering guidelines
*Systems Engineering Guidelines for the groundwork, road and hydraulic engineering sector, version 3*
Rijkswaterstaat, November 2013

[4] NEN 2767-4-1
*Condition Measurement - Part 4: Infrastructure - Part 1: Methodology*
Netherlands Institute of Standardization (NEN), July 2011

[5] *Life Cycle Cost Framework (LCC) 2014*
ww edition #1485
Rijkswaterstaat, December 2002

[6] Beem, R.C.A., editor
*Guidelines for Flood Defence and Reliability Requirements – Consequences of requirements for Flood Defences, Sluices and Traffic on land and on water for the design of Structures in Wet Infrastructure*
Rijkswaterstaat, September 1998

[7] *Landelijke tunnelstandaard [national tunnel standard]*
Rijkswaterstaat, October 2012

[8] *Performing functional analysis, Systems Engineering Procedure Description, WWB-SE-0022*
ww edition #849
Rijkswaterstaat, April 2017

[9] NEN-EN-IEC 60812
*Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)*
Netherlands Institute of Standardization (NEN), May 2006

[10] *Template simple ORA movable structures, version 2.1.1*
ww edition #1560
Rijkswaterstaat, November 2017

[11] *Reference framework management and maintenance (RMM 2015)*
ww edition #3041
Rijkswaterstaat, July 2015

[12] *Guidelines for the LEM model (Model version 1.4.1)*
Stijnen, J.W., J.M. van Noortwijk and M.J. Kallen, February 2011

[13] *Availability workbench*
Isograph, 2013

[14] *Guidelines for Failure Database – Generic, pessimistic failure data, for use by contractors, version 1.0.1*
ww edition #5499
Rijkswaterstaat, November 2015
**(see Rijkswaterstaat Werkwijzer (manual) for prevailing version)**

[15] Cooke, R.M.
*Experts in Uncertainty*
Oxford University Press, New York, 1991

[16] *Guidelines for Bayesian update – Adjusting failure data based on measurements, version 1.0.1*
ww edition #5500
Rijkswaterstaat, November 2017
**(see Rijkswaterstaat Werkwijzer (manual) for prevailing version)**

[17] *Guidelines for TOPAAS A structural approach for failure probability analysis of software-intensive systems, version 0.7*
ww edition #1319
Rijkswaterstaat, January 2013
**(see Rijkswaterstaat Werkwijzer (manual) for prevailing version)**

[18] *Guidelines for Quantification of human actions  using the OPSCHEP model, version 1.0.2*
ww edition #5533
Rijkswaterstaat, November 2017
***(see Rijkswaterstaat Werkwijzer (manual) for prevailing version)***

[19] *Guidelines for external events – Screening, version 1.0.1*
*ww edition #5501*
Rijkswaterstaat, November 2017
**(see Rijkswaterstaat Werkwijzer (manual) for prevailing version)**

[20] *Guidelines for quantitative analysis of lightning risk, version 2.0.2*
*ww edition #5534*
Rijkswaterstaat, November 2017
**(see Rijkswaterstaat Werkwijzer (manual) for prevailing version)**

[21] *Guidelines for External Event – Fire, version 1.0.1*
*ww edition #5502*
Rijkswaterstaat, November 2017
**(see Rijkswaterstaat Werkwijzer (manual) for prevailing version)**

[22] *Guidelines for quantification of collision risk, version 1.0.1*
*ww edition #5555*
Rijkswaterstaat, November 2017
**(see Rijkswaterstaat Werkwijzer (manual) for prevailing version)**

[23] *Guidelines for Basic Model for Spare Parts, version 1.0.1*
*ww edition #5534*
Rijkswaterstaat, November 2017
**(see Rijkswaterstaat Werkwijzer (manual) for prevailing version)**

[24] *NBL Nationwide bridges and locks – frameworks for operation and control of movable objects, Release 3.1*
ww framework #1334
Rijkswaterstaat, September 2016

[25] NEN-EN-ISO 9000
*Quality management system*
Netherlands Institute of Standardization (NEN), October 2015

[26] NEN-ISO 55000
*Asset management*
Netherlands Institute of Standardization (NEN), February 2014

[27] *Guidelines for Reliability and Availability Verification Method*
*ww edition #1567*
Rijkswaterstaat, November 2017
**(see Rijkswaterstaat Werkwijzer (manual) for prevailing version)**

# Appendix A: Terms and definitions

**Area**: the aggregate of subsystems in Rijkswaterstaat's three networks (HWN, HVWN and HWS): roads, waterways, bridges, locks, viaducts, weirs, pumping stations, flood defence systems, etc.

**Aspect:** specific characteristic of a system (or system yet to be developed).

**Aspect requirement**: describes the precondition subject to which a system is to fulfil its functions. Examples include: reliability, availability, maintainability and safety.

**Asset management:** systematic and coordinated activities and procedures employed by Rijkswaterstaat for the optimal and sustainable management of its networks and the associated performance, risks and life-cycle costs, in order to fulfil the agreements made with the Ministry of Infrastructure and Water Management.

**Availability** has two definitions:
1. the expected fraction of the total time over which a system is functioning, under certain conditions.
2. the probability of a system functioning, under certain conditions, when it is put to use at a random juncture.

**Basic event:** the failure of a subsystem, with the subsystem not being broken down further to calculate the probability of failure.

**Capacity**: maximum quantity or maximum number that a system is capable of containing or supporting. In the case of Rijkswaterstaat, this refers to, for instance, the maximum number of vehicles or vessels that can move along a stretch of roadway/waterway per unit of time. Capacity is usually set out in functional requirements.

**CBM: condition-based maintenance.** This maintenance strategy entails one (or more) condition thresholds being measured and, based on this measurement, a decision being made to either wait until a subsequent measurement or carry out replacement or repair work. A well-known example is measuring car tyre tread.

**Condition threshold**: a measurable, physical characteristic of a component, which is a measure of the component's condition and, therefore, a measure of the probability that the component will fail within a specific period of time.

**CM: corrective maintenance.** This maintenance strategy entails waiting until the component fails, and it does not have any parameters. A well-known example is replacement of a car light.

**Common Cause Failure:** failure due to a common cause, causing correlation between components. This means that a component's probability of failure depends on the failure of another component. The component will fail due to a mechanism (cause) that could also lead to failure in the other component. Particularly in the case of redundancy, which entails two identical components

being capable of taking over each other's function, Common Cause Failure makes the (shared) probability of failure much higher than would be expected if the components were independent of one another.

**Common Mode Failure**: synonym of Common Cause Failure.

**Component**: hardware system element.

**Cut set:** minimum subset.

**Event tree:** graphic representation of the possible scenarios that can arise following a given initiating event. The purpose of an event tree is to calculate consequences. This graphic depiction is usually facilitated by software, which also calculates the probabilities of the different scenarios occurring.

**Failure**: an event, or a collection of events, that results in a system losing its function or no longer being capable of fulfilling its function (no longer satisfying the function requirement). The system is not said to have failed if the system cannot fulfil its function due to planned maintenance work or lack of capacity.

**Failure definition**: a recorded relationship between the failure of a function of a (sub)system and the consequences this has for the system's functioning. The record will comprise a failure definition (when the system or subsystem can be deemed to have failed) and the measures to be taken if the system has failed according to the agreement.

**Failure frequency:** the average number of times per unit of time that failure occurs. Also termed failure rate.

**Failure mechanism**: the way in which the system fails, such that it is no longer performing its function.

**Failure rate**: the average number of times per unit of time that failure occurs. Also termed failure frequency.

**Fault tree**: graphic representation of the relationship between the failure of system elements and the failure of the system, expressed by means of the Top Event. This graphic depiction is usually facilitated by software, which also calculates the probability or non-availability of the Top Event.

**FMEA**: *Failure mode and effect analysi*s. The FMEA is a method used to inventory a system's causes of failure in a structured way. This is done by systematically investigating the role of the system elements that the system comprises. Hence an FMEA reveals failure mechanisms.

**Function:** the intended function and/or actions of a system. A function is a task that is being performed. Systems exist because they perform functions.

**Functional requirement**: primary requirement set for the function. This provides the answer to the question 'what does the system have to be capable of doing?' A functional requirement predominantly pertains to the capacity a system is required to provide in fulfilling the function.

**Functional test:** testing the operation of a system's function.

**Interface requirement**: requirement set for a system that results from an interface analysis. Such an analysis inventories the requirements that the system's environment sets for the system.

**Management**: the aggregate of activities aimed at enabling a system to fulfil its function satisfactorily over the course of its life cycle. This pertains in particular to the organizational aspects: performing maintenance, ensuring the correct operating procedures, etc.

**Maintainability:** probability that a system or system element can be repaired, inspected or subjected to preventive maintenance within a specific period of time, under certain conditions. In practice, maintainability is often also regarded as the length of the interval itself within which maintenance work can be carried out.

**Maintenance:** physical activities geared towards enabling a system to fulfil its function satisfactorily over the course of its life cycle.

**Maintenance analysis:** analysis used to determine a component's optimum maintenance strategy, including the accompanying parameters. This analysis is pretty much always based on life cycle costs (LCC) and results in CM, PM or CBM.

**MP:** maintenance plan.

**Minimum subset:** a minimum set of system elements which, if they all fail, will result in failure of the system (or a primary function of the system). If the set comprises a single system element, failure of that system element is termed a 'single point of failure'. If the set consists of two system elements, this is termed 'second-order cut set', etc.

**MTBF:** *mean time between failures*, the average lifespan. This is the same as the MTTF for a new system element.

**MTTF:** *mean time to failure*, the average time to failure from the time of assessment.

**Network:** aggregate of interconnected objects that collectively fulfil a function. Rijkswaterstaat has three networks: the main road network (HWN), the main waterways network (HVWN) and the main water system (HWS). The first two networks have a single function: to make it possible to get from A to B, by road or on water. The main water system has multiple (primary) functions: ensuring sufficient water, ensuring clean water and safely retaining water.

**Object:** individually identifiable part of a network with a specific function, e.g. tunnels, locks, weirs, bridges, viaducts, sound barriers. There is considerable overlap with the term structure, but sections of waterways, road sections and parts of structures are also referred to as objects.

**Operational maintenance**: maintenance geared towards maintaining an object's condition. This includes conserving, washing, cleaning, lubricating, greasing, topping up, draining, replenishing, ventilating, minor servicing (gear box), minor replacements (connecting terminals), etc.

**Operational reliability:** synonym of reliability.

**ORA:** object risk analysis. This term has been chosen to make it clear that this is about a risk analysis of a physical system, an object. This is to distinguish it from

risk analysis applied to a process, as is done in the case of risk management.

**PDCA cycle:** Plan, Do, Check, Act quality cycle (developed by the American statistician William Deming), used to describe activities geared towards effecting improvements within organizations.

**Performance**: efficiency of a system; indicating how well the system works. Sometimes specifically in terms of reliability and/or availability.

**Performance analysis:** an analysis of a system's performance, in terms of reliability and/or availability, and focusing on the primary functions that the system is required to perform. In practice, performance analysis is synonymous with reliability or availability analysis.

**Performance requirements:** requirements set for the primary function(s) of an object, in terms of *RAMSSHE€P.* Sometimes specifically quantitative reliability and availability requirements.

**Plateau level:** the level reached by an organization and/or object once a systematic and fully stabilized form of risk-based management and maintenance is applied, allowing the demonstrable fulfilment of the performance requirements at any time.

**Planned maintenance:** work on a system that is known about in advance. This usually pertains to maintenance work that limits the system's functioning and affects availability. Because the planned non-availability of the system is known in advance to that system's users, those users are in a position to mitigate the consequences, considerably reducing their perceived severity in comparison to the counterpart of planned maintenance: unplanned maintenance.

**PM: Preventive Maintenance**. This maintenance strategy entails a component being replaced after a certain calendar time, period of use or number of times being put into use. There is one parameter for this form of maintenance: the replacement interval. A well-known example is replacement of the cam belt in a car's engine.

**Probability of failure**: probability of a system's function failing, with failure being defined as part of a failure definition.

**Qualitative ORA:** calculating probabilities and consequences of undesired events based on experience and expert opinion, with both the probabilities and the consequences being categorized instead of points values.

**Quantitative ORA**: calculating the probability of a single consequence (the Top Event) based on numerical data and mathematical analyses, with the result being a points value for both probability and severity/consequence. There are two important quantitative methods for calculating probability: the '*structural analysis*' and the '*systems analysis*'. A *structural analysis* proceeds from a model of the actual situation in which the input comprises statistical quantities: stochastic functions. A *systems analysis* proceeds from system elements whose failure context is a known quantity in statistical terms. Reliability and availability analyses, as described in this document, are based on systems analysis.

**RASCI tables**: matrix to depict the relationship between people's roles, tasks and authorizations.

**RAMSSHE€P**: acronym for:
R: reliability;
A: availability;
M: maintainability;
S: safety;
S: security;
H: health;
E: environment;
€: economics;
P: politics.

**Recovery time:** the period of time between the point at which a fault is noticed and the point at which the failed component is given the all-clear for use.

**Redundancy:** using multiple system components to ensure that the aggregate continues to function properly if one or more components fail.

**Reliability**: the probability of a system fulfilling its function over a specific period without failing, under certain conditions.

**Risk-based Asset Management**: a risk-based method of managing and maintaining objects that can be used to demonstrate that a set performance requirement is being satisfied, in line with the approach presented in this document.

**Risk:** probability that an undesired event will occur, 'multiplied' by the 'consequence' of that event. If the consequence is quantifiable, this could actually be a multiplication. The result will then be the expectational score of the consequence.

**Risk analysis:** a consideration of the probability and the consequences of an undesired event. See qualitative and quantitative ORA.

**Risk-based*:*** performance of a risk-based activity is aimed at reducing the probability of an undesired event, or at reducing the severity of the effects of the undesired event. The more the undesired event threatens the performance to be attained by the system, the more control is applied. A risk-based approach therefore focuses primarily on the biggest performance threats.

**Root cause analysis (RCA):** a method used to establish the underlying causes of faults or problems. A cause is termed a root cause if remedying it would definitely eliminate the fault or definitely solve the problem.

**Safety:** the probability that the system will not cause human casualties (injuries, fatalities) over a particular period of time. If a system will only cause harm in the event of it failing, this is termed reliability. The probability of flooding due to heavy rainfall with no risk of human casualties arising is often referred to in common parlance as safety, but it is in fact a matter of reliability. A more reliable system will discharge the water rapidly, resulting in less frequent flooding, whereas an unreliable system will result in frequent flooding.

**Semi-quantitative:** using categories or orders of magnitude.

**Single point of failure**: a single part of a system which, if it fails, will result in the system's function failing.

**SOM**: standard operational maintenance, also referred to as regular maintenance.

**Structure:** civil engineering structure, non-residential. The term is used solely for structures found in infrastructure. A road is not a structure, but a bridge is. A river, or a section of canal, is not a structure, but a weir or lock is.

**Subfunction**: a subfunction is part of a function performed by a subsystem. The operating mechanism of a movable bridge is a subsystem of a movable bridge. The subfunction is making the bridge deck move.

**Subsystem**: part of a system. Within the context of the bigger picture, these are also referred to as system elements.

**System:** coherent aggregate of (physical) parts intended to fulfil a certain function. In other words: a discernible, interrelated collection of elements within the aggregate that is dependent on the set objective.
RWS 's networks are systems, but so are their components. Each system is part of a larger entity, making it actually a subsystem. Where the boundaries of the system are drawn will therefore be context-dependent. Rijkswaterstaat draws the boundaries at its primary systems: the main road network (HWN), the main waterways network (HVWN) and the main water system (HWS).

**System element:** smallest unit of a system for which the internal structure and relationships are no longer considered.

**System requirement:** all requirements set for the system. The functional requirements, the aspect requirements and the interface requirements are collectively referred to as 'the requirements' at Rijkswaterstaat. For the purposes of recognizability, we have opted for the distinguishing term system requirement. The most important sources for a system requirement are: the functional analysis, the aspect analysis and the interface analysis. These analyses produce functional requirements, aspect requirements and interface requirements, respectively.

**Top Event:** loss or partial loss of a system function. The top event is the event of which probability is calculated in a quantitative risk analysis. Usually this pertains to failure of the system's primary functions, such as retaining water, allowing vessels to pass through, allowing road traffic to pass through, discharging water, etc.

**Undesired event:** event that can contribute to the failure of a system function: the top event.

**Unplanned maintenance:** work on a system that is unexpectedly necessary and cannot therefore be known about in advance. This always pertains to unexpected faults that limit the functioning of the system. They determine the system's reliability and affect the system's availability. Because system limitation occurs unexpectedly, users of the system are not able to mitigate the consequences. The unexpected nature often gives rise to additional annoyance. For that reason, this form of non-availability is perceived to be far more serious than its counterpart: planned maintenance.

This is an issue of

Rijkswaterstaat

www.rijkswaterstaat.nl
0800 - 8002

March 2018