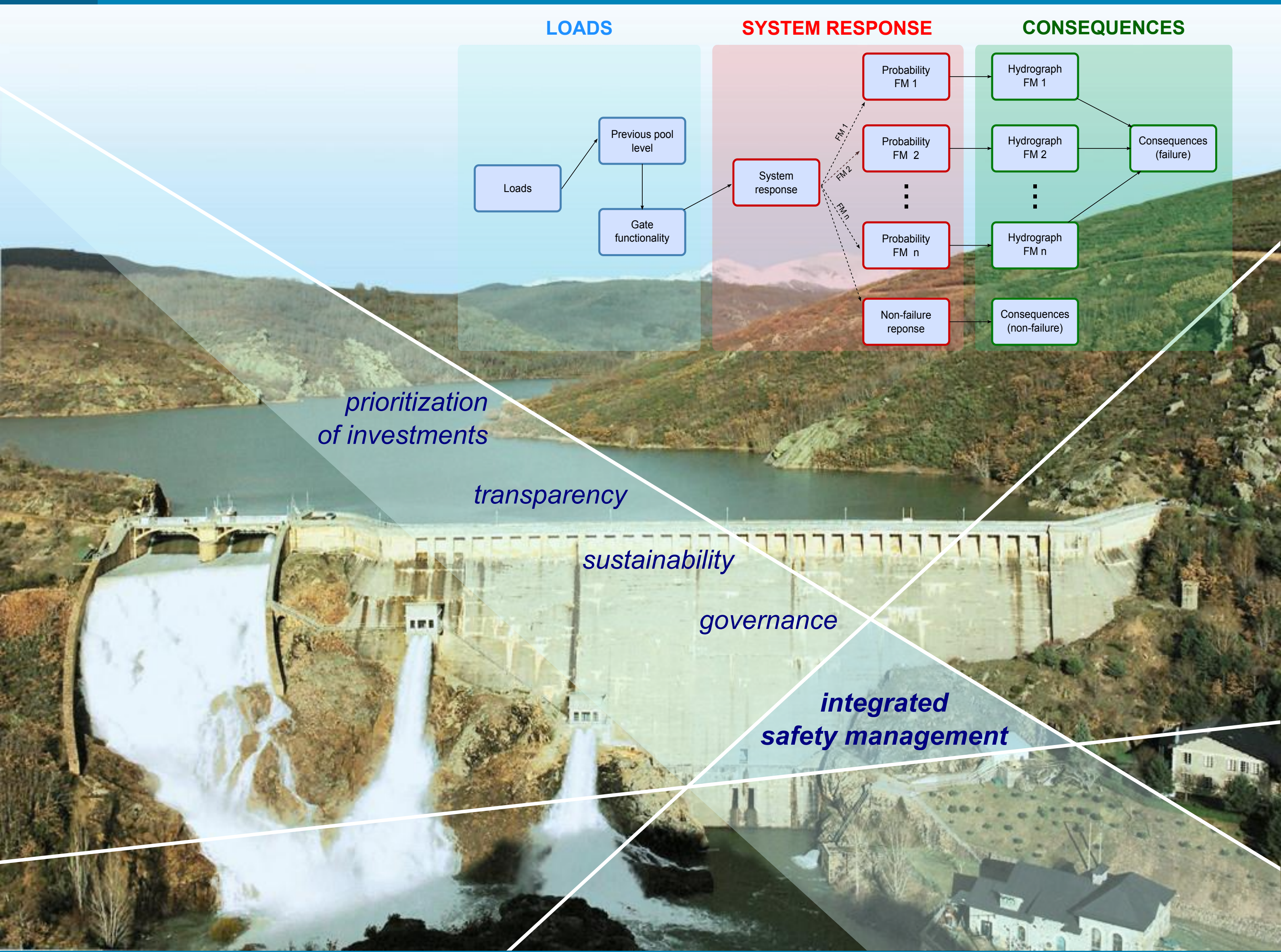
P - 8

TECHNICAL GUIDES ON DAM SAFETY

TECHNICAL GUIDE ON OPERATION OF DAMS AND RESERVOIRS
VOLUME 1

RISK ANALYSIS APPLIED TO MANAGEMENT OF DAM SAFETY



PROFESSIONAL ASSOCIATION OF CIVIL ENGINEERS

SPANCOLD CNEGP

SPANISH NATIONAL COMMITTEE ON LARGE DAMS v2 - 12/12/2012

P - 8

TECHNICAL GUIDES ON DAM SAFETY

TECHNICAL GUIDE ON OPERATION OF DAMS AND RESERVOIRS

VOL. 1

RISK ANALYSIS APPLIED TO MANAGEMENT OF DAM SAFETY

PROFESSIONAL ASSOCIATION
OF CIVIL ENGINEERS

CNEGP
SPANCOLD

SPANISH NATIONAL
COMMITTEE ON LARGE DAMS

Cover photo: Requejada dam
Translation by Universidad Politécnica de Valencia and iPresas (spin-off UPV)

Presentation

The legal framework defining the general aspects and criteria on Dam Safety in Spain is under the responsibility of the *Ministerio de Agricultura, Alimentación y Medio Ambiente (MAGRAMA)* through the *Secretaría de Estado de Medio Ambiente* and the *Dirección General del Agua*.

Development of this legal framework started in 1967 with the *"Instrucción para el Proyecto, Construcción y Explotación de Grandes Presas"*, which has been active througout the time of greater activity in design and construction of dams, and which even today is in force.

On 1996, the *"Reglamento Técnico sobre Seguridad de Presas y Embalses"* was approved, updating dam safety concepts and criteria which had evolved significantly since the publication of the *Instrucción*. This *Reglamento*, which impinges more specifically on topics related to safety, has had a partial application, though progressive thanks to its global focus on safety.

The overlap in application of both legal documents (*Instrucción* and *Reglamento*) and the need to have a single legal body in dam safety has lead MAGRAMA to write the *Normas Técnicas de Seguridad (NTS)*, presently pending approval.

On the other hand, Dam Safety Technical Guides, written by working groups composed of experienced professionals in the field, have been edited by the Spanish National Committee (SPANCOLD) of the International Commission On Large Dams (ICOLD) with collaboration of the Spanish Professional Association of Civil Engineers (CICCP). They present the state of the art in several issues relative to dam safety, offering guidelines to evaluate and achieve the safety goals set in legal documents. Therefore, they are a reference for technological development of normative criteria and are used by dam professionals both inside and outside of Spain.

The collection of technical guides published by SPANCOLD since 1997 is:

1. Dam Safety *(Compendium of legal requirements)*
2. Guidelines for Projects of Dams and Appurtenant Structures
    1. Concrete Dams *(The update of the part corresponding to Roller Compacted Concrete (RCC) has been recently edited and an English version was distributed in the International Symposium on RCC Dams, Zaragoza, 2012.)*
    2. Embankment Dams *(To be edited in 2013)*

3. Geological - Geotechnical Studies
4. Design Flood
5. Spillways and Outlet Works
6. Construction of Dams and Quality Control
7. Monitoring of Dams and their Foundations
8. Operation of Dams and Reservoirs. *Currently under development. It will be composed of three volumes, the first one being the present document:*
    1. **Risk Analysis applied to Management of Dam Safety**
9. Environmental Issues *(To be edited in 2013)*

This document presents the current state of the art in Risk Analysis, which has emerged as a very useful tool in dam management. Its methodology can be an aid to the governance of these important facilities, contributing guidelines, foundations, references and national and international examples with which to implant integral safety management systems.

Owners, administrations, regulators, consultants, users, civil protection services and all type of related entities and agents are here presented with a body of knowledge which is specially useful in the justification and prioritization of investments, inspired by the principles of transparency and sustainability. Therefore, this Technical Guide can answer and complement current legislation without, in any case, substituting it or substituting engineering good practices.

Finally, I'd like to express my gratitude to *Ministerio de Agricultura, Alimentación y Medio Ambiente*, to the SPANCOLD's Safety Technical Committee and to the working group which has written this monograph.

José Polimón

President of the Spanish National Committee On Large Dams (SPANCOLD)

Foreword

The edition of the present Monograph by the Spanish National Committee on Large Dams (SPANCOLD) has been possible thanks to the development of project BIA 2006-08948 funded by the Spanish Ministry of Science and Innovation.

This project, named "Application of Risk Analysis to Programs of Conservation, Maintenance, Rehabilitation and Safety Management of Dams and Reservoirs", is part of the National R&D Plan 2004-2007 and was assigned in December 2006 to Universidad Politécnica of Valencia (UPV) with Dr. Ignacio Escuder Bueno acting as Principal Investigator.

The project has benefited from the participation of SPANCOLD as Observing Promoting Entity. The Monograph has been coordinated by the Technical Committee of Dam Safety of SPANCOLD, chaired by Dr. Arturo Gil García and with the efficient contribution of its secretary, Dr. Eduardo Rojo Martínez.

The main source of this text is a chapter from Dr. Armando Serrano Lombillo's Doctoral Thesis called "Development of a Complete Tool of Risk Analysis and Assessment in Dam Safety" that reviews the state-of-the-art within the mentioned field. Dr. Serrano's Thesis was directed by Dr. Ignacio Escuder and Dr. Manuel Gómez de Membrillera Ortuño, defended in March 2011 and funded by the aforementioned project BIA 2006-08948.

The guiding theme of the present document is the design and implementation of risk models to analyze, assess and manage dam safety. Indeed, with risk analysis applications growing worldwide, there is an increasing need to structure the available information from both a theoretical and a practical point of view. Hence, this Monograph intends to act as a structured guide for the reader, based on more than 100 scientific references, techniques and practices published during the last years in the field of risk analysis applied to dam safety. In this perspective, the works developed within the scope of the Duero River Authority under the direction of Liana Ardiles López and Daniel Sanz Jiménez allowed the creation of a reference corpus that constitutes one of the most complete and best-documented examples in the field at an international level.

This Monograph is based on the aforementioned works and is the result of the enrichment and update of the original text with:

- The discussions with the members of the Technical Committee of Dam Safety of SPANCOLD and their continuous contributions.

- The enriching practical experiences published by different infrastructure owners throughout Spain (Duero River Authority, Ministry of the Environment, Rural and Marine Areas, Catalonian Water Agency, Iberdrola) since 2008.
- Several recent references to the best international practices in the field, as the ones presented during the Third International Forum on Risk Analysis, Dam Safety and Critical Infrastructure Management, held in Valencia in October 2011 and organized by UPV jointly with the Department of Homeland Security of the United States (DHS, USA).

Thanks to all of you who have made it possible.

Contents

Part I

Chapters

Chapter 1

Introduction

Since the failure of Teton dam (USA) in 1976, there has been a significant evolution in the understanding of floods, dams and other critical infrastructures on which modern society and people's wellbeing rely.

Today, society demands an increase in the safety and reliability levels of such infrastructures considered as essential. The only way to respond positively to these expectations is to integrate dam's design, construction and operation in a framework of risk management that ensures the effective mitigations of both natural and anthropic threats. Consequently, global strategies of risk management have gained much importance during the last years and efforts carried out to implement them include already and systematically aspects such as sustainability, resilience and public participation.

In this context, Risk Analysis has meant a paradigm shift which has allowed us to advance in the evaluation and management of flooding risks, as well as all other risks which can, after all, affect people, the environment and human development.

The European Directive on Floods of 2007 (2007/60/CE) or the European Directive of Protection of Critical Infrastructures of 2008 (208/114/CE) reflects this change. In the United States, the U.S. Army Corps of Engineers (USACE) along with the Federal Energy Regulatory Commission (FERC) started their own process of dam safety based on risk information in 2005, following the trend started by the Bureau of Reclamation (USBR) during the second half of the 1990's. Meanwhile, in other countries such as France, specific laws were promulgated (2008) to carry out the same process at a national level.

These international practices and regulations acknowledge risk analysis utility and exhort modern countries explicitly to employ risk analysis as an indispensable management tool. This aims at reinforcing risk management processes throughout the improvement of natural phenomena forecast, the adequate operation and maintenance of critical infrastructures or the establishment of a good praxis able to minimize the impacts on the environment and the population.

In the specific field of dam and reservoir safety, the understanding and acknowledgment of the different risk factors present in the activities related to safety constitute the conceptual basis required to elaborate logical systems or models to inform safety decision-making. For instance, the Spanish Regulations of the Hydraulic Public Domain (RD January 16th 2008) state the need to contemplate risk management as an essential element on Dams Safety, following the example of some of the most developed countries in the world.

However, until very recently, dams and reservoir safety had focused almost exclusively on the structure or the civil works and this, with an eminently determinist approach. In this respect, risks were controlled through the respect of certain rules and practices sanctioned by experience, as well as by checking safety factors that were understood as conservative measures of prudence. This approach systematically ignored the consequences ensuing dam failure, which constitute the second component of risk.

In Spain, the effective acknowledgment at a legal level of the double nature of flood risk did not occur until 1995, with the publication of the "Basic Directive on Planning of Civil Protection against Flood Risk" (BOE February 14th 1995).

The transcendence of this regulation lies on the explicit acknowledgment of the component *consequences* as a determining factor of flood risk. Besides, the mentioned Directive is of particular importance since it established the compulsory character of writing and implementing Safety Emergency Plans of Dams for those dams that had been previously classified as "A" or "B" in relation to their *potential risk*.

Beyond the importance accorded to the consequences of the flood, the Directive of 1995 imposed on the dam owners new duties related to the global understanding of risk. If until the 1990's dams owners dealt fundamentally with the management of the structures' response against adverse loads (respecting the codes in place such as the Instruction for the Project of Construction and Operation of Large Dams of 1967), in 1995 they were made responsible for the management of the consequences component through the obligation of writing and implementing Emergency Plans.

The Technical Code of Dams and Reservoirs Safety of 1996, also echoing this reality, included all the prescriptions promulgated the previous year in the Directive and contained in the scope of a Dam Emergency Plan. This marked an important step forward by establishing that dam safety actions should be guided by *potential* risk.

Beyond the legal context at a Spanish, European or international level, a series of practical conditions have contributed to the development of risks analysis over the last 15 years begetting a modern, efficient and transparent management of dam safety. These conditions include:

- The first time inclusion of dam owners' *public liability* in the different regulations joined to the social demand for higher safety levels and for justification of the use of private and public funds.

- The need to prioritize corrective actions to achieve the greatest and quickest possible risk reduction.

- The need to optimize the water resources system management as well as to increase their regulation capacity to respond to important challenges such as Climate Change and its manifestation as severe droughts or severe floods.
- The difficulty of building new structures mainly due to social and environmental reasons, that will predictably make necessary to extend the operational phase of the existing structures beyond their originally planned useful life.
- The aging of the existing dams (most of the structures are over 30 years old and, an important percentage of them have been operated for more than 50 years), along with the differences in the engineering knowledge of today with regard to when they were designed and built.

As it will emerge from the present Monograph, all this has resulted in a continuous investment in research and development (e.g., continuous improvements of the estimations and the uncertainty analysis, software development, etc.). Thus, it can be said that the analysis, evaluation and management of risk requires uninterrupted training and research. The work developed herein constitutes an example of the social benefits of the investment in research, development and innovation.

The coexistence between the standards (codes) of safety and risk analysis techniques is not only beneficial but also necessary to ensure an effective aid to decision-making. This is why this coexistence is at the core of the elaboration of risk models like the ones presented in this document.

Some of the advantages (and challenges) introduced by risk analysis into dam safety management are summarized as follows:

- Incorporation of the different agents (civil protection, administrations, etc.) in the process, essentially in the tasks regarding the estimation of consequences and in some cases, within the estimation of loads (dam operators of other dams of the system, etc.). This allows every relevant person to feel engaged and integrated in the process.
- Sustaining risk analysis as an ongoing living process over time.
- Identification of the most effective and better-justified measures of risk mitigation.
- Promotion and adoption of clear procedures to carry out risk analysis as well as tolerability guidelines that would inspire risk evaluation and decision-making.

With all this in mind, the content of the present Monograph aims at consolidating the most updated information on the best international practices of risk analysis, assessment and management in the field of dam safety. Additionally, it does not renounce to a didactic component that is achieved thanks to the inclusion of a first chapter *Glossary*, the repeated *application cases* interspersed along the text and the four *Appendixes* of an eminently practical character that complete the document.

Finally, a chronologically ordered reading of the whole of the contributions of the River Duero Authority [47, 46, 12, 9, 10, 111, 8, 11, 112, 114, 105, 113, 51, 52] is suggested. These documents can help consolidating all the aspects developed in the text and allow the reader to visualize the complete process of implementation of risk analysis tools and their practical utilities in a structured and complete way, according to the best international practices.

Chapter 2

Glossary

Risk. *Risk* is the combination of three concepts: what can happen, how likely it is to happen and which are its consequences [80]. In Risk Analysis applied to dam safety, *what can happen* refers to dam failure (see definition of failure mode). El *How likely it is to happen* is the combination of the probability of occurrence of certain loads and the conditional failure probability of the dam given those loads (see definition of failure). Finally, the *consequences* are the facts resulting from the failure of the dam, including economic consequences and loss of life among others (see definition of consequences).

There are several forms of representing risk (see definitions of graph FN and fN). However, on some occasions it is useful to reduce the three former concepts to just one figure by using the product of failure probability times its consequences[1]. When the consequences are loss of life, this risk is also known as *annualized loss of life* or *social risk*. As opposed to the latter, there is the concept of *individual risk*, which is the probability that at least one person dies and that, sometimes, is supposed equal to the failure probability of the dam.

There are different types of risk:

Total risk. It is the total risk of flooding downstream of the dam. It is produced by both the cases in which the dam fails and the ones it does not. Conceptually, it can be apprehended as:

$$R_T = \sum p(l) \cdot \left[p(f|l) \cdot C(l,f) + p(nf|l) \cdot C(l,nf) \right]$$

where $p(l)$ is the probability that certain loads may occur, $p(f|l)$ is the conditional probability of failure given those loads, $C(l,f)$ are the consequences in case of failure, $p(nf|l)$ is the probability of non-failure and $C(l,nf)$ are the consequences of non-failure.

Risk of failure. It is the part of total risk due to the dam break:

$$R_f = \sum p(l) \cdot p(f|l) \cdot C(l,f)$$

[1] In a more formal way, the extended integral to all the potential consequences events times their probability of occurrence.

Risk of non-failure. It concerns the situations of downstream flooding when the dam has not failed:

$$R_{nf} = \sum p(l) \cdot p(nf|l) \cdot C(l, nf)$$

Incremental risk. It is the part of risk exclusively due to the dam failure. It is obtained by subtracting from the consequences of the dam failure the ones that would have happen anyway, that is, even if the dam had not failed:

$$R_{\Delta} = \sum p(l) \cdot p(f|l) \cdot C_{\Delta}(l, f) = \sum p(l) \cdot p(f|l) \cdot [C(l, f) - C(l, nf]$$

where $C_{\Delta}(l, f)$ are the incremental consequences.

Failure probability. Within the scope of Risk Analysis applied to dam safety, the concept *failure* is not limited exclusively to the catastrophic breakage of the dam but includes any event that might produce adverse consequences. In this sense, the terms failure and breakage are interchangeable in this document, which gives them a broader sense. Conceptually, the *failure probability* of a dam can be defined through the following equation:

$$p(f) = \sum p(l) \cdot p(f|l)$$

As the equation reflects, failure probability has two components: one corresponding to the *loads* ($p(l)$) and one corresponding to the *response of the system* ($p(f|l)$).

Risk Analysis methodology is not limited in its approach to one single failure mode but instead it studies all the possible ways in which a dam could fail. Each of them is called *failure mode* (see definition below). Thus, the total failure probability is the sum of the probabilities of each failure mode.

Additionally, in Risk Analysis the term probability is used with two meanings [13], depending on the type of uncertainty they deal with (see also definition of uncertainty below):

Objective probability. It is the observed frequency of events that happen randomly. This probability is related to random or natural uncertainty.

Subjective probability. It is the degree of confidence in a result based on the available information. This probability is related to epistemological uncertainty.

In practice, it is usual to find both types of uncertainty simultaneously in the definition of a variable. An example of observed frequency will be the probability that certain flood takes place obtained from a distribution of annual exceedance probabilities. The conditional failure probability of a dam for a given situation can be an example of predominant subjective uncertainty. This probability is not intrinsic to the dam but it is based on the available information and on the perception engineers have of it. Consequently, this probability will vary as the knowledge of the dam increases.

Finally, failure probability in Risk Analysis can be treated as an *annual* probability, that is, as the probability that in any given year the dam fails. This is due to the common use of annualized loads ($p(l)$ has units of 1/ year) and to the fact that the rest of probabilities are non-dimensional.

Consequences. Several adverse effects or *consequences* can ensue a dam failure:

Damage to people. In principle, apart from loss of life, damage to people could also consider other aspects such as people injured with different degrees of gravity. However, due to the difficulty of quantification of wounded numbers, quantitative analysis usually focuses only on the first aspect.

Direct economic damage Damage caused directly by the impact of the flood and the most visible type. It includes the cost associated with the damage suffered by the dam itself.

Indirect economic damage Damage happening after the event as a result of the interruption of the economy and other activities in the area.

Other damages. Related to environmental damage, social disturbing, loss of reputation, attachment to historical or cultural heritage, etc. All of these aspects are difficult to quantify thereby they are usually treated in a qualitative way.

As mentioned in the definition of risk, in Risk Analysis it is common practice to deal with *incremental consequences*. This means that in case of a flood arriving and the dam failing, only the additional consequences due to the dam failure are considered and not those that would have also taken place if the dam had not failed (in other words, only the consequences of the flood itself are considered). For the purposes of calculation, this means that it is necessary to perform the calculation of consequences for both cases of failure and non-failure, then obtaining the incremental consequences through the subtraction of both results.

Section 5.9 outlines consequences with more detail and presents a summary with the different existing methodologies to estimate them.

Loading scenario. To obtain the risk associated with a dam, the calculation is usually disaggregated into various scenarios, depending on the event that originates failure. For instance, a dam can fail when subjected to a flooding or to an earthquake, and it is convenient to do those calculations in a separate way, each situation being called loading scenario. The most common loading scenarios are [13]:

- Normal scenario
- Hydrological scenario

- Seismic scenario
- Other scenarios

The hydrological and seismic scenarios deal with unusual events (*what can happen when a flood arrives? what can happen when an earthquake occurs?*) whereas a normal (or static) scenario deals with the normal situation of everyday, in which there is no flood or earthquake (*what can happen in a day-to-day situation?*). The category of *other scenarios* includes actions of sabotage, vandalism [44] or other situations that could not be included in the previous three categories. Theoretically, the combination of several loads (such as earthquake and flood) could also be studied but in practice, the probability of simultaneous occurrence is usually so small that its risk is negligible in comparison with the other risks.

Failure mode. A failure mode is the particular sequence of events that can cause failure or disrupt function of the dam-reservoir system or part of it. This series of events is associated with a determined loading scenario and has a logical sequence, which starts with a main initial triggering event, is followed by a chain of development or propagation events and culminates in dam failure.

Depending on the scope and the objective of the analysis, the definition of failure mode can be restricted to those implying a potential loss of life or can include any failure mode with the potential to induce uncontrolled flows and therefore cause damage of different kind (economic, to human life, etc.). It could even include any mechanism able to harm (even without the production of a spill), e.g., one with economic consequences due to loss of mission. In the same sense, the analysis of failure modes is not circumscribed to the embankment structures of a reservoir, but considers as well any element belonging to the system dam-reservoir.

The procedure to identify and describe failure modes is described in more detail in section 4.2.

fN graph. An fN graph is a way of representing risk. In this graph, the probability of failure is represented in the vertical axis (f) and its consequences are represented in the horizontal one (N). Thus, risk will be the dimension that combines both axes. In this way risk would be smaller in the lower left corner (orthogonal sense) and would grow towards the upper right corner. The diagonal lines in an orthogonal sense to the one depicted would be the iso-risk lines (lines made of combinations of equal risk value). Logarithmic scales are usually used in this kind of graphs.

One possible way of using these graphs is to represent the probability and the consequences of all possible events, or, in practical terms, of all the individual branches of the events tree (see definition of events tree further). Figure 2.1 is an example of this kind of representation, though for the purposes of risk evaluation it is usual not to represent all the pairs fN separately but to aggregate them by failure modes, loading scenarios or dam (figure 2.2). In order to represent this sum, the sum of all probabilities is taken in the vertical axis whereas in the horizontal one the weighted mean of the consequences is the used parameter. This one can be easily obtained by dividing the total annual risk by the total annual probability.

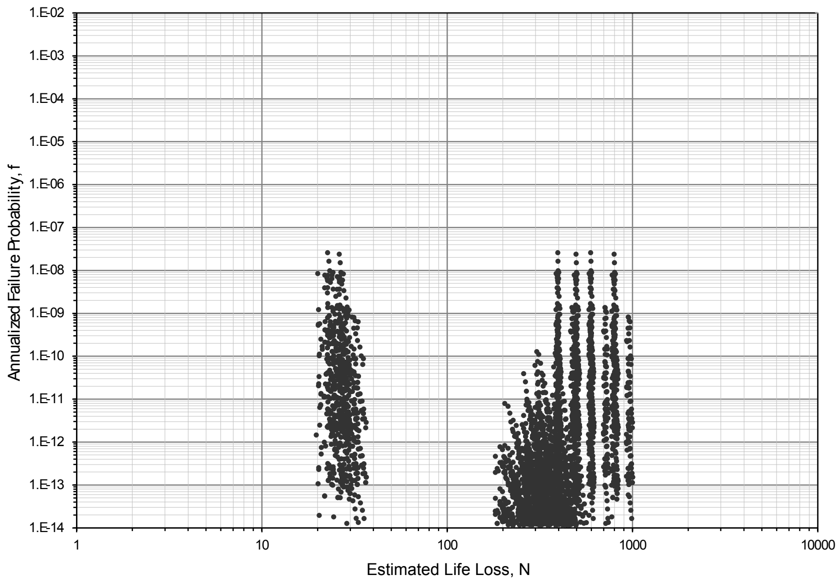


Figure 2.1: Example of representation of fN pairs.

FN graph. One of the most extended representations of risk is the FN graph, which is simply the cumulated form of fN graphs. In this way a curve is obtained instead of discreet points. In this curve, the horizontal axis represents the consequences (N) and the vertical axis the probability that these consequences (F) are exceeded. Figure 2.3 shows an example of an FN graph. As can be noticed, the curve decreases monotonically, since it is a cummulative distribution function. It is also usual to use double logarithmic scales when using theses graphs.

Despite their extended use, curves FN have some drawbacks such as a more difficult interpretation in comparison with the fN graphs (particularly for people not used to interpret them)[2] and that they may be an inconsistent form of fixing tolerability guidelines (see [53] for demonstration).

Event tree. An *event tree* is a representation of a logical model that includes all the possible chains of events resulting from an initiating event. As its name indicates it is based on the mathematical structure known as *tree* that is widely used in many other contexts. Figure 2.4 shows an example of tree along with the notation used to refer to its parts.

Each node of the tree represents an *event*. The root node is called *initiating event*. The branches that grow from an event represent the possible outcomes

[2]This drawback is not negligible when it comes to transmit the results of risk to the decision-makers.

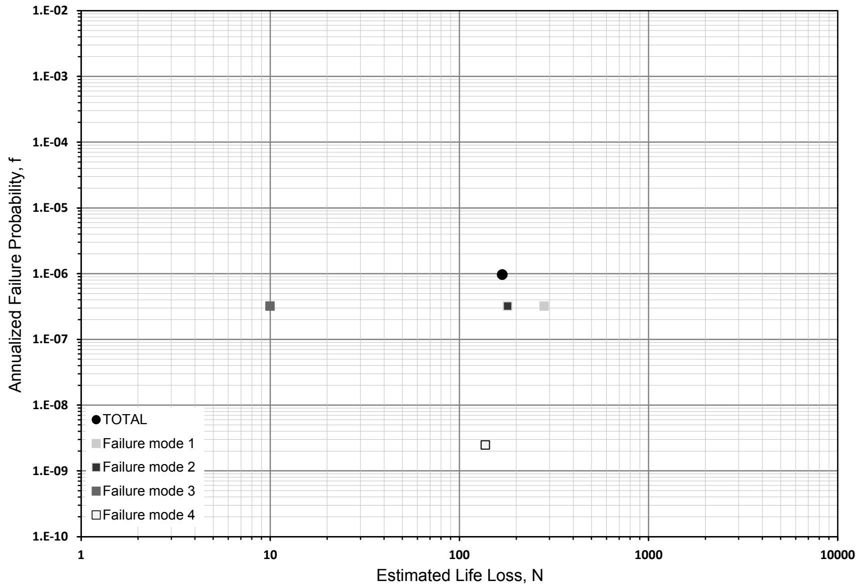


Figure 2.2: Example of fN graph.

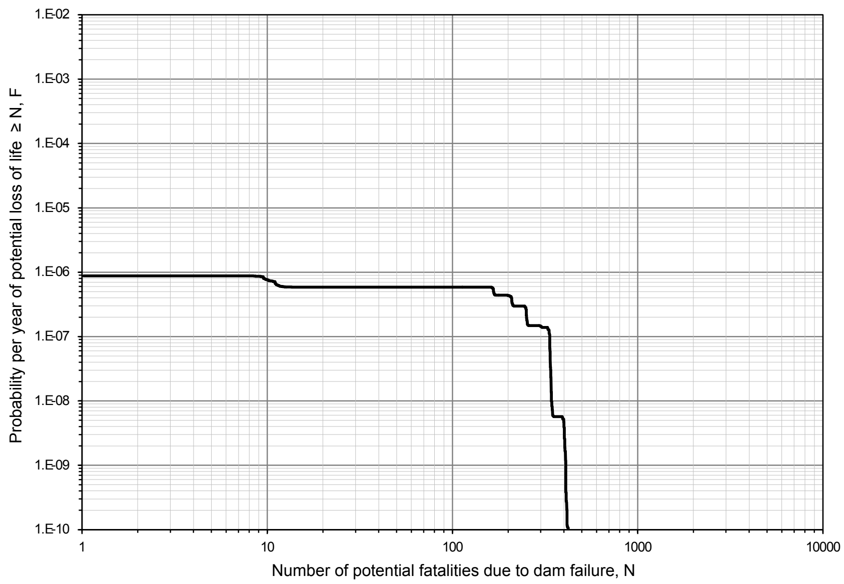


Figure 2.3: Example of FN graph.

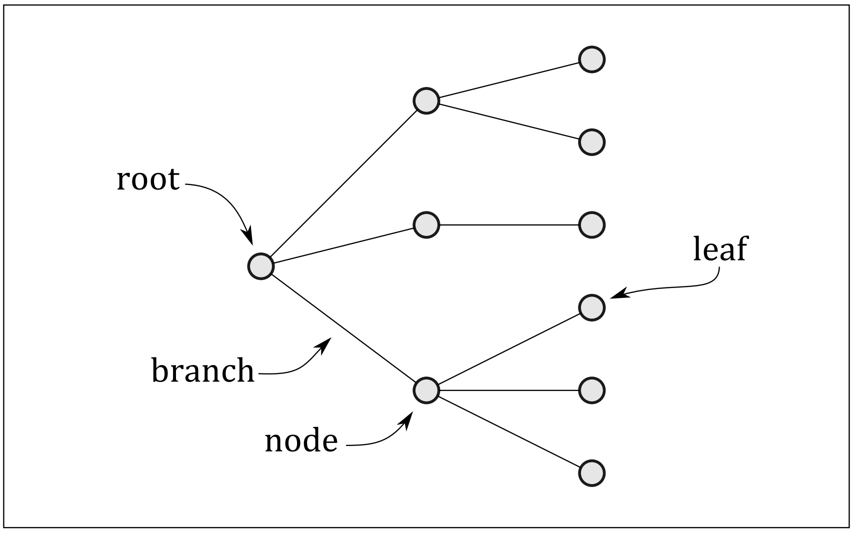


Figure 2.4: Example of tree.

of their event of origin. The branches must represent *mutually exclusive* and *collectively exhaustive* events so an event will always be reflected in one and only one branch. In this way, if a probability is assigned to each branch, the sum of all the probabilities arising from a node whatever will be 1.

Probabilities in event trees, except for the initiating event, are always conditional, that is, for any intermediate node it is assumed that all preceding events (parent nodes) have already happened. For example, figure 2.5 shows an event tree with two events: season and moment of the day. As it can be seen, the probabilities assigned to the second event (moment) are conditional to the season and therefore different in the sub-tree corresponding to summer and in the sub-tree corresponding to the winter.

Any path between the initiating node and each of the leaves of the tree represents one of the possible outcomes that might result from the original event. Thus, each of these chains will be unique and defined by the results of all the events that will have occurred in the tree (defined by the values that certain representative variables will have adopted). All of these values compose the fingerprint or signature that identifies each of the paths and is known as *pedigree*.

In order to calculate the probability of occurrence of one of the chains of events the conditional probabilities in the branch must be multiplied. Since the rule requires the branches from a same node to be mutually exclusive and collectively exhaustive, the sum of the probabilities of all of them must be one. Figure 2.6 illustrates this calculation of probabilities for the example shown previously. It can be checked that the global sum makes 1.

Influence diagram. The *influence diagrams* are compact conceptual representations of the logic of a system. On its most generic form, an influence diagram is any

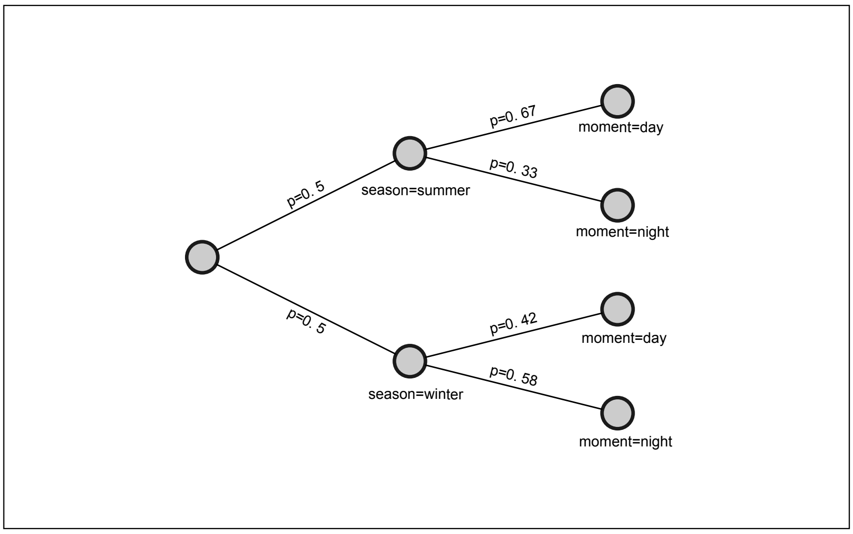


Figure 2.5: Example of an event tree showing seasonal events (summer/winter) and moment events (day/night) along with their conditional probabilities.

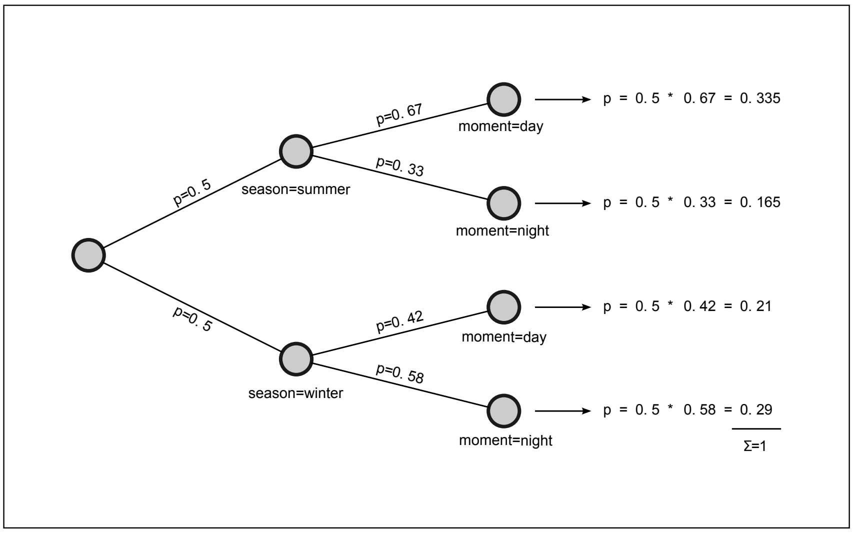


Figure 2.6: Calculation of the probabilities of all the possible chains of events for the example of figure 2.5.

representation including the relations between possible events, states of the environment, states of the system or subsystems, and consequences.

An influence diagram offers a visual representation of a risk model. Each variable of the system is represented as a node and each relation as a connector or arc. It is possible to build an event tree from an influence diagram in order to perform a calculation at a later stage [119].

Figure 2.7 shows an example of influence diagram. As it can be observed, the direction of the connectors indicates that the maximum pool level depends on the flood and on the previous pool level in the reservoir.

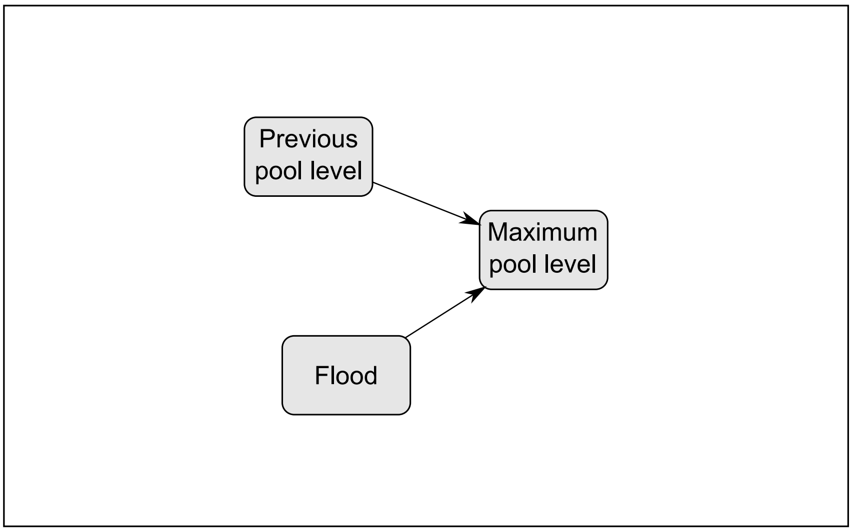


Figure 2.7: Example of influence diagram.

Finally, figure 2.8 shows an example of two representations (equivalent ones) of the same model, through a diagram of influence and through an event tree.

Fault tree. A *fault tree* is a top-down, deductive logical tool in which a major undesired event (failure) is postulated then analyzed systematically.

The goal of *Fault Tree Analysis* (FTA) is to develop all events or combination of events that might cause failure. These events can be of any nature: mechanical faults, human faults, external conditions, etc. The failure or undesirable event analyzed in the tree is called *top event* and it is drawn in the top part of the diagram. Under it, all the events that might induce the top event to happen are drawn. This is done successively until reaching the lowest level where the *basic events* (i.e., the ones that do not require further development) are found. Figure 2.9 shows an example of fault tree (see Appendix A for an explanation of symbols and notation).

A fault tree does not represent a physical system but the way failure can happen. For example, the fault tree of a gate does not require a representation of all the pieces of the device but it must include all the events that might lead

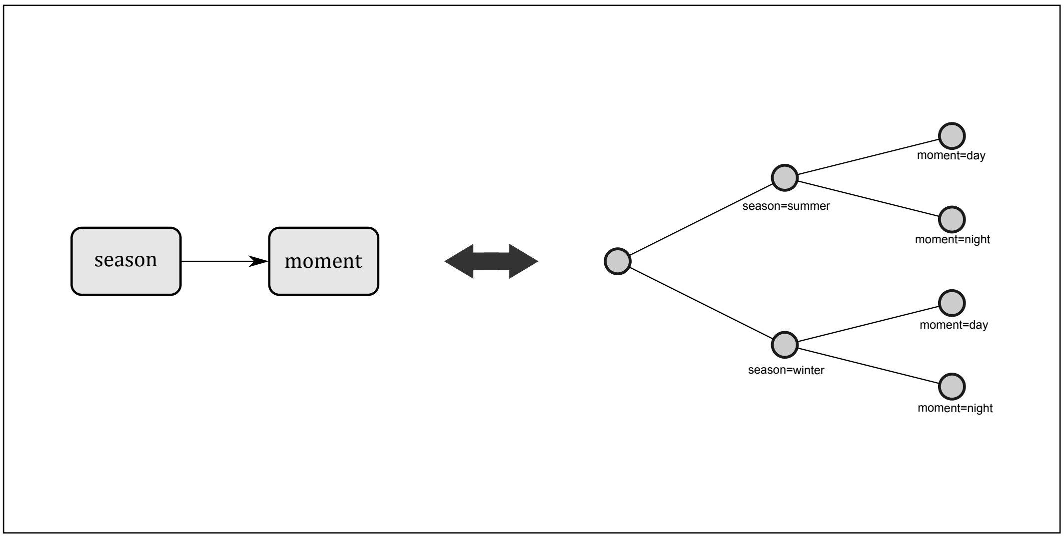


Figure 2.8: Correspondence between influence diagram (left) and event tree (right)

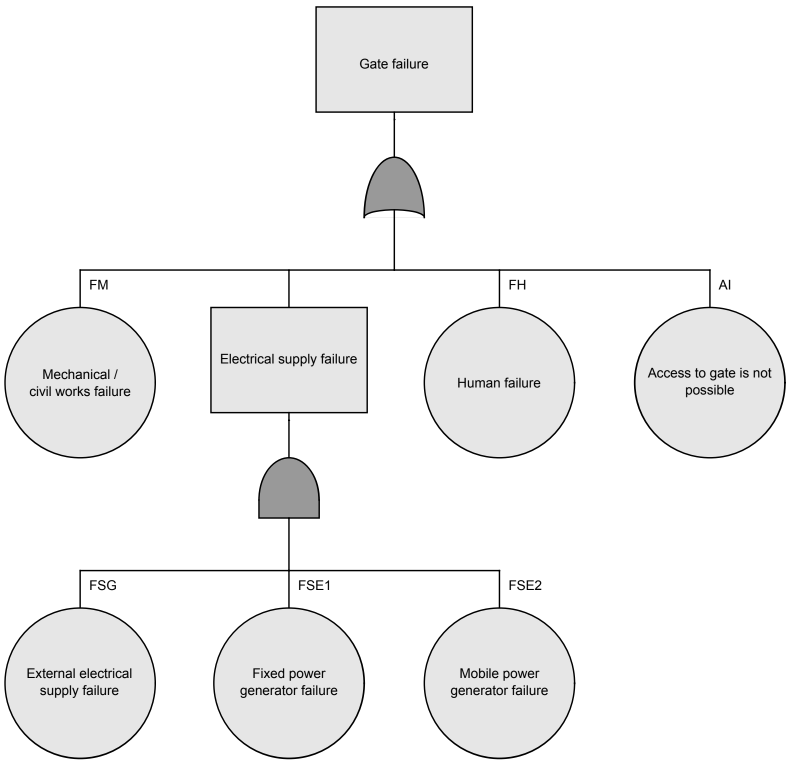


Figure 2.9: Example of fault tree.

to a dysfunction. Moreover, as any kind of model, fault trees can never aim at being totally exhaustive.

Each node of a fault tree represents a binary event (i.e., it can happen or not). For example, it considers a gate works or does not, there is electrical supply or there is not, a piston is broken or not, etc. Logic gates (AND gates, OR gates, etc.) relate events in between. Appendix A contains an explanation of the different types of nodes and logic gates found in a fault tree.

A fault tree can be used as a qualitative tool for analyzing the logic of a system. This means it is not necessary to assign any figure to the diagram for this to be useful. However, once the fault tree is developed, it is possible to obtain the probability of occurrence of the top event by assigning probabilities of occurrence to each individual event. Once the estimations of probability are assigned, the calculation of the probability of the top event is just an algebraic question easily automatized and calculated thanks to modern software.

Finally, a fault tree must not be mistaken for an event tree. Indeed, an event tree represents an inductive way of reasoning (from specific to general) that starts from a triggering event and evolves step by step, exploring all development possibilities until reaching failure. As opposed to it, a fault tree represents a deductive way of reasoning (from general to specific) where the starting point is a failure of the system and what is explored are all the possible causes that might have produced it. Thus, it could be stated that the main difference between both methods is the direction of the analysis: whereas the event tree is bottom-up, the fault tree is top-down. In practice, a combination of both methods is used: an event tree is drawn to represent the global risk model of a dam and a fault tree is done for estimating some of the probabilities of the former one (e.g., gates reliability).

Risk Evaluation. Risk evaluation is the process of evaluating the importance of the risk associated with the failure of a dam. The phase of risk evaluation is the point where judgments and values are (implicitly or explicitly) introduced in decision-making by including the notion of risk importance [34].

The *Health and Safety Executive* (HSE) [69] established as a basis for risk assessment the concepts of unacceptable risk, tolerable risk and broadly acceptable risk, concepts in which most of the international recommendations on tolerability are based.

- An *unacceptable risk* is one that cannot be accepted by society, whatever the benefits it might bring.
- A *tolerable risk* is one society is ready to live with in exchange of certain benefits as compensation. This risk is not considered negligible and therefore cannot be ignored. It has to be managed, periodically reviewed and reduced if possible.
- A *broadly acceptable risk* is in general one that can be considered as negligible and properly controlled. However, risks associated with dams fall

rarely into this category due to the huge destructive potential of this infrastructure.

The three concepts are illustrated in figure 2.10.

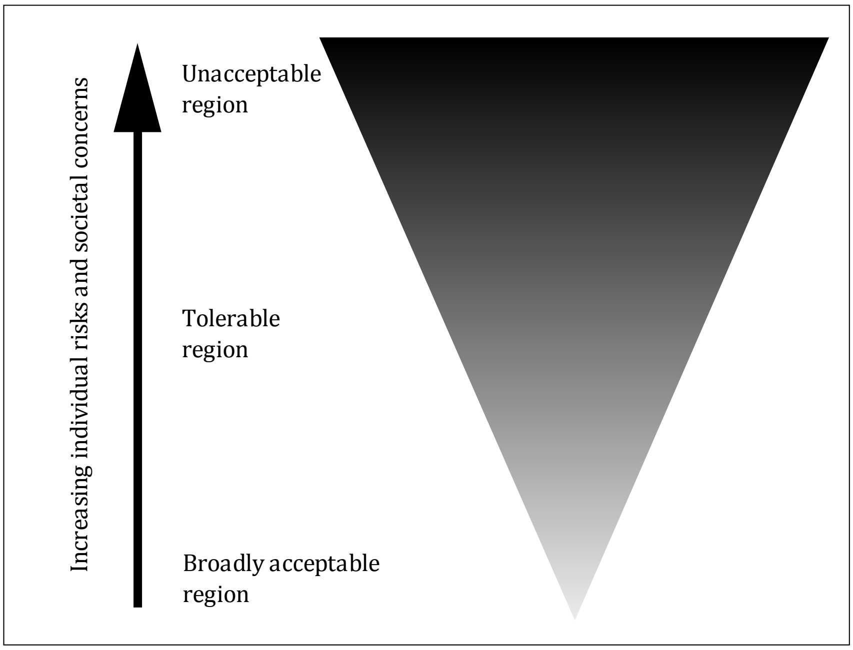


Figure 2.10: Framework of reference of the HSE for risk tolerability [69].

The criterion ALARP (*As low as reasonably practicable*) is a concept related to tolerable risks. It means that in order to accept a risk as tolerable, all mitigation measures must be applied as long as their cost is not disproportionably high with regard to the risks they reduce.

Two other central concepts in risk assessment are *equity* and *efficiency*. Equity is the right of citizens to be treated in a just manner, with no discrimination in favor or against any of them. Within this context, it can be deducted that no citizen should be subjected to excessive risks. The concept of efficiency refers to the need of employing limited resources to reduce risks as much as possible. In other words, equity is related to *individual risk* while efficiency aims at minimizing *societal or collective risk*.

However, there is an inherent conflict between equity and efficiency, since the most effective measures to reduce individual risk may not be the most efficient to reduce global risk on the whole of the population. Consequently, a compromise in decision-making must be done in order to reach a proper balance between equity and efficiency.

All these concepts have set the basis for different international institutions to formulate recommendations on risk tolerability. Chapter 6 exposes the most relevant ones.

Uncertainty. The process of Risk Analysis incorporates a series of uncertainties that have a relevant impact in the understanding and interpretation of the probability results of the model. The term uncertainty encompasses mainly two concepts of different essence: natural variability and epistemological uncertainty. This can be observed in figure 2.11.

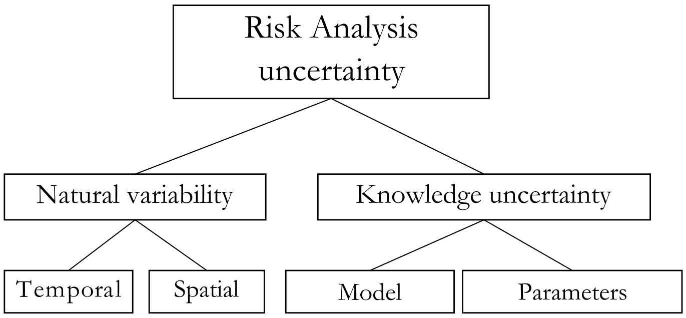


Figure 2.11: Taxonomy of uncertainty in Risk Analysis (adapted from [68]).

It is understood by natural variability the random character inherent to natural processes. It can manifest as the variability along time of phenomena that take place in a precise point of the space (temporal variability) or the variability across the space of phenomena that take place in different points but simultaneously (spatial variability). Classic examples of temporal variability are the magnitude of a flood in a certain section of a river or the intensity of a seismic event in a certain location. Natural variability can be quantified through mathematical models adjusted to reproduce the analyzed phenomenon in a more or less approximate way. The larger amount of available data, the better the adjustment will be. However, the variability inherent to the natural phenomenon cannot be reduced.

Epistemological uncertainty is related to the lack of knowledge resulting from either insufficient data, or from the incapacity to understand the operating mechanisms of a given phenomenon. This uncertainty can be reduced through the collection of additional information, the gathering of more data and an increase of knowledge. On the contrary, this uncertainty is very difficult to quantify. Epistemological uncertainty can be divided in two categories: uncertainty of the model and uncertainty of the parameters. The uncertainty of the model refers to the ignorance of the extent to which a model reproduces reality faithfully. It reflects the incapacity of representing reality or of identifying the best model to do it. The uncertainty in the parameters arises from the restricted capacity to estimate them in an adequate manner from a limited number of data from tests or calibration, and also from the inherent limitations of the statistical techniques used in their estimation.

In practice, part of the epistemological uncertainty is usually modeled as natural variability. A typical case of this assimilation is the modeling of geotechnical or material's parameters: these characteristics are modeled as if they would present natural variability (by treating them as random variables) whereas in reality it would be possible to know them if enough resources (time and monetary ones) were employed.

Screening analysis *Screening analysis* is a semi-quantitative analysis based on risk principles. Sieving analysis is usually applied to a portfolio of dams. This analysis, instead of estimating each of the probabilities considered in the risk equation, assigns risk indexes on the basis of the available information and provides in the end a risk index for each of the studied dams. This methodology is useful to do a preliminary ordering of the dams according to their importance in terms of safety, thus helping to determine how to focus ulterior efforts. There are several documented cases of the use of these techniques in Spain [47, 38, 64, 62] as well as at an international level [29].

Chapter 3

Risk-informed safety management

Risk Analysis is a helpful tool for decision-making, since it enables the integration of all the available information on dam safety that is tipically analyzed separately in other documents. As an example, these are some of the disseminated pieces of information that might have been gathered: a stability calculation providing a safety factor lower than the recommended one would show the dam might have a safety problem in this aspect; maintenance tasks could reveal a gate does not behave the way it should; monitoring data might detect an increase of seepage or of uplift pressures and allow to take action before the problems grow; while writing or reviewing an Emergency Action Plan measures can be designed to improve population safety in case of breakage of the dam.

Today, thanks to Risk Analysis, we have a tool that allows the integration of all of these aspects and that enables to measure the importance each of them has on the global safety of the dam. This aggregating capacity is precisely one of the greatest advantages of Risk Analysis.

Risk Analysis builds a global model of the dam where all relevant aspects are included: the complete set of loads (hydrologic, seismic and of any other kind), all possible consequences and the responses of the system. This risk model is fed with the information provided by the different safety documents of the dam that can be found in the Dam Safety File. Some of the most relevant documents are the Emergency Action Plan, the Operation Rules, the Annual Reports, the Safety Reviews and the Behavior Reports. When doing a Risk Analysis the whole Dam Safety File is studied and a field visit is also done to complement the information contained in these documents.

With the model defined and all the pertinent information introduced, it becomes possible to assess the importance each of these matters has. Moreover, it is possible to put the current condition of the dam into context thanks to a comparison with the international recommendations on risk tolerability (see chapter 6). The process of contrasting a situation with given recommendations is called *Risk Evaluation*. With a risk model it is also possible to evaluate the impact and efficiency of potential measures for risk reduction and even to compare their efficacy and efficiency on different dams in a homogenized way. Finally, it is possible to model portfolios of multiple dams to optimize their global management.

Figure 3.1 sums up the process of management of dams and reservoirs safety when *informed* by risk models. The risk model of the dam is the tool that allows the integration of all the information concerning safety and the production of useful results on decision-making.

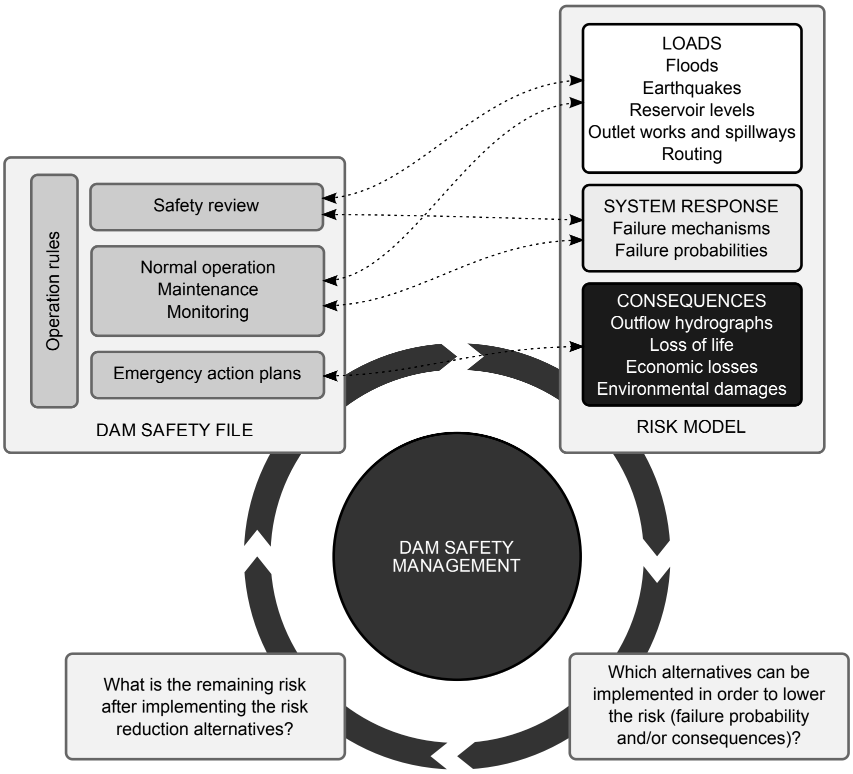


Figure 3.1: Global management of dams and reservoirs safety and links between the risk model and the Dam Safety File (adapted from [118]).

As it can be noticed, the risk model is divided in three areas: loads, failure probabilities (also known as responses of the system) and consequences. Each of these areas of the model corresponds to one or several documents of the Dam Safety File. The operation rules have been represented as a transversal document that concerns all areas.

As the figure shows, the relation between the Dam Safety File and the risk model has a double-direction. The relation from left to right represents the need of the model to use the Dam Safety File as a source of information whereas the direction from right to left indicates that the elaboration of a risk model generates information that can be reincorporated into the Dam Safety File. As examples of that relation:

- A Safety Review of a dam can benefit from the results extracted from a risk model.
- Possibility of assessing different strategies of flood management can contribute

to the improvement of the Operation Rules or the Emergency Action Plan.

Chapter 4

The process of Risk Analysis

4.1 The steps of Risk Analysis

This section exposes the different steps of Risk Analysis. The scheme of Figure 4.1 shows the sequence to be followed.

As in any other type of study, the first step of a Risk Analysis consists of determining the scope, objectives and deadlines of the analysis. It is not always advisable to do a Risk Analysis with a maximum level of detail. On some occasions, it can be more helpful to follow an iterative process in which the analysis is done with a low level of detail for the first time. Doing this at a first stage allows the identification of the issues and/or the dams that require a deeper study. Chapter 5 contains some recommendations of the level of detail to apply in each part of the Risk Analysis. It is also at first stage that the team of professionals that will carry out the study must be formed. This team should count with the presence of the dam operator and it is also very helpful if it includes some external consultant.

The process of reviewing the Dam Safety File is of particular relevance to Risk Analysis. Under no circumstance should this process be limited to a simple gathering of information, but this one should be discussed thoroughly in one or several group sessions. At this point of the analysis it is also possible to identify additional needs in terms of studies. The enhancement, structuration and review of the information of the Technical Review constitute by themselves some of the immediate benefits of doing a Risk Analysis.

Once the information has been made available for consultation to the whole group, an inspection of the dam must be done to check its current condition and to identify potential problems. This field visit has to conclude with a group discussion on the current state of the dam.

Failure modes identification is a collective process that aims at spotting, defining and structuring all the possible ways in which the dam may fail, without limiting itself to a predetermined check list (see section 4.2).

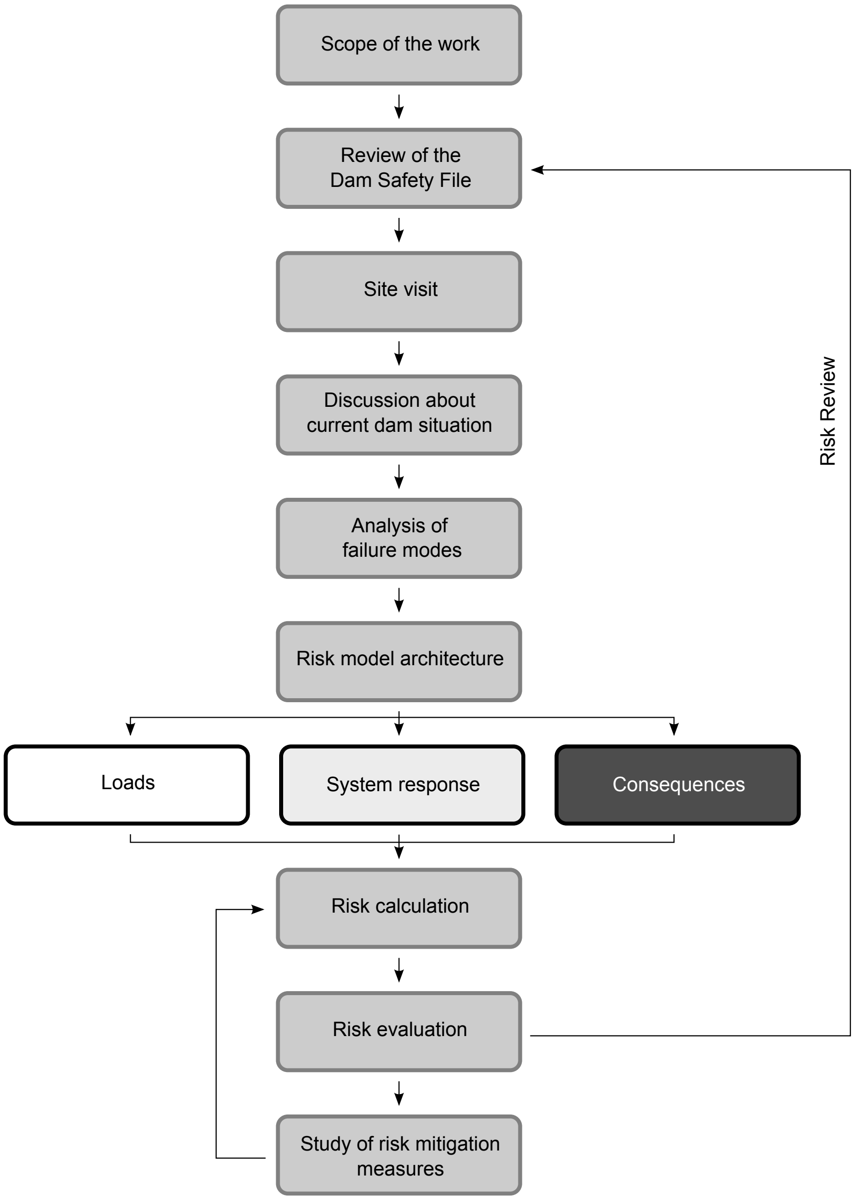


Figure 4.1: Scheme of the process of Risk Analysis.

The following steps of the Risk Analysis (architecture of the model, loads analysis, failure probabilities and consequences estimation and risk calculation) concern the elaboration of a quantitative *risk model* and are explained in chapter 5.

As already outlined in the general scheme of safety management based on risk, Risk Evaluation aims at determining whether the existing risks are tolerable or not. Chapter 6 discusses the available recommendations on the matter at an international level.

Risk Analysis must be applied to the current state of the dam, but also to its future one, i.e., after the implementation of certain mitigation measures. By this doing, it is possible to evaluate by comparison the efficacy and efficiency of these actions. Besides, the process must be updated and reviewed in time as the conditions of the dam evolve.

4.2 Identification and definition of failure modes

Within the global process of Risk Analysis, the identification of failure modes is the step preceding the making of the risk model (see figure 4.1) and a very important one. Indeed, if a relevant failure mode is missed in the identification sessions, it will not be included in the model, which might lead to a calculated risk very different from the real value. In other words, the identification of failure modes determines the scope and the soundness of the risk model.

The identification of failure modes is paramount to all risk based approaches. It is thus not surprising it has been used for such a long time. Aerospace -along with nuclear industry- pioneered the application of methodologies based on risk, and developed during the 1960's a systematic process known as Failure Modes and Effects Analysis (FMEA).

The FMEA consists of several steps. First, all the components of the system and their function are listed. Secondly, all potential *hazards* and events leading to any element's dysfunction are analyzed along with their ensuing effects. For this, local effects (on the proper element) are analyzed first and then, in a progressive way, the effect on the whole system emerges. In the first stage of an FMEA, failure modes are studied without caring about their occurrence probability. For guiding the process, charts and templates are available.

Subsequently, the FMEA spread over and was named FMECA (Failure Modes Effects and Criticality Analysis). In the FMECA, additionally to the steps of the FMEA, a last step is added to grade all failure modes in a qualitative way depending on their probability of occurrence. This is of limited application in quantitative Risk Analysis like the ones described in this Monograph since the probability of occurrence on these ones is obtained throughout a more rigorous process.

For information on FMEA and FMECA the following references can be consulted [13, 31, 138, 74, 128]. These methodologies are still in use in many industries [106] today.

Though these methodologies have been applied to dam safety evaluation, new methodologies have also appeared. Among them, the one applied by the Federal Energy Regulatory Commission (FERC) of the USA can be highlighted. This methodology is presented in chapter 14 (*Dam safety performance monitoring programs*) of the document *"Engineering guidelines for the evaluation of hydropower projects"* [56] and it is summarized hereafter.

FERC, organization in charge for the coding, regulation and normalization of the energy supply in the USA, proposes in this document a technique for developing a monitoring program (*Dam Safety Performance Monitoring Program*) applied to their hydroelectric plants. This methodology suggests some procedures to assess dam safety and to evaluate performance based on failure mode analysis.

FERC supports this methodology arguing that the analysis of failure modes linked to survey and auscultation programs, and the writing of technical reports result in a more efficient program of dam safety. The essential steps that make up the *Dam Safety Performance Monitoring Program* are:

- Creation of a work team to perform a failure modes analysis.
- Compilation of all documents and available data in order to be reviewed by the team.
- Interview of the personal with a closest knowledge of the dam: managers, surveyors and if possible, people involved in the construction of the dam.
- Exhaustive review and total understanding of all the available information about the dam.
- Organization of a session to identify failure modes and assignment to each of them of a qualitative category, according to the following scale:

  I - Highlighted Potential Failure Modes: Those potential failure modes of greatest significance considering need for awareness, potential for occurrence, magnitude of consequence and likelihood of adverse response (physical possibility is evident, fundamental flaw or weakness is identified and conditions and events leading to failure seemed reasonable and credible) are highlighted.

  II - Potential Failure Modes Considered but not Highlighted: These are judged to be of lesser significance and likelihood. Note that even though these potential failure modes are considered less significant than Category I they are all also described and included with reasons for and against the occurrence of the potential failure mode. The reason for the lesser significance is noted and summarized in the documentation report or notes.

  III - More Information or Analyses are Needed: These potential failure modes to some degree lacked information to allow a confident judgment of significance and thus a dam safety investigative action or analyses can be recommended. Because action is required before resolution the need for this action may also be highlighted.

IV - Potential Failure Mode Ruled Out: Potential failure modes may be ruled out because the physical possibility does not exist, information came to light which eliminated the concern that had generated the development of the potential failure mode, or the potential failure mode is clearly so remote a possibility as to be non-credible or not reasonable to postulate.

- Establishment of the needs in terms of auscultation and survey and of the reduction measures for the identified failure modes.
- Elaboration of a document including the totality of the works carried out by the team.

All the steps are done with the help of a facilitator that acts as a guide or group leader during the whole process.

In Spain, this methodology has been adapted, spread and applied to do a quantitative Risk Analysis [60]. Other examples of identification of failure modes in Spain are the ones done in the Catalonian Water Agency [15], Iberdrola [45] or River Duero Authority [114, 9, 11]. Additionally, more specific tools have been developed to help structuring the collective work sessions including assistance devices such as notebooks and charts [61]. The advantages offered by these tools are:

- They guide the sessions of failure modes identification.
- They present a collection of failure modes for concrete and embankment dams that:
  - Help to identify typical failure modes so they cannot be forgotten.
  - Help to structure the definitions so they are coherent, consistent, auditable and more easily quantifiable.
  - Help to relate failure modes to dam monitoring.

Chapter 5

The risk model

5.1 Introduction

This chapter deals with the elaboration of risk models and corresponds with the highlighted part of the scheme in figure 5.1 that defines the steps of Risk Analysis.

First, a series of generic architectures of risk models for different loading scenarios are introduced. Secondly, a section is devoted to each of the entries of the model. Finally, a section outlines the calculations of the risk model and a last one provides some recommendations on the level of detail to use in each of them.

Each section is rounded off with an example. The example does not correspond to any real case and its purpose is purely demonstrative.

5.2 Architecture of the risk model

5.2.1 Defining the problem

The first step in the development of a risk model is defining its architecture. When setting the architecture the variables that will be included in the model and the relations between them must be defined. Besides, depending on the failure modes spotted during the identification and description phase, it will be necessary to do a risk model for each of the loading scenarios to be studied. In this section, three generic architectures are presented for the hydrologic, seismic and normal scenarios. Risk models are represented through influence diagrams (see definition in chapter 2).

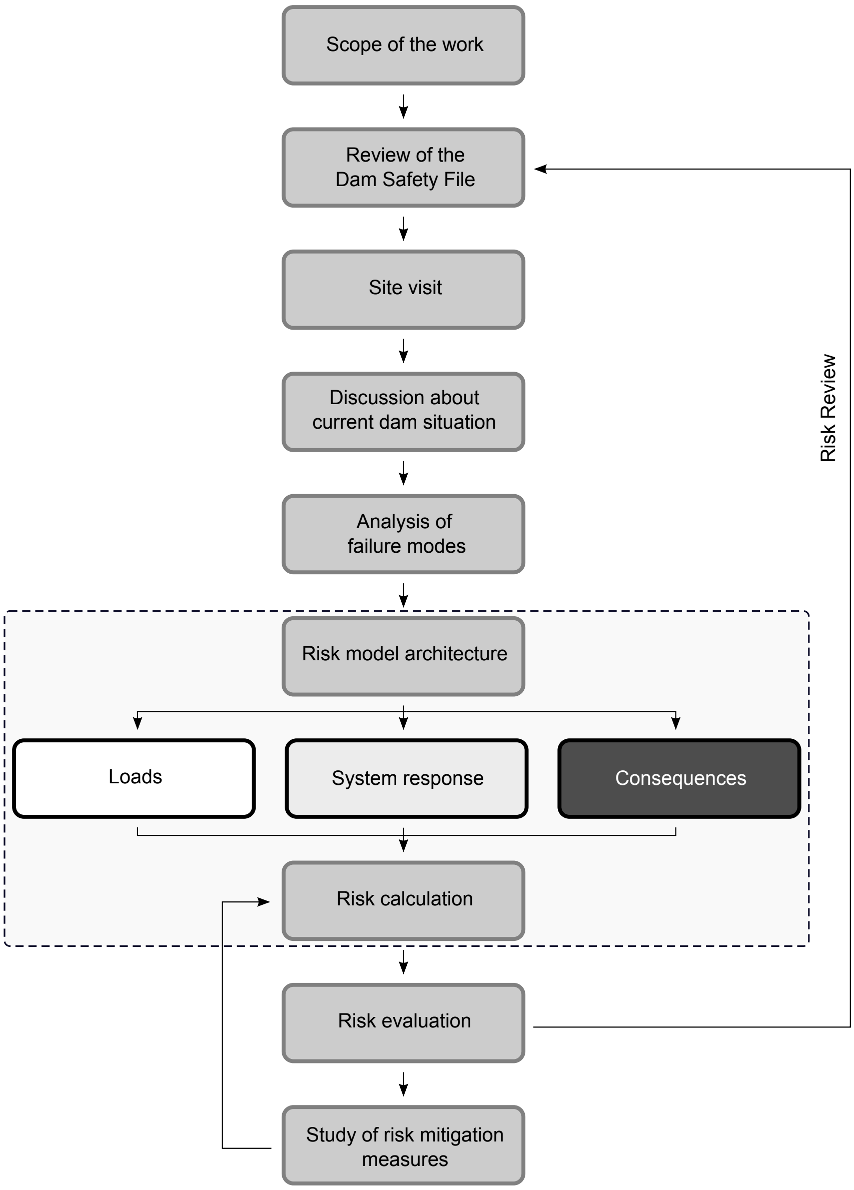


Figure 5.1: Scheme of the process of Risk Analysis, highlighting the specific steps of the architecture and calculation of the risk model.

5.2.2 Normal scenario

This section outlines the structure of a standard risk model for a normal scenario. It introduces the analyses that will require further development and that are discussed in the following sections.

The analyses have been divided into three groups that correspond with the three terms of the risk equation:

- Analyses corresponding to the modeling of the loads.
- Analyses corresponding to the modeling of the response of the system.
- Analyses corresponding to the modeling of the consequences.

In order to identify each of them, the same color code (white, light gray and dark gray) used in the general scheme of Risk Analysis (figure 5.2) has been kept[1].

The first node of the diagram corresponds to the action represented by the water level in the reservoir. The starting information is usually the exceedance probability curve for the water levels of the reservoir. This curve can be obtained in many cases by adjusting an empirical curve to the historic registers. For this it is necessary to count with a register sufficiently long and representative of the current operating situation. Whenever this condition is not met or when it is intended to analyze a potential future situation (for example, freeboard requirements in the reservoir) simulation proves a helpful tool. These subjects are detailed in section 5.4.

The following nodes, in light gray, contain the information of the failure modes. There will be a branch in the diagram for each failure mode. It will be possible to model the failure probability of each mode in the diagram through one or more nodes. Section 5.7 deals with the way of assigning probabilities to each of the steps of a failure mode. The objective is to obtain a curve that relates the water level in the reservoir with the annual failure probability.

A node estimating the failure hydrograph follows each failure mode. Concerning the event tree, it is usual to characterize the failure hydrograph with a significant variable (usually the peak discharge), so for these nodes it suffices to obtain a curve relating the pool level of the reservoir with this variable. In any case, it will always be necessary to have a series of complete failure hydrographs in order to do the ulterior flooding simulations in the following step. Different methods for doing these studies are discussed in section 5.8.

Finally, there are the nodes of consequences estimation where the relations between the consequences and the failure hydrographs must be introduced. In the normal scenario, the consequences of the non-failure case are null, so it is not necessary to evaluate them to obtain the incremental consequences. The case shown in figure 5.2 is the simplest one, but the calculation could be sharpened if the consequences

[1] In figure 5.2 it has been included a list of the works to be done for each of the three scenarios (normal, hydrological and seismic). In the influence diagram it is indicated which of them are necessary for a normal scenario.

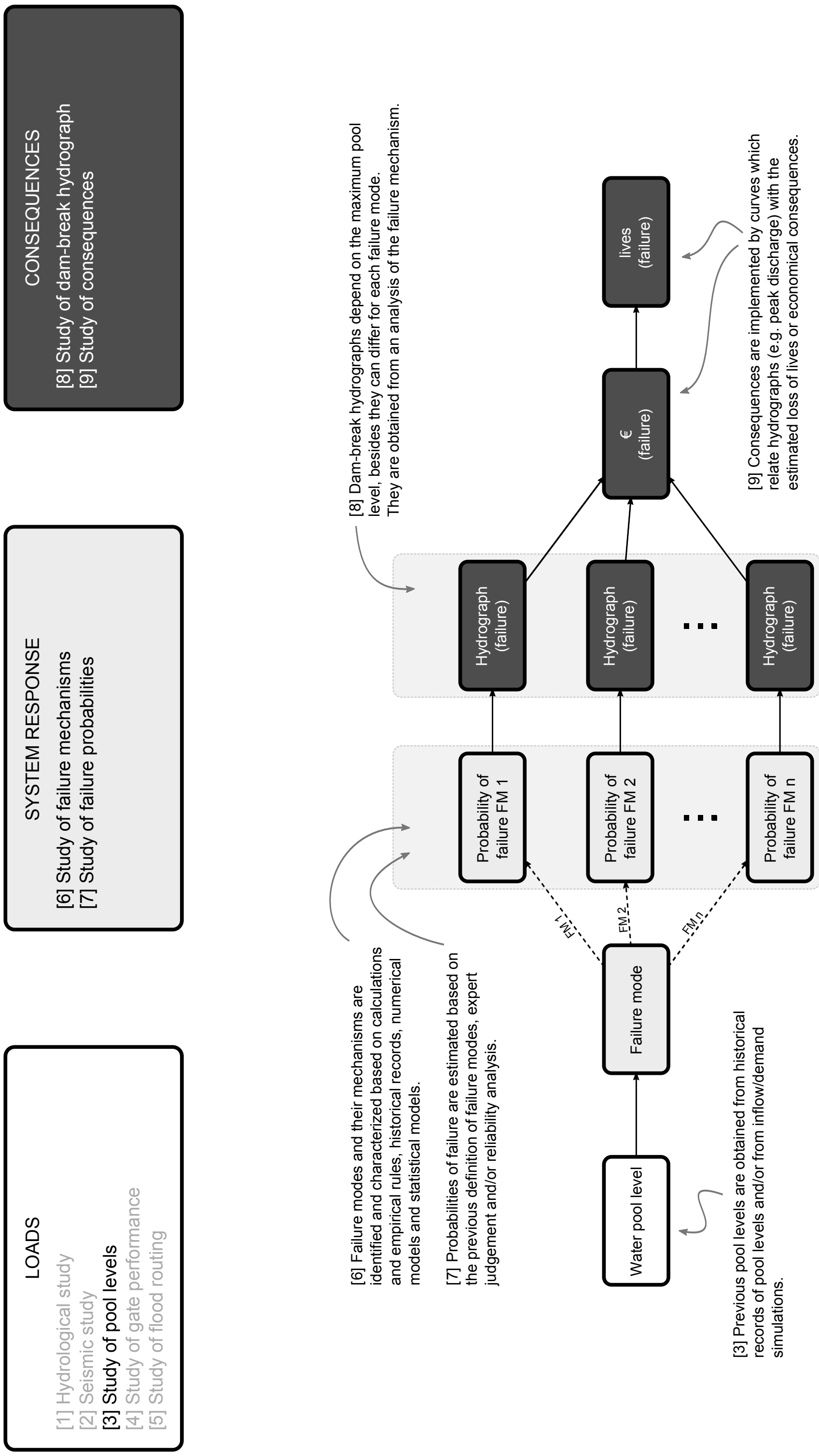


Figure 5.2: Influence diagram of a standard risk model for the normal scenario showing the works to be done to define each of the variables.

were disaggregated as a function of other variables such as the moment of the day, the week or the year, the moment the warning took place or the failure mode. The different types of consequences that can be found and the existing methodologies for studying them are discussed in section 5.9.

Figure 5.3 shows in a summarized way the minimum available data usually required to feed an event tree in a normal scenario. It goes without saying that if any other factors are taken into account (season, day/time, higher level of disaggregation of failure modes, etc.) it will be necessary to incorporate more relations to the ones shown in the figure.

5.2.3 Hydrologic scenario

The present section sums up the works required in order to do a standard model in a hydrologic scenario (figure 5.4).

The first node introduces the flood entering the reservoir. A probabilistic hydrologic analysis will be necessary to obtain the annual exceedance probability of the possible floods. Though it does not appear in the figure, it is possible to incorporate seasonal hydrologic studies. Section 5.3 deals with hydrologic studies.

The next node (previous pool level) is very similar to the node of pool level of reservoir in the normal scenario. However, there is a conceptual difference between the previous pool level in a normal and a hydrologic scenario: whereas the former represents the pool level of the reservoir any day of the year, the latter represents the pool level in the reservoir at the instant preceding the arrival of the largest flood of the year. Therefore, the comments of section 5.4 are also entirely applicable here. In a simplified way and in some cases it is possible not to incorporate this variable by admitting the dam is always at its Maximum Operating Level (MOL). This falls on the safe side, that is, it will produce higher probabilities of failure. In dry climates with severe floods (such as the case of Mediterranean areas) where it is normal to find a pool level much lower than the MOL, this simplification can be excessively distant from reality and offer too conservative results, not suitable for comparison with the results of other dams where the calculation considers the real fluctuation of pool levels.

The reliability of outlet works and spillways is the probability of these devices functioning properly (or not) when a flood arrives. This aspect is very difficult to introduce in a traditional calculation based on safety factors but fits naturally into a risk based analysis. The different reasons to discard an outlet works or spillway (i.e., consider it does not work) are discussed in section 5.5 and it is also explained how to do other estimations from operation registers, expert judgment and fault trees.

The following two nodes, maximum pool level and hydrograph with no-failure, will be studied in the flood routing study (see section 5.6). These variables will have to be determined for each possible combination of previous pool level, arriving flood and availability of the gates. Depending on the failure modes to be studied, some additional variables as time of overtopping will need to be obtained in certain cases.

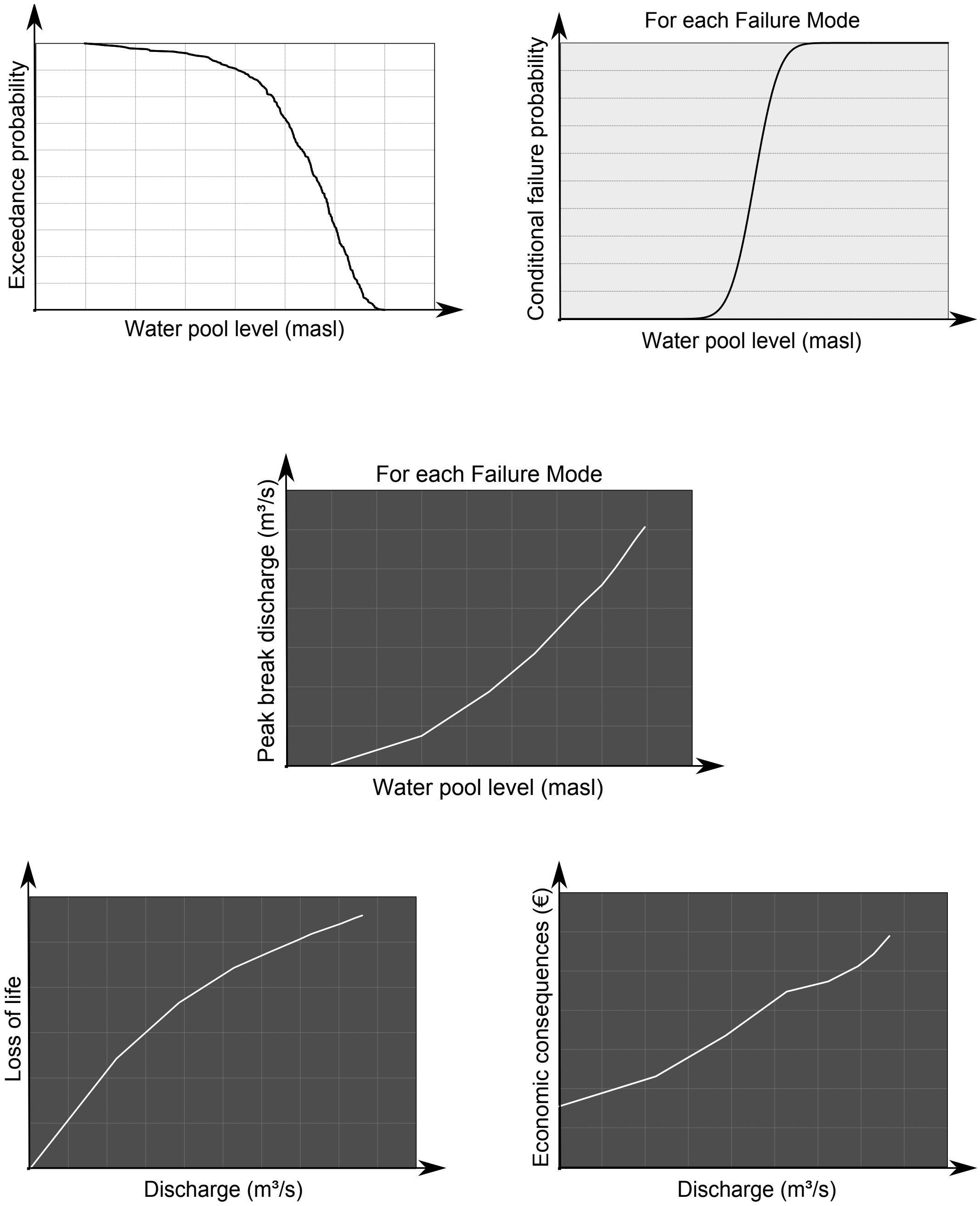


Figure 5.3: Summary of the basic relations to feed a risk model for normal scenario.

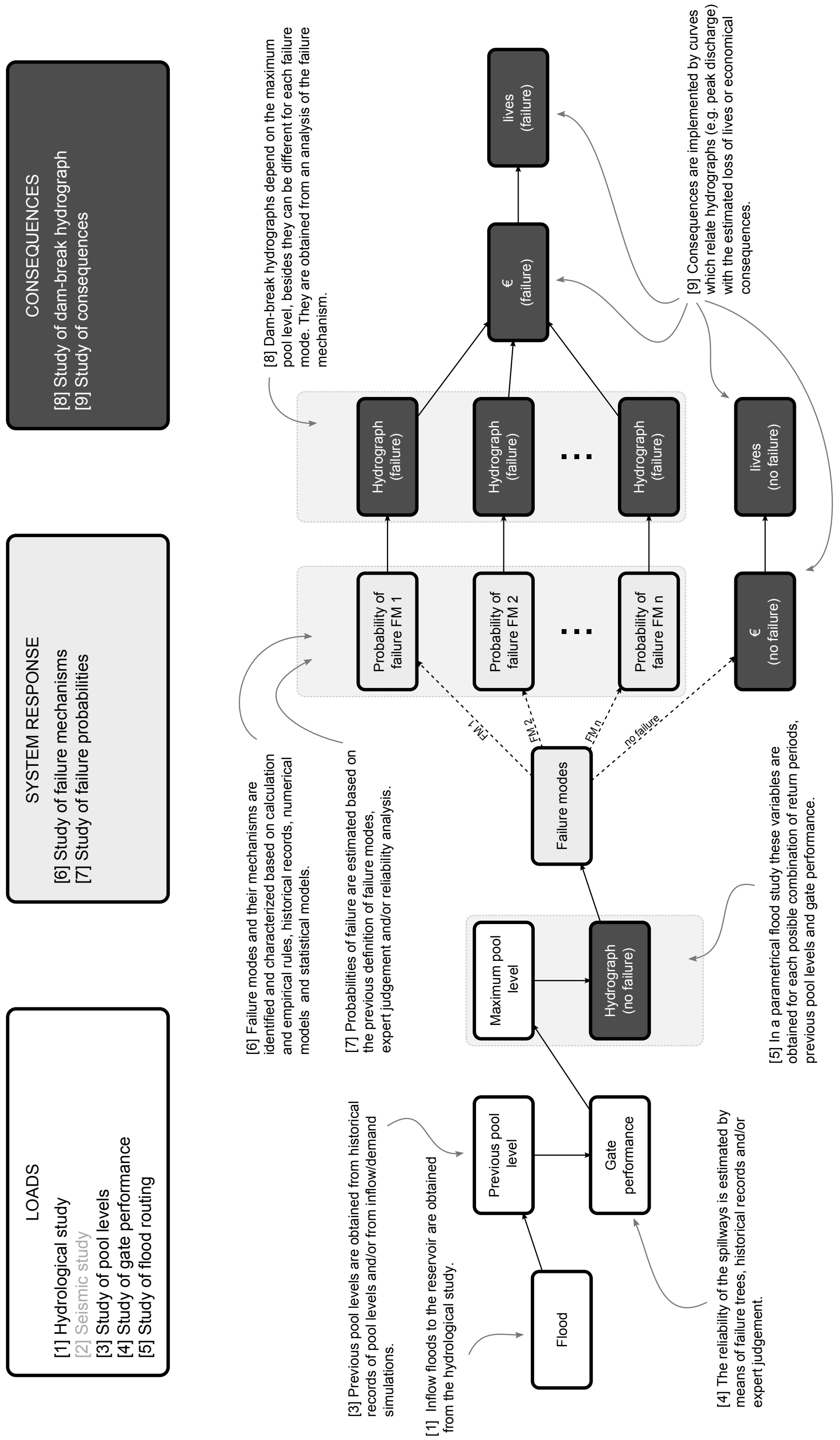


Figure 5.4: Influence diagram of a standard risk model for the hydrologic scenario showing the works to be done to define each of the variables.

In order to do a flood routing study it is necessary to have the characteristic curve of the reservoir that relates pool level to storage volume, the curves of discharge of the outlet works and spillways and the operation rules for flood management.

With regard to failure modes and failure hydrographs, the same comments as for the normal scenario are generally valid, the only difference being that failure probabilities will be dimensionless instead of annual.

Concerning consequences, the only difference with respect to the normal scenario is that the consequences of the non-failure case will need to be calculated in order to obtain the incremental risks.

Figure 5.5 shows a summary of the outlined relations.

5.2.4 Seismic scenario

Finally, the works required to complete a risk model for a seismic scenario are outlined (see Figure 5.6) in this sub-section.

The two first nodes (that could be regrouped in a single one) model the probability of occurrence of the earthquake through a representative variable, usually the basic seismic acceleration. This relation must be obtained from a seismic study (see section 5.3). In the cases where seismicity is very low it is possible to disregard this scenario entirely as the risk it will bring up will be negligible in comparison with the ones provided by the other two scenarios.

As in the two previous situations, it is also necessary to model the water level of the reservoir at the moment the earthquake takes place. The failure modes present in this scenario are equivalent to those found in previous scenarios and can be considered in a similar way. The same can be said of the nodes of the failure hydrograph.

Finally, the consequences will depend only on the failure hydrograph and, as it was the case in the normal scenario, it will not be necessary to evaluate the consequences for the non-failure case (because there is no flood in such a case). A more accurate analysis could consider the combined consequences of an earthquake and a flood in a breakage case and also the consequences of the earthquake with no flood in the non-failure case.

Figure 5.7 shows a summary of the outlined relations.

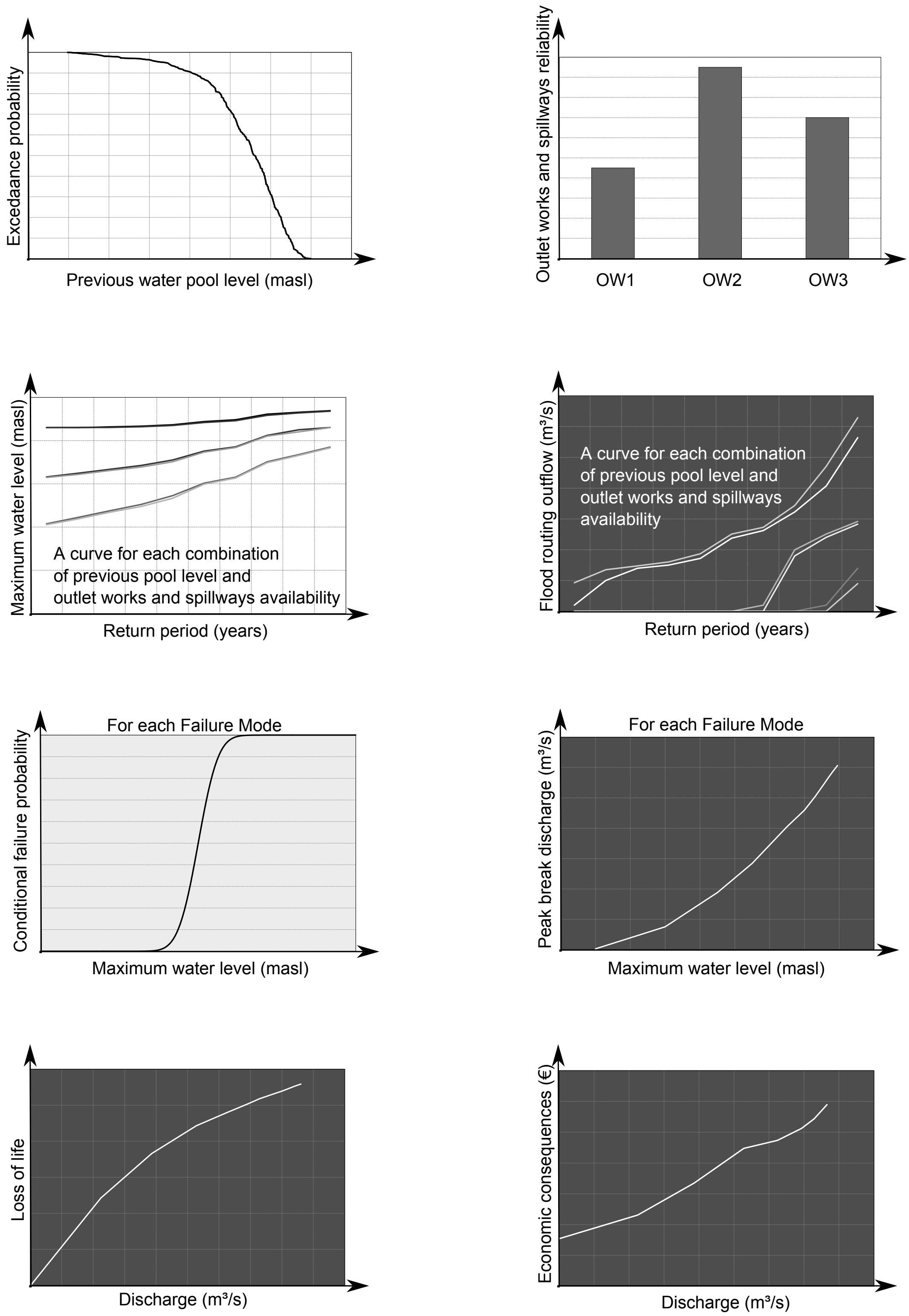


Figure 5.5: Summary of the basic relations necessary to feed a risk model for the hydrologic scenario.

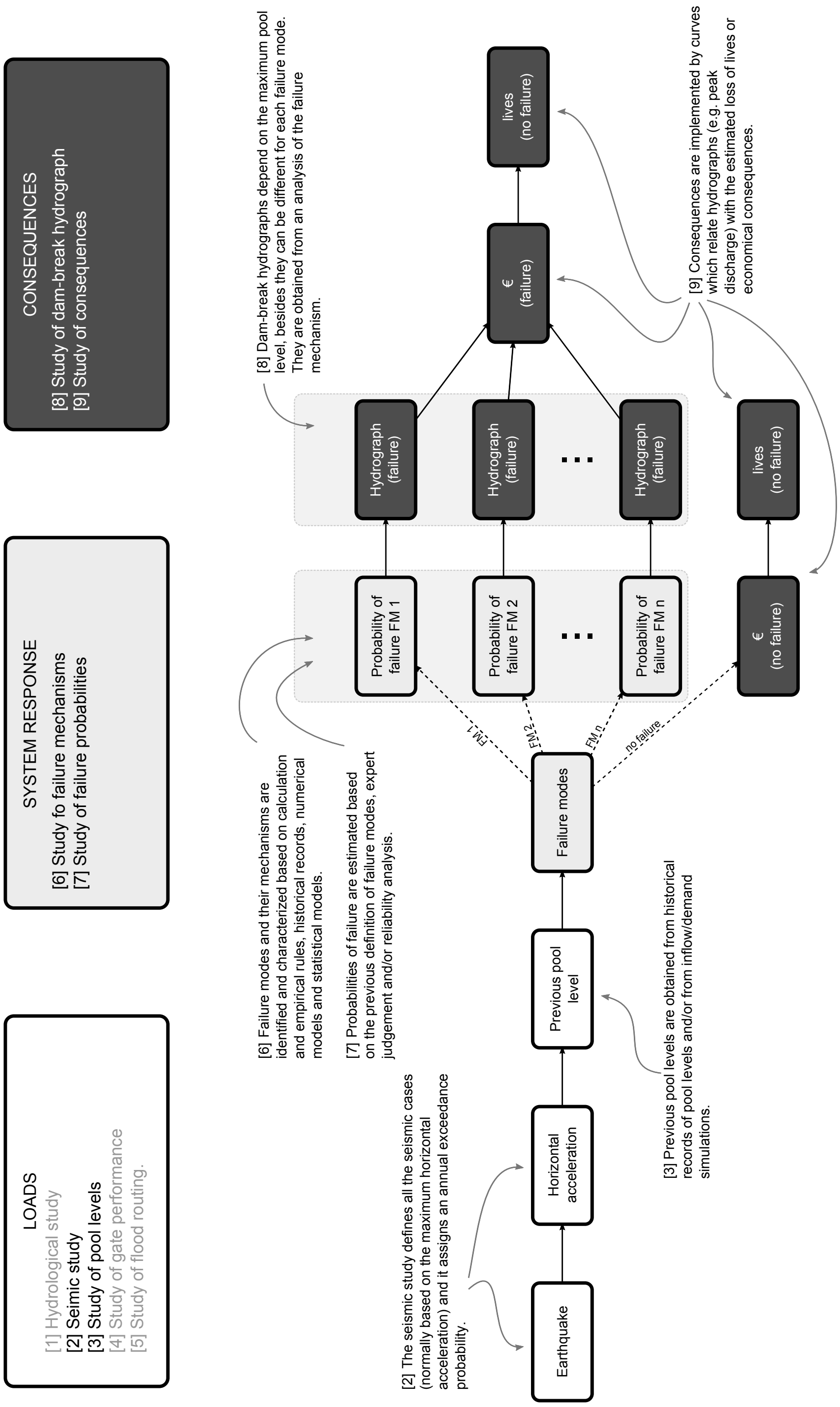


Figure 5.6: Influence diagram of a standard event tree for seismic scenario showing the works required to define each variable.

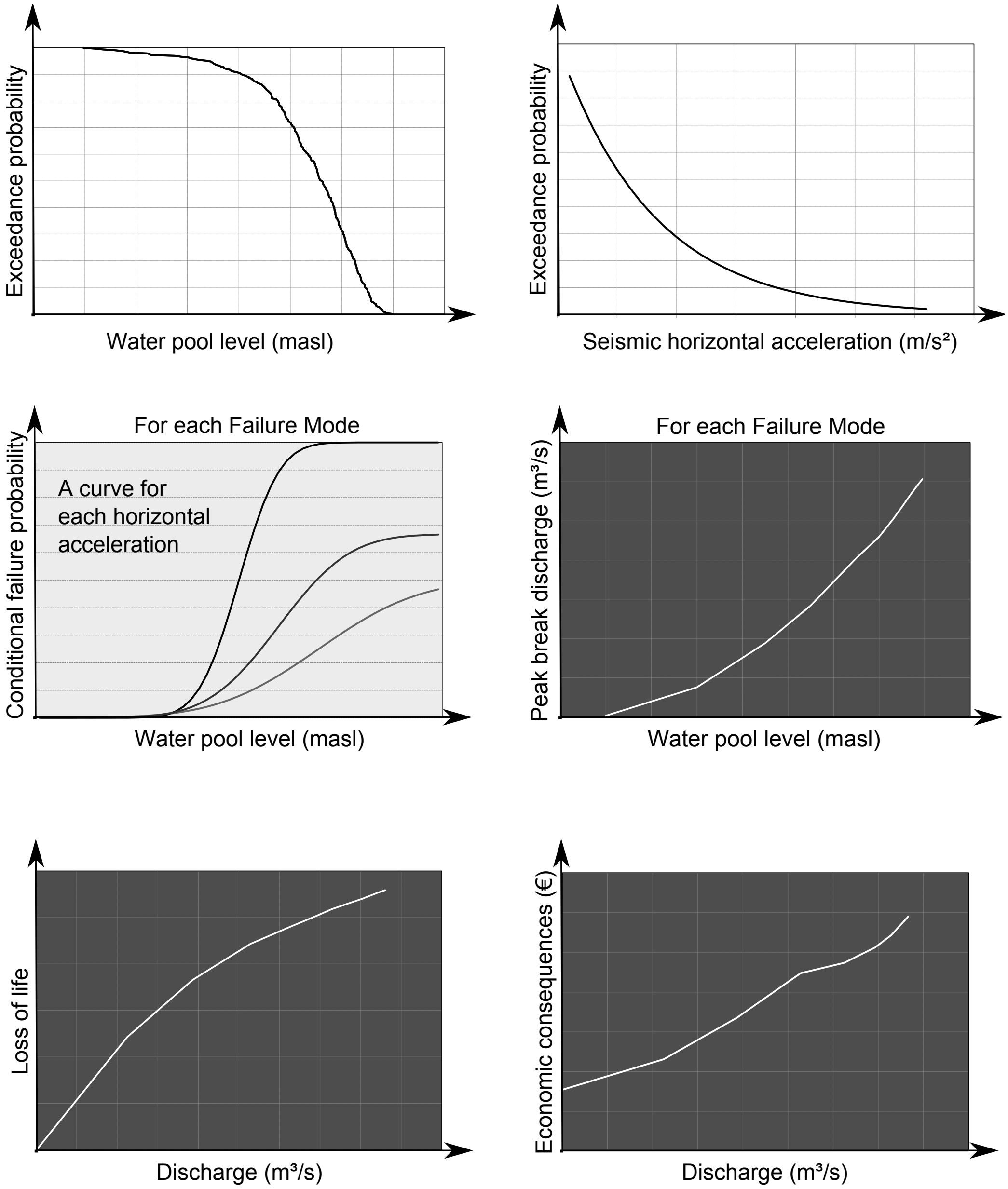


Figure 5.7: Summary of the basic relations to feed a risk model for a seismic scenario.

5.2.5 Example

The problem that will be developed along the document is set herein. It is a fictitious dam with the following characteristics:

- Concrete gravity dam
- Maximum Operating Level (MOL) = 218.5 m
- Crest level = 222.3 m
- Spillway controlled by 2 gates

The hydrologic scenario is going to be analyzed. The following two failure modes have been spotted at the step of identification:

- Sliding of a block due to the water level of the reservoir and the existence of high uplift pressures.
- Erosion of the foot of the dam and sliding produced by overtopping.

Figure 5.8 shows the architecture of the risk model adopted for the example.

5.3 Study of loads: floods and earthquake

5.3.1 Loads in Risk Analysis

A risk model starts with an initiating event that creates the loads to which the dam is subjected. In the hydrologic scenario this event is usually a flood and in the seismic scenario the event is an earthquake. In the normal scenario, there is no unusual event that causes the failure of the dam, since what is modeled is precisely the probability of breakage in the absence of any unusual action.

This chapter exposes how floods and earthquakes are introduced in risk models. Hence, in the general process of Risk Analysis, the hydrologic and seismic studies fall within the section of loads analysis(see figure 5.1).

In the hydrologic scenario, floods are the phenomena under study. Floods can be defined through several variables, though the most common way to do it is through their peak discharge Q_p. Moreover, they are associated with a certain probability of occurrence, explicitly expressed by its annual exceedance probability AEP (probability that the peak discharge of the largest flood in a year whatever is larger than a given discharge Q) or its return period T (the inverse of AEP).

In the seismic scenario, the probability of occurrence of an earthquake is modeled through a representative variable, usually the peak ground acceleration.

In the normal scenario, the loads are the daily water levels in the reservoir (their modeling being explained in section 5.4), with no intervention of any unusual flood or earthquake.

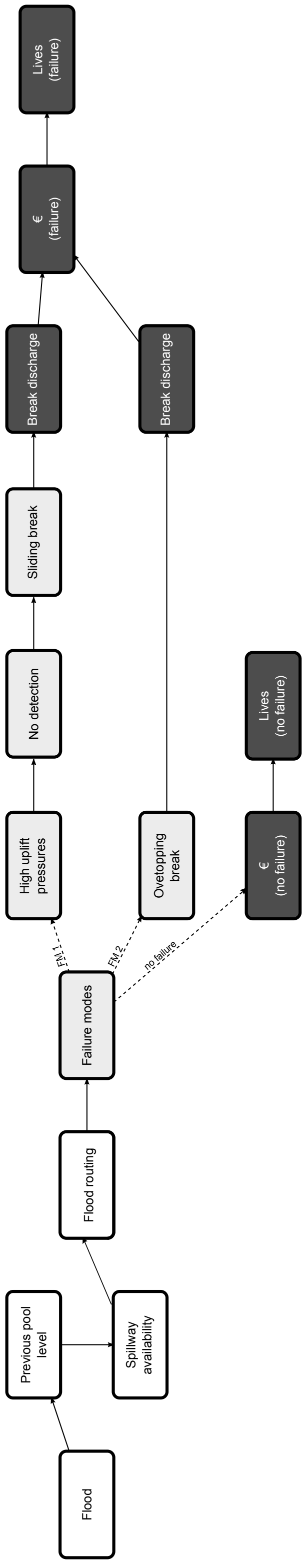


Figure 5.8: Architecture of the risk model of the example.

5.3.2 Estimation of seismic loads

The objective of the seismic study is to estimate a series of seismic occurrences for the analyzed returned periods. For this, two paths can be followed. The first one would consist in generating synthetic seismic loads for the required return periods. The second one would be adopting just a single value that would define the earthquake and that could be used to perform a simplified analysis of its effect; for example, the maximum horizontal acceleration. In this second option, what it is looked for is the statistical definition of this variable.

In Spain, the first option can be developed thanks to the use of the response spectra provided by the norms in force, today NCSE-02 [95]. With them, it is possible to obtain synthetic accelerographs that can be used subsequently to estimate failure probabilities. In high seismicity areas or under special circumstances, it might be necessary to resort to seismotectonic studies [33].

Concerning the second option, NCSE-02 provides with a hazard seismic map with the peak ground horizontal acceleration associated with a return period of 500 years [33]. From this acceleration it is possible to obtain the acceleration related to any return period through the formula provided by NCSE-94 [98]:

$$a_T = a_{500} \cdot \left(\frac{T}{500}\right)^{0.37}$$

5.3.3 Estimation of floods hydrographs

The goal of the hydrologic study in Risk Analysis is estimating a series of complete flood hydrographs associated with certain return periods. This means that for each flood both the shape of the hydrograph and its magnitude (usually defined by the value of its peak discharge or its total volume) must be obtained.

In principle, any method is valid to attain this objective as long as it provides a set of input hydrographs (i.e., hydrographs arriving into the reservoir) with its associated return periods. This is the case, for example, of the so called hydrometeorological methods.

Limits of application

Within the context of Risk Analysis it is usual to work with exceedance probabilities of an order of 10^{-4}, 10^{-5} or even smaller. The first limitation in the extrapolation of floods probability is based on the accuracy of the data and the length of the registers used for the analysis. Each Risk Analysis might require a different AEP range and therefore, analysis procedures and data sources must be selected accordingly to the requirements of the project [131].

In general, the data used to obtain hydrographs are based in registers less than 100 years old, though they can be lengthened up to 150 years by using historic information. There are different sources of information useful to set the extrapolation to small enough AEPs:

- Discharge data.
- Climatological data.
- Historical data.
- Paleoflood data.

When it comes to estimate severe floods in a reliable way the better results can be obtained by combining regional data of different sources. Thus, the analysis based on rainfall, discharges and regional paleofloods information should offer the most accurate results in the definition of floods with low AEPs.

Table 5.1 shows a list of the different type of data that can be used as a basis for the estimation of frequent floods, and the optimal limits of their extrapolation for obtaining AEPs. Anyhow, each situation is different and must be assessed individually. For this it is important to perform a sensitivity analysis to evaluate the optimal level of detail for every study [97].

Type of Data Used for Flood Frequency Analysis	Limit of Credible Extrapolation for Annual Exceedance Probability	
	Typical	Optimal
At-site streamflow data	1 in 100	1 in 200
Regional streamflow data	1 in 750	1 in 1,000
At-site streamflow and at-site paleoflood data	1 in 4,000	1 in 10,000
Regional precipitation data	1 in 2,000	1 in 10,000
Regional streamflow and regional paleoflood data	1 in 15,000	1 in 40,000
Combinations of regional data sets and extrapolation	1 in 40,000	1 in 100,000

Table 5.1: Types of hydrometeorological data used and suggested limits of extrapolation in the analysis of floods frequency [131].

5.3.4 Example

The floods to be introduced in the model of the example have been extracted from the data about floods found in the First Review and General Safety Analysis. These floods correspond to return periods from 10 to 10,000 years (figure 5.9). A flood with null discharge that corresponds to the return period T=1 is also included. In a real case, it should be checked as well whether the maximum return period is sufficient for the analysis that is being carried out.

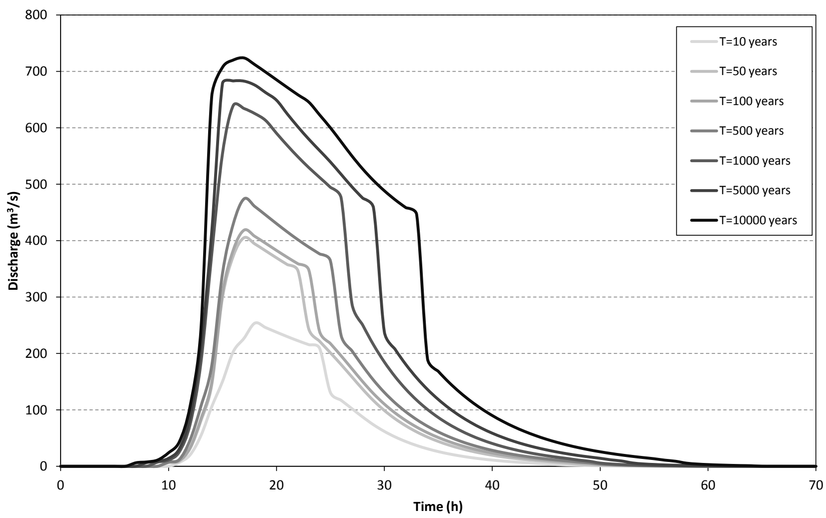


Figure 5.9: Floods from 10 to 10,000 years of return period.

5.4 Study of pool levels in the reservoir

5.4.1 Previous pool levels in Risk Analysis

The study of previous pool levels aims at analyzing the probability of finding a certain pool level in the reservoir at the moment of arrival of a flood; in other words, it defines the starting situation in the reservoir when studying the loads induced by the flood. Therefore, within the general process of Risk Analysis, the study of the previous pool levels falls in the loads analysis part (see figure 5.1).

The relation between probability and pool levels can be obtained by using the register of historic pool levels. As mentioned before in this document, it is necessary to count with a register that is long enough and sufficiently representative of the current situation. When this is not possible or when a potential future situation is to be assessed, it becomes necessary to resort to simulation.

5.4.2 Estimation of the relation between previous level and probability

The relation between previous pool level and its probability of occurrence is usually included in the model through the exceedance probability graph of the reservoir. This graph is obtained from a series of data that can come from real or synthetic series, as it is explained in section 5.4.3.

To obtain the empiric exceedance probability of the pool levels of a reservoir it is necessary to order all the data in an increasing order. In this way, the probability of exceedance of each pool level is given by the following formula [143]:

$$PE_n = 1 - \frac{i_n - 1}{N - 1}$$

Where PE_n is the probability of excedence for a poll level n, i_n, is the number of order of pool level n within the series of ordered pool levels and N is the length of the series.

When the pool levels of the reservoir and their exceedance probabilities are represented graphically, a curve like the one showed in figure 5.10. appears.

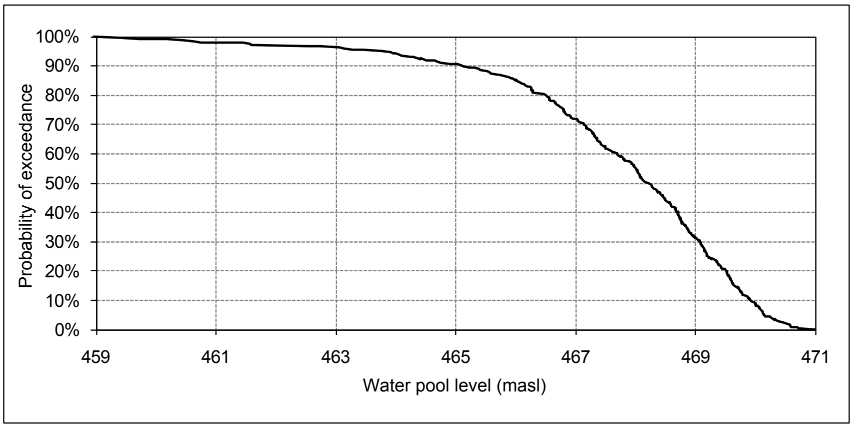


Figure 5.10: Example of an exceedance probability curve of the previous pool pool levels in the reservoir.

5.4.3 Required data

Historic registers

Data from historic registers of measurements of the pool level in the reservoir (figure 5.11) can be usually used to obtain a relation between previous pool level and probability. Yet, those data must satisfy certain conditions in order to be valid for the risk model purpose.

First of all, data must be consistent and reliable, for which the utilized series must be filtered so that erroneous data can be discarded.

If these data are to be used in the model it is necessary to ensure they represent properly the distribution of the pool levels in the reservoir. Therefore, the series must be lengthy enough to guarantee that the pool levels variability is properly represented. The bibliography states that a length of 25 years is usually sufficient in most of the cases for hydrologic variables such us the discharge [70]. Nevertheless, it is convenient to study the effect of the length of the data series in the obtained

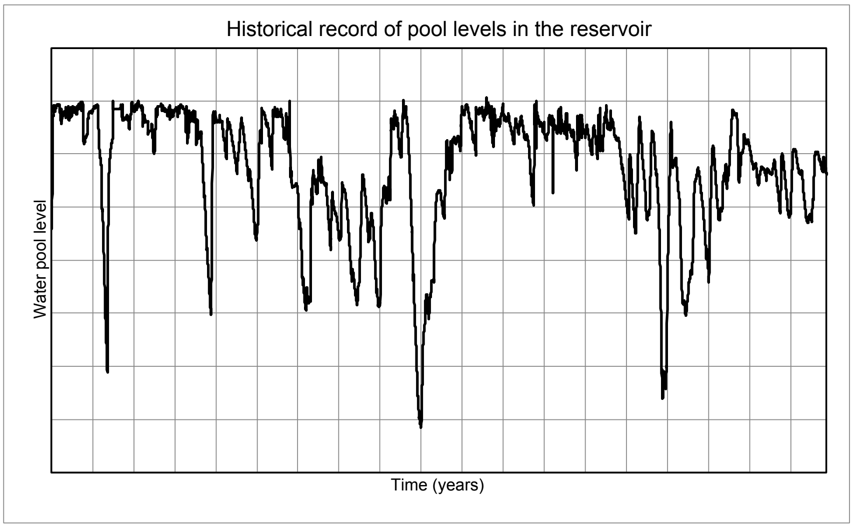


Figure 5.11: Example of historic register of the pool levels in the reservoir.

probability curve and to ensure the adopted length is appropriate, as the extension of the period of data can impact the results sometimes [7].

Moreover, data corresponding to exceptional situations must be removed for the analysis to avoid the introduction of events that do not represent the normal situation of the reservoir. This is the case of:

- The filling-up of the reservoir.
- The emptying of the reservoir for rehabilitation works.
- Other situations unusual in the normal operation of the reservoir.

To obtain a correct definition of the current situation of the pool levels in the reservoir it is also important to remove the data corresponding to the occurrence of any event that has modified substantially the variation of the pool levels, such as it might be the construction of a dam upstream or the rising of the crest of the dam.

Additionally, when analyzing the hydrologic scenario it is necessary to remove the flood situations in the register because the increase of the pool level produced by the flood is introduced independently in the risk model through the flood routing study.

In general, it suffices to truncate the curve of exceedance probability obtained in the MOL (Maximum Operating Level), admitting this way that whenever the level in the reservoir is over the MOL this is due to a flood situation[2].

On the contrary, data corresponding to other unusual situations in the reservoir (e.g., draught periods) must be included in the analysis of the register of historic

[2]In a more detailed studied, it could be removed from this year the pool levels attained during the maximum annual flood. These pool levels do not need to coincide with the maximum annual pool levels in the reservoir so it will be required to analyze the entering floods every year.

pool levels.

Whenever the register of pool levels does not satisfy the mentioned conditions or in case a potential future situation (e.g., a restriction of the operation pool levels) is to be assessed, it is necessary to resort to simulation to obtain the level data.

Simulations of reservoir level

An alternative to the use of historic registers for obtaining the relation between previous pool level and probability is to perform a simulation of the system of water resources management. The objective of a simulation model is to estimate the functions of distribution of a variable by analyzing its behavior. In this case, the simulation reproduces the work of a reservoir according to the current or suggested management rules of the system.

In general, the simulation of a reservoir is done within the frame of a more complex simulation that concerns the planning of the system of water resources and that can include several reservoirs. The model consists of a sequential calculation of the location and use of the water resources. For this, the equation of mass balance is used taking into account the physic restrictions of water and the rules of infrastructure management. There are several software tools for the planning of basins such as AQUATOOLD-MA [126] or HEC-ResSim [83] that could make this type of calculations easier.

Certain data are necessary when doing a simulation of the reservoir [7]:

- Inflows, either through a series of historic inflows to the reservoir or through a stochastic analysis for creating synthetic series of contributions.
- Demands.
- Reservoir management.
- Evaporation and infiltration water losses.

Although performing a simulation is more laborious than using historic data, this option presents some advantages: [132]:

- It enables a large register of pool levels in the reservoir.
- The pool levels are representative of the way the reservoir works.
- It allows the consideration of alternatives on dam safety and on the planning or management of the water resources system.

5.4.4 Example

The distribution of previous pool levels for the example has been obtained by analyzing the distribution of historic pool levels in the reservoir. Then, the obtained probability curve has been discretized in 18 intervals. Figure 5.12 shows the exceedance probability curve for the previous pool levels and the adopted discretization.

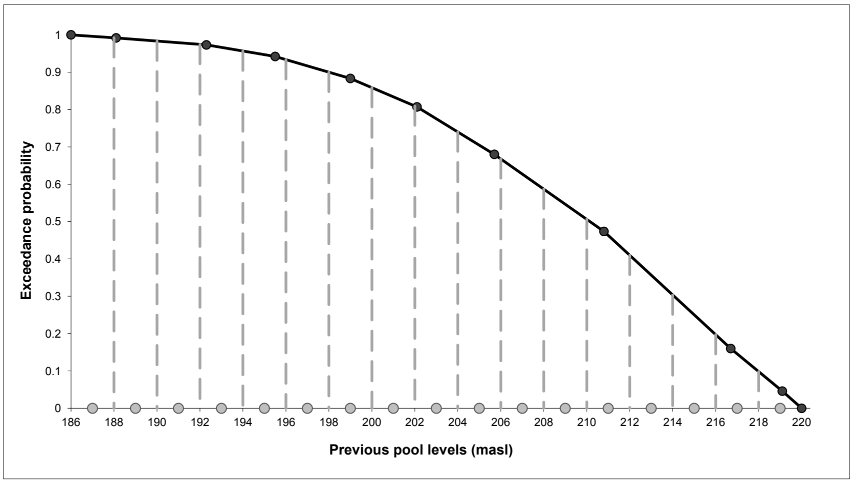


Figure 5.12: Curve of exceedance probability for the previous pool levels and adopted discretization.

It is necessary to introduce in the risk model the exceedance probability curve (defined by the black points in figure 5.12)) through a chart, as it is shown in table 5.2. The intervals of the discretization have to be introduced too.

Previous pool level (m)	Exceedance probability
185.5	1
187.6	0.9918
191.8	0.9730
195.0	0.9420
198.5	0.8832
201.6	0.8070
205.2	0.6800
210.3	0.4736
216.2	0.1600
218.6	0.0460
219.5	0

Table 5.2: Information of the previous pool levels introduced in the model.

5.5 Outlet works and spillways reliability study

5.5.1 Outlet works and spillways reliability in Risk Analysis

Outlet works and spillways reliability is of great relevance to dam safety, and has played a fundamental role in many catastrophic failures. It is well known the importance outlet works and spillway had in the case of the dam of Tous in Spain, whereas a multiplicity of similar cases can be found in the international scene [84].

Despite its manifest importance, outlet works and spillways reliability has remained an aspect of difficult integration into dam safety analysis thereby, has been usually treated separately. In the context of Risk Analysis, this aspect gets integrated in the risk model and its impact on safety becomes quantifiable.

Within the global process of Risk Analysis, the estimation of the reliability of outlet works and spillways makes part of the studies required to feed a risk model, more precisely, the part concerning the loads (see figure 5.1).

The effect on dam safety of the reliability of outlet works and spillways is indirect: a low reliability increases the probability of reaching high pool levels in the reservoir (or even overtopping), which increases failure probability.

Therefore, the information these nodes should include is the probability that every outlet works and spillway behaves properly, that is, that in the moment of the arrival of the flood the outlet work or spillway can be used. It is usual (and most of the times sufficient) to make the hypothesis that each outlet works and spillway (each gate of a spillway, each conduit of a bottom outlet) works perfectly or does not work at all. In principle, it would be possible to study intermediate scenarios of partial dysfunction though it would be necessary to determine whether the improvement of the results would be significative.

Outlet works and spillway reliability should not be mistaken for the possibility they undergo a sudden collapse or opening that creates an artificial flood downstream. This aspect must be equally analyzed but not as a component of the loads acting on the system but as a potential failure mode. Summing up, this section does not deal with the possibility of the gates opening at an undesired time but of they not opening when desired.

5.5.2 The process of reliability estimation

As already explained, the objective is to estimate the probability that an outlet works or spillway passes a certain discharge when required by the arrival of a certain flood. The analysis of the causes that must lead to this not happening cannot be limited to a mechanical failure as experience shows failures can be due to very disparate reasons [84]. When the whole system is analyzed it becomes apparent there are several causes that might induce failure:

- Human failure (either because the need of opening a gate is not identified, or because the order is not transmitted or because the person in charge of operating a gate makes a mistake, etc.).
- Lack of access to the maneuver chamber (e.g., due to the snow).
- Mechanical failure (breakage of a piece, blockage, etc.).

- Mechanical failure of the civil works (that could render the outlet works or spillway useless).
- Electrical failure (either in the supply or in the components of the outlet works or spillway themselves).
- Blockage of the outlet works or spillway (e.g., due to the presence of logs and debris).
- Failure in the software controlling the gate or the valve (in case it exists).
- Other.

Therefore, all these assumptions must be considered to estimate the global probability of failure of the gate. Fault trees are the best tools to combine these different probabilities and to study each of them in detail.

A fault tree is a deductive logical tool in which a major undesired event -failure- is postulated and from which all the possible manners it can occur are deducted systematically. Appendix A outlines a technique of fault tree analysis in more detail.

In this sense it must be noticed that a fault tree (as many other methods) is not a quantitative model itself. In reality, it is just a qualitative tool that can be evaluated quantitatively. Thus, it is usual to employ a fault tree as a mere tool for aiding in the understanding of a system or for rationalizing a discussion, without doing any numerical evaluation. Even in these cases, the knowledge provided by the FTA will prove very helpful in the assignment of reliability probabilities. Concerning the level of detail of the analysis, it can be classified into three categories:

Basic. After discussing all the possible causes of failure, a probability that encompasses all of them is then estimated.

Intermediate. A fault tree with a high-level of detail is done, disaggregating all the causes of failure, but without including the quartering of the system into mechanical and other components. The disaggregated probabilities are then estimated and the global probability is calculated through the fault tree.

Detailed. A fault tree as exhaustive as possible is done, modeling even the different mechanical, electrical supply and chain of command components. The probabilities of the disaggregated elements are estimated and then the global one is obtained through the fault tree.

It is advisable to perform intermediate level analysis at minimum, since trying to estimate the probability with a single figure is very complicated and can lead to unnecessary imprecisions and biases. On the other extreme, a detailed level could not be at reach for all analysis, due to either a lack of information or to the excessive time and effort it demands. Additionally, it is essential to keep the same level of detail along the whole risk model as it is not efficient to analyze with a maximal level of detail a part of the system while other parts are being estimated in a coarser way (unless it is demonstrated that this part has a very high contribution on the quality of the global result). In every case a sensitivity analysis of the results must be done. As a minimum, optimal and worst results should be obtained in order to determine an interval that delimits the results.

The relative importance each outlet works and spillway has in dam safety must be considered too. For instance, if an analysis of the outlet works or spillway reliability is being performed on a dam with a spillway capacity of 500 m^3/s and a bottom outlet capacity of 50 m^3/s it will be probably more efficient to consecrate more efforts to the estimation of the reliability of the spillway. Similarly, it will be more sensible to perform a detailed analysis in a dam highly reliable on their outlet works and spillways for flood routing than in a dam with a very comfortable margin in terms of hydrologic safety. The relative importance of the outlet works and spillways can be determined by doing a preliminary risk model in which the impact of reliability can be assessed through a sensitivity analysis.

Figure 5.13 shows an example of fault tree with an intermediate level of analysis. The tree is very generic and a real case should be studied in more depth by considering all its specificities. Appendix A provides an example of a fault tree developed at a high level of detail along with a technical explanation of fault tree analysis technique.

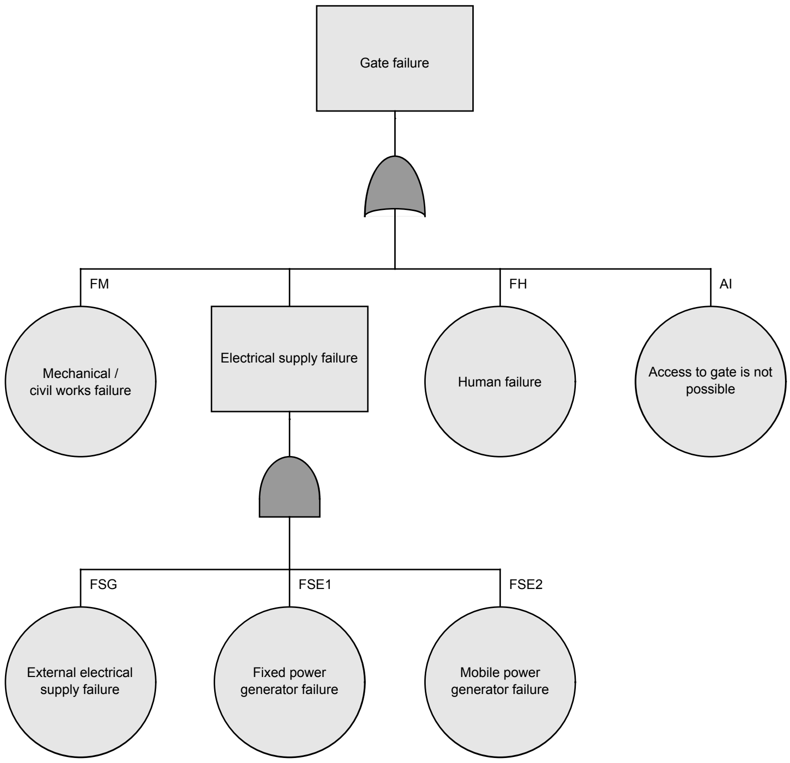


Figure 5.13: Example of generic fault tree for an analysis with an intermediate level of detail.

Once the logic of the system has been modeled through fault trees, individual probabilities have to be estimated. For this, there exist mainly two tools:

Analysis of historic registers. It consists of estimating the reliability of the system or of any of its components based on past failure frequencies.

On some occasions, the operators of the dam can access the registers of all the maneuvers that have been done in the outlet works or spillway and that specify if the operation was carried out successfully or if any problem was encountered. These registers must be long enough to be statistically significant. When an outlet works or spillway comprises several gates, it must be considered that failure probability might differ from one to another (e.g., from exterior spans to interior ones). In this respect, a disaggregation of the registers by gate can be helpful. However, not all operators count with this kind of register since the reliability of outlet works and spillways has not always received the same level of attention in the past. In every case, the values contained in the historic register do not have to be adopted directly as the reliability values introduced in the risk model, but can rather act as a starting point for discussion.

To carry out a detailed analysis (see above) it is necessary to count with reliability values for each component. This is the approach employed by other industries such as Aerospace where a production series is done thus providing very large and reliable databases. In the field of dams, these external databases are of limited utility (and availability), though manufacturers can provide the databases of some of the components.

Assignment of probabilities by expert judgment. The process of probabilities assignment by expert judgment during group sessions is the same as the one followed to assign failure probabilities to the different failure modes. Thus, the same comments of section 5.7 are applicable.

5.5.3 Example

Lets assume two gates are available in the spillway of the dam of the example. The individual reliability of each gate has been estimated through expert judgment from the available documentation with a value of 95%. From these data and assuming independency between the different gates, the probability of availability of each gate has been obtained through a binomial distribution (figure 5.14).

5.6 Flood routing study

5.6.1 Flood routing in Risk Analysis

When analyzing a hydrologic scenario it is necessary to carry out a flood routing study with the objective of estimating the response of the system dam-reservoir when confronted to hydrologic loads. This is obtained through the calculation of the function that relates the evacuated discharges downstream of the dam and the pool levels reached in the reservoir along time. This curve provides the data necessary to estimate:

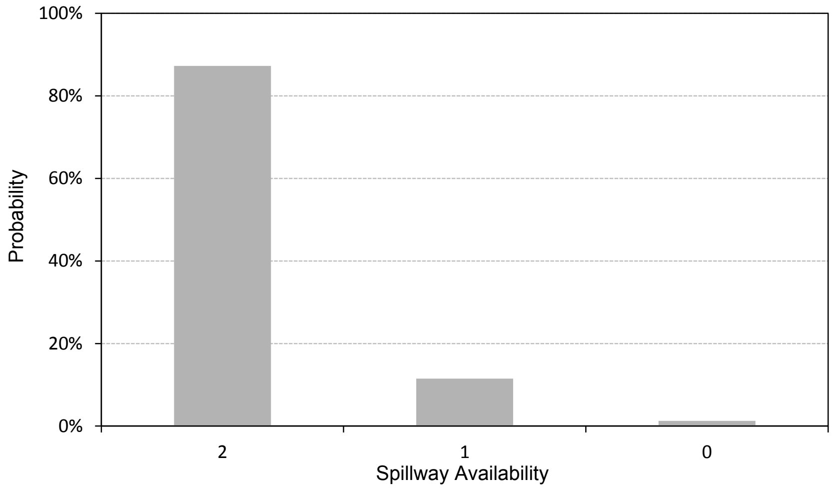


Figure 5.14: Availability of the spillway gates introduced in the example.

- The consequences downstream of the dam resulting from the spills released in case of non-break of the dam.

- The probabilities of reaching certain pool levels of loading (maximum pool level in the reservoir, potential overtopping, duration of the overtopping situation...), that will serve to quantify the probabilities of dam failure.

Therefore, within the process of Risk Analysis, the calculation of flood routing falls into both the loading and the consequences parts (see figure 5.1).

To systematize the calculations, it will be necessary to calculate each of the three variables of every combination (i.e., previous pool level, entering flood and availability of the gates). In some cases and depending on the failure mode, it will be also necessary to calculate some additional variables, such as the overtopping time. The output hydrograph is usually defined by its peak discharge, though it could be defined by other representative variables depending on the specificities of each dam.

5.6.2 Flood routing calculation

In a hydrologic system, the input variables $E(t)$[3], output $Q(t)$ and storage $V(t)$ are related by the continuity equation:

$$\frac{dV}{dt} = E(t) - Q(t)$$

This equation must be solved numerically, either through a simple direct discretization or using more sophisticated techniques such as the modified Puls method and the method of Runge-Kutta.

The data required to carry out a flood routing calculation are:

- Hydrograph entering the reservoir (inflow hydrograph).
- Previous pool level.
- Characteristic curve of the reservoir.
- Discharge curves of the outlet works and spilways.
- Gates operation rules.

5.6.3 Particularities of flood routing in Risk Analysis

Over-release by overtopping

As opposed to other deterministic studies, Risk Analysis contemplates for each action both possibilities of the dam breaking and resisting. Therefore, in order to model properly the cases in which important loads are acting and the dam does not fail, it will be required to model the overtopping process and to integrate it as part of the capacity of response of the system when facing hydrologic loading. In this case it is considered that an uncontrolled spill takes place, similar to the one produced by a gateless spillway, with a length of spillway approximately equal to the length of the crest of the dam (or, when it is possible, to the length the spill is forecast to take place along).

[3] In general, the entries to the reservoir will depend on time and will be represented by the input or inflow hydrographs. In the case of a very large reservoir, the movement of the flood wave will depend on the dimensions of the reservoir too, and at its arrival to the dam it will do a backwater curve from the tail of the reservoir. Thus, and since what is looked for are the pool levels in the dam, E will be a function of time, of the surface of water in the reservoir and of its dimensions. In most reservoirs this distinction is not needed as it can be considered that the entries E to the reservoir depend exclusively on time; this means that the surface of water in the reservoir is supposed horizontal during all the process, that there are no effects of backwater in the tail and that at any instant the discharge that arrives in the reservoir affects directly the water levels in the dam.

Existence of parapets

The existence or absence of a parapet (small protection wall built all along the crest of the dam to protect the passage and avoid falls) can impact the calculation of the flood routing, if water reaches the crest. Parapets can be continuous walls of a certain height or include openings.

On the one hand, if the parapet is closed, continuous and resistant enough to support a certain hydraulic load on its upstream side, it could be considered as an additional height added to the one of the dam proper. Thus, part of the increase of the pool levels induced by the flood could be absorbed and an additional volume of water could be stored which would favor the flood routing.

On the other hand, if the pool level in the reservoir was to reach the crest and find an open or semi-open parapet, a certain overtopping will take place. Then, the possibility of the parapet breaking under the effect of the hydraulic loading of the rising water must be considered.

In every case it must be checked that the parapet is resistant enough to absorb the hydraulic action imposed by the pool levels in the reservoir.

Dealing with non-monotonic relations

Sometimes, for the same situation of previous pool level in the reservoir and availability of the gates, a higher return period flood - thereby, a lower annual exceedance probability (AEP)- results in a lower maximum pool level of reservoir (MaxPL). This can happen due to the operation sequence of the gates: when a larger flood arrives more gates are open and a smaller MaxPL might be found (obviously, these phenomena only take place in dams regulated through gates). Consequently, the relation AEP-MaxPL can be non-monotonically decreasing. Figure 5.15 shows a relation AEP-MaxL for a real case presenting this characteristic.

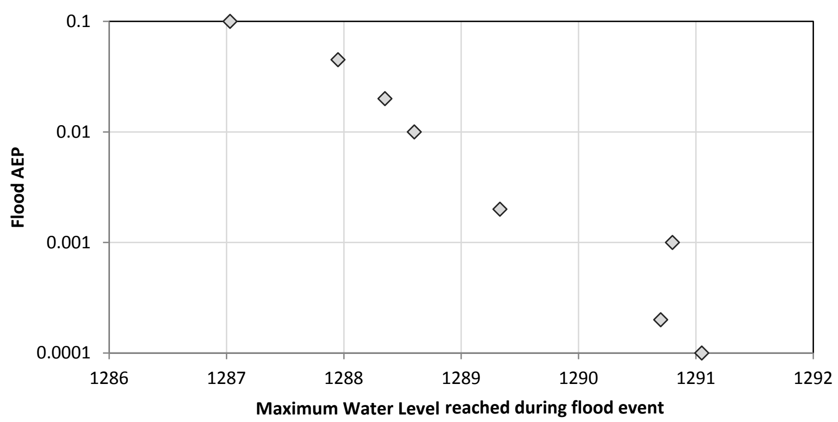


Figure 5.15: Example of the non-monotonic relation AEP-Max Pool Level.

Depending on how routing results are introduced in the risk model, in those cases it might be necessary to post-process the results of the routing study before incorporating them to the model. The problem lies on the fact that two variables are being modeled: the magnitude of the flood and another one derived from the former, the maximum pool level in the reservoir, and it is usually assumed that both share the same AEP. However, in the cases where the function is non-monotonic, this hypothesis is not verified. That is, the AEP of the flood is not the same as the AEP corresponding to the maximum pool level. In these cases, you should either explicitly model the AEP of floods and then calculate for each branch the maximum pool level associated with each flood or you should properly calculate the AEP-MaxPL curve.

Dam systems

It is important to notice that the hydraulic loads on a dam that makes part of a system of dams 1, 2, 3... (where dam i is upstream $i + 1$ and downstream $i - 1$) depend as much on the hydrologic phenomena entering its basin, as on the operation rules of the dams upstream.

If in the relevant basin of dam i rainfall is happening and creates a flood, in the basins of dams $i - 1, i - 2, \ldots$ the same rainfall is able to produce other loads that have to be related to releases of water in these dams. Therefore, when calculating the routing associated with a certain dam i, it will be possible to take into account the possible routings of the upstream dams $i - 1, i - 2, \ldots$ since these ones would imply additional hydraulic loading. Similarly, the number of scenarios will be doubled if the potential breakage of a dam upstream of another is considered. All these considerations increase the complexity of the studies, so before performing any calculation, it is advisable to assess the importance they might have in the final results depending on the relative size of the reservoirs and their associated basins.

5.6.4 Example

In the example, the step after estimating floods, previous pool levels and reliabilities of the gates, is to perform the dam routing study with the help of a spreadsheet. For this, the characteristic curve of the reservoir has been used along with the discharge curves of each of the spillway and the operation rules of the reservoir. Figure 5.16 shows the result of routing for a certain previous pool level, gates availability and flood.

This routing calculation has been done for each considered flood and for each combination of spillway gates availability. The result of these calculations can be summarized in a large table where each line represents one of the routing calculations that will have to be introduced in the risk model. Table 5.3 shows the first lines of this table that is composed of the different combinations of:

- Previous water level, PWL.

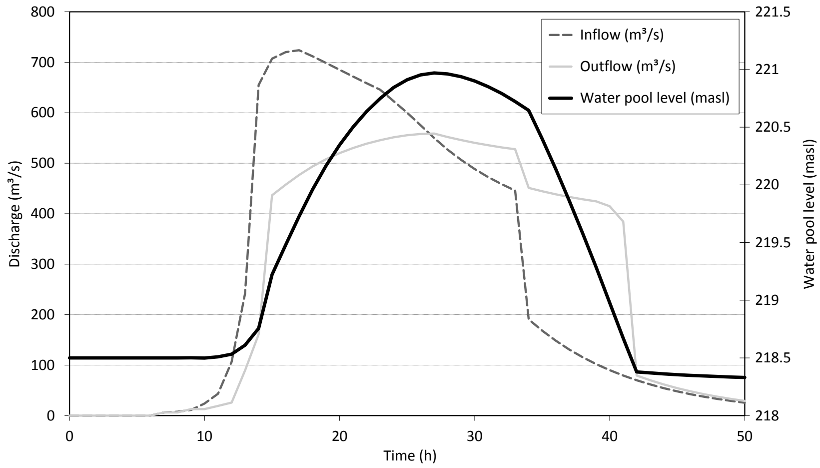


Figure 5.16: Routing example.

- Annual probability of exceedance, AEP (or its inverse, the return period).
- Availability of the spillway, ASp.

And it offers, for each previous combination, the value of the following variables:

- Maximum water level reached in the reservoir, MaxWL.
- Maximum overtopping height, HOv.
- Discharge routed by the dam, QRou.
- Time of overtopping, TOv.

5.7 Study of failure probabilities

5.7.1 Estimating failure probabilities in Risk Analysis.

The study of failure probabilities is an integrating piece of the risk model necessary to feed it once its architecture has been defined. Within the field of dam safety, this study is rarely done out of the scope of Risk Analysis. The study deals with the second component of the three that define risk (loads, probability of failure and consequences, see figure 5.1). The study of failure probabilities follows the identification of failure modes; therefore, all failure models to be included in the model must have been identified and disaggregated into their failure mechanisms prior to perform the present study.

Once the failure modes have been split in well-defined steps, the probability of each of them must be estimated. The split is done on the basis of event trees and influence diagrams. To do an estimation of the probabilities several tools are at hand, mainly:

PWL	AEP	T	ASp	MaxWL	HOv	QRou	TOv
186.5	0.0001	10000	0	210.64	0.00	0.00	0
188.5	0.0001	10000	0	211.46	0.00	0.00	0
190.5	0.0001	10000	0	212.34	0.00	0.00	0
192.5	0.0001	10000	0	213.29	0.00	0.00	0
194.5	0.0001	10000	0	214.30	0.00	0.00	0
196.5	0.0001	10000	0	215.38	0.00	0.00	0
198.5	0.0001	10000	0	216.53	0.00	0.00	0
200.5	0.0001	10000	0	217.73	0.00	0.00	0
202.5	0.0001	10000	0	218.97	0.00	0.00	0
204.5	0.0001	10000	0	220.29	0.00	0.00	0
206.5	0.0001	10000	0	221.69	0.00	0.00	0
208.5	0.0001	10000	0	223.09	0.00	11.08	18
210.5	0.0001	10000	0	223.47	0.00	132.57	37
212.5	0.0001	10000	0	224.03	0.23	424.67	41
214.5	0.0001	10000	0	224.12	0.32	481.67	44
216.5	0.0001	10000	0	224.23	0.43	550.11	47
218.5	0.0001	10000	0	224.33	0.53	621.44	50
186.5	0.0001	10000	1	210.64	0.00	0.00	0
188.5	0.0001	10000	1	211.46	0.00	0.00	0
190.5	0.0001	10000	1	212.34	0.00	0.00	0
192.5	0.0001	10000	1	213.29	0.00	0.00	0
194.5	0.0001	10000	1	214.30	0.00	0.00	0
196.5	0.0001	10000	1	215.38	0.00	0.00	0
198.5	0.0001	10000	1	216.53	0.00	0.00	0
200.5	0.0001	10000	1	217.73	0.00	0.00	0
202.5	0.0001	10000	1	218.54	0.00	64.15	0
204.5	0.0001	10000	1	218.82	0.00	199.70	0
206.5	0.0001	10000	1	219.61	0.00	233.76	0
208.5	0.0001	10000	1	220.37	0.00	260.84	0
210.5	0.0001	10000	1	221.13	0.00	284.24	0
212.5	0.0001	10000	1	221.92	0.00	305.54	0
214.5	0.0001	10000	1	222.96	0.00	330.80	0
216.5	0.0001	10000	1	223.35	0.00	421.83	5
218.5	0.0001	10000	1	223.56	0.00	512.76	11
186.5	0.0001	10000	2	210.64	0.00	0.00	0
188.5	0.0001	10000	2	211.46	0.00	0.00	0
190.5	0.0001	10000	2	212.34	0.00	0.00	0
192.5	0.0001	10000	2	213.29	0.00	0.00	0
194.5	0.0001	10000	2	214.30	0.00	0.00	0
196.5	0.0001	10000	2	215.38	0.00	0.00	0
198.5	0.0001	10000	2	216.53	0.00	0.00	0
200.5	0.0001	10000	2	217.73	0.00	0.00	0
202.5	0.0001	10000	2	218.54	0.00	64.15	0
204.5	0.0001	10000	2	218.82	0.00	358.74	0
206.5	0.0001	10000	2	219.04	0.00	420.70	0
208.5	0.0001	10000	2	219.26	0.00	439.64	0
210.5	0.0001	10000	2	219.49	0.00	458.64	0
212.5	0.0001	10000	2	219.77	0.00	480.16	0
214.5	0.0001	10000	2	220.49	0.00	529.21	0
216.5	0.0001	10000	2	220.38	0.00	522.29	0

⋮

Table 5.3: First lines of routing results in the example.

- Reliability tools
- Expert judgment
- Specific methodologies to estimate failure probabilities

At its turn, these tools are based on other ones such as numerical models (deterministic and statistic), Monte Carlo techniques or the standardized charts of verbal descriptors, as the ones outlined next.

In reality, the former classification is not composed by hermetic cases. For example, it is valid to study some probabilities of the same failure mode through expert judgment and other ones throughout reliability techniques. It is also possible to employ both methods in the estimation of the same probability, as reliability techniques require data that can be estimated through expert judgment.

5.7.2 Estimation through reliability techniques

Any probability of a failure mode that can be modeled by a deterministic numerical model is a potential candidate to be numerically assessed throughout reliability techniques. Reliability techniques (or reliability analysis) consist of propagating the uncertainties of the input of a model until reaching a result, in such a way that a probability is obtained instead of a deterministic value.

A paradigmatic case is the sliding of a concrete dam [6], but there are more applications. For example, Fell et al. [57] have developed an event tree for failure due to internal erosion. The first node corresponds to the question "is the existent gradient higher than the critical one (for the considered loads)?" This question could be answered by a "yes" or "no" (probability 1 for one of the branches and 0 to the other one) if a completely deterministic model of the flow net of the dam was done. As more uncertainty is introduced in the model (e.g., through stochastic modeling of the permeability of the materials) the results will be more adjusted and the original probabilities will cease being 1 and 0.

In the cases where it is possible (and so decided) to do a quantitative analysis of conditional failure probabilities, the numerical models are usually related to Monte Carlo techniques. The uncertainties they must incorporate include: the scenario (levels of water, earthquakes to be considered, etc.), the way in which the loads act (uplift pressure, effective pressure, etc.) and the properties of the materials. Other common difficulty lies in the definition of failure itself, in particular when the seismic scenario is under study. Therefore, though the model is built on a deterministic basis, at least, part of its input parameters have a stochastic structure, causing the output of the model to be also of stochastic nature.

To estimate failure probability it is possible to use a Monte Carlo Crossed-Validation or techniques from experimental design to reduce the number of executions of the model (e.g., the Latin Hypercube). However, the number of necessary executions required for reaching an acceptable level of accuracy combined with the long times of execution of the usual models, can make the problem impossible to tackle in a direct way. A technique to overcome this obstacle is to deduce an analytic failure function (limit surface) from a few runs of the model and with the help of expert engineering judgment. Simplified analysis techniques as *First Order Second Moment* (FOSM) are also acceptable. Finally, it is worth mentioning that apart from studying the relevant failure probability it is convenient to correlate it to safety factors.

At Universidad PolitÃ©cnica de Valencia (Spain), a methodology has been developed for the systematic application of reliability techniques for failure probability estimation that can be of help [5].

5.7.3 Estimation by expert judgment

The estimation of probabilities by expert judgment consists of recording the opinion a subject has about the plausibility of an event. Therefore, it is a subjective probability (see definition in chapter 2). In order to give more solidity to this estimation, the average of the estimations of several individuals is always done. Moreover, there is a series of good practice rules that must be followed when doing this kind of estimations (see Appendix B).

When probabilities are estimated through expert judgment, numerical models usually play a relevant role too. Although a numerical model does not provide directly failure probability, it can contribute to the understanding of the problem through the different parts composing the process. It can also delimit the boundaries of the debate, demonstrating a failure mode is more or less plausible or quantifying the effect of some characteristic on which there exist some uncertainty through sensitivity studies. The process of estimating failure probabilities throughout expert judgment has an information role in which deterministic models are as valid as statistic or hybrid ones.

How to get probabilities by means of expert judgment is exposed with more detail in Appendix B.

5.7.4 Specific methodologies to estimate failure probabilities

With the cumulated experience of years of estimating failure probabilities in dams, some methodologies have emerged to help with this estimation in a more or less guided way. In some occasions they are very detailed methodologies for a specific failure mode, with charts and procedures that correlate the different variables with probabilities [57, 22, 28]. In other cases, the methodologies consist of a collection of recommendations, tables and good practices that act as an aid in the estimation of the different probabilities encountered in a Risk Analysis [29].

An interesting example has been developed by Silva et al. [122], that analyses the probability of failure in slopes. The paper suggests a relation between the safety coefficient of a slope and its probability of failure. The relation is also affected by aspects that cause uncertainty, like the level of control of the works during the construction of the slope.

To employ the proposed methodology, first of all, according to existing information on its properties, the slope has to be classified.

After that, a numerical model of the slope must be done to evaluate the safety coefficient. Finally, the coefficient must be entered in a graph that relates the annual probability of failure as a function of the safety coefficient. With this, an estimation of the failure probability of the dam is obtained. This relation was found by several experts from data of 75 projects along more than four decades and respecting probability axioms. It is interesting to notice the curves that relate safety coefficient and probability tend to the horizontal as the safety coefficient increases. This reflects reality where over-dimensioning in excess a structure does not reduce its failure probability. This is due to the fact that, beyond a certain point, factors such us discontinuities, soft areas, damp areas, zones of high or low permeability and other elements that might have been disregarded in the geotechnical study, will start controlling the problem.

5.7.5 Example

The example comprises two failure modes. The failure probabilities by overtopping have been estimated directly from the height of overtopping using a standard curve of failure by overtopping for gravity dams.

The failure by sliding has been studied for two different situations of uplift pressures, where the failure probability for each level in the reservoir has been estimated with a model of dam stability employing Monte Carlo techniques. One of the situations considers the stability of the dam against a level of water in the reservoir for high uplift pressures (assuming a triangular distribution) while the other one concerns the stability in case of low uplift pressures (admitting an efficient relieve of uplift pressures).

The probability of being in one or the other situation is defined by the two previous nodes, that estimate the probability of finding high pressures in the dam (30%) and the probability of these ones being detected and avoided before the sliding takes place (30%). The probabilities of those two nodes have been estimated through expert judgment after analyzing all the available information on the drainage and monitoring systems.

Figure 5.17 shows the fragility curves for both failure modes.

5.8 Study of failure hydrographs

5.8.1 Estimating failure hydrographs in Risk Analysis

The estimation of the failure hydrographs is integrated into the analysis of consequences of the process of Risk Analysis (see figure 5.1). The first step of the analysis

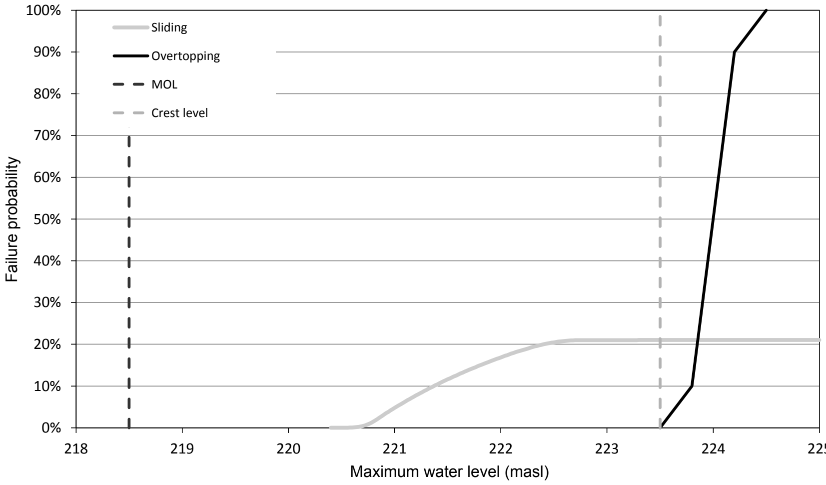


Figure 5.17: Fragility curves for the two failure modes of the example.

of consequences is to estimate the failure hydrographs due to the dam failure. Afterwards, these hydrographs will be used in the estimation of the consequences curves (section 5.9).

The first step in the estimation of failure hydrographs is to estimate the dam failure breach. This breach may be different for different failure modes and its progression will also vary as the water level in the reservoir changes. Consequently, as opposed to the studies usually developed for an Emergency Action Plan in which only a few failure scenarios are studied (e.g., breakage with the reservoir at its crest level), Risk Analysis contemplates the failure hydrographs corresponding to the whole range of possible pool levels in the reservoir and to each of its failure modes.

In risk models, failure hydrographs are usually characterized throughout a significant variable (usually the peak discharge). This makes the required works to be split in two parts:

- Estimation of a curve relating the maximum pool level with any representative variable of the failure diagram (e.g., breakage peak discharge) for each failure mode. These curves are introduced in the risk model.
- Estimation of the complete failure hydrographs (not just their peak discharge). These hydrographs are not introduced directly in the risk model but serve in the calculation of the curves of consequences in case of peak discharge (section 5.9), which are the ones introduced in the model.

For this, two approaches are suggested depending on the intended level of detail:

Detailed: The failure hydrographs for several pool levels of reservoir are obtained (and for each failure mode if it affects the failure hydrograph). The curve of peak discharge vs. pool level is obtained by correlating the peak discharges of the hydrographs with the maximum pool levels to which they correspond.

Basic: A single failure hydrograph is obtained and then, it is escalated for smaller and larger peak discharges. The dam break peak discharge curve vs. pool level is obtained from empirical relations (see section 5.8.3).

The basic level of detail can be particularly advantageous when there are already one or several available failure hydrographs, for example, the ones contained in the Emergency Action Plan. In this case, the proposed methodology provides the required results with little effort. On the contrary, if it is necessary to calculate the failure hydrograph, the additional effort required to develop the explained methodology is relatively small.

5.8.2 Calculation of failure hydrographs

Nowadays, the dam engineer counts with a broad range of hydraulic numerical models that allow him or her to simulate the creation of a fracture in a dam (for both embankment or concrete gravity types) and the resulting output hydrograph through this breach and along the riverbed.

Wahl [140] compiles the different models that have been developed with both a parametrical and physical basis. Currently, parametrical models are widely extended and are found as integrating parts of hydraulic packages of a more general scope such as HEC-HMS [115], HEC-RAS [20] or MIKE [39].

5.8.3 Calculation of peak discharges through empirical relations

Some researchers have used past dam failures to develop empirical equations that relate peak discharges at failure with one or several parameters of the dam or the reservoir (height of the dam, storage volume, water level at the moment of failure, etc.).

Among the most renowned methods the ones developed by the following entities and people can be highlighted: Kirpatrick [81], Soil Conservation Service [125], Bureau of Reclamation [21], MacDonald and Langridge-Monopolis [88], Singh and Snorrason [123], Costa [36], Froehlich [59] and Walder and O'Connor [142]. More information can be found by comparing these methods in several compilation works [73, 140, 141].

Among all the aforementioned methods, Froehlich's one [59], is briefly explained hereafter. Froehlich developed a simple regression equation in 1995 to estimate the peak discharge as a function of the reservoir volume and its height, from the data of peak discharge of 22 cases:

$$Q_p = 0.607 \cdot V_w^{0.295} \cdot h_w^{1.24}$$

Where Q_p is the predicted peak discharge in m3/s, V_w is the volume of stored water at the moment of failure in m^3 and h_w is the pool level in the reservoir calculated from the lower point of the final breach until the water surface expressed in m. Figure 5.18 compares the values of peak discharge calculated using Froehlich equation against the ones measured in the 22 mentioned cases, along with other 10 cases of study that serve as validation-points.

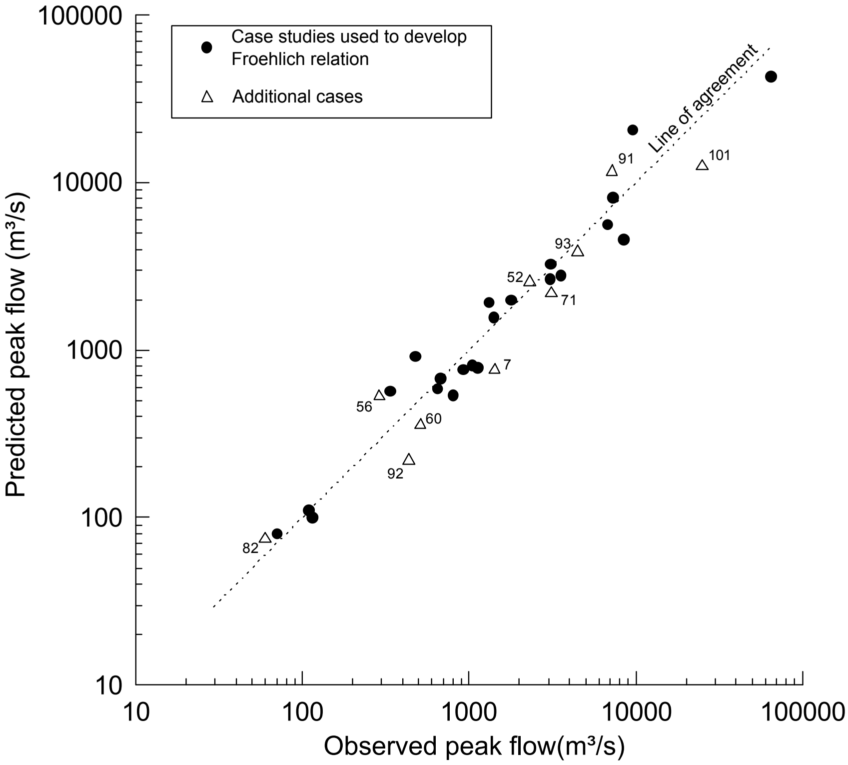


Figure 5.18: Observed peak discharges vs. predicted peak discharges using Froehlich equation. Source: [140].

Finally, it is worth mentioning that some of these methods can present a conservative bias, undesirable for the purposes of Risk Analysis. Thus, some investigators suggest adjusting the results provided by the direct use of these methods [32]. In every case, whenever an hydrograph issued from the calculations of a method considered more accurate is available, its peak discharge can be used to scale the relation obtained through the application of empiric relations.

5.8.4 Example

The data used to introduce the relation between the pool level in the reservoir and the failure peak discharge in the example are issued from hydraulic simulations of the failure breach with different water levels of reservoir. The geometrical characteristics of the considered breaches differ and depend on the failure mode. In this example, whereas in the failure by sliding failure happens in the center of the dam, in case of overtopping failure starts in the abutments. Figure 5.19 shows the relation between the maximum level in the reservoir and the failure peak discharge, which constitute the data to be introduced in the risk model at this stage. The failure hydrographs are employed in the following step to calculate the consequences of failure.

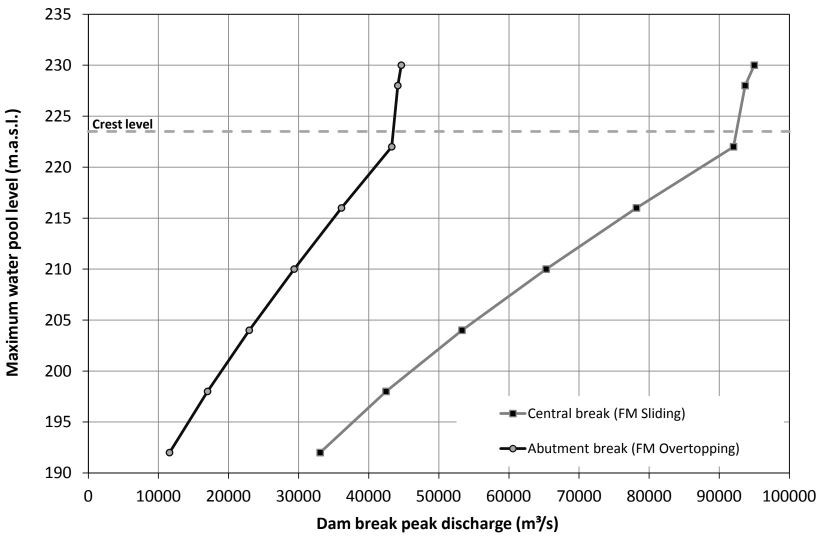


Figure 5.19: Relation between the maximum water level attained in the reservoir and failure peak discharge.

5.9 Study of consequences

5.9.1 Estimating consequences in Risk Analysis

Damage produced by a dam failure is in general very important, causing serious economic consequences and in many cases, loss of life. In Spain, the most relevant examples of these disasters are the failure of Tous dam in Valencia in 1982 [94] and the failure of the dam of Vega de Tera in Zamora in 1959. It is therefore substantial to include a quantification of damage ensuing the potential failure of a dam in order to incorporate them in the Risk Analysis.

Table 5.4 shows a summary of the consequences that can result from dam failure. These consequences can be classified accordingly to the instant in which they take place and the way they are assessed. Regarding the first classification, they can be divided into direct and indirect. Direct consequences are those created directly by the impact of the flood and are the most visible ones. On the contrary, indirect consequences appear after the impact of the event and are reflected in the economy and in other activities of the area. With regard to the second classification, consequences can be split into tangible and intangible ones, depending on whether the consequences can be evaluated in economic terms or not.

The emphasis put in the estimation on each of these consequences will depend in

	Tangible	Intangible
Direct	Residences Structure inventory Vehicles Agriculture Infrastructure and other public facilities Business interruption (inside flooded area) Evacuation and rescue operations Reconstruction of flood defences Clean-up costs	Fatalities Injuries Animals Utilities and communication Historical and cultural losses Enviromental losses
Indirect	Damage for companies outside flooded area Substitution of production outside flooded area. Temporary housing of evacuees	Social disruption Damage to government

Table 5.4: Overal classification of flooding consequences [79].

great measure on the objectives and scope of the study. For example, for the purposes of the comparison of risk results with international recommendations on risk tolerability (chapter 6), it is particularly relevant to estimate loss of life. However, for estimating the efficiency of the measures targeting risk reduction, the estimation of the economic loss acquires a great importance.

The analysis of consequences consists of three parts: estimation of the failure discharge, study of the flood and estimation of its consequences. This section deals with the two latter. The main objective is to obtain a relation between the dam output hydrograph (in case of failure and non-failure) and its consequences. This makes possible to relate them directly with the analyzed situation. It is worth stressing that consequences will be analyzed for each case of study twice: on the hypothesis of failure of the dam and on the hypothesis of non-failure. By doing this, the incremental consequences required in the risk model will be obtained afterwards throughout a simple subtraction. In general, consequences are analyzed in economic terms and in loss of life, which makes that four curves are usually introduced in the model (two parameters combined with two hypotheses).

This section explains how to estimate consequences from the failure hydrographs obtained in the previous section (i.e., how to obtain the relation between consequences and hydrographs).

Within the risk model, consequences can be introduced throughout the use of curves relating consequences to one representative variable of the output hydrograph of the dam. In general, an appropriate variable is the maximum discharge evacuated by the dam: either the maximum routed discharge for estimating the consequences in the case of non-failure or the peak dam break discharge in the failure case. This variable is relatively easy to calculate within Risk Analysis and it is very important in the definition of the hydrograph characteristics. Besides, its is a decisive variable in the definition of the characteristics of the resulting flood, since usually larger discharges flood larger areas, with higher depths and heavier costs.

5.9.2 The process of estimating consequences

The estimation of consequences is based on the dam output hydrographs obtained from flood routing (section 5.6) and the dam failure hydrographs (section 5.8), as it is shown in 5.20.

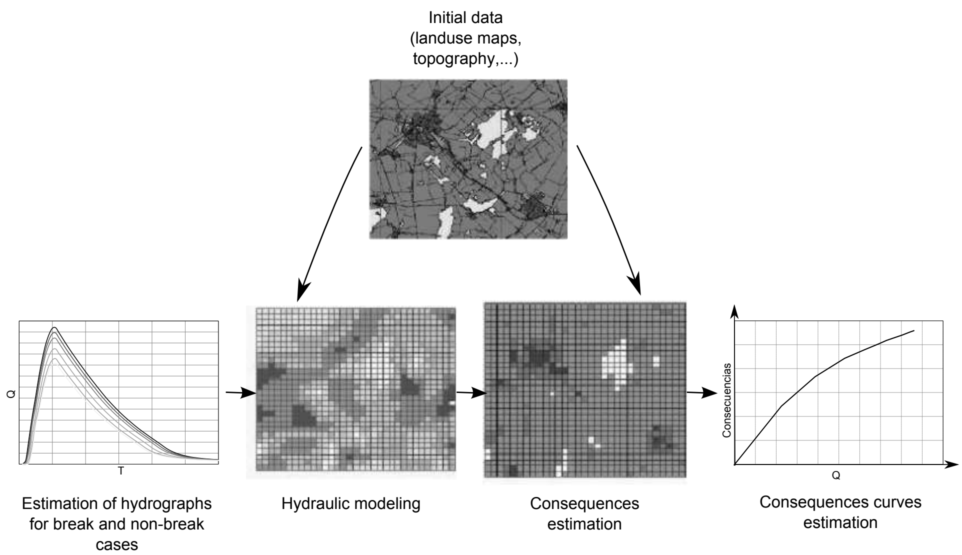


Figure 5.20: General procedure to estimate flood consequences.

A hydraulic modeling of the flood is done based on these data and to apply the different methodologies for estimating consequences. In this document, consequences have been gathered as follows:

- Loss of life: estimation of the number of fatalities resulting from the dam failure. As it has been mentioned, the existent recommendations on risk tolerability give a lot of importance to this type of consequences. Due to its relevance, a whole appendix is dedicated to detail the existent methodologies for determining this parameter (Appendix C).
- Economic consequences: they include direct economic consequences produced by the flood wave, indirect consequences produced by the flood and losses created due to the absence of the dam. Due to its relevance, a whole appendix is devoted to detail the existent methodologies for calculating them (Appendix D).
- Other consequences: there exists a series of damage that cannot be included in

the economic consequences or loss of life such as environmental damage, social disturbance or destruction of historic and cultural heritage [13]. These kinds of damage are difficult to define numerically and therefore difficult to integrate in a quantitative analysis but it is important to take them into consideration. However, environmental damage must be considered in the decision-making process due to their great social relevance [137]. In this respect, the European Directive 2007/60/EC on Calculation and Management of Flood Risks specifies that environmental risks must be included in the analysis. At present, it is impractical to integrate this kind of damage numerically within a quantitative risk model, but it is possible and convenient to study the impacts the different events of the analysis would produce in the environment qualitatively.

The values obtained for all this damage allow the definition of curves relating peak failure discharge to consequences. These curves will finally allow the introduction of consequences in the risk model (section 5.9.3).

Regarding the hydraulic model, the characteristics that are particularly important in the estimation of consequences are: time of arrival of the wave of the flood, maximum speed, maximum depth and time at which this water level is found. Moreover, other data such as the speed of rising of the depth and the duration of the flood can also be useful.

There is a broad variety of hydraulic models to do this kind of simulation and, in order to choose an adequate one, it is important to be particularly attentive to the type of regime, type of flow and the way turbulent flow is treated [96]. To make the choice easier accordingly to the particular case under study, ICOLD [73] has analyzed 27 different hydraulic models and explained their mechanisms, properties and how to adapt each of them to the characteristics of the flood wave.

Additionally, in order to represent geographic variability properly it is necessary to define the geometry of the streambed well from the available topography and to choose intelligently the cross sections required for the hydraulic model. Also, all parameters introduced in the model must be studied carefully, particularly the roughness coefficient [4].

Using previous studies

In Spain, the Emergency Action Plan is the document that contains more information for estimating consequences. In this document the following relevant information can be found [96]:

- Flood maps for different scenarios.
- List of disruptions and damage ensuing a flood.
- Peak discharge causing the first important disturbances and marking the starting point of the curve discharge-consequences.

These data can be used to do a first estimation of the consequences at a basic level. Besides, they can serve as a basis for more detailed analysis.

5.9.3 Estimating consequence curves

The final goal of consequence assessment is the estimation of curves relating the dam output hydrograph with the resulting consequences so risks can be obtained. The peak discharge used to define a flood is usually employed to associate consequences to hydrographs, since damage will depend in great measure on this value.

Several floods with different maximum peak discharges must be studied to determine these curves. In this way, the consequences of each flood would define a point of the curve. Thus, the number of points will coincide with the number of studied floods. The larger the amount of studied points, the better defined the curve and the more accurate risk results will be. It can be concluded that the number of points will depend on the desired level of detail intended in the Risk Analysis. In general, it is advisable to use at least 4 or 5 points to avoid an incomplete definition of the curve.

On some occasions these curves present an S shape, as it is the case of the one shown in figure 5.21. This is due to the influence of the employed depth-damage and severity-depth curves, which usually follow this shape. However, shape can vary since it is also dependent on the characteristics of the flood. For instance, a consequences curve can rise almost vertically if from a certain value of discharge the flood overtops a levee of population protection (i.e., from this discharge onwards all the population would be totally flooded). It is therefore essential to study the shape of the curve and to contrast that its changes in shape correspond to what effectively happens during a flood.

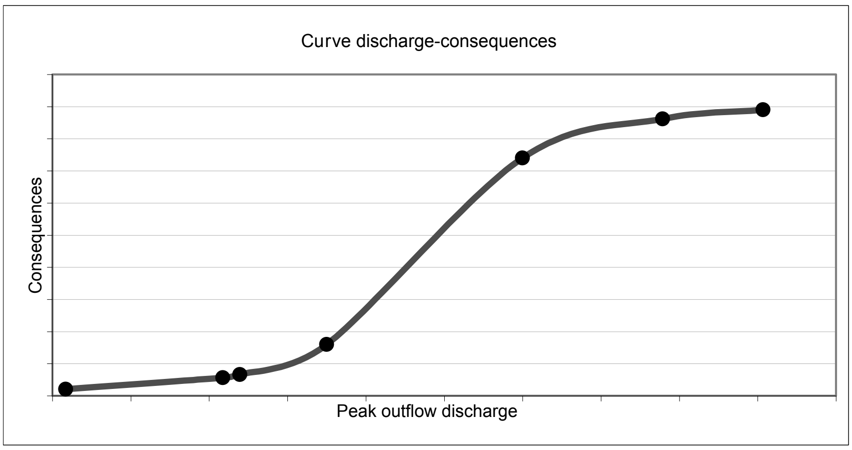


Figure 5.21: Typical shape of the discharge-consequences curve.

In general, two curves characterize consequences, one relating discharge with economic consequences and another one that relates it to loss of life. For the curve discharge-economic consequences, the points are obtained by adding direct economic consequences, indirect ones, damage due to the absence of the dam and the cost of rebuilding the dam. For the curve discharge-loss of life, the points are obtained directly following the methodology of loss of life estimation.

Additionally, the Dam Safety File of the Dam (e.g., the Emergency Action Plan) might contain data allowing the direct obtention of certain points of the curve with no need for calculations. For example, if it establishes a certain discharge from which significant consequences appear, this point can be taken as the starting point of the curve.

In general, for Risk Analysis, it is necessary to obtain incremental consequences (reminder: difference between the consequences in the case of failure and non-failure). Since the shape of the hydrographs can change substantially between a routed and a failure hydrograph, it can be required to calculate different discharge-consequences curves for each case (failure and non-failure), or even a different curve for each failure mode. Finally, it must be noted that damage to the structure will be included in the economic consequences associated with the failure of the dam.

5.9.4 Example

The estimation of consequences in the example has been done from the hydraulic models of flood for different water levels in the reservoir, obtaining the maximum depth, the peak discharge and the time of arrival of the flood wave for each case. The hydraulic model is the same one used to develop the Emergency Action Plan of the dam.

The PATRICOVA methodology [35] has been used to estimate the economic consequences. This methodology estimates a value of total destruction for each flooded area that is afterwards multiplied by a damage coefficient depending on the depth of water in the flooded area. This calculation has been based on the repercussions identified by the Emergency Action Plans. The results are shown in figure 5.22.

The SUFRI [49] methodology is employed to estimate loss of life. The rates of this method have been adapted to enable the consideration of different degrees of understanding of severity of the flood accordingly to the systems of warning, the existence or absence of an Emergency Action Plan, the coordination between the emergency services and the authorities and training of the population. The results are shown in figure 5.23.

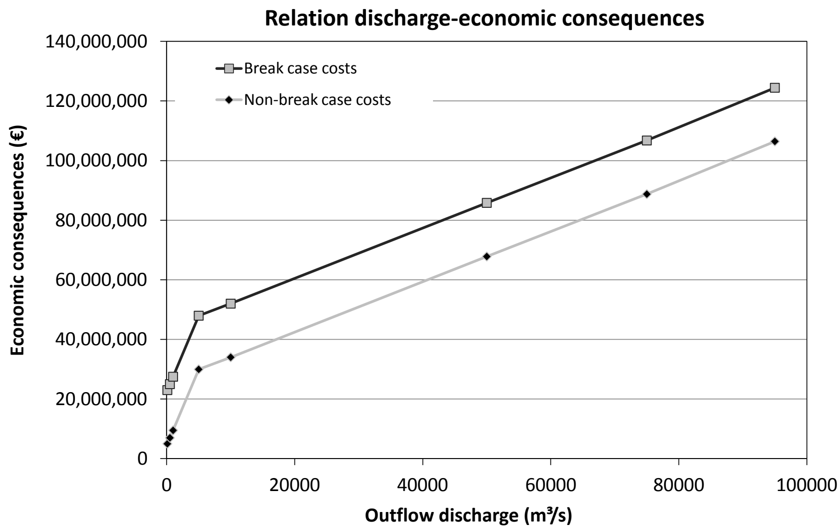


Figure 5.22: Estimation of economic consequences.

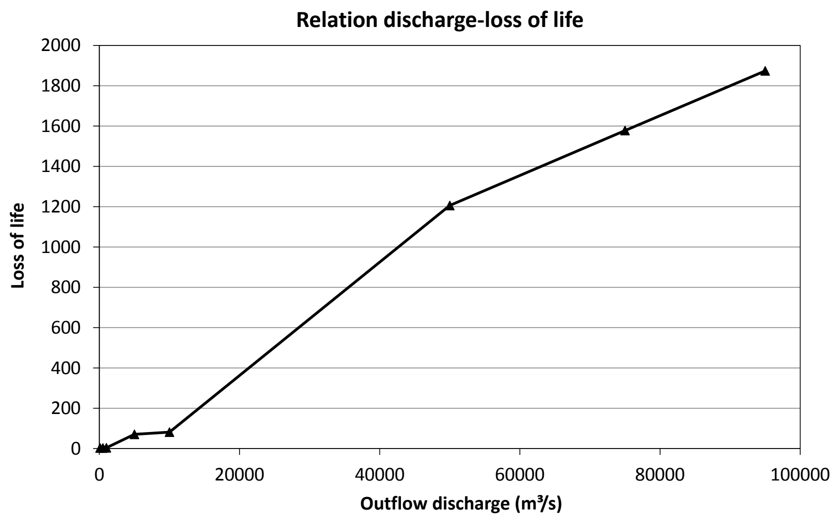


Figure 5.23: Estimation of loss of life.

5.10 Risk calculation

5.10.1 Set up

With all the input variables of the risk model in place, the calculation of the risk can be performed. It is usual to do a first calculation for the current situation, which is sometimes called *base case*. From this calculation it is possible to evaluate the risk in the current situation (see chapter 6).

The following step consists of modifying the risk model to reflect the effect of the mitigation measures to be evaluated. Then, the calculation is repeated for each of them. Finally, the subtraction of the risk result obtained in the situation with a measure from the base case result provides the impact on risk of any particular measure.

The execution of the risk model provides all the results that can be useful in the definition of a dam: probability of failure, annualized loss of life, annualized economic loss, minimal and maximal consequences, curves fN and curves FN. These results can be obtained in total risk terms for failure and non-failure cases or as incremental results (see chapter 2). It is also useful to classify many of these results according to different variables, for example, by failure mode or by pool level in the reservoir.

With regard to the calculation itself, the procedure is conceptually simple. The probability of each branch of the event tree is obtained as the multiplication of all the conditional probabilities of the sub-branches that compose it. Failure probability and total risk can be determined by adding up the results of all the branches.

In addition to what has been discussed so far, there are some considerations specific to the obtention of risk in dam safety that should be considered when performing a calculation. These ones are outlined herein:

Discretization of continuous variables

Some of the variables appearing in risk models, such as the water level in the reservoir or the return period of a flood, are continuous. When they are to be modeled through event trees these variables must be discretized in several branches. Each of these branches will represent a range of values this variable can adopt. For ulterior calculations, a representative value of this branch will have to be taken, usually the average value of the interval. The probability of each branch will then be the probability of falling within any of the values of the range. If there is an available curve of probability of exceedance (PE) of the modeled variable, the probability of the variable being between v_i and v_{i+1}, i.e., the probability of the branch i can be calculated as $PE(v_i) - PE(v_{i+1})$.

Figure 5.24 is an example of discretization of a continuous variable, in this case, the water level of the reservoir. Starting from a relation between the water level of the reservoir and the exceedance probability, that goes from $PE = 1$ for the minimum pool level to $PE = 0$ for the maximum pool level. As an example, it is divided into 10 intervals. Each of them becomes a branch, whose probability and representative pool level can be calculated as it has been explained.

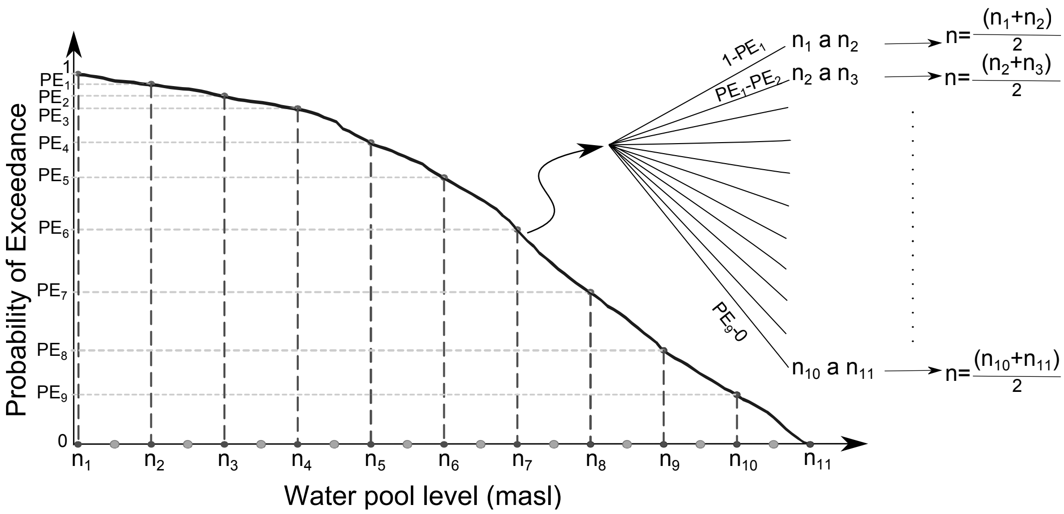


Figure 5.24: Example of discretization of a continuous variable.

When a continuous variable is discretized in intervals, accuracy increases as the intervals decrease. Consequently, this leads to a higher number of branches in the event tree. If the event tree was about to be calculated manually, the number of intervals should be necessarily small. With the employment of software to automatize the calculations, this ceases being a problem. Additionally, the intervals do not require being equidistant, and with the same number of intervals, a proper distribution can be very important in the consecution of useful and accurate results.

Adjustments related to the consideration of several failure modes

When studying dams with different failure modes it is good to consider some specific adjustments such as the common cause adjustment and the freezing of variables. A discussion of these concepts and the way they affect the discussed calculations is provided herein. For more information, [71] can be consulted.

A numerical tool that intends to perform risk calculations in the field of dam safety, must be able to do the following adjustments:

- **Common cause adjustment.** When there are k non-mutually exclusive failure modes within a same scenario (each one with an individual probability p_i), the total probability of failure of the scenario is found within the range fixed by the Theorem of the unimodal limits [92]. This theorem is therefore one way of bounding the magnitude of the total failure probability in scenarios resulting from a common cause:

$$\max(p_i) \leq p_r^e \leq 1 - \prod_{i=1}^{k}(1 - p_i)$$

If it is decided to do an adjustment from the lower limit, an option with physical meaning is to maintain without adjustment the probability of the most likely failure mode and to reduce the rest of the probabilities to 0. This corresponds to a dominance process and is equivalent to saying that if the dam fails, it will do so first due to this failure mode, preventing other failure modes from happening. Figure 5.25 illustrates the situation through a Venn diagram.

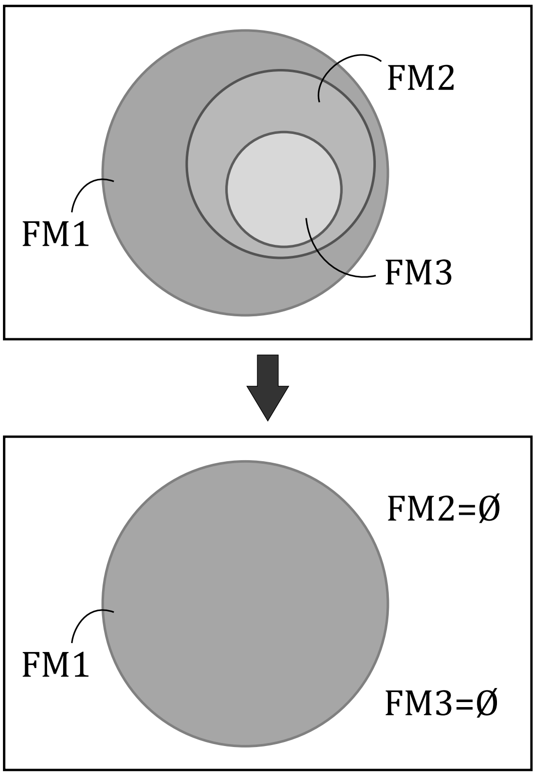


Figure 5.25: Diagram of Venn of the common cause adjustment from the lower limit.

If an adjustment from the higher limit is preferred, all the failure modes can be adjusted in the same measure so the sum of the probabilities is equal to the one calculated through its higher limit. The diagram of Venn of figure 5.26 illustrates this situation. It is also possible to perform some intermediate types of adjustment between the two detailed ones.

Many times, as there is no firm reason to prefer one type of adjustment over the other, both adjustments are calculated and the average between them is taken.

- **Freezing.** This adjustment is done to correct a limitation of the calculation of the event trees associated with the way it is usually set up. In a hydrologic scenario the action imposed by a flood is a process that develops in time. This can be appreciated for example in the reservoir, where the pool level starts from a certain value and rises (in a relatively slow way) until reaching its maximum (for this particular event). For a certain pool level, it is possible to find failure modes with a higher probability of occurrence and this distribution

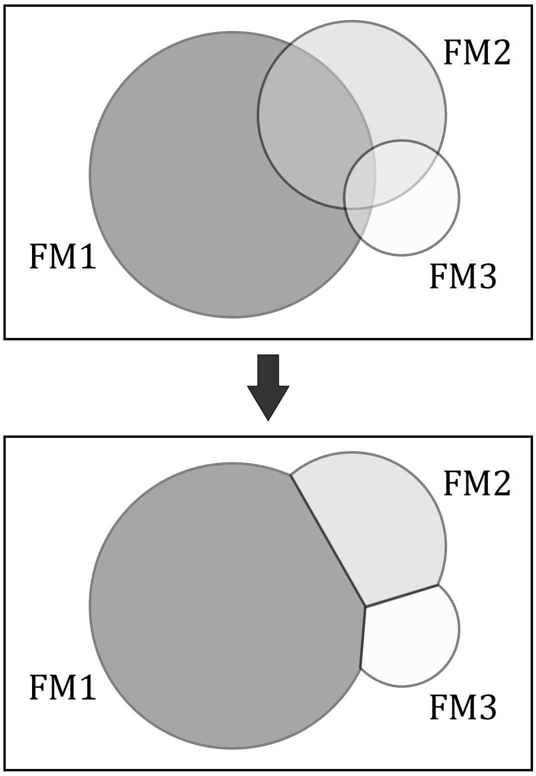


Figure 5.26: Diagram of Venn of common cause adjustment from higher limit

might be different for a superior pool level. However, there is the possibility of not reaching the second pool level because the dam might fail before it is attained.

This temporal process is intrinsically difficult to model through event trees. The approximations that can be followed to correct this simplification is admitting that when a total failure probability of 1 is reached for a given pool level, the same distribution of failure probability is maintained, remaining "frozen" for higher pool levels. This freezing can also be extended to other variables, such as failure discharge.

However, it must be emphasized that this approach remains an approximation and that in cases like the seismic scenario where the loads are almost instantaneous, there is no point in applying it.

Calculation of dams systems

Risk Analysis enables the calculation of systems composed by several dams so it is possible to capture the effects some dams have on others.

However, one must be aware that the calculations of dams systems are very expensive in terms of computational capacity as a consequence of the nature of event trees. As an example, let's admit there are two dams a and b with their event trees of n_a and n_b branches respectively. If they are analyzed separately, between the two trees it will be necessary to calculate $n_a + n_b$ branches. On the contrary, if they are analyzed as a system, the event tree can have as many as $n_a \cdot n_b$ branches (admitting they do not share any node). As n_a and n_b are usually large numbers, their multiplication is much larger than their mere addition, that is, $n_a \cdot n_b >> n_a + n_b$.

For more information about calculation of dams systems [121] can be consulted.

5.10.2 Example

Once all the input variables of the risk model are available, the risk calculation of the example can be performed.[4]

Though many other results can be extracted from the model, only the annual failure probability, the incremental economic risk and the societal incremental risk are shown (see table 5.5) as an example. The results of risk are also shown in an fN graph (figure 5.27) and in an FN graph (figure 5.28).

	Failure mode		TOTAL
	Overtopping	Sliding	
Failure probability [year^{-1}]	2.13E-06	3.68E-05	3.89E-05
Economic risk [€/year]	1.57E+02	4.28E+03	4.44E+03
Social risk [lives/year]	2.18E-03	6.71E-02	6.93E-02

Table 5.5: Results of incremental risk of the example split by failure mode.

5.11 Levels of detail

Depending on the depth of the analysis, it will be sensible to employ a higher or lower level of detail. In general, the level of detail must be reasonably consistent between the different parts of an analysis, putting more effort into the variables that will have a bigger impact on the final result. A way of finding out which are the most influent variables is to start from a simple model and to do a sensitivity analysis of the different variables. The same reflection is valid with regard to the level of detail in the analysis of a portfolio of several dams.

Table 5.6 (adapted from [50]) is included as a guide providing indications on what constitutes a simplified, intermediate or advanced level in the different components of the risk model.

[4] All of the risk calculations shown here are made with the iPresas software [117, 120, 75].

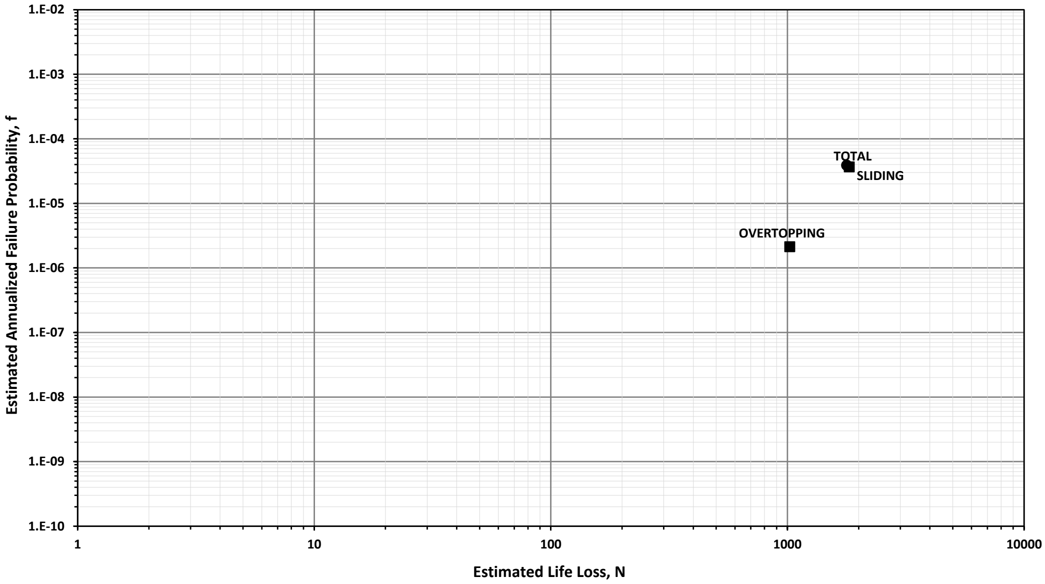


Figure 5.27: fN graph with the results of the example.

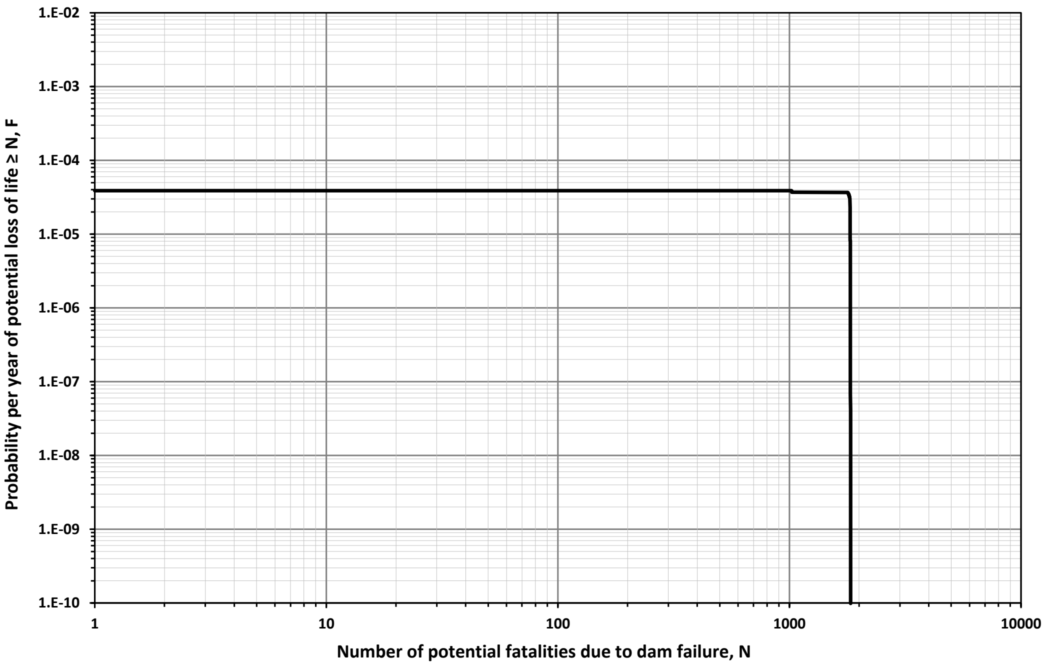


Figure 5.28: FN graph with the results of the example.

MODEL COMPONENT	COMPLEXITY LEVEL 1	COMPLEXITY LEVEL 2	COMPLEXITY LEVEL 3
FLOODS	Existing annual hydrographs and interpolation/extrapolation if needed	Uncertainty analysis over existing hydrology	Seasonal hydrology incorporating uncertainty analysis
PREVIOUS POOL LEVEL	Maximum Operating Pool Level	Historical records adjustment	Inflows and water demands simulation
OUTLET WORKS AND SPILLWAYS AVAILABILITY	Standard recommended values	Simplified fault trees plus probability estimates	Complete fault trees plus probability estimates
FLOOD ROUTING	Inflow equals Outflow until maximum discharge capacity	Operating Rules procedures or clear existing rules for flood routing	Consideration of a full and potentially complex system of water resources
FAILURE MODES	Overtopping	Overtopping Internal Erosion (Emb. D.) Sliding (Concr. D)	All failure modes from expert judgement working sessions
CONDITIONAL FAILURE PROBABILITY	Published general curves	Expert judgment	Numerical modelling and Montecarlo simulations
DAM BREACH AND HYDROGRAPHS	Those included in Emergency Action Plan	Expert judment and distinguishing for each failure mode	Numerical modeling and Montecarlo simulations
CONSEQUENCES	Empirical methods for damage plus interpolation from Emergency Action Plans	Empirical methods for damage plus hydraulic simulation of downstream response	Simulation methods for damage plus hydraulic simulation of downstream response
CORRECTIVE MEASURES	Standard actions (many published in scientific literature)	Detailed particular solutions plus approximate budget	Detailed to construction project level
OVERALL UNCERTAINTY	Only sensitivity analysis	Uncertinty over most relevant variables	Complete uncertainty analysis over natural and epistemic components

Table 5.6: Levels of detail in Risk Analysis (adapted from [50]).

Chapter 6

Risk evaluation and support to decision-making

6.1 Introduction

As mentioned in chapter 2, Risk Evaluation is the process followed to evaluate the importance of the risk associated with a dam failure.

In Spain, there is no legal criteria or recommendation providing quantitative limits within the scope of risk evaluation. Thus, when it comes to do this estimation, it is usual to compare the calculated risks with the recommendations published by international organizations. Though it must not be assumed that the tolerability recommendations of an organization are directly applicable in the context of a different one, these guidelines can serve as a useful reference in a general way. This is true for any kind of guidelines, but even more in the case of risk tolerability where factors such as public protection, the image of the responsible for the dam or economic estimations are intermixed.

Although more recommendations exist, the ones that will be discussed hereafter are the most used ones nowadays and include: the ones suggested by USBR (United States Bureau of Reclamation) [27], ANCOLD (Australian Committee on Large Dams) [13] and USACE (United States Corp of Engineers) [100]. In addition to these three well-known recommendations, other relevant documents are the ones employed in Holland due to their legal status [139] and the British guidelines [69] since they were precursors of the concepts used in risk evaluation nowadays.

The character of *recommendation* of the documents discussed hereafter must be stressed. For instance, USBR [27] says explicitly that they are not prescriptions in any case, but recommendations (*broad advisory guidance*) and that due to the approximate nature of the calculations, a risk just below a certain threshold should be treated exactly as one just above it.

6.2 USBR tolerability guidelines

USBR is an organization with a long history in the application of Risk Analysis. By 2003 it had edited a document [24] with recommendations to assess risk tolerability in their dams. In 2011, these recommendations were updated in a new document [27] that is discussed here below.

Basically, USBR establishes their recommendations of tolerability on the basis of: the annual failure probability (that for practical purposes is considered equivalent to individual risk) and the expected value of loss of life (annual risk). Their recommendations can be summarized in an f-N graph that is shown in figure 6.1.

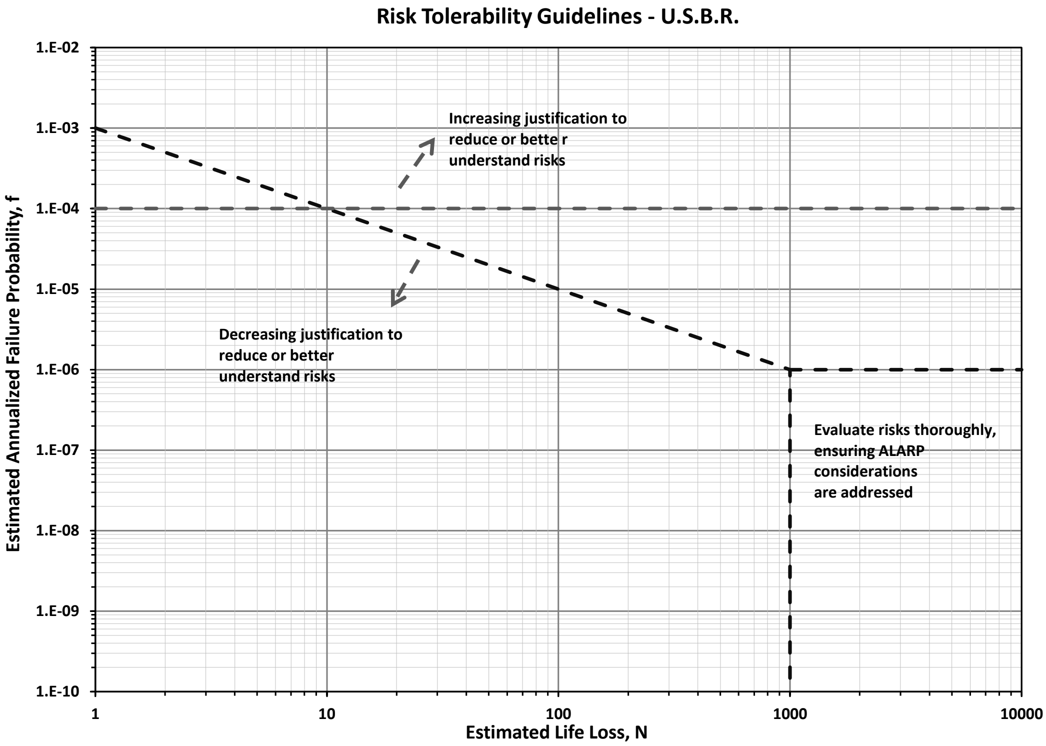


Figure 6.1: Graph for the representation of the estimation of failure probability, loss of life and risk (adapted from USBR [27]).

6.3 ANCOLD tolerability guidelines

In the absence of other guidelines, ANCOLD proposes three recommendations of risk tolerability:

- The risk of the most exposed person is limited to 10^{-4} a year for existing dams and 10^{-5} for new dams or big increases of height of the existing ones (*unacceptable risk*). In practice, it is common to make this value equal to the failure probability.

- The societal risk is limited through an F-N criterion, which is shown in figure 6.2. When risks fall above the criterion, it is said that the risk in unacceptable *except under exceptional circumstances*. According to ANCOLD the decision on when these exceptional circumstances are met must not belong to the owner of the dam but to the government or organization operating the dams. For instance, high risks that would normally be unacceptable could be tolerable if they are necessary to ensure some exceptional benefits, but it is not up to the owner of the dam to do this judgment.

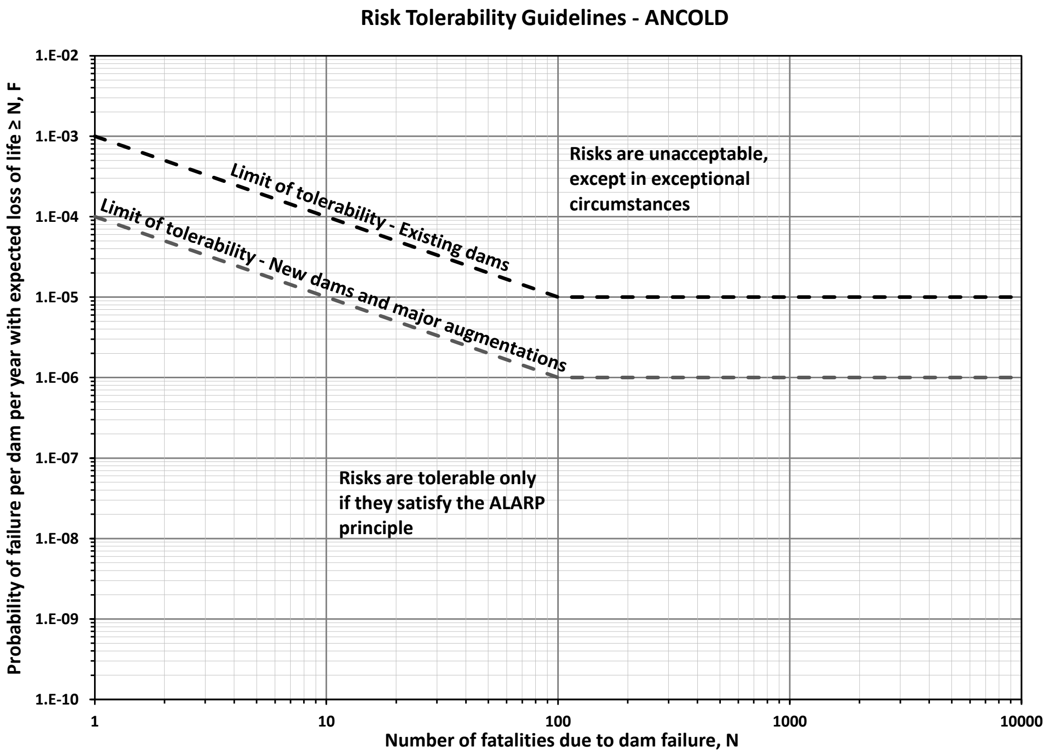


Figure 6.2: Societal tolerability guidelines by ANCOLD (Adapted from [13]).

- In every case, the criterion ALARP must always be applied. In this respect, it suggests the use of the adjusted cost per saved life and without adjustment as a quantitative measure (see section 6.5).

With regard to economic risks (and intangible risks), it says they must be limited, though it does not specify any criterion and leaves it to the responsible of each dam.

6.4 USACE tolerability guidelines

In 2009, USACE presented some provisional recommendations on tolerability developed along with USBR and FERC (Federal Energy Regulatory Commission) with the objective of reaching a common framework [100]. These recommendations are based on those of USBR, ANCOLD and NSW [102]. These provisional recommendations were later adopted in the official ”Safety of dams - policy and procedures” (USACE ER 1110-2-1156, 2011).

Basically, they adopt USBR’s risk guidelines and a modified version of ANCOLD’s F-N criterion that is shown in the figures 6.3 (existing dams) and 6.4 (new or highly modified dams). The same comments regarding the qualifier “*except under exceptional circumstances*” of ANCOLD are valid, and they are also applied to the cases in which there are more than 1000 fatalities, independently of the occurrence probability.

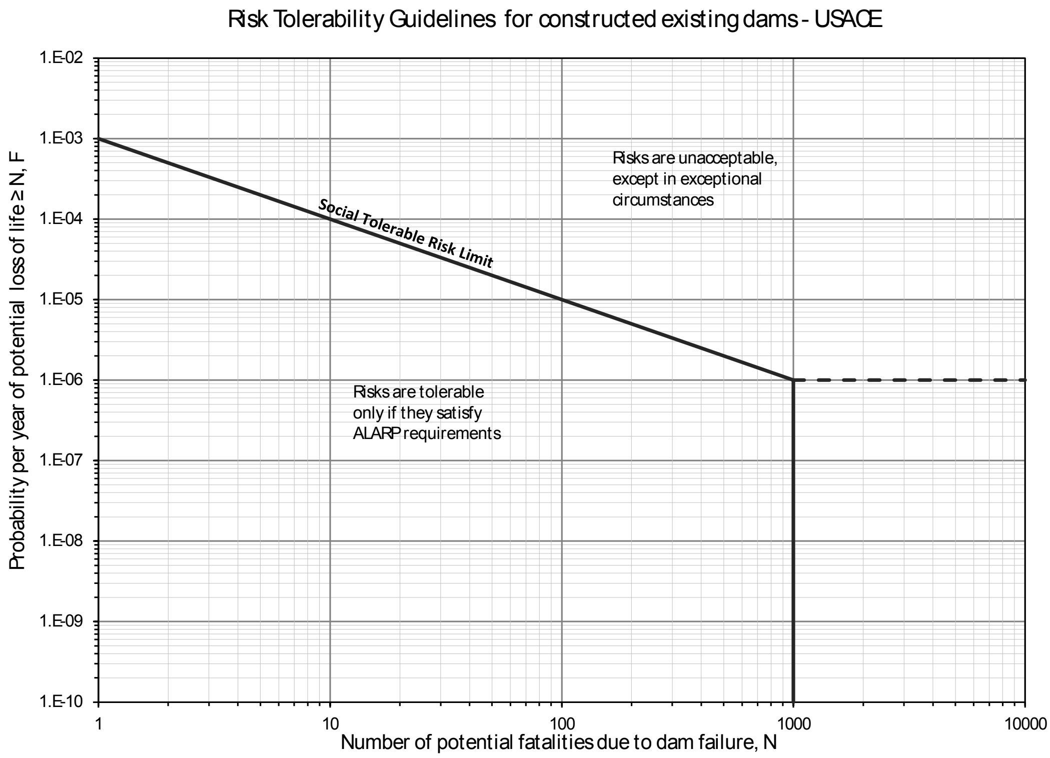


Figure 6.3: Guide to societal risk for existing dams (Adapted from USACE ER 1110-2-1156).

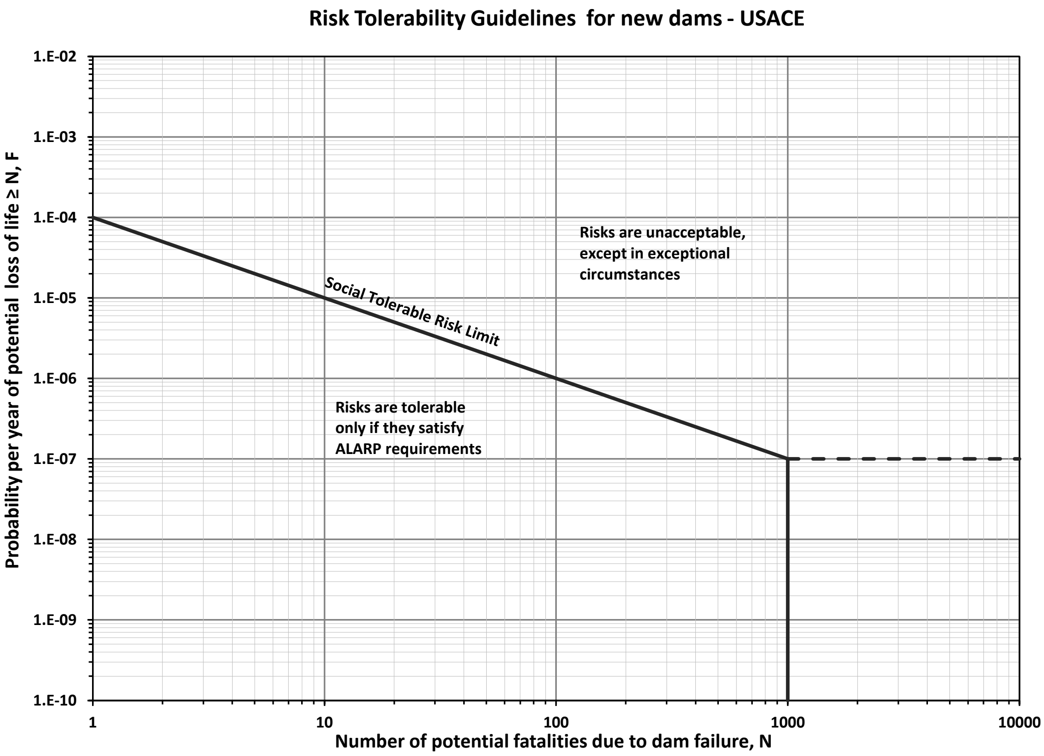


Figure 6.4: Guide to societal risk for new dams or important modifications (Adapted from USACE ER 1110-2-1156).

6.5 Efficiency indicators

The indicators of efficiency have a double purpose: serving as a quantitative guide to materialize the criterion ALARP and acting as optimization variables to prioritize different alternatives of risk reduction.

As a guide to quantify the ALARP criterion, these are the most used indicators:

Cost per Statistical Life Saved. It is usually known by its acronym $CSSL$ (*Cost to Save a Statistical Life*) or $CSLS$ (*Cost per Statistical Life Saved*). It also appears written with the letter U from unadjusted before or after to differentiate it from the following indicator. To calculate it, the following formula is employed:

$$CSLS = \frac{C_A - (O_{cb} - O_A)}{R(v)_{cb} - R(v)_A}$$

where C_A is the annualized cost of the reduction measure (€/year), O_{cb} is the existing operation cost (€/year), O_a is the operation cost with the measure (€/year), $R(v)_{cb}$ is the existing annual risk (lives/year) and $R(v)_A$ is the annual risk in human lives after the implementation of the measures (lives/year). Therefore, the CSLS has € units per life and the lower the $CSLS$ the more efficient a measure is.

Adjusted Cost per Statistical Life Saved. It is usually known by its acronym: $ACSLS$. It is calculated as the previous operator, but subtracting to it the cost of the measure, the benefit resulting from the risk reduction being:

$$ACSLS = \frac{C_A - (O_{cb} - O_A) - (R(\mathrm{EUR})_{cb} - R(\mathrm{EUR})_A)}{R(v)_{cb} - R(v)_A}$$

where $R(\mathrm{EUR})_{cb}$ is the existing annual economic risk (in €/year units) and $R(\mathrm{EUR})_A$ the annual economic risk (in €/year units) after the implementation of the measure. Therefore, the $ACSLS$ has also units of € per life, a measure being better (and more efficient) as the index is lower.

If the benefit resulting as a reduction of economic risk is higher than the measure, the $ACSLS$ is negative and then it is usually assimilated to 0 (refer to [13] for an example)[1].

Disproportionality ratio. Usually denoted by the letter R, it is the result of dividing the cost per saved life (adjusted or not) by a standard value of cost of saved life (an average value as used in other industries can be used) that is called *VPF* (*Value of Preventing Fatality*), *WTP* (*Willingness to Prevent a Statistical Fatality*) or *VSL* (*Value of Statistical Life*). In 2001, the HSE estimated *VPF* as a million pounds and indicated that whenever the risk is higher, measures with a higher R must be accepted [69]. On this basis, ANCOLD [13] indicates that for the

[1] When intending to use ACSLS to prioritize alternatives with negative values of this indicator, it is possible to move the term $R(v)_{cb} - R(v)_A$ to the numerator so the best *measures* have a more negative ACSLS value. However, whenever this is done, the meaning of the obtained value will be different.

cases just below the tolerability guidelines, the justification in order to carry out measures of risk reduction are (values in millions of Australian dollars):

- Very strong if $0 \leq CSLS < 5$
- Strong if $5 \leq CSLS < 20$
- Moderate if $20 \leq CSLS < 100$
- Poor if $100 \leq CSLS$

And for the cases above the Broadly Acceptable Risk:

- Very strong if $0 \leq CSLS < 1.5$
- Strong if $1.5 \leq CSLS < 6$
- Moderate if $6 \leq CSLS < 30$
- Poor if $30 \leq CSLS$

Finally, USACE (USACE ER 1110-2-11569) gave a value of 5.8 million dollars to the *WTP* and fixed the following guidelines for cases just below the tolerability limit:

- Very strong if $0 \leq R < 1$
- Strong if $1 \leq R < 4$
- Moderate if $4 \leq R < 20$
- Poor if $20 \leq R$

And for the cases above the Broadly Acceptable Risk:

- Very Strong if $0 \leq R < 0.3$
- Strong if $0.3 \leq R < 1$
- Moderate if $1 \leq R < 6$
- Poor if $6 \leq R$

For the purposes of prioritizing and evaluating alternatives, the same recomendations of efficiency already shown are valid, along with other ones such as the benefit-cost relation or the neat present value (NPV). For more information, an example can be consulted [37, 19, 18].

In Spain, the criterion *Equity Weighed Adjusted Cost per Statistical Life Saved (EWACSLS)* [119] has also been used to prioritize the measures adopted in a system of 27 dams of the River Duero Authority [114, 9, 11]. This index, *EWACSLS*, is a modification of the ACSLS obtained by dividing the latter by an equity factor (K_E) in order to give a bigger weigh to the alternatives that bring the failure probability of the dam to values lower than 10^{-4}.

$$EWACSLS = \frac{ACSLS}{(K_E)^n}$$

$$K_E = \frac{\max[10^{-4}, pr_e]}{\max[10^{-4}, pr_r]}$$

where n is a parameter that has been included for the means of a higher versatility and that can be, in principle, assimilated to 1 (a higher value would bestow a larger weigh to the equity in regard to efficiency and a lower value a lower weigh). The *EWACSLS* is therefore a mixed criterion of efficiency and equity.

6.6 Example

This section shows how to do a risk evaluation by using the example developed so far to illustrate the risk model. For this, two situations will be assessed: the *current situation* already modeled in the previous chapter, then the situation after the implementation of two mitigation measures. The first of the measures would consist on the establishment of an Emergency Action Plan (as an example of non-structural measure) and the second, an improvement of the drainage system (as an example of structural measure). To capture the impact on risk of the first measure, the ratios of mortality employed in the estimation of loss of life have been recalculated. In order to capture the impact on risk of the second measure, the probability of encountering high uplift pressures in the foundation of the dam has been reduced.

The obtained results are shown in table 6.1 and they are compared with the tolerability recommendations of USBR, ANCOLD and USACE in figures 6.5 and 6.6.

	Current situation	Emergency Plan	Drainage improv.
Failure probability [year^{-1}]	3.89E-05	3.89E-05	4.59E-06
Economic risk [€/year]	4.44E+03	4.44E+03	4.43E+02
Social risk [lives/year]	6.93E-02	7.23E-03	6.67E-03
Minimum loss of life	0	0	0
Maximum loss o life	1836	194	1836
Economic risk reduction [€/year]		0.00E+00	4.00E+03
Measure annualized cost [€/year]		54,383	21,995
Total economic cost [€/year]		58,822	22,438
Benefit/Cost ratio		0.00%	18.17%
ACSLS [€]		876,128	287,328
EWACSLS [€]		876,128	287,328

Table 6.1: Comparison of the current situation and the situation after the implementation of two risk reduction measures.

As it can be observed, the implementation of an Emergency Action Plan affects only the consequences, so the estimated risk diminishes, moving towards the left in figures 6.5 and 6.6. On the contrary, the improvement measure of the drainage system

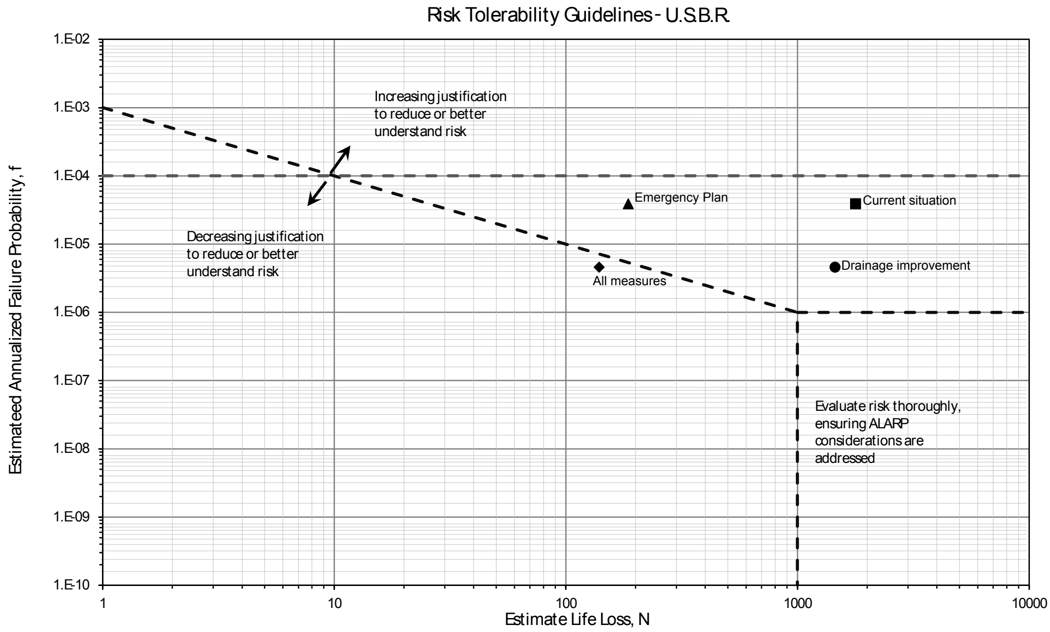


Figure 6.5: fN graph with the results of the example with risk reduction measures.

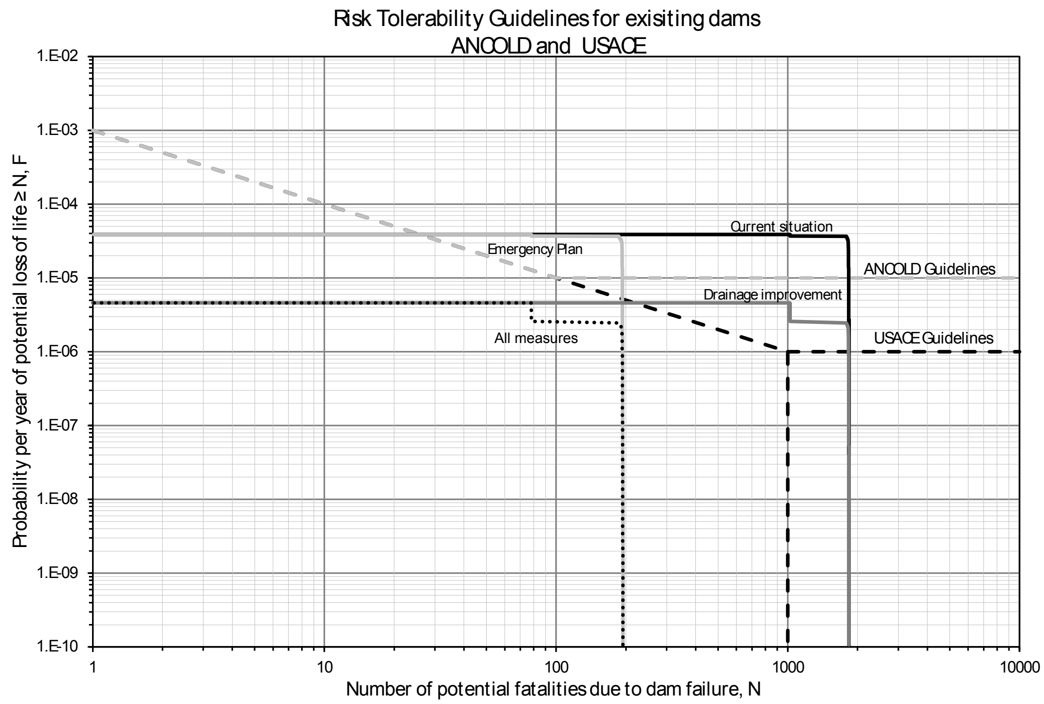


Figure 6.6: FN graph with the results of the example with risk reduction measures.

impacts fundamentally the probability of failure so risk moves down in the graph. In fact, as figure 6.5 shows, only one of the failure modes is affected.

It can be checked that the combination of both measures is sufficient for the dam to comply with the used tolerability recommendations. It can also be observed that the improvement of drainage is in this case more efficient to reduce the risk (smaller ACSLS). Besides this, as in this case the probabilities of failure are lower than 10^{-4}, the EWACSLS is equal to the ACSLS and it indicates that both measures are very *strongly justified*.

Chapter 7

Towards integrated management tools to support dam safety governance

The present Monograph on Risk Analysis Applied to Management of Dam Safety has emphasized risk analysis and risk modeling supporting such type of analysis with regard to natural (seismic, flooding, etc.) and engineering (foundations, internal erosion, etc.) risks.

It can be considered a significant contribution which, in any case, is a first piece of a bigger puzzle: integrated safety management of infrastructures which are relevant for the society.

This start by focusing on identification, analysis and evaluation of dam safety risk analysis is due to the importance of dams in terms of flood protection, energy production, water supply, irrigation, etc. and its potential to affect human lives, economy, environment and cultural heritage (through their exposure to natural and man-made threats).

The existence of overarching legislative pieces in Europe (Directives) and in other parts of the world, which go beyond specific codes and standards on dam safety (i.e in Spain, Title VII of Royal Decree 9/2008) provides basis for the development and implementation of integrated safety management schemes of many different types of risk and a wide spectrum of infrastructures.

Particularly in Europe, the following Directives acknowledge and explicitly require that risk analysis be utilized as the primary tool for critical infrastructure management:

- European Directive 2007/60/EC on the assessment and management of flood risks (so-called EU Flood Directive) considers that floods can be caused by the interaction of a range of sources such as rainfall, river flood, maritime flood or structural collapse (including effects of climate change) in addition to other important hazards such as terrorism, sabotage and vandalism, aimed at destroying flood defense infrastructures.

- European Directive 2008/114/EC on the identification and designation of European critical infrastructures and assessment of the need to improve their safety levels defines “critical infrastructure” as an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

An integrated and broad vision of safety management (governance) aims at improving practices on the way authorities and owners manage infrastructures, preparedness for disaster mitigation and speed of recovery from such catastrophic events.

In order to achieve the above mentioned goals, main requirements are prioritization of investments (in terms of efficiency in risk reduction) and harmonization of safety standards (ensuring equity), aspects which will secure owners business, and will provide operational and financial stability.

In this context, it is worth recalling that the essential conditions required for any type of risk management approach to be effective, as stated by ISO 31000: 2009, should be kept in mind. Those conditions are: the approach creates and protects value, is an integral part of organizational processes, is part of decision making, explicitly addresses uncertainty, is systematic, structured and timely, is based on the best available information, is tailored, takes human and cultural factors into account, is transparent and inclusive, is dynamic, iterative and responsive to change, and facilitates continual improvement and enhancement of the organization.

Consequently, integrated risk management tools to support Dam Safety Governance have to take into account the mission of the operator plus their restrictions, objectives and context, so that they can be integrated into the overall risk management process (figure 7.1).

In summary, the needed prioritization of investments and of optimizing management for more or less complex and large portfolios of dams provides insight and key information to decision makers. Software tools for this purpose already exist [76], and an application of this tool to a Spanish case has already been published [52].

In this mentioned experience undertaken by the Duero River Authority, adopting both equity and efficiency principles to define indicators to prioritize investments provided not only a robust outcome but also a transparent and socially defensible policy [51].

In addition, owners, operators and authorities in charge of dams can be provided with new information to communicate and inform citizens about the tolerable level of risk and the expenses of the investments made to achieve it. This can increase risk awareness and general willingness to accept further measures, that is, it will enhance social resilience while ensuring strategic economic sectors in terms of sustainability and financial stability for the future.

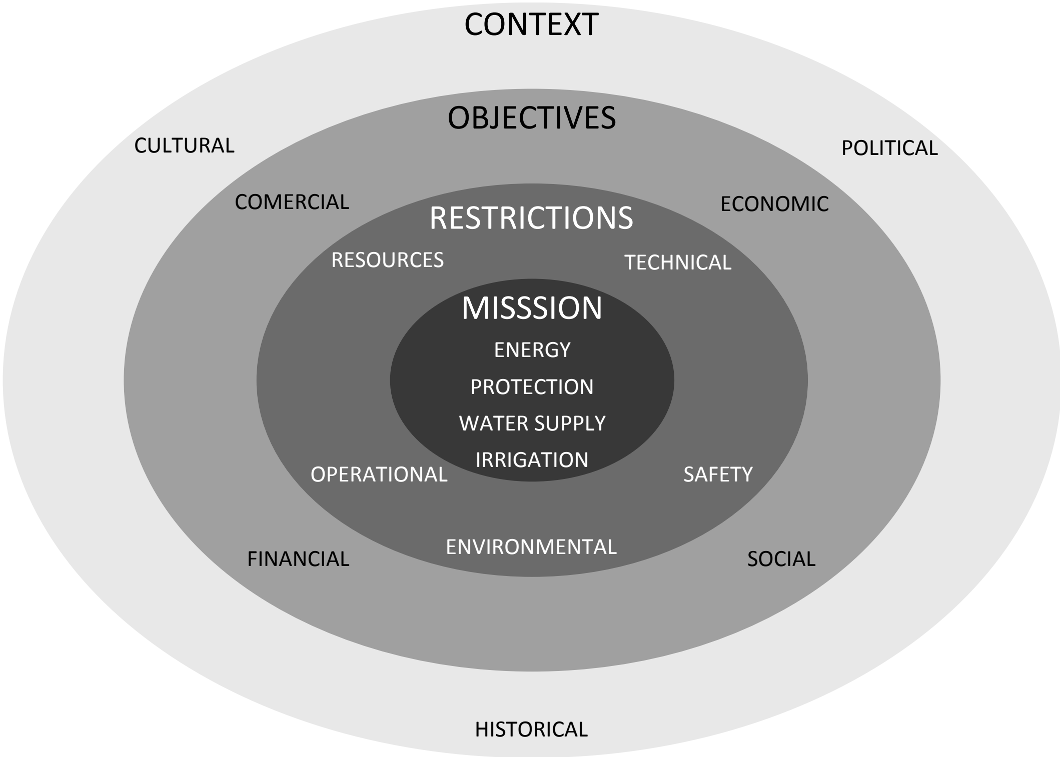


Figure 7.1: Mission, restrictions, objectives and context of dam safety governance.

Another hot topic in an integrated management is the inclusion of security issues. In principle, security can be managed using the same overall framework though research is still ongoing in some key parts of this field [116, 44, 82].

Finally, it is worth noting that an increased capacity for risk management through the development and sharing of common tools and best practices on protective measures cannot be achieved without the extensive and willing participation of public and private sectors. Therefore, partnering, including international collaboration, is critical as no organization (or country) can effectively achieve its infrastructure safety, security, resilience, and other overarching risk management goals without the assistance of other members of the partnership.

Part II

Appendixes

Appendix A

Estimating gate reliability

A.1 Introduction

The present appendix provides an introduction to the use of fault trees in the estimation of the failure probability of gates. It is therefore an appendix to the content of section 5.5, in which the reliability of outlet works and spillways was outlined. It should be noted that the concept of outlet works and spillways reliability (i.e., the probability of not working when necessary) must not be mistaken for their potential collapse or sudden opening that might produce an artificial flood downstream. The latter scenarios must also be analyzed but not as a component of the loads of the system, but as potential failure modes[1].

Fault Tree Analysis (FTA) is a technique originally developed during the 1960's by the military industry [43]. At a later date it was incorporated as a tool for Risk Analysis in nuclear [136] and aerospace [127] industries and, nowadays, it is used in a myriad fields, among which dam safety.

A.2 The logic of fault trees

The objective of a FTA is to develop all events and event combinations that can produce a failure. For this doing, fault trees are employed. Fault trees consist of a graphic representation of the logic of a system. The events in a tree can be of any kind: mechanical, human, due to external conditions, etc. The failure or undesired event that is analyzed is named *top event*. Under it, the events that can lead to the top event happening are drawn and this is done successively in a recursive way until reaching the lower level of the tree where the *basic events* lye. Basic events are therefore the ones that do not require further development. Figure 2.9 refer to glossary) shows an example of fault tree, in which the top event is the failure of a gate and where basic events are represented by circles.

[1] It is also convenient to notice that fault trees have also been used to model failure modes [68].

A fault tree is not a representation of the physical system but of the way a failure can occur. For example, in the fault tree of a gate, there is no reason to represent all the pieces of the gate but all the events that can contribute to a dysfunction of the gate must be present. Besides, as any other model, fault trees can never aspire at being totally exhaustive.

Each node of a fault tree represents a binary event (it can happen or not). For example: a gate works or does not, there is electrical supply or not, a piston breaks or does not, etc. In other words, it is always a binary relation.

Events are interrelated throughout logic gates. The simplest ones are the *AND* and *OR* gates. If a top event A relates throughout an AND gate with the lower elements B and C, it means that in order to event A to happen, events B and C should both take place. On the contrary, if a top event A is related to lower events B and C by means of an OR gate, it means that in order for event A to happen, event B or event C should happen (or both can happen). Further in the text, more logic gates are explained, though these are the most common ones.

A fault tree can be used as a qualitative tool to analyze the logic of a system. It is not necessary to assign any kind of figure to the diagram for this to be useful. However, once the fault tree is developed, it is possible to obtain the occurrence probability of the top event by assigning occurrence probabilities to each basic event. Once these estimations are assigned, the calculation of the top event is just an algebraic matter, automatized by current software. For this purposes, there are some free software [58] and many other commercial packages in the market [86].

With regard to the use of fault trees as a qualitative tool, besides the knowledge provided by the mere use of drawing them, there exist some calculations that can be done with no need for assigning probabilities to the base events. The most usual calculation is the determination of the *Minimal Cut Sets* (MCS), a *Cut Set* being a combination of basic events leading to failure. A MCS is a minimal combination of effects that would cause failure (or top event) to happen. The software packages of fault trees are able to calculate automatically all the MCS of a top event from a failure tree. Besides this, due to the recursive nature of fault trees, the MCS could be obtained for any event, not just for the top one. The MCS of first level are the ones that only contain a single event. Thus, the most critical points in the system can be identified, as any event appearing in the first level MCS would involve the failure of the system. A system with many MCS of first level is a system with a small level of redundancy and therefore fragile. It is also necessary to calculate MCS of superior levels.

With regard to the quantitative use of fault trees, the main calculation to do is the determination of the occurrence probability of the top event, that is the result that will be introduced in the global risk model. Another calculation that can be done is to order all MCS by occurrence probability; this has a certain utility from the point of view of the understanding of the system but that is not a requirement for the risk model. It becomes also possible to perform more advanced calculations such as uncertainty calculations or calculations relying on time. Obviously, these calculations demand the model to be fed with more data and an extra amount of work.

Finally, it is important not mistaking an event tree for a fault tree. The event tree represents an inductive way of reasoning (from specific to general). It starts from an original event and it progresses step by step, exploring all the possibilities until reaching failure. As opposed to it, a fault tree works in a deductive, top-down way (from general to specific). It starts from a failure in the system and explores all the possible causes that might have induced it. Therefore, it can be said that the main difference between both methods lies on the direction of the analysis they carry out. In practice, a combination of both methods is used. A tree of events is used to represent the global risk model whereas to estimate some of the probabilities of failure contained on this tree (e.g., the reliability of the gates), fault trees can be used. Figure A.1 shows this relation.

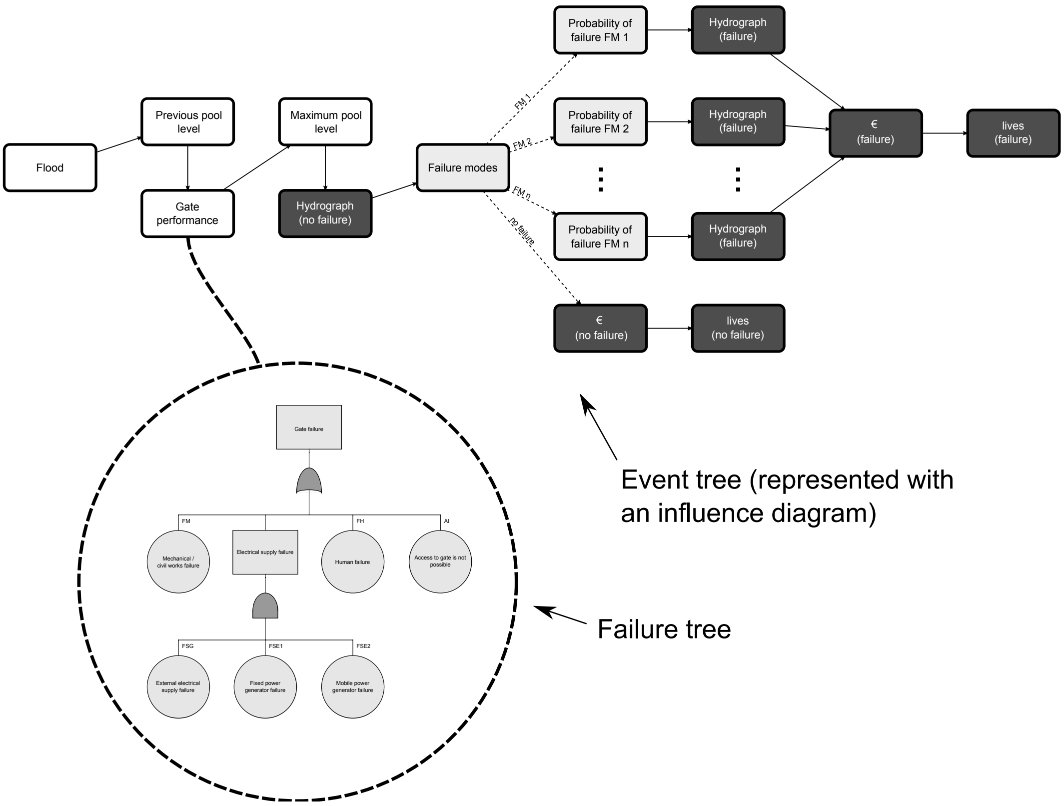


Figure A.1: Relation between fault trees and risk models.

A.3 Symbology

The different symbols employed in failure trees are explained in this section.

First, there are the events. Table A.1 shows the most common symbols used to represent all possible types of events that can happen in a fault tree. In practice, the most commonly employed are the basic and the intermediate events. The basic event (circle) is the one appearing at the lower end of each branch; it is not developed any further and is assigned an occurrence probability. The intermediate level (rectangles) events are the ones that can be developed through the analysis of the sub-events able to cause them. Therefore, those events are not assigned a probability directly, but it is calculated accordingly to the logic of the fault tree.

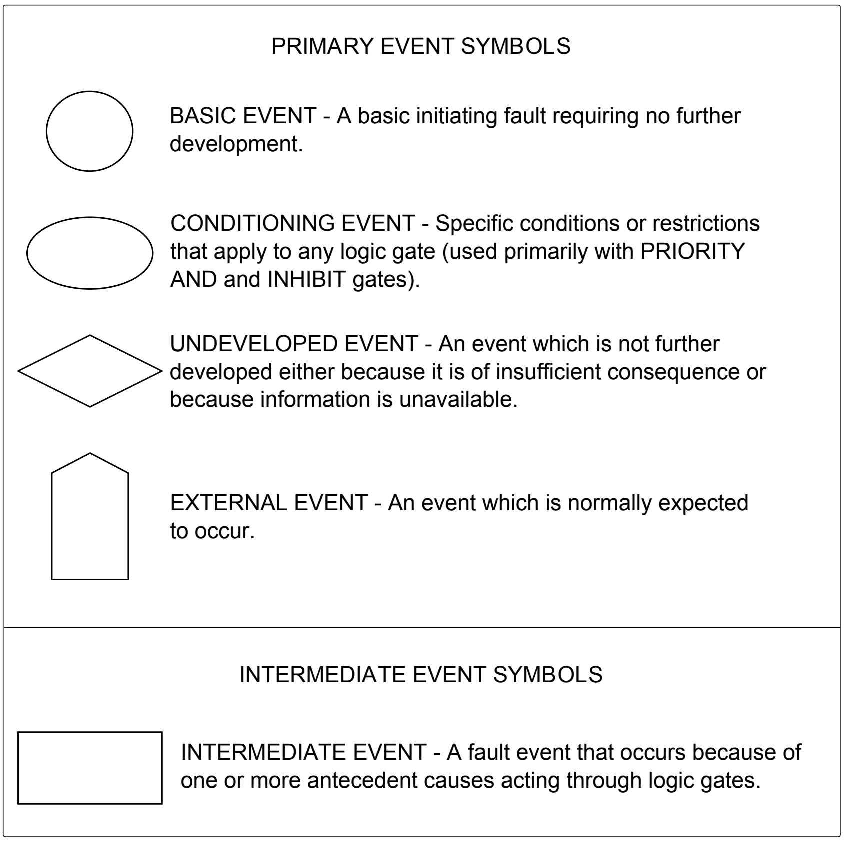


Table A.1: Symbols used in the representation of the different types of events in fault trees.

Secondly, there are the symbols use to denote relations among events which are called logic gates. Table A.2 shows the commonly accepted symbols for the main logic gates along with an explanation of their meaning. Among them, the most important ones are AND and OR gates, previously explained.

Finally, there are the auxiliary symbols that help disaggregating a big fault tree into several smaller ones (table A.3). In the cases where a fault tree is developed in a detailed way until reaching the different mechanical pieces of the gates, these symbols are essentials because the tress can reach impractically large sizes.

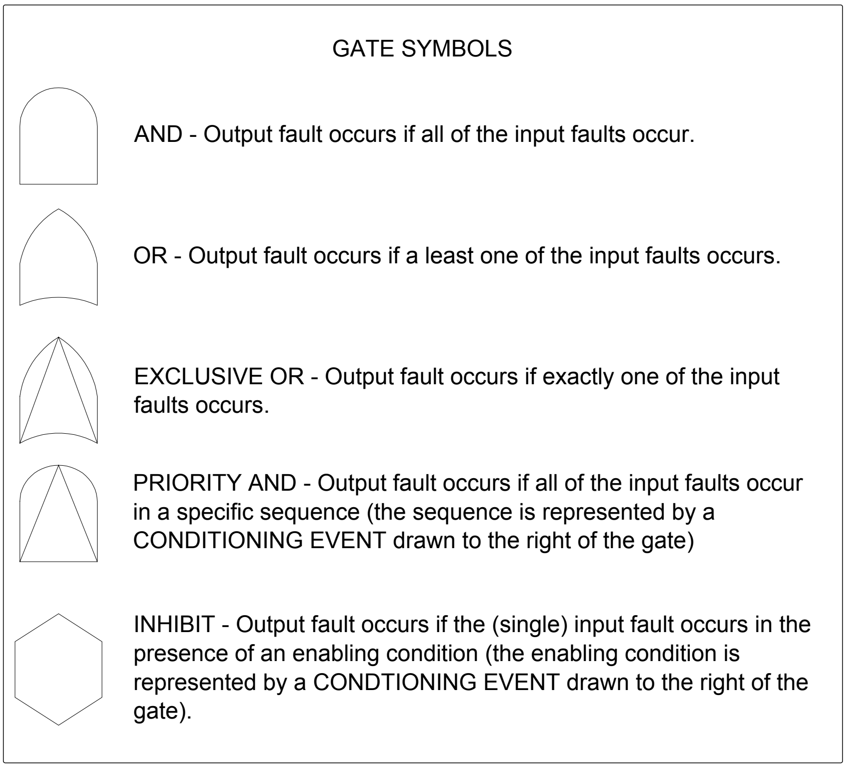


Table A.2: Symbols to represent the different logic gates in fault trees.

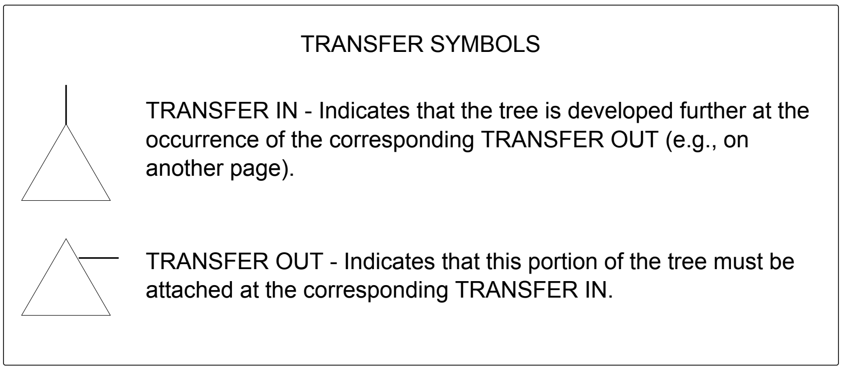


Table A.3: Auxiliary symbols for fault trees.

A.4 Examples

Two examples of fault trees are shown hereafter where the calculations for both cases are explained. The first one is a fault tree such that could be employed in an intermediate level of calculation and the second is an example of a more detailed analysis. Figure A.2 shows the first example. Four possible causes of failure have been identified at first level:

- Mechanical failure / civil works
- Failure in the electrical supply
- Human failure
- Lack of access

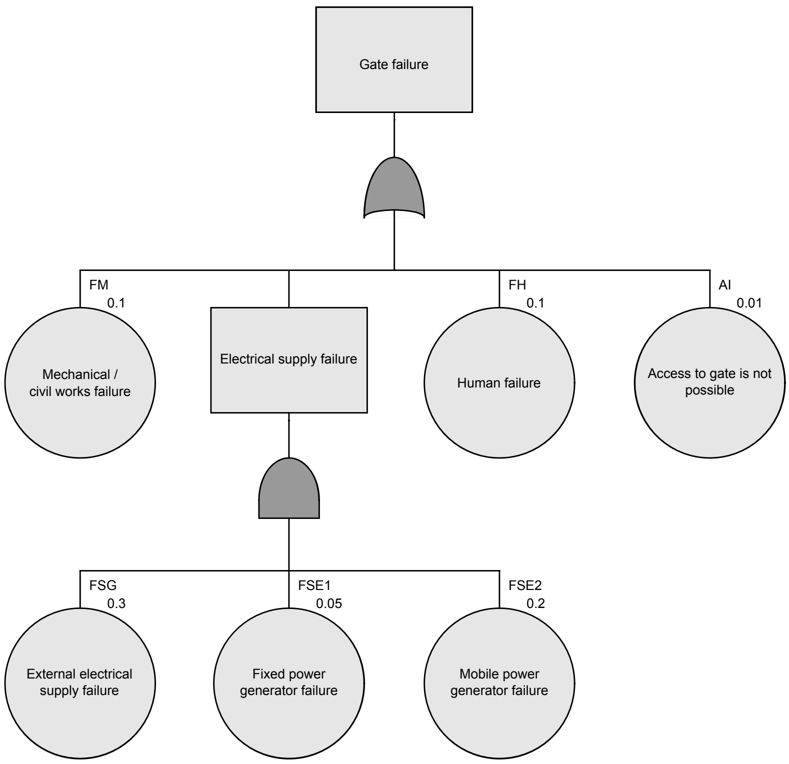


Figure A.2: Example of fault tree for an intermediate level of detail.

As any of this causes by itself would prevent the operation of the gate, they have been related to the top event through an OR gate. Among these causes, the first, third and fourth ones have been assigned occurrence probabilities of 0.1, 0.1 and 0.01 respectively. The failure in the electrical supply has been developed slightly more, identifying that in order for this to happen, besides a failure in the general supply, the emergency systems should also fail (the fixed generator and the mobile one in this case). Therefore, these two events are related to the event electrical supply failure through an AND gate. The three events have not been developed any further and they have been assigned respectively the following probabilities: 0.3, 0.05 and 0.2.

The first calculation that can be performed is the one of MCS, as it is a qualitative one. The results can be seen in table A.4. It is reminded that each MCS is the minimal combination of basic events sufficient to cause failure (i.e.; occurrence of the top event) since if a single event of the combination was removed, failure would not take place. This case is a simple one and show there exist three MCS of first level and one of third level. The three MCS of first level correspond to the mechanical, human and lack of access failures and just one of them would be enough to prevent the operation of the gate. On the other hand, the electrical supply presents a higher redundancy as in order for it to happen three things must fail simultaneously, which is reflected in the 3rd level MCS.

```
Minimal Cut Sets
================

Tree   : ejemplo.fta
Time   : Thu Feb 11 19:39:43 2010

Method : Algebraic

No. of primary events = 6
Minimal cut set order = 1 to 6

Order 1:
    1)  AI
    2)  FH
    3)  FM

Order 2:

Order 3:
    1)  FSE1 FSE2 FSG

Order 4:

Order 5:

Order 6:


Qualitative Importance Analysis:

Order        Number
-----        ------
   1           3
   2           0
   3           1
   4           0
   5           0
   6           0
  ALL          4
```

Table A.4: Minimal Cut Sets of the developed example (results obtained with Open-FTA [58]).

The calculation of the probability of the top event is an iterative process. When there is an OR gate, if the events were mutually exclusive (i.e., could not be concomitant) the probability of the top event would be calculated simply by adding the probabilities of the basic events. However, if the events were assumed independent, the intersection of the different events should be subtracted form to the previous sum.

Mathematically it is expressed as:

$$P(E_1 \vee E_2 \vee \cdots \vee E_n) = \sum_{i=1}^{n} P(E_i) - \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} P(E_i \wedge E_j) +$$
$$+ \sum_{i=1}^{n-2} \sum_{j=i+1}^{n-1} \sum_{k=j+1}^{n} P(E_i \wedge E_j \wedge E_k) + \cdots + (-1)^n P(E_1 \wedge E_2 \wedge \cdots \wedge E_n)$$

where $\wedge$ is the mathematical symbol to denote AND and $\vee$ the one for OR gates. The expansion of this formula gives place to a series where the first term is the probability admitting the events are not mutually exclusive and the successive terms are alternated in sign and decreasing in magnitude, in such a way that if terms are being added to the calculation the real result gets delimited. Thus, a few terms are enough and the higher order terms can be neglected. This process can be appreciated in table A.5, where it is observed that the 4 first terms have been calculated, reaching a final result of $2.005057 \cdot 10^{-1}$, which is the failure probability of the gate. The contribution to the final probability of each of the basic events is also calculated, showing that in this case, human and mechanical failures are the ones that contribute the most to the global probability of failure.

Finally, figure A.3 shows an example of a fault tree in which the mechanical part has been developed in detail.

A.5 Combining probabilities

To this point, we have dealt with the probability that an outlet works or spillway is not working. However, dams usually have several outlet works and/or spillways, or several gates of the same element. For example, in a spillway with three gates, for the risk model purposes, it will be required to calculate the probability of 0, 1, 2 or 3 gates working.

If there are several operational gates (or if they stop being it) in a totally independent way and the probability of working of each of them is known a binomial distribution can be employed to calculate in an accurate way the probability of each of them working. The binomial distribution measures the number of successes in a sequence of several independent tests of Bernouilli (A Bernouilli test is a random experience with only two possible outcomes: yes or no) , each with a fixed probability of s. In the opposed case, that is, if the gates do not function independently (i.e., if one gate does not work then all fail), the probability that all gates function properly is equal to the probability of one of them working, the probability of none of them working is 1 minus the probability of one working and the probability of any other intermediate number of gates working is 0.

The real probability will be usually in between both cases; that is, there will be some failures able to affect some of the gates and not others, and some cases able to affect just one gate. For example: a failure in the electrical supply might make none of

```
Probabilities Analysis
======================

Tree   : ejemplo.fta
Time   : Thu Feb 11 19:49:24 2010

Number of primary events   = 6
Number of minimal cut sets = 4
Order of minimal cut sets  = 6

Unit time span         = 1.000000

Minimal cut set probabilities :

  1    AI                               1.000000E-002
  2    FH                               1.000000E-001
  3    FM                               1.000000E-001
  4    FSE1 FSE2 FSG                    3.000000E-003


Probability of top level event (minimal cut sets up to order 6 used):

 1 term    +2.130000E-001   = 2.130000E-001 (upper bound)
 2 terms   -1.263000E-002   = 2.003700E-001 (lower bound)
 3 terms   +1.360000E-004   = 2.005060E-001 (upper bound)
 4 terms   -3.000000E-007   = 2.005057E-001 (lower bound)

Exact value : 2.005057E-001


Primary Event Analysis:

 Event          Failure contrib.    Importance

 AI             1.000000E-002           4.99%
 FH             1.000000E-001          49.87%
 FM             1.000000E-001          49.87%
 FSE1           3.000000E-003           1.50%
 FSE2           3.000000E-003           1.50%
 FSG            3.000000E-003           1.50%
```

Table A.5: Quantitative calculation of the developed example (results obtained with OpenFTA [58]).

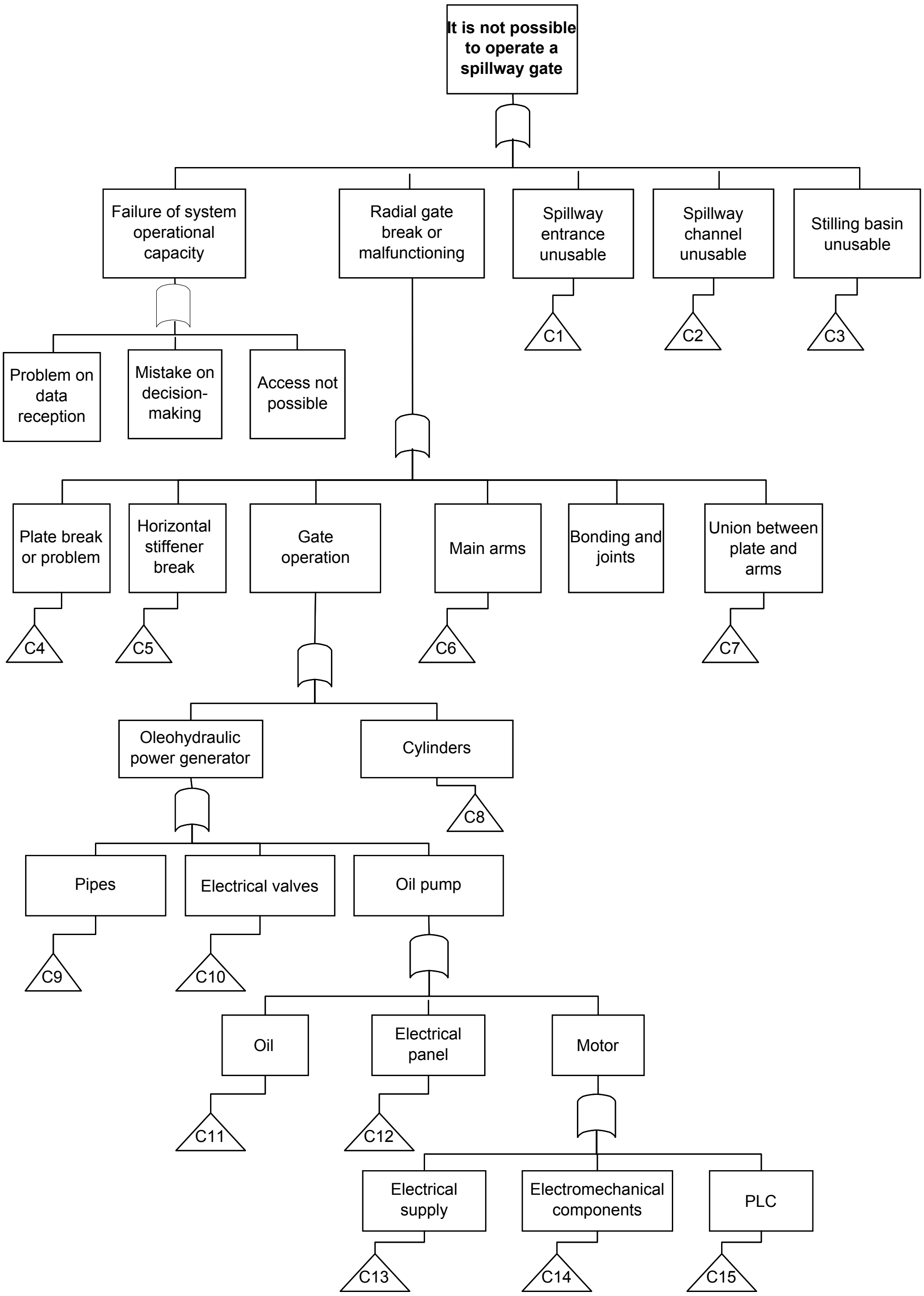


Figure A.3: Example of detailed fault tree.

the gates work (though it may be possible to operate some of them throughout the use of generators), a failure in a chain could make a gate non-operational without affecting the other ones, a failure in a battery could affect two gates, etc. Reality can be very complex when analyzed in detail.

In such a case, the adequate model is neither immediate nor simple. Depending on each case, it might suffice to adopt one of the extremes as an approximation, or to analyze both with a sensitivity analysis to bound the results. In the cases these processes need to be modeled properly, a single fault tree will not be enough. Then, different fault trees will have to be performed for the failures affecting a single gate and for those affecting several ones and integrate their results in the risk model throughout several nodes, instead of a single one.

Finally, a related aspect is the possibility of having in the same fault tree several correlated basic events due to a common cause failure. Although it carries its own complexities, this can be modeled within the fault tree paradigm [127]. For example, let's consider a system such as the one in figure A.4.

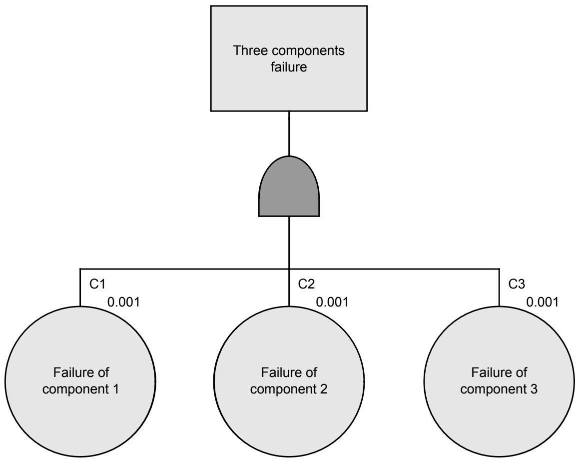


Figure A.4: Example of fault tree with independent failures.

The failure under study can only happen if 3 components fail at the same time. Each of them has a probability of failure of 10^{-3}. Therefore, the probability of failure of the top event is 10^{-9}. If we consider then that 1% of the failures have a common cause (in which case the three components fail simultaneously), then the probability of failure due to a common cause is $10^{-3} \cdot 10^{-2} = 10^{-5}$. Figure A.5 shows a possible way of modeling this. As it can be observed, failures have been split into two branches. One of them contains the independent failures and the other one the common cause. The events of independent failure have now a probability of $10^{-3} - 10^{-5} = 9.9 \cdot 10^{-4}$, whereas the failure due to a common cause has a probability of 10^{-5}. The failure probability calculated this way is of $1.000097 \cdot 10^{-5}$, which is substantially higher than the one calculated in the first example.

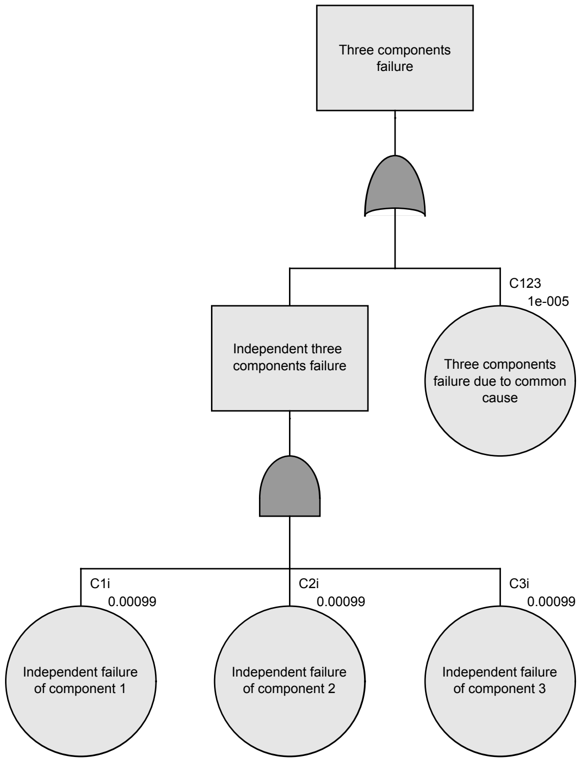


Figure A.5: Example off tree considering fault due to common cause.

Appendix B

Probability elicitation through expert judgment

B.1 Introduction

This section contains some helpful recommendations for estimating probabilities by expert judgment.

Expert judgment is the opinion of an expert on the plausibility of an event, under controlled and specified circumstances. In Risk Analysis applied to dams it cannot be avoided having to resort to subjective judgments, but it is necessary to follow structured processes and a series of basic rules in order to attain valid conditions that can be audited.

The structured use of this type of subjective techniques goes back to 1946, when the project RAND was established in the USA and predicted that the first aerospace satellite would be launched in 1957. Ten years afterwards, in October 1957, the launching of the Soviet satellite Sputnik confirmed that prediction. Since then, these techniques have been broadly used to evaluate probabilities otherwise difficult to quantify in the Aerospace industry, nuclear industry, in socio-politics and economy. One of the most famous methods to carry out these estimations is the one called DELPHI, developed by the same corporation RAND in the 1950's [110]. Many examples of its applications are available in the literature.

Within the particular context of dam Risk Analysis and according to ANCOLD recommendations [13], in order to guarantee the intended degree of soundness of the estimations throughout expert judgment, the following minimal conditions must be respected:

- The estimations must be done by professionals with an extensive experience in dam engineering and a broad knowledge of dam failures, though it can also be beneficial to include some generalists as well as specialist in some subjects relevant to the process.

- Before estimating the probabilities, the logic of the failure must have been defined (see chapter 4), usually though an event tree, in such a way that the failure probability estimations are focused exclusively in the estimation of those probabilities.
- All the reasoning processes leading to the estimation of probabilities must be documented.
- The values and the process of its estimation must be reviewed externally.

A methodology to obtain probabilities throughout expert judgment that complies with the above-mentioned conditions is outlined hereafter. This methodology is based on the recommendations gathered in several works, mainly [14, 103, 13, 119].

B.2 Identifying the needs of the study

The identification of the needs of the study precedes the estimation of probabilities through expert judgment. In general, whenever it is possible and the data available allow the application of a methodology like the reliability techniques exposed in the next section, it will not be necessary to resort to expert judgment, as these techniques imply a lower degree of subjectivity (although they do not lack it totally).

However, reliability techniques are not often of easy applicability in the field of Risk Analysis. Indeed, in the context of dam safety, probabilities are often difficult to analyze through numerical models that allow the employment of this type of techniques. In other cases, the available data can be insufficient to carry out an analysis through reliability techniques with guarantees. If this were the case, the use of a complex numerical model and the estimation of probabilities through Monte Carlo techniques would provide a false feeling of soundness and objectivity.

Identifying the needs and communicating them to the experts is an important part if the process is intended to succeed. Establishing the importance of the estimations and transmitting them to the experts that are going to take part in the process serves the double function of integrating them in the estimation of the results and augmenting their attention and honesty.

B.3 Selecting the level of the study and the leader of the process

The U.S. Nuclear Regulatory Commission (NRC) classifies the subjects to be evaluated throughout expert judgment into three levels of complexity [103]:

A. Non-controversial, insignificant effect on risk.

B. Significant uncertainty and diversity, controversial, complex.

C. Highly controversial, significant effect on risk, highly complex.

Also according to NRC, the requirements of level of complexity are classified in four categories (see below for the definition of involved agents):

I. The *technical integrator* (TI) evaluates and assigns weighs to the models based on the review of the literature, the experience and the estimation of the required variables.

II. The TI interacts with the *proposers* and *specialists*, evaluates their interpretations and estimates the required variables.

III. The TI organizes a debate with the *proposers* and the *specialists*. The TI directs the debate, evaluates the interpretations and estimates the required variables.

IV. The TI and the *technical facilitator* (TF), or the TIF is they are the same entity, organizes a panel of experts so they interpret and assess the relevant topics, directing the discussions, moderating the debate, summarizing and integrating opinions and estimating the required variables.

The different agents named above are defined as follows:

Technical integrator (TI): Is responsible for aggregating the results on the basis of the generated information. He is responsible for the defense of these aggregated results in front of the experts, the external experts, the external reviewers, the regulators and the people responsible for the final result, for gathering all their comments and for reviewing the aggregated results.

Technical facilitator (TF): Is responsible for structuring and facilitating the discussions and interactions among the experts. He or she must ensure these interactions take place and that there exists equity in the exposed information and opinions. He or she is the one responsible for obtaining the formal evaluations of each expert (expert judgment) and for creating the proper conditions for a direct aggregation of opinions, extent from controversy.

Technical facilitator and integrator (TIF): When both functions TI and TF concentrate in the same person.

Proposer: An expert that advocates for a certain hypothesis or technical position.

Specialist: A technical expert with a deep and detailed knowledge on some data, theme or methodology of interest to the process.

These classifications can serve as a reference to think about the complexity of the problem and the adequate level of study. When facing a problem of complexity A, the levels of study I, II and III are all appropriate. For problems with a degree of complexity C, studies of level IV must be developed.

The *leader* of the study is the responsible for determining the estimations. The characteristics he or she must combine are:

- A good professional record, recognition and level of competence, based on his/her academic education and experience.

- Good interpersonal and communicative skills, flexibility, impartiality and analysis and synthesis skills.
- Contacts within the sector: engineers, investigators, managers, etc.
- Leading and consensus forming skills. The leader of the study does not need to be an expert in the matter that is being studied but must possess a sound knowledge of it.

B.4 Selecting the experts and the external reviewers

External reviews are highly advisable in general and necessary when very controversial themes and/or with a big impact are being discussed. The external review can be done simultaneously with the progress of the study or afterwards. The first option presents the advantage that the comments of the external reviewer can be incorporated as the project moves on.

The characteristics a good external reviewer must possess are:

- A good professional record, recognition and level of competence based on his/her academic education and experience.
- Knowledge and experience on the subject under study and related areas.
- Availability and willingness to consecrate the required time and effort.
- Good interpersonal and communicative skills, flexibility, impartiality and analysis and synthesis skills.

With regard to the selection of the candidates, the size of the group will be chosen depending on the cases of study. To guarantee a reliable result, it is very important that the group is big and diverse enough. The group must be balanced by encompassing different points of view in the questions to be treated.

The experts can be people with a close knowledge of the dam (operators, design engineers, builders, etc.) or specialist in any area relevant to the estimations that are going to be done (soil mechanics, hydraulics, etc.). It is also make use of observers that will take place in the discussion but will not emit their evaluations at the moment of estimating the probabilities.

B.5 Preparing the sessions

First of all, it is a requisite that the participants have at their disposal all relevant documentation considerably in advance of the date of the sessions.

In the preparation of the sessions, it is also important to formulate clearly all the aspects on which the expert judgment will be demanded. The topics must be separated so they can be treated one by one. The formulation of the questions must be clear and avoid all ambiguity. When using terms that could give place to different interpretations, these ones must be defined. It must be emphasized that the writing of the questions can bias the discussion -and consequently the results-, so they must be formulated in the most neutral way.

First, the relevant information will be presented. Then, the different factors (favoring or going against the occurrence of the event) will be discussed. Finally, opinions will be emitted. All the information used in the session must be prepared in advance in a format that enables its quickly presentation. To speed up the gathering of information it is convenient to prepare forms that will be distributed to each participant. Once the personal evaluations have been gathered, these must be shared and discussed within the group. For this, it is very useful to make this comparison in a graphic and quick way.

B.6 Probability elicitation

B.6.1 Preliminary tasks

The estimation of probabilities throughout expert judgment is done in a group session. The day of the session it is convenient to start with a brief general presentation of the dam contextualizing the themes that will be treated and highlighting the way they will impact the results obtained during the Risk Analysis session.

It is also convenient to consecrate some time to train the members of the group on the themes of uncertainty and probabilities estimation if this is the first time they take place in a session of the kind.

B.6.2 Presentation of available information

For each topic analyzed with expert judgment, a presentation with the relevant information must be prepared. This presentation must be brief, because the information must already be presented and discussed in the failure modes identification session and must be available for the experts before the session. However, this presentation is necessary to remind the available information, to add some new data or a new study done after the failure modes identification session and to solve any doubt from the experts.

B.6.3 Discussion of the more-likely and less-likely factors

For each topic, the more-likely and less-likely factors must be enumerated after the presentation of the information. Formally, this can be done as a separate step or, in simpler cases, as part of the discussion about the information. Sometimes, there might be some misunderstanding with regard to the meaning of “more-likely” and “less-likely” (in favor of the occurrence of the event or in favor of the safety of the dam?). This must be clarified at the beginning of the sessions to avoid all confusion.

B.6.4 Elicitation of probabilities (first round)

At this point, each expert is required to assign individually a value of probability to the event that is being discussed.

If the failure modes were not sufficiently disaggregated, the experts could be forced to express very low probabilities. This is problematic because when probabilities fall outside the range 0.1-0.9, the capacity of understanding disappears so it becomes difficult to emit impartial judgments. This is why the disaggregation done in the definition of a failure mode is very important and if it is sufficiently detailed it will make this step of the Risk Analysis easier.

The tables of verbal descriptors are very helpful to guide the process of expression of probabilities. The descriptors relate terms such as "implausible", "possible" or "very probable" with numerical values. The use of this kind of table has been broadly cited in the scientific literature [14]. Despite their limitations they present several advantages: they help to overcome the initial resistance to express probabilities by people not accustomed to it, they speed up the process, the make easier to reach a consensus and they make the results more repeatable. Additionally, using the same table for all failure modes and in different dams helps the comparison and consistency of the results. For the type of process outlined in this document, where all failure modes must have been decomposed sufficiently so the probabilities are not too low, table B.1 can prove helpful.

Expression	Single-number probability, % (median of responses)	Specified range, % (median upper and lower bounds)
Almost impossible	2	0-5
Very improbable	5	1-15
Very unlikely	10	2-15
Very low chance	10	5-15
Improbable	15	5-20
Unlikely	15	10-25
Low chance	20	10-20
Possible	40	40-70
Medium chance	50	40-60
Even chance	50	45-55
Probable	70	60-75
Likely	70	65-85
Very possible	80	70-87,5
Very probable	80	75-92
High chance	80	80-92
Very likely	85	75-90
Very high chance	90	85-99
Almost certain	90	90-99,5

Table B.1: Table of verbal descriptors (Reagan [107]).

Similar to the previous table, the one developed by Lichtenstein and Newman [85] can also be helpful. It can be consulted at [14].

Hereafter, there are two tables (B.2 and B.3) to assist in the cases where the probabilities to be estimated fall out of the previous range, though these cases should be avoided in general.

Verbal descriptor	Order of Magnitude of Probability Assigned
Occurrence is virtually certain	1 = 100%
Occurrence of the condition or event are observed in the available database	$0{,}1 = 10^{-1}$ = 10%
The occurrence of the condition or event is not observed, or is observed in one isolated instance, in the available database; several potential failure scenarios can be identified.	$0{,}01 = 10^{-2}$ = 1%
The occurrence of the condition or event is not observed in the available database. It is difficult to think about any plausible failure scenario; however, a single scenario could be identified after considerable effort.	$0{,}001 = 10^{-3}$ = 0,1%
The condition or event has not been observed, and no plausible scenario could be identified, even after considerable effort.	$0{,}0001 = 10^{-4}$ = 0,01%

Table B.2: Table of verbal descriptors (Barneich [16]).

Verbal descriptor	Associated probability
Virtually certain	0,999
Very likely	0,99
Likely	0,9
Neutral	0,5
Unlikely	$0{,}1 = 10^{-1}$
Very unlikely	$0{,}01 = 10^{-2}$
Virtually impossible	$0{,}001 = 10^{-3}$

Table B.3: Table of verbal descriptors (USBR [135]).

Within the process of providing probabilities it is a good practice not to give a single value but three: lower limit, best estimation and upper limit. In this way, each expert assesses the confidence they have on their own probability. Moreover, this makes the comparison with the results of the next section easier.

B.6.5 Comparison of results and re-elicitation of probabilities (second round)

During the same session of failure modes identification, it is convenient to aggregate the results and to show them graphically so they can be discussed in-group. This can be done through different types of charts (see for example figure B.1 or [113]).

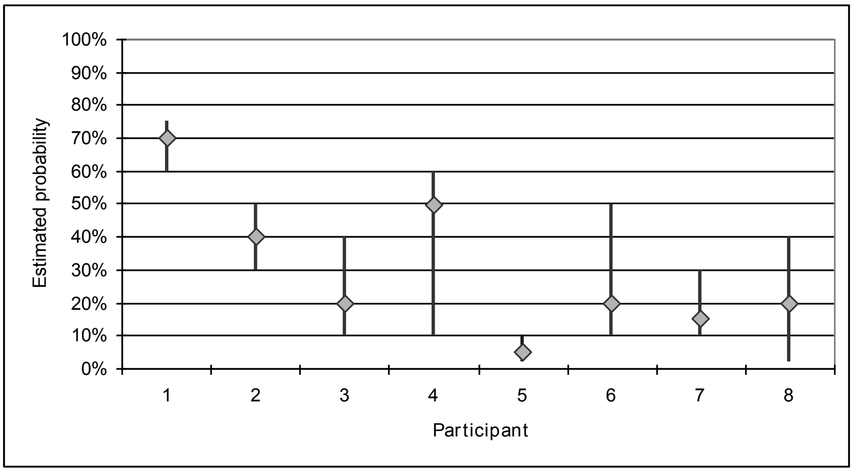


Figure B.1: Example of comparison in linear scale of the probabilities expressed by expert judgment.

At the sight of the comparison, if an expert has expressed a probability that falls out of the range of the group, he or she must argue his/her reasons. It is perfectly admissible to count with different points of view, that must be documented and that are a positive treat of the diversity of the group. It is important to create an atmosphere in which the person who sustains an opinion different from the predominant in the group does not feel uncomfortable at expressing and defending it. This aims at avoiding the *groupthink* phenomenon [130]. This phenomenon can happen when there is too much pressure to reach a consensus and in some cases it can lead to the adoption of irrational conclusion shared by no member of the group.

After this discussion, and now on concrete figures, all the experts have the possibility to change their assignments. In general it is not necessary neither advisable to do more than two rounds.

B.7 Aggregating the results

The last step in the obtention of probabilities throughout expert judgment is the aggregation of the results. According to the notation of NRC, the responsibility of this tasks lies on the TI. The range of possibilities when doing this aggregation is large and includes: arithmetic mean, geometric mean, harmonic mean, weighed mean, median, diffuse logics, minimization of uncertainty, self-weighing by the experts, etc. (see [14]). However, many of these methods are more interesting from a theoretical than from a practical point of view. Within the scope of application of Risk Analysis, the most practical methods are the arithmetic mean, the median or the geometric mean.

In some cases, the TI can decide to exclude the extreme values when calculating the means, though in general this is not advisable.

B.8 Comments for application to gate reliability estimation

When the expert judgment process is done for estimating the failure probability of gates (see chapter 5.5), the basis of the process remains the same. However, there are some worth commenting particularities. In the modeling of gate failure probabilities through fault trees, it is usually impossible or unpractical to decompose all events until reaching individual probabilities higher than 0.1. In this case, the table commented in section B.6.4 loses its utility. As an alternative, any of the other two tables of the same section can be used. Another approach is to change the form of the question. Instead of asking *which is the probability of failure* it can be much more convenient to ask *how many operations are required before failure takes place*. In the end, the question is the same, but most people find easier to estimate that a certain failure would take place every 1,000 operations than estimating the probability of failure to be 0.001.

When these kind of estimations are done, the results must be represented in logarithmic axis, as figure B.2 shows.

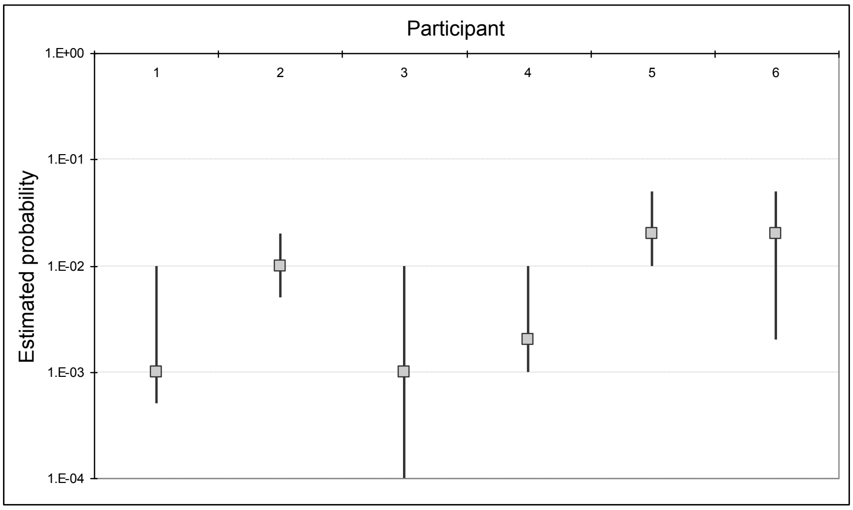


Figure B.2: Example of comparison in logarithmic scale of probabilities expressed by expert judgment.

Finally, when aggregating the results, it has more sense to do a geometric than an arithmetic mean. When using geometric means zero values cannot be accepted (since they will make the mean equal to 0) neither arbitrarily values as low as 10^{-10} (that would distort the result). This problem is avoided by employing the arithmetic mean, where a null or arbitrarily low value would no distort the final result.

Appendix C

Estimating loss of life

C.1 Introduction

When a flood due to a dam failure produces loss of life, this is clearly the most serious consequence and the one that causes the biggest impact on the public perception of the disaster [79]. This is why this consequence has been the object of most consequences studies and therefore, the one for which more calculation methods are available.

Loss of life is an intangible consequence that cannot be estimated directly in economic terms. It falls within the category of direct consequences since it is generally produced directly by the flood wave. For other kind of floods, and especially in tropical areas, the indirect loss of life due to diseases or lack of drinkable water can reach important magnitudes and should also be studied. Other damage to people can also be considered such as the numbers of wounded, though its quantification is more complicated.

The methods to estimate loss of life provide an indicative value of the magnitude of this parameter, but cannot provide an accurate figure. This is due to the fact that numerous of the variables involved in this process are difficult to model properly (e.g., people's behavior). It is important to understand the limitations of these methods, since they model a great number of complex processes and the database of loss of life is quite limited [13]. According to Graham [65], the main causes of uncertainty of these methods are:

- The moment of failure of the dam on which the existing conditions (snow, darkness, rain, etc.) and the population exposed to the flood will depend.
- The form of warning in case of flood, since it is unknown when the public warning will start exactly and how it will propagate.
- The uncertainty inherent to the applied methodologies of loss life estimation.

The study of the available data of loss of life it reveals that the ratios of mortality within the exposed population are quite consistent all over the world for a given type of flood (fluvial, coastal, drainage, dam failure, pluvial, etc.) [79]. The severity of the flood and the warning and evacuation times are also decisive factors.

In general, most of the current methodologies follow this scheme [66]:

1. Identifying a particular scenario to be assessed, including the moment of the day or of the year and also the failure mode of the dam, since they can affect the results.

2. Obtaining data of the characteristics of the flood such as water speed, depth, rapidity, duration, etc. from flood maps.

3. Determining for the evaluated scenario when and how the messages to the population are broadcast.

4. Determining for the different nucleus of population downstream the time elapsed since the warning message was received and the arrival of the flood wave.

5. Estimating the number of people on each of the zones in which the floodable area is divided, according to the flood and the warning time. People remaining in the flooded areas will be there either because they were not warned or because they could not be evacuated.

6. The loss of life is estimated from the exposed population in each area by using the mortality rates based on the characteristics of the flow and the available refuges (buildings, constructions, etc.).

Consequently, the first step of each methodology is to define the scenarios of the study. This step consists of defining the characteristics of the situation in which the dam failure is produced that could affect the results. These characteristics can be:

- The moment of the day, since during the night people will be concentrated for its most in residential areas, whereas during the day they will concentrate in industrial and commercial ones. Moreover, the processes of warning and evacuating are slower during the night.

- The season of the year, especially in cities with important seasonable variations, such as touristic places.

- The failure mode since it affects the way of warning and the way the population perceives the severity of the event. Each failure situation produces different consequences. Therefore, different curves discharge-consequences need to be obtained for their introduction in the risk model (section 5.9.3). The particular situation under study must have been defined when doing the hydraulic model to obtain the flooded areas.

It must be recalled that, in general, these methodologies have been developed and calibrated for the failure case, so their application for non-failure situations can provide less accurate results. Be as it may be, in the absence of more specific methodologies for the non-failure case, the same methodologies are usually applied.

C.2 Graham methodology (1999)

In 1999, Graham [65] developed a new method to estimate loss of life as a consequence of a dam failure using fixed mortality rates. Since then this model has been the reference for the rest of methods and it has been broadly used.

Graham's method proposes fixed fatality rates that are applied to the population in the locations flooded due to a dam failure. These fatality rates depend on:

Severity of the flood: It represents the degree of destruction of buildings and refuges, so it is a function of the depth of the flood.

Warning time: Time elapsed since the first warning is issued to the population and the moment of arrival of the flood to this population. Therefore, it is an indicator of the available time to evacuate or protect people.

Understanding of the severity of the flood: This parameter introduces the understanding by the population of the potential consequences and dangers to which they are exposed and their alertness with regard to a possible flood.

Taking into account these three values, Graham suggests the fatality rates shown in table C.1.

Flood severity	Warning time (minutes)	Flood severity understanding	Fatality Rate (Fraction of people at risk that died)	
			Average	Range
High	No warning	Not applicable	0.75	0.3-1.00
	15 a 60	Vague	* No case fit this category.	
		Precise		
	More than 60	Vague		
		Precise		
Medium	No warning	Not applicable	0.15	0.03-0.35
	15 a 60	Vague	0.04	0.01-0.08
		Precise	0.02	0.005-0.04
	More than 60	Vague	0.03	0.005-0.06
		Precise	0.01	0.002-0.02
Low	No warning	Not applicable	0.01	0-0.02
	15 a 60	Vague	0.007	0-0.015
		Precise	0.002	0-0.004
	More than 60	Vague	0.0003	0-0.0006
		Precise	0.0002	0-0.0004

Table C.1: Table to estimate loss of life caused by a flood [65].

C.2.1 Population at risk

First of all, the population at risk is estimated. In this method, the population at risk is defined as the population within the flooded area when the dam fails, therefore, it does not take into account explicitly the evacuation procedures. In order to do it, it is important to study the population located in each of the locations affected by the considered situation. It is possible to resort to census data and also to population studies performed by public institutions that reflect seasonal variations. Other data, such as the number of working people in the commercial and industrial areas along with their origin are also important to estimate the daily variations of population.

C.2.2 Severity of the flood

The next step is to define the severity of the flood that makes reference to the degree of destruction of the buildings and the threats to the population. Therefore, it depends on the characteristics of the flood. Graham' method divides severity into three categories:

High severity: when the flood wave causes a total destruction of the buildings and structures, producing death to most of the people inside.

Medium severity: some of the buildings suffer serious damages, particularly homes, though there remain trees and buildings where people can seek refuge in.

Low severity: there are no buildings totally destroyed and damages are only superficial.

There are several recommendations explaining how to describe the degree of severity. According to Graham, a high severity is only adequate to the areas located very close to the dam, that will be affected by a great wave of flood very quickly, in a few minutes, with high depths of flood and will result on a total swept of all human life trace. Thus, the method does not recommend any numerical values to define it. Technical literature provides some values to define a high severity zone, depending on the product of speed and depth of flood, though they are very influenced by the construction materials of the buildings and their height, that is, by local characteristics. According to Graham's recommendation, high severity must only be used for concrete dams that fail instantaneously, since earth dams tend to fail more gradually, except for the case of liquefaction produced by an earthquake.

Regarding the differences between the low and medium levels of severity, Graham recommends for a first approximation, to adopt a medium severity level from 10 feet (circa 3 m). For more detail, the parameter DV can be employed:

$$DV = \frac{Q_{df} - Q_m}{W_{df}}$$

where Q_{df} is the peak discharge caused by the flood in the section where the population is located, Q_m is the annual average discharge in the same section and W_{df} is the maximal width of the flood within the considered section. As it can be observed, this parameter is a function of the speed of the flow and of its depth, so it is an indicator of its degree of destruction. Values of this parameter higher then 4.6 m^2/s indicate a medium severity.

C.2.3 Warning time

The next step is to define warning time. As explained before, this parameter corresponds to the time elapsed between the beginning of the warning procedure towards the population and the arrival of the flood wave to the same people. Therefore, it makes reference to the time available for people to seek refuge or being evacuated. Its proper estimation is very important in order to find proper values of loss of life. Warning time must be calculated for each of the groups of houses or populations within the flooded area, and it will be different for each of them. Moreover, it is important to fix an initiation time (or zero) as a reference to measure all times. Figure C.1 shows the different times used in the breakage of a dam.

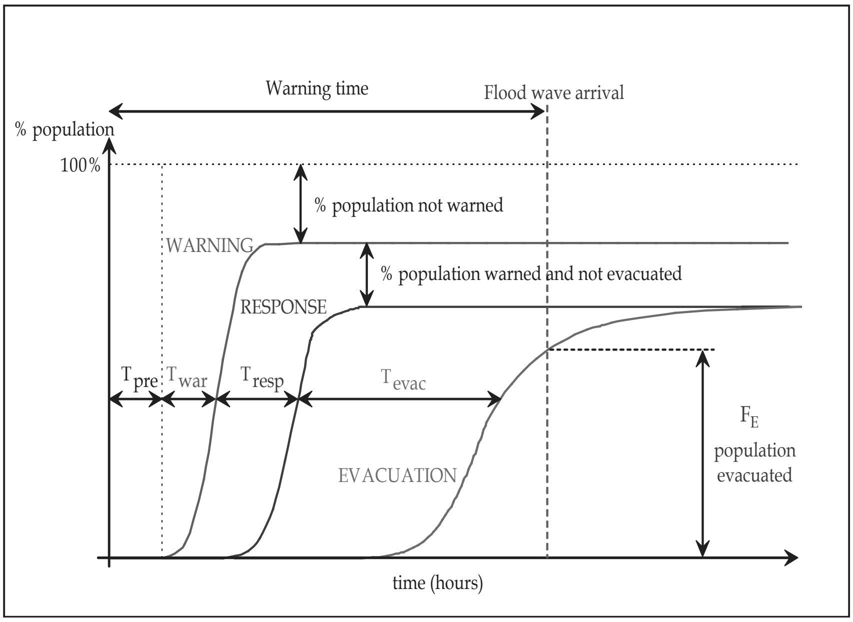


Figure C.1: Distribution of times in a process of evacuation of the population at risk (adapted from [78]).

Within Graham's method, warning time is also divided into three categories:

None warning: when the warning time is lower than 15 minutes. There is no warning, since there is no time for the official sources to issue a warning to the population before the arrival of the flood. The population is only warned when seeing or listening to the incoming flood wave.

Some warning: when the warning time is between 15 and 60 minutes. In this case, it is admitted official warnings have been issued prior the arrival of the flood. The warning is propagated to some people through different communication channels, although not everybody is properly warned.

Adequate warning: when the warning time is higher than 60 minutes. It is admitted proper warning has taken place before the arrival of the flood. Most of the people at risk know a flood is coming.

Due to the impact of warning time on fatality rates, a lineal interpolation can be done between the fatality rate with no warning and the rate with enough warning, passing through the insufficient warning time. In this way, illogical results are avoided.

When intending to determine a first approximation of warning time in a low detail level study, it is possible to use the time elapsed between the dam failure and the arrival of the flood wave. That is the same as admitting that the warning is issued when the flood reaches the population. This simplification is adequate for sudden failure modes, such as the typical of concrete dams.

In a more detailed level of study, first of all, it is necessary to estimate the moment in which the warning to the population is initiated in relation to the moment the dam breaks. For this, the type of failure mode must be considered as it can have a remarkable influence [23]. The failure modes associated with severe floods in large basins take a considerable time to develop, during which monitoring and warning loads usually take place. In smaller basins floods develop in a much quicker way, reducing warning time. Failures due to internal erosion will permit in most of the cases to warn the population a few hours in advance, providing a proper system of monitoring is in place. The failure modes allowing shorter warning times are the ones associated to seismic events. This can be different if there is a local awareness of the risk of dam failure in case of a seismic event, case in which the evacuation after the earthquake might start spontaneously and with no official warning.

Other factor able to affect warning time is the moment of the day at which the flood happens. Indeed, as corroborated by the analysis of floods caused by dam failures, observations are clearer and the propagation of the warning works better during the day [65].

For earth dams, Graham developed table C.2 that explains how to calculate the moment when the warning starts being issued. From this table and knowing how the propagation of the wave of flood happens (thanks to the hydraulic model), warning times for every group of population can be easily estimated. The estimation corresponds to the difference between the arrival time of the flood and the moment the warning starts.

Additionally, USBR [23] suggests the following formula to estimate warning time for all type of dam.

$$WT = T_v + b - FM$$

where WT is the warning time, T_v is the time elapsed between the failure of the dam and the arrival of the flood to the settlement studied, B is the time necessary to the formation of a breach in the dam and FM is a factor related to the failure mode.

Moreover, all the procedures detailed in the Emergency Action Plan of the dam should be considered. This document describes the way in which warnings must be issued and the time at which they should start, so it can prove a very helpful tool when estimating warning times. In general, the existence of a proper Emergency

Cause of failure	Special considerations	Time of failure	Dam Failure Warning Initiation	
			Many observers at dam	**No observers at dam**
Overtopping	Drainage area ta dam less than 260 km^2	Day	15 min before dam failure	15 min after flood wave reaches a populated area
		Night	15 min after dam failure	60 min after flood wave reaches a populated area
	Drainage area ta dam more than 260 km^3	Day	120 min min before dam failure	60 min min before dam failure
		Night	60 to 120 min before dam failure	0 to 60 min before dam failure
Piping (full reservoir, normal weather)		Day	60 min before dam failure	15 min after flood wave reaches a populated area
		Night	30 min after dam failure	60 min after flood wave reaches a populated area
Seismic	Inmediate failure	Day	15 min after dam failure	15 min after flood wave reaches a populated area
		Night	30 min after dam failure	60 min after flood wave reaches a populated area
	Delayed failure	Day	2 hours before dam failure	30 min before flood wave reaches a populated area
		Night	2 hours before dam failure	30 min before flood wave reaches a populated area

Table C.2: Estimation of starting time of the warning in case of earth dams failure [65].

Action Plan along with a good monitoring program of the behavior of the dam, improve warning time.

C.2.4 Understanding of the severity of the flood

The last characteristic of the flood that needs to be defined in the method developed by Graham is the understanding of the severity of the flood. This parameter depends highly on the type of warning messages issued and the way the population assimilates them. Two categories of understanding are defined:

Vague understanding: when the population receiving the warning has never witnessed an event of flood or does not understand the magnitude of the flood that is about to happen.

Precise understanding: when the population understands properly the warning messages and seizes the magnitude of the flood.

One of the most decisive aspects in the understanding of the flood is the time elapsed between the dam failure and the arrival of the flood. Indeed, when this time is high enough, the population can learn about the first consequences of the flood in other settlements thanks to the media and so become aware of the severity of the event.

Also, the type of warning messages is influential. Clear, direct and decisive messages produce a better understanding of the severity of the flood.

Besides, the failure mode affects the warning too since in the case severe floods, by the time failure happens, people will have been observing the rain and suffering from small urban floods for a while; there will be consequently in a state of alert and will understand better the severity of the flood.

Moreover, the existence or remembrance of past important floods in the area is also decisive, as in those cases people know the consequences of a flood and will react more quickly to the warning messages.

Additionally, USBR [23] recommends getting an accurate understanding of the severity of the flood whenever there is an Emergency Action Plan of the dam, since then, it is understood that the Authorities will know how to act to transmit properly the messages and therefore, the population will understand the severity of the event.

C.2.5 Results

With warning time, exposed population, severity of the flood and understanding of severity determined for each population settlement, the number of victims is estimated directly through the application of table C.1, which indicates which fatality rate must be applied to the population at risk. The total number of victims produced by the flood is obtained by adding the number of victims in each population settlement.

Graham's method can be applied in different levels of detail, from isolated homes to large areas, to obtain general approximations of the number of victims. The degree of detail it can be applied with depends much on the available data of population distribution

When the method provides values that fall in between two categories, i.e., medium-low severity or medium understanding of the flood, it is possible to employ average values of the fatality rates for both categories [134]. In order to make the calculations easier, it is possible to use GIS software, with digital maps showing the distribution of the population that can be directly compared with the results obtained through a hydraulic model. For this, digital maps must have enough resolution and indicate the situation of the distribution of the population at different moments of the day and the year, when there are important variations. Figure C.2 shows the general structure of the calculation of loss of life when employing GIS.

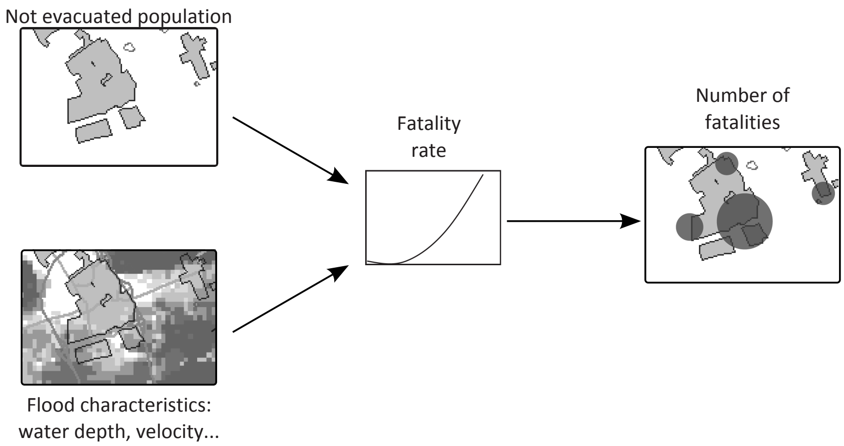


Figure C.2: Basic components of any model employing GIS for the estimation of loss of life [63].

C.2.6 Discussion on Grahams' Methodology (1999)

The main advantages of using Graham's method [66] lay on the important databases of past floods used to obtain the fatality rates and in the simplicity of its application and understanding. Besides, since all the parameters have a clear correspondence with reality it is easy to modify them in case the situation do not fit exactly to what is established by default. The method also allows different degrees of detail and general approximations from a few original data.

On the other hand, it has some drawbacks such as the existence of factors changing with the type of flood that are not taken into account or the fact that the evacuation is not calculated as a separated process. The method uses average values of the characteristics of the flood and of the buildings in the same settlement, which can produce important mistakes if the variations are important. These considerations explain why it is required to choose the smallest available units of population.

Moreover, the different channels of propagation of the warning and their efficiency are not considered in the calculation of warning time.

C.3 Other methodologies

There are many methods to estimate loss of life. In the bibliography, Graham [66] describes many of the methods explained in this section, analyzing their general methodology along with their advantages and drawbacks.

C.3.1 Upgrades to Graham's methodology (1999)

In 2001, USBR [23] proposed a modification of Graham's method, adding a new variable that affects the fatality rate: breach formation time. This parameter is divided into three categories, according to the characteristics of the dam and its failure, explained above for obtaining warning time. On the other hand, it eliminates the part related to the understanding of the severity. With this new variable, new fatality rates based on the ones obtained by Graham are proposed. The fatality rates of the modified version are in general higher than in Graham's one, which might lead to an overestimation of the number of victims with regard to the original method.

Reiter [108] recommended in 2001 to correct Graham's fatality rates through the application of a vulnerability factor to the population at risk in order to include very aged areas, hospital areas or with a great number of children. His argument was that these populations would increase the difficulty of the process of protection and evacuation, hence, would be more affected by the wave of the flood.

In 2006, USBR [25] developed a new method that incorporated an additional step to Graham's one. USBR's version applies evacuation rates to the population as a function of warning time, moment of the day, rising speed of the depth and channel of propagation of the warning. The fatality rates, different from the ones proposed by Graham, are applied to the population that remains in the flooded area after the direct evacuation, taking into account just the severity of the flood. In this way, it makes possible to consider evacuation as a separated process. Like Graham's method, it is solid and easy to apply, but it also has some drawbacks [66]: the estimation of the evacuation rates can produce important mistakes due to the complexity of modeling this process.

Additionally, FEMA [54] has also developed a method based on Graham's one. It assumes that fatality rates are higher next to the dam. These rates are also higher when discharges are much higher than the usual discharges of the river, because the population is taken by surprise by the flood. The flooded area is divided in three zones and then mortality is calculated according to the relation between the discharge associated with the flood of 10 years return period and the maximum discharge produced with the dam failure. This method is very simplistic, so its application is only advisable for volumes of storage smaller than 25 hm^3 [66].

ANCOLD [13] recommends at its turn other fatality rates different from the ones of Graham for highly vulnerable areas such as geriatric residences, schools or touristic areas.

C.3.2 SUFRI methodology

The European project SUFRI (*Sustainable Strategies of Urban Flood Risk Management with non-structural measures to cope with the residual risk*) [49, 48], within the framework of the initiative ERA-Net CRUE, has recently developed a tool allowing the characterization of the residual risk and the study of the effect non-structural measures have on the reduction of the consequences, and so on the flood risk. This tool is based on the development of FN curves for each urban environment, enabling the global characterization of the risk in a quantitative way and the application of tolerability guidelines for the existent risk. The project includes a methodology that details the different phases necessary to elaborate risk models in the cases of pluvial and fluvial floods, as well as the procedures of analysis and preparation of data to feed those models.

In particular, project SUFRI describes in more detail the phase of estimation of flood consequences. With regard to fluvial flood, it proposes a classification of ten categories for the studied population, according to the existence of warning systems, coordination between the emergency systems and the local authorities, mass media, training of the population, etc. Each category is related to some referential fatality rates (see table C.3), depending on the warning time and the degree of severity of the flood, which are based on the studies done by Graham in 1999.

SUFRI has put a particular focus on the affected population, expected to act in a proper way to reduce possible consequences of flooding. In this context, an effective risk communication plays a major role to initiate, support, maintain and keep up the knowledge about flood reducing measures and adequate behaviour. Therefore, the questionnaire developed within the SUFRI project, as part of the 'Method for the investigation of risk awareness of the population concerned' [144], provides empirical data on the subjective view of the citizens regarding flooding. Particular attention is paid to the desired communication and information before, during and after a flood [67]. In fact, results of the opinion poll support the category selected from the classification described in table C.3 (C1 to C10).

C.3.3 Jonkman Methodology

One method similar to Graham's one is the one developed by Jonkman [78], which calculates loss of life from population at risk, estimating the different processes that happen during the flood.

First, it obtains the population exposed to the flood after the evacuation processes and their relocation in refuges. The efficiency of the population at risk evacuation is a direct function of the available time, taken into account there always remains

Category for the case study (C)		Warning time TW (h)	Flood severity (Sv) High (3)	Medium (2)	Low (1)
1	- There is no public education on flood risk terms. - No warning systems, no EAP. - There is no coordination between emergency agencies and authorities. - No communication mechanisms to the public.	*0*	0.9	0.3	0.02
		0.25	0.9	0.3	0.02
		0.625	0.7	0.08	0.015
		1	-	0.06	0.0006
		1.5	-	0.0002	0.0002
		24	-	0.0002	0.0001
2	- There is no public education on flood risk terms. - There is **no EAP,** but there are other warning systems. - There is no coordination between emergency agencies and authorities. - No communication mechanisms to the public.	*0*	0.9	0.3	0.02
		0.25	0.9	0.3	0.02
		0.625	0.675	0.075	0.014
		1	-	0.055	0.00055
		1.5	-	0.0002	0.0002
		24	-	0.0002	0.0001
3	- There is no public education on flood risk terms. - There is **EAP,** but it has not been applied yet. - Some **coordination** between emergency agencies and authorities (but protocols are not established). - No communication mechanisms to the public.	*0*	0.9	0.3	0.02
		0.25	0.85	0.2	0.015
		0.625	0.6	0.07	0.012
		1	-	0.05	0.0005
		1.5	-	0.0002	0.0002
		24	-	0.0002	0.0001
4	- There is no public education on flood risk terms. - **EAP** is already applied. - Coordination between emergency agencies and authorities (there are **protocols**). - No communication mechanisms to the public.	*0*	0.9	0.3	0.02
		0.25	0.75	0.15	0.01
		0.625	0.5	0.04	0.007
		1	-	0.03	0.0003
		1.5	-	0.0002	0.0002
		24	-	0.0002	0.0001
5	- There is no public education on flood risk terms. - EAP is already applied. - Coordination between emergency agencies and authorities (there are protocols). - **Communication** mechanisms to the public (not checked yet).	*0*	0.9	0.3	0.02
		0.25	0.75	0.15	0.01
		0.625	0.5	0.0375	0.0065
		1	-	0.0275	0.000275
		1.5	-	0.0002	0.0002
		24	-	0.0002	0.0001
6	- There is no public education on flood risk terms. - EAP is already applied. - Coordination between emergency agencies and authorities (there are protocols). - Communication mechanisms to the public.	*0*	0.9	0.3	0.02
		0.25	0.75	0.15	0.01
		0.625	0.475	0.035	0.006
		1	-	0.025	0.00025
		1.5	-	0.0002	0.0002
		24	-	0.0002	0.0001
7	- **Public education.** - EAP is already applied. - Coordination between emergency agencies and authorities (there are protocols). - Communication mechanisms to the public. **Or Dam break with no hydrologic scenario.**	*0*	0.9	0.3	0.02
		0.25	0.65	0.1	0.0075
		0.625	0.4	0.02	0.002
		1	-	0.01	0.0002
		1.5	-	0.0002	0.0002
		24	-	0.0002	0.0001
8	- Public education - EAP is already applied. It has been proved or used **previously.** - Coordination between emergency agencies and authorities (there are protocols). - Communication mechanisms to the public.	*0*	0.9	0.3	0.02
		0.25	0.55	0.06	0.006
		0.625	0.35	0.01	0.0015
		1	-	0.005	0.00015
		1.5	-	0.0002	0.00015
		24	-	0.0002	0.0001
9	- Public education. - EAP is already applied. It has been proved or used previously. - **High** coordination between emergency agencies and authorities (there are protocols). - Communication mechanisms to the public.	*0*	0.9	0.3	0.02
		0.25	0.55	0.06	0.006
		0.625	0.35	0.008	0.0015
		1	-	0.004	0.000125
		1.5	-	0.0002	0.0001
		24	-	0.0002	0.0001
10	- **Regular** activities and plans for public education. - EAP is already applied. It has been proved or used previously. - High coordination between emergency agencies and authorities (there are protocols). - Communication mechanisms to the public.	*0*	0.9	0.3	0.02
		0.25	0.5	0.03	0.005
		0.625	0.3	0.005	0.001
		1	-	0.002	0.0001
		1.5	-	0.0002	0.0001
		24	-	0.0002	0.0001

Table C.3: Fatality rates used in the application of Graham method developed in the SUFRI project [49].

a part of the population that cannot be evacuated. With regard to the movement towards refuges or protected places, it is a function of the warning time and the population living in high buildings. Moreover, to estimate the exposed population, the population rescued during the flood must also be removed.

From the population at risk, the number of victims can be calculated through the fatality rates that are estimated as a function of the depth of water. These rates are extracted from non-lineal functions that differ according to the severity of the flood, which is divided into three categories.

In general, this method depends on the same data as Graham's one, that is, population at risk, warning time and flood severity, though it makes a more detailed study of each process. The main problem of this method is that it has been developed for general floods and has only been applied to model floods produced by the breakage of levees below water level, such as the ones that affected New Orleans in 2005. Therefore, it has not been sufficiently tested or adapted for modeling dam failures yet.

C.3.4 LIFESim

In order to perform a detailed analysis it is possible to apply other methods that require more data but whose results represent more faithfully the physical reality and the development of the flooding process. LIFESim [2, 1] outstands among this kind of models. This model allows the simulation of people's behavior in case of flood, providing results at a much smaller scale (micro-scale) than the previously outlined methods. For this doing, it employs three different modules:

1. Warning and evacuation: this module redistributes the population considering a curve of warning propagation that depends on the moment of the day and a mobilization curve that simulates the escape of the population according to the existent communication infrastructures. Data used include type of warning, evacuation methods, distance until safe areas and the characteristics of the roads and other communication infrastructures. Moreover, in order to represent those processes, aspects such as the characteristics of the traffic and the blockage of roads are considered.

2. Loss of shelter: it estimates the consequences flood has on the buildings, so it depends on the characteristics of both the flood and the constructions. To carry out this estimation it is necessary to gather data of the constructions, the buildings and the distribution of the population with regard to the buildings high enough to act as potential refuges.

3. Loss of life: calculates victims by applying fixed mortality rates according to three categories of flood severity. The rates are applied to the population that stays within the flooded area and whose shelter is destroyed. The rates are fixed for each area and are obtained from measurements and studies of historic floods [91].

This method is particularly adequate to city-centers, where the roads capacity and the propagation of warning messages might have a huge impact on the number of victims. However, it demands a very important amount of data (about population distribution, roads, warning systems, etc.) and a great effort of modeling.

In order to solve this problem of LIFESim, a Simplified LIFESim [101] has been developed, more adapted to the simulation of loss of life within the context of infrastructure risk management. This simplified version reduces considerably the amount of data required in the hydraulic modeling, since it does not consider the speed of the flow in the loss of refuges. It also simplifies the evacuation processes thanks to two assumptions: there is a fixed speed of evacuation and people is evacuated from their building of origin towards the closest safe area following a straight line.

Though this simplified method reduces significantly the data necessary to estimate loss of life, it remains much more complex than Graham's one. Besides this, it requires many data about the different population settlements, which can make its application difficult when the flood affects a great number of settlements, as it is usually the case if a large dam fails. In any case, it is a good option for an intermediate-detailed Risk Analysis.

C.3.5 BCHydro methodology

Another method for application to small scales is the one developed by BCHydro and HR Wallingford [72, 87]. This methodology called Life Safety Model uses GIS data with a two-dimensional model of flow and a population characterization. The loss of life is estimated combining the following aspects:

- The number of people that are killed or injured by an inundation.
- The movement of vehicles is modeled by a simple traffic model.
- The dynamic interaction of the floodwave with vehicles.
- The capacity of each building to withstand the floodwater.
- People movement model as individuals and also as groups.
- The speed of the dissemination of flood warnings.
- The evacuation of people.

This method has a high level of detail, so requires a considerable number of data about the location of the population, the buildings and the roads.

Appendix D

Estimating economic consequences

D.1 Estimation of direct damages

This section develops the methodology required to calculate direct and tangible economic damages produced by the wave of the flood, including damages to homes, industry, commerce, buildings, infrastructure, services, agriculture, etc.

According to Messner et al. [93], the calculation of flood direct consequences can be done at three different scales:

Macro-scale: In this case the calculation of consequences encompasses several municipalities, the official data being the main source of information. In general, the damages by municipality or the differences on the distribution of homes are not differentiated and average values for the whole flooded area are adopted, which produces important inaccuracies.

Medium-scale: As in the previous case, the calculation also deals with aggregated data, but at a smaller scale, using for these purposes maps of land-use that discretize the flooded area in smaller lots. In this way, it is possible to differentiate among the areas with a high population density and the agricultural ones. Official data are also the main source of information. This is the most adequate scale of study to analyze the consequences of a flood by dam failure at an intermediate or basic level.

Micro-scale: This scale is usually used for a single urban area and it considers the value of each building or infrastructure affected by the flood, so it demands a very detailed work in terms of data collection. This scale provides better results but it is very expensive for large areas as it is the case of a flood caused by a dam (which usually comprises several municipalities). Hence, its use is also recommended for studies of a high level of detail.

In general, current methods to estimate direct consequences consist of two steps.

The first one is estimating the total value of land use, that is, which would be the costs if every building and crop existing in the analyzed land were totally destroyed as a result of the flood. The second step consists of applying those costs to the curve depth-cost, that relates the maximum depth of a flood with an associated value of destruction. In this way, by multiplying the degree of destruction by the economic cost of a maximal destruction it is possible to estimate the economic consequences of the relevant flood. Consequently, in order to apply this methodology it will be necessary to use as a starting point land-use maps and flood maps showing the depth of water at each location. These two steps are outlined herein:

D.1.1 Estimating value of land

The first step will be estimating the total value of the land, that is, the cost involved by the total destruction of the different land-uses within the flooded area. This cost is divided according to land-use, expressed per squared meters and will depend on the socio-economic characteristics of the area. These costs have been calculated for different countries in studies such as the one done by the Ministry of Construction of Japan [99] or the one done by Oliveri et al. [104] in Palermo.

In Spain, it is possible to use the recommended values given by the Territorial Action Plan with Sector Character on Flood Risk Prevention in the Valencian Region (PATRICOVA) [35]. This Plan defines vulnerability with regard to a given flood as the variable that quantifies the value of the damages caused by this flood. Thereby, vulnerability is a way of quantifying the economic consequences of a flood. The PATRICOVA defines values for direct damages and land-uses with a total destruction, called vulnerability factors. These values represent the first estimation of land-use value in non-dimensional terms, within a scale from 0 to 100. Following a similar methodology, there exist also some referential land-use values in Catalonia, specified in the INUNCAT [3].

Two values are defined for each land-use (a high and a low one), which makes possible the adoption of an intermediate value if there are no accurate data available. This variable has been non-dimesionalized, with a maximal value of 100 that corresponds to the maximum damages that can happen in a residential and highly populated area. In order to transform these vulnerability values into economic terms, the PATRICOVA assigned to the vulnerability value of 100 a corresponding cost of 82 €/m^2in the year 2002. This equivalence has been obtained for the case of the Valencian Region, and it is essential to adjust it to the area of the study. In this way, estimating economic costs from vulnerability is a direct process that only requires transforming the results into a current economic value through the use of economic indicators such as the consumer price index (CPI).

The value determined in this section will make reference to the economic costs in the case of total destruction of the land. This scenario is not the most likeable one since buildings and structures usually remain after the flood. In order to estimate a more realistic degree of destruction, it is possible to apply curves depth of water-damages, as explained in the next section.

D.1.2 Water depth-damages curves

The next step after estimating the economic value of flood direct consequences for a total destruction hypothesis is to estimate the real degree of destruction due to the particular flood under study. For this purpose, most methodologies employ water depth-damages curves that relate the depth of the flood with the attained degree of destruction. Depth is used since it is the feature that defines the best the consequences of a flood, though other characteristics such as warning time and flood duration can also impact consequences.

PATRICOVA proposes a water depth-damages curve for all land-uses [35]. This curve presents a clear S shape that corresponds with a normal evolution of flood consequences. There is a water depth over 0.8 meters from which the consequences rise very steeply until reaching a depth of 1.2 meters, value from which consequences rise at a slower pace. From 2 meters there is a stabilization of damage that keep on rising little by little. This makes possible to admit damage is constant (or slightly higher) after this point.

For a higher level of detail it is possible to use different curves for every land-use, since, for example, damage to crops follow a different distribution than damage endured by homes. This is why several curves have been developed for the different land-uses and in different areas where floods have been studied in more detail. As an example, figure D.1 shows the curves obtained for the German coast for seven different uses. From these curves it will be possible to estimate damage to buildings within the urban areas, to industry, agriculture, stockbreeding, the road network and also to the vehicles within the flooded area. In general, these curves present an S shape but not always.

These detailed curves have not been obtained in a generic form for the Spanish case, though they can be estimated in a simple way according to the land-uses of each area, and some specific studies can be found [30]. In agriculture, for instance, they can be estimated through the knowledge of the characteristics of the predominant crops. This permits to consider facts such as the better resistance of arboreal crops in comparison with herbaceous ones. With regard to stockbreeding, the curves depend on the type of cattle. However, for depths over 2 m damages are virtually total (100%) and for all varieties, as shown in figure D.1. Regarding the industry, the curves will depend on the characteristics of the local industries, their equipment and related buildings. A detailed description of damage allows the correct definition of these curves for each case.

Concerning homes, the degree of destructions depends enormously on the analyzed type of construction, since for a given depth the damage suffered by a house will differ a lot from the one endured by a high building. Some authors [90] have proposed the calculation of different curves depth-damages according to the type of homes, since aspects such as the number of floors or the construction materials will be essential when estimating the degree of destruction. It is also possible to admit that the largest damages are found as the respective floors are flooded, which will produce a higher rise in the degree of destruction. For example, first floor will be

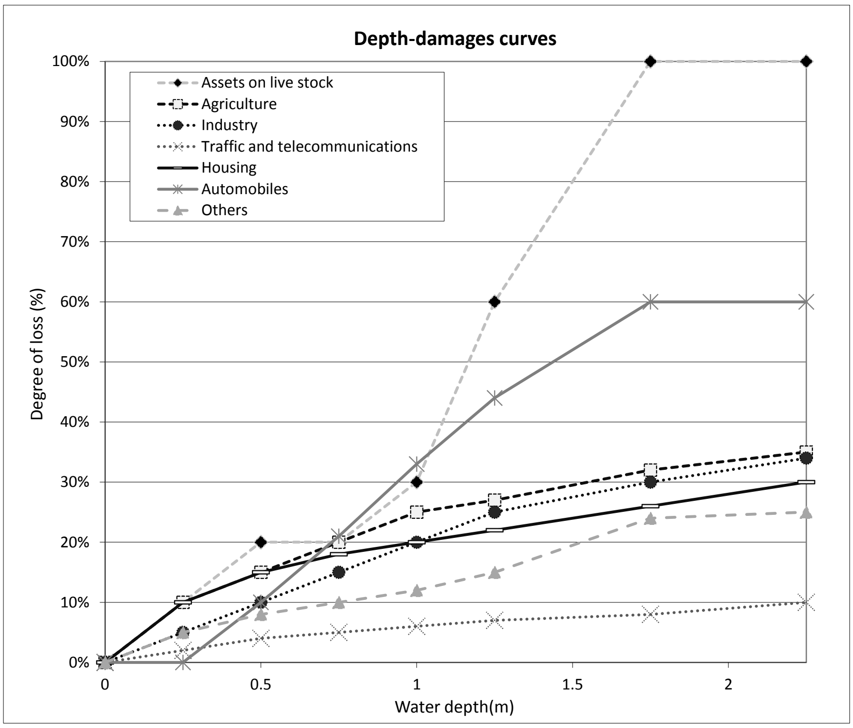


Figure D.1: Curves water depth-damages for different land-uses in Germany [42].

flooded around a depth of 0.8 meters, when the depth-damages curve starts rising. Moreover, the degree of destruction depends on the construction materials, since it is always superior in wooden constructions than in concrete ones.

The curves in urban areas can also be improved through the use of surveys to the population that will define the characteristics of their homes and the effects of previous floods. McBean et al. [90] have developed a methodology to obtain these curves directly from the data of the surveys.

When a higher accuracy is intended these curves can be calibrated with data of degree of destruction caused by past floods, which will provide a better adjustment of the results to reality.

It is also important noticing that other parameters of the flood can influence the definition of these curves. According to McBean et al. [89], they can also depend on:

Warning time: with enough time, the inhabitants of the flooded area can organize their belongings and move them to higher places or away from the affected areas. In general, warning time is defined as the time elapsed between the moment the population find out about the arriving flood (on many occasions this moment is made equal to the instant the dam fails) and the moment the flood wave reaches the first person of the population at risk.

Duration of the flood: it is important since damages increase with the deterioration induced by water.

Water speed: the dynamics of water movement can cause failures to the structures if the combination of speed and depth make the design maximal loads are overpassed [124].

Finally, when applying the curves depth-damages it is important to consider a change of life-style might have happened since the times when the curves were determined until the moment they are effectively used [89, 90]. This is why the curves must be reviewed every time they are applied to ensure they reflect the reality of the affected area.

D.1.3 Results

Flood direct consequences are obtained multiplying the value of land-use by the attained degree of destruction extracted from depth-damages curves.

This method can be implemented through the use of digital maps of land-use and flood-consequences thanks to GIS. The use of GIS makes the calculations easier and provide more accurate data. These software programs associate to each land-use a curve depth-damage and a price. The flood costs are obtained by comparing the map of flood depths with the maps of land-use and the curves depth-damage. This process is shown in Figure D.2. The method has been employed along with GIS software to study flood consequences in cases such as river Ichinomiya (Japan) [40], in China [109] and in Shir-Jr (Taiwan) [129].

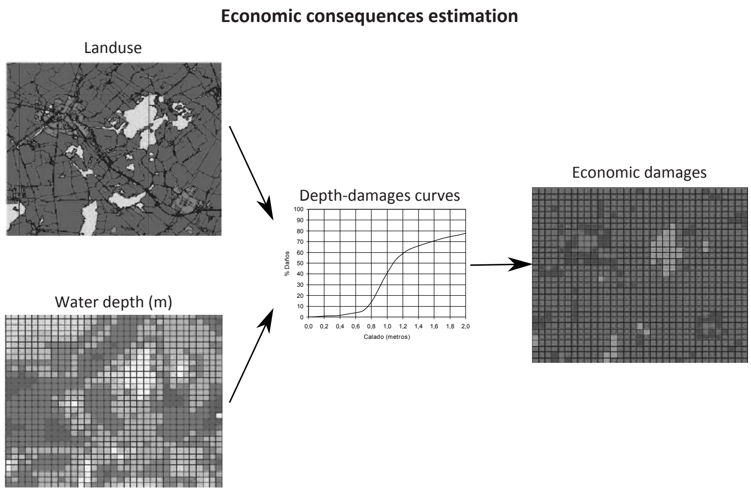


Figure D.2: Basic components of a model to estimate economic damages through the use of geographical information systems (GIS) (SIG) [63].

An example of software that employs GIS in the calculation of consequences is HAZUS-HM [55], a package developed by FEMA that calculates consequences from

700 depth-damages curves for different land-uses. Additionally, it enables an analysis with different levels of detail [133].

D.2 Estimating general indirect damage

Indirect damage refers to the economic consequences that are not produced directly by the flood wave. That is, the effects the flood has on the area beyond the effect of water itself. Some clear examples of this kind of effects are the consequences due to the stop of the economic activity in the area and the cost of accommodating the people whose homes have been affected by the flood.

The estimation of indirect damage is very complicated as there are myriad components involved and the processes implied are very complex. One factor of particular importance is time, since, as opposed to direct conditions, indirect damages appear prolonged in time. This section presents a methodology to perform a general approximation to the economic disruption produced by a flood without doing a detailed study by economic sector or by cause.

In general, it is obvious that if the economic activity stops temporarily in a certain area, there will be a loss of production and a shrink of the offer. Besides, other consequences can ensue this interruption and some of them can be particularly severe in certain industries related to intermediate products, commerce, services such as electric supply, telecommunications supply and relations between firms [93]. These consequences can be of a special gravity if they affect the production of exportation goods or if the affected activities are highly specialized or concentrated, cases in which there is no possibility of compensating with other national producers.

On the other hand, indirect damage will include other costs non-related to the economic activity such as the accommodation of the populations whose homes have been affected, the costs of rescue actions or of protection structures.

First of all, it is possible to estimate indirect costs as a fix percentage of direct costs. The values of this percentage vary largely according to the authors and the area in which they are applied. James et al. [77] recommend adopting indirect damages as a 15% of direct damages in urban areas and as a 10% in agricultural areas. Instead, Japanese Ministry of Construction [99] estimated the loss in economic activities as a 6% of total direct costs.

In Spain, the recommendations of PATRICOVA [35] can be applied. This consists in obtaining indirect costs by applying a percentage of the direct costs that might vary between 0 and 55%, depending on the relative importance of the former with regard to the latter.

There are some cases in which the application of a fixed percentage can produce very important mistakes since the indirect costs are much more important than the direct ones. This is the case, for example, of an airport, where the direct costs induced by the flood on the landing lanes are much lower than the indirect costs involved by the interruption of the aerial traffic. In these cases it is recommended to carry out a more detailed study of the potential indirect costs, based on past similar events.

For studies with a high level of detail, some methodologies are being developed at the moment to estimate indirect costs through analytic methods. An existing method is the application of an "Input-Output" model [133]. This one, admitting the prices are constant, studies the variations of the economic flows after the flood, thus enables the analysis of its consequences on the economic system. An example of this kind is the study developed by Bockarjova et al. [17] in Holland.

Other possible method is the use of an analysis of Global Balance [133] that is more complex but considers prices variations. In general terms it is admitted that variations are made within each sector to reach a new economic balance, and so the responses of the market to the flood are analyzed.

D.3 Estimating damages due to the dam destruction

If the failure mode corresponds to the breakage of the dam, the related cost must be included in the analysis. When estimating the costs of destruction of a dam, two approaches are valid. One is admitting that the dam would never be rebuilt then trying to estimate the cost ensuing the absence of the structure. The second one is admitting that the dam would be rebuilt and therefore estimating the costs of its reconstruction (and in case it was necessary, the costs resulting of the absence of the dam during the construction period).

Both costs are an estimation of the same concept, that is, the breakage of the dam thus it would not be correct to add them since it would mean they are being counted twice. Comments on both approaches are outlined in the following sub-sections.

D.3.1 Cost of dam reconstruction

The cost of dam reconstruction is usually classified as a direct cost though it is not produced directly by the flood wave, but by the action (overtopping, earthquake, etc.) producing the flood. This is a tangible cost as it can be expressed in economic terms. The costs of reconstruction must be separated from the rest of tangible consequences estimated in section D.1, since it is important to know its value independently from the rest of economic costs. This is due to the fact that this cost would only be applicable in the event the dam fails (they are not applicable to calculate the costs without breakage of the dam and the curve discharge-consequences related to them).

The investigations presented to estimate this type of costs are very little developed, since in general it is usually estimated from the original project of the dam or from similar current projects under construction. Besides, sometimes this cost is not included, especially when the flood affects great areas of population and the magnitude of the reconstruction costs is very low in comparison with the rest of economic consequences.

One methodology developed to estimate these costs is the one proposed by Ekstrand [41] for a first approximation. It consists of a lineal interpolation of the reconstruction cost as a function of the volume of the reservoir. This interpolation presents a R2 of 0.47 and is shown in the equation that follows:

$$CR = 17.606 + 0.13965 \cdot KAF$$

Where CR is the cost of reconstruction in millions of dollars (year 2000) and KAF is the volume of the reservoir in thousands of acre-foot.

This interpolation was obtained from the data of several dams in the USA, so their transposition to the Spanish case is difficult. Moreover, the own author only recommends its use in the cases where there are no available data about the original costs of the construction of the dam.

In general, Ekstrand [41] recommends the transposition of the total construction budget of the original dam into current economic terms, using for that economic factors such as IPC or other similar economic indexes related to the construction industry, such as the ones recommended by USBR [26] that show the variation indexes of prices in dam projects since 1977 until today in the USA. In old dams, the use of this equation can lead to very important mistakes, since the standard of living and the constructive conditions might have changed considerably.

The recommendation to estimate construction costs in old dams is estimating the construction costs of a new dam of similar characteristics, using for that expert engineer judgment and the budgets of other similar dams built recently. The obtained results can be compared with the ones provided by Ekstrand's equation.

Moreover, in every case, the result must be adjusted according to other factors such as the installation of electrical substations, the need for additional constructions and other extra aspects independent from the general construction of the dam.

Damage due to the absence of the dam

The indirect costs due to the absence of the dam make reference to the economic losses caused by the fact of being unable to manage part of the volume as a consequence of the dam failure. According to Ekstrand [41], the losses produced by the breakage of the dam on the water resources are:

- Loss of agricultural benefits: since water cannot be stored its use for irrigation becomes impossible and so the culture of certain crops, which causes economic losses.
- Loss of water supply: the loss of water storage can produce a lack of industrial production and economic costs resulting for the extra measures adopted to guarantee water supply to the population.

- Loss of recreational use: the loss of the water storage makes impossible its use for recreational activities in the reservoir, which might induce significant economic losses depending on the usual number of visitors and the existing installations.
- Loss of benefits of flood control: the existence of the reservoir enables the routing of floods and the reduction of the flood consequences downstream; therefore, its destruction can imply future damage by flood.
- Loss of electric supply: if there is a hydroelectric plant in the dam, its destruction produces a loss of electric supply that must be estimated, particularly in dams with an important production.

These consequences only happen in the case of breakage of the dam so they must not be included in the calculation of the consequences curve in the case of non-breakage. Each consequence is analyzed individually below.

Damage on the water resources system

This type of damage refer to the economic consequences on the water resources system produced by the non-satisfaction of the demands as a consequence of the absence of the dam. Hence, it includes the loss of agricultural benefits and the loss of water supply. In general, these damages are the most important of all the created by the absence of the dam, particularly in semi-arid areas where the availability of water is essential to human development.

An approximation to this result can be done using fictive prices of water demand [133], that is the price the users of each type of water use would be willing to pay to have access to water in good conditions. The, this price is multiplied by the annual average volume of water supplied to that particular use by the dam. Finally, the annual loss can be obtained by adding the losses related to each type of water use that must be multiplied at its turn by the duration in years of the reconstruction of the dam.

In Spain, a methodology has been developed and applied to the estimation of these costs [132]. This methodology enables to obtain the consequences on the various uses of water, that is, on urban, industrial and agricultural uses through the simulation of the water resources system. The methodology concept is based on the fact that the economic prejudice of being unable to satisfy the water demands due to dam failure is defined as the difference between the economic benefits of each of the users of the system as a consequence of the use of the resource in case of non-failure (or non-failure) and the same benefit after the failure (or failure).

D.3.2 Other damages due to the non-existence of the dam

In addition to the abovementioned, the non-existence of the dam induces other damages:

Loss of recreational use. In general, the methodology to estimate this type of consequences consists of estimating the value an average person is willing to pay to do these activities [133]. This value is multiplied by the average number of visitors that follows each of the activities during the time of reconstruction of the dam, which provides the total value of the consequences. This method can be applied to a high level of detail study in case these consequences are studied in depth.

Loss of the benefits of flood routing. A first approximation to the estimation of these consequences would be the use of the annual average economic consequences found downstream as a result of a flood before the existence of the dam. These annual consequences must be multiplied by the reconstruction time of the dam and transformed to current value through the use of indexes such as the CPI. If a more detailed analysis is required, it is possible to do new hydraulic models admitting the non-existence of the dam, and calculating the economic consequences of the studied cases.

Loss of electric supply. With the unit price of electric production, it is possible to estimate the total loss of production with the average energy generated per year and the delay of reconstruction.

Bibliography

[1] Aboelata, Maged and David S. Bowles: *Lifesim: A tool for estimating and reducing life-loss resulting from dam and levee failures*. 2008.

[2] Aboelata, Maged, David S. Bowles, and Duane M. McClelland: *A model for estimating dam failure life loss*. In *Proceedings of the Australian Comittee on Large Dams Risk Workshop*, October 2003.

[3] Agència Catalana de l'Aigua: *INUNCAT - Pla Espècial d'Emergències per Inundacions*, 2009.

[4] Altarejos-García, L., M. L. Martínez-Chenoll, I. Escuder-Bueno, and A. Serrano-Lombillo: *Assessing the impact of uncertainty on flood risk estimates with reliability analysis using 1-d and 2-d hydraulic models*. Hydrology and Earth System Sciences, 16:1895–1914, 2012.

[5] Altarejos García, Luis: *Contribución a la estimación de la probabilidad de fallo de presas de hormigón en el análisis de riesgos*. PhD thesis, Universidad Politécnica de Valencia, November 2009.

[6] Altarejos-García, Luis, Ignacio Escuder-Bueno, Armando Serrano-Lombillo, and Manuel Gómez de Membrillera-Ortuño: *Methodology for estimating the probability of failure by sliding in concrete gravity dams in the context of risk analysis*. Structural safety, 2012. `http://dx.doi.org/10.1016/j.strusafe.2012.01.00`.

[7] Andreu, Joaquín: *Conceptos y métodos para la planificación hidrológica*. Centro Internacional de Métodos Numéricos en Ingeniería, Barcelona, 1993.

[8] Ardiles, L., P. Moreno, E. Jenaro, J. Fleitz, and I. Escuder: *Dam safety risk analysis, assessment and management in the duero river basin (spain)*. In *Canadian Dam Association Annual Meeting*, Canadá, October 2010.

[9] Ardiles, L., P. Moreno, E. Jenaro, J. Fleitz, and I. Escuder: *La gestión del riesgo en el ámbito de la seguridad de las presas de titularidad estatal de la cuenca del duero*. In *IX Jornadas Españolas de Presas*. Colegio de Ingenieros de Caminos, Canales y Puertos, June 2010. ISBN 978-84-92626-68-7.

[10] Ardiles, L., D. Sanz, J. Fleitz, and I. Escuder: *Hacia una gestión integral de la seguridad de las presas de la confederación hidrográfica del duero*. In *II In-*

ternational Congress on Dam Maintenance and Rehabilitation 2010, Zaragoza, November 2010.

[11] Ardiles, L., D. Sanz, P. Moreno, J. Fleitz, and I. Escuder: *Risk assessment and management of 26 dams operated by the duero river authority in spain*. In *DAM ENGINEERING. International papers of technical excellence*, volume XXI, April 2011. ISSN: 0-617-00563-X.

[12] Ardiles López, Liana, Esther Jenaro Rabadán, Pedro Moreno Sánchez, Ignacio Escuder, Manuel G. de Membrillera, Óscar Pérez Arroyo, and Armando Serrano Lombillo: *Modelo de riesgo de las presas de Camporredondo y Compuerto (río Carrión)*. In *VIII Jornadas Españolas de Presas*, November 2008.

[13] Australian National Committee on Large Dams Incorporated: *Guidelines on Risk Assessment*, October 2003.

[14] Ayyub, Bilal M.: *Elicitation of expert opinions for uncertainty and risks*. CRC Press, 2001.

[15] Barbero Lartigau, C., X. Fernàndez Caballé, J.A. Díaz Porto, and A. Almagro Morales: *Análisis de riesgos aplicado a la gestión de seguridad de la presa de sant ponç*. In *Risk Analysis, Dam Safety, Dam Security and Critical Infrastructure Management*. Taylor & Francis Group, 2012. ISBN 978-0-415-62078-9.

[16] Barneich, J., D. Majors, Y. Moriwaki, R. Kulkarni, and R. Davidson: *Application of reliability analysis in the environmental impact report (EIR) and design of a major dam project*. In *Proceedings of Uncertainty 1996, Geotechnical Engineering Division, ASCE*, August 1996.

[17] Bockarjova, Marija, Albert E. Steenge, and Anne van der Veen: *On direct estimation of initial damage in the case of a major catastrophe: derivation of the "basic equation"*. Disaster Prevention and Management, 13(4):330–336, 2004.

[18] Bowles, D. S.: *Alarp evaluation: Using cost effectiveness and disproportionality to justify risk reduction.* In *ANCOLD Bulletin 127:89-106*, August 2004.

[19] Bowles, D. S.: *Tolerable risk for dams: How safe is safe enough?* In *Proceedings of the 2007 USSD Annual Lecture, Philadelphia, Pennsylvania.*, March 2007.

[20] Brunner, Gary W.: *HEC-RAS River Analysis System User's Manual*. US Army Corps of Engineers, Institute for Water Resources, Hydrologic Engineering Center (HEC), 4.1 edition, January 2010.

[21] Bureau of Reclamation: *Guidelines for defining inundated areas downstream from Bureau of Reclamation dams*. Reclamation Planning Instruction nº 82-11, 1982.

[22] Bureau of Reclamation: *Risk analysis methodology. appendix e. estimating risk of internal erosion and material transport failure modes for embankment dams.* Technical report, U. S. Department of the Interior, 2001. Draft.

[23] Bureau of Reclamation: *Risk Based Profiling System*. Technical Service Center, January 2001.

[24] Bureau of Reclamation: *Guidelines for achieving public protection in dam safety decision making*. Technical report, U. S. Department of the Interior, June 2003.

[25] Bureau of Reclamation: *A procedure for estimating loss of life caused by dam failure*. U.S. Department of Interior, October 2006.

[26] Bureau of Reclamation: *Construction Cost Trends*. Technical Service Center, http://www.usbr.gov/pmts/estimate/cost_trend.html, April 2010.

[27] Bureau of Reclamation: *Dam Safety Public Protection Guidelines (Interim)*. Denver, Colorado, August 2011.

[28] Bureau of Reclamation, U.S. Army Corps of Engineers, University of New South Wales, and URS: *Risk Analysis for Dam Safety*, chapter A Unified Method for Estimating Probabilities of Failure of Embankment Dams by Internal Erosion and Piping. 2009. Draft.

[29] Bureau of Reclamation in cooperation with U.S. Army Corps of Engineers: *Dam Safety Risk Analysis Best Practices Training Manual*. Denver, Colorado, version 2.2 edition, April 2011.

[30] Bussi, G., E. Ortiz, F. Francés, L. Pujol, R. Gabaldón, V. Guna, V. Bellver, and J.A. Sempere: *Modelación hidráulica y análisis del riesgo de inundación según las líneas guía de la Directiva Marco del Agua. El caso de la Marina Alta y la Marina Baja (Alicante)*. In *II Jornadas de Ingeniería del Agua "Modelos Numéricos en Dinámica Fluvial. Barcelona, Spain.*, 2011.

[31] Canadian Standards Association: *Risk Analysis Requirements and Guidelines*. Number CSA Q634-M91. National Standard of Canada, November 1991.

[32] Chauhan, Sanjay S., David S. Bowles, and Loren R. Anderson: *Do current breach parameter estimation techniques provide reasonable estimates for use in breach modeling?* Technical report, Utah State University, 2008.

[33] Comité Nacional Español de Grandes Presas: *Guía Técnica de Seguridad de Presas: Nº3. Estudios geológico-geotécnicos y de prospección de materiales*, 1999.

[34] Committee on dam safety: *Risk assessment in dam safety management. A reconnaissance of benefits, methods and current applications*. Bulletin 130, International Comission on Large Dams, January 2005.

[35] Conselleria D'Obres Públiques Urbanisme i Transports Generalitat Valenciana: *Plan de Acción Territorial de Carácter Sectorial sobre Prevención de Riesgo de Inundación en la Comunidad Valenciana (PATRICOVA)*, 2002.

[36] Costa, J. E.: *Floods from dam failures*. Technical report, U.S. Geological Survey Open-File Report, 1985.

[37] Dam Safety Committee, International Commission on Large Dams: *Bulletin on dam safety management*. Borrador, October 2010.

[38] De Cea, J.C., S. García, and I. Escuder-Bueno: *Análisis de riesgos de algunas presas de titularidad estatal mediante la técnica de screening*. In *IX Jornadas Españolas de Presas*, Valladolid, June 2010.

[39] DHI: *Mike by dhi*. http://mikebydhi.com.

[40] Dutta, Dushmanta, Srikantha Herath, and Katumi Musiakec: *A mathematical model for flood loss estimation*. 2003.

[41] Ekstrand, E. R.: *Estimating economic consequences from dam failure in the safety dams program*. U.S. Department of the Interior. Bureau of Reclamation, EC-2000-01, 2000.

[42] Elsner, Anne, Stephan Mai, Claus Zimmermann, and Volker Meyer: *Integration of flood risk in coastal hinterland management*. In *International COnference on CoastGis, Genua, Italy*, 2003.

[43] Ericson, Clifton A.: *Fault tree analysis – a history*. In *17th International System Safety Conference*, 1999.

[44] Escuder, I., M. G. de Membrillera, M. Meghella, and A. Serrano: *Damse: a european methodology for risk based security assessment of dams*. In *Twenty-third International Congress on Large Dams*, May 2009.

[45] Escuder, I., R. Landín, A. Gil, E. Rojo, and J.C. Elipe: *Análisis de riesgo aplicado a la gestión de la seguridad de una presa piloto*. In *IX Jornadas Españolas de Presas*, Valladolid, June 2010.

[46] Escuder, I., M. G. de Membrillera, P. Moreno, O. Pérez, L. Ardiles, and E. Jenaro: *Desarrollo de un programa complementario de seguridad basado en análisis de riesgos para las presas de la confederación hidrográfica del duero*. In *V Congreso de Ingeniería Civil, Territorio y Medio Ambiente*, Sevilla, November 2007.

[47] Escuder, I, M. G. de Membrillera, P. Moreno, O. Pérez, L. Ardiles, and E. Jenaro: *First risk-based screening on a spanish portfolio of 20 dams owned by the duero river authority*. In *Hydrovision*, Sacramento (USA), July 2008.

[48] Escuder-Bueno, I., J. T. Castillo-Rodríguez, S. Zechner, C. Jöbstl, S. Perales-Momparler, and G. Petaccia: *A quantitative flood risk analysis methodology for urban areas with integration of social research data*. Natural Hazards and Earth System Sciences, 2012. `doi:10.5194/nhess-12-2843-2012`.

[49] Escuder-Bueno, I., J.T. Castillo-Rodríguez, S. Perales-Momparler, and A Morales-Torres: *SUFRI Methodology for flood risk evaluation in urban areas. Decision guidance for decision maker*, September 2011. SUFRI project. WP3.

[50] Escuder-Bueno, I., A. Serrano-Lombillo, J. Fluixá-Sanmartín, and A. Morales-Torres: *Evaluación de la seguridad hidrológica de presas mediante modelos de riesgo simplificados*. In *3IWRDD-FORUM*, Valencia, October 2011.

[51] Escuder-Bueno, Ignacio and Liana Ardiles: *Role of dams as critical infrastructures to protect citizens from flooding and climate change*. In *ICOLD*, 2012.

[52] Escuder-Bueno, Ignacio, Enrique Matheu, Liana Ardiles, Massimo Meghella, and Jesica T Castillo-Rodríguez: *Building a common framework for integrating dam safety and security management in the context of risk analysis*. In *ASDSO*, 2012.

[53] Evans, Andrew W. and Verlander: *What is wrong with criterion fn-lines for judging the tolerability of risk?* Risk Analysis, 17(2):157–168, 1997.

[54] Federal Emergency Management Agency: *Prioritization of dams through risk categorization*. URS, 2006.

[55] Federal Emergency Management Agency: *HAZUS. FEMA's Methodology for Estimating Potential Losses from Disasters*. United States Department of Homeland Security, http://www.fema.gov/plan/prevent/hazus, May 2010.

[56] Federal Energy Regulatory Commission: *Engineering Guidelines for the Evaluation of Hydropower Projects*, chapter Dam Safety Performance Monitoring Program. July 2005.

[57] Fell, Robin, Chi Fai Wan, and Mark Foster: *Methods for estimating the probability of failure of embankment dams by internal erosion and piping - piping through the embankment*. The University of New South Wales, 5, ISBN 85841-395-7.

[58] Formal Software Construction Ltd.: *OpenFTA*. http://www.openfta.com.

[59] Froehlich, D. C.: *Embankment dam breach parameters revisited*. Proceedings of the 1995 ASCE Conference on Water Resources Engineering, San Antonio, Texas, 1995:887–891, 1995.

[60] G. de Membrillera Ortuño, Manuel: *Contribución a la aplicación del análisis y declaración de riesgos en presas españolas, incluyendo priorización de inversiones*. PhD thesis, Universidad Politécnica de Valencia, September 2007.

[61] García Kabbabe, Luis, Luis Chaparro Carrasquel, Ignacio Escuder Bueno, and Armando Serrano Lombillo: *Metodología para estructurar modos de fallo en sistemas presa-embalse*. In *IX Jornadas Españolas de Presas*, June 2010.

[62] García-Wolfrum, S. and J. Gutiérrez: *Análisis de riesgo como elemento adicional a las revisiones de seguridad*. In *Risk Analysis, Dam Safety, Dam Security and Critical Infrastructure Management*. Taylor & Francis Group, 2012. ISBN 978-0-415-62078-9.

[63] Gelder, P.H.A.J.M. van and J.K. Vrijling: *Reliabilty based design of flood defenses and river dikes*. Technical report, Department of Civil Engineering, Delft University of Technology, 2003.

[64] González Corral, M.: *Análisis de riesgos mediante la técnica de screening de presas y balsas de regadío en catilla y león*. Master's thesis, Máster en Explotación y Seguridad de Presas y Balsas, July 2011.

[65] Graham, Wayne J.: *A procedure for estimating loss of life caused by dam failure*. U.S. Department of Interior. Bureau of Reclamation, DSO-99-06, 1999.

[66] Graham, Wayne J.: *A comparison of methods for estimating loss of life from dam failure*. In *29th USSD Annual Meeting and Conference on Managing our Water Retention Systems*, pages 1145–1165, Abril 2009.

[67] Grossmann, G. and T. Seiser: *Survey about risk awareness, SUFRI project, Final Report (unpublished report)*, 2011.

[68] Hartford, Desmond N. D. and Gregory B. Baecher: *Risk and uncertainty in dam safety*. Thomas Telford Limited, 2004.

[69] Health and Safety Executive: *Reducing risks, protecting people - HSE's decision-making process*. Health and Safety Executive, 2001, ISBN 0-7176-2151-0.

[70] Heras, Rafael: *Hidrología y recursos hidráulicos*. Centro de Estudios Hidrográficos, Dirección General de Obras Hidráulicas, Madrid, 1976.

[71] Hill, P.I., D.S. Bowles, P. Jordan, and R.J. Nathan: *Estimating overall risk of dam failure: Practical considerations in combining failure probalities*. In *ANCOLD Bulletin 127*, pages 63–72, August 2004.

[72] Hydro, BC: *Bc Hydro Life Safety Model System V1.0, Guidelines, Procedures Calibration and Support Manual*, engineering report e310 edition, Agosto 2006.

[73] International Commission of Large Dams: *Dam-break flood analysis*, volume Bulletin 111. 1998.

[74] International Electrotechnical Commission: *Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)*. Number Reference number: IEC 60812:2006(E). International Standard, 2006.

[75] iPresas: *iPresas Calc User Guide*. http://www.ipresas.com, 2012.

[76] iPresas: *iPresas Manager User Guide*. http://www.ipresas.com, 2012.

[77] James, L. and R. Lee: *Economics of Water Resources Planning*. Water Ressources and Environmental Engineering. McGraw-Hill, 1971.

[78] Jonkman, Sebastiaan Nicolaas: *Loss of life estimation in flood risk assessment. Theory and applications*. PhD thesis, Civil Engineering Faculty, Technical University of Delft, 2007.

[79] Jonkman, S.N. and J.K. Vrijling: *Loss of life due to floods*. Flood Risk Maangement, 1:43–56, 2008.

[80] Kaplan, Stan: *The words of risk analysis*. Risk Analysis, 17(4):407–417, 1997.

[81] Kirkpatrick, G. W.: *Evaluation guidelines for spillways adequacy*. In *The evaluation of dam safety, Engineering Foundation Conference, Pacific Grove, California, ASCE*, 1977.

[82] Kirpichevsky, Yev, Enrique E. Matheu, and Yazmin Seda-Sanabria: *Modeling adaptive threats: incorporating a terrorist decision model into security risk assessments*. In *USSD Annual Meeting*, New Orleans, 2012.

[83] Klipsch, Joan D. and Marilyn B. Hurst: *HEC-ResSim Reservoir System Simulation User's Manual*. US Army Corps of Engineers, Institute for Water Resources, Hydrologic Engineering Center (HEC), 3.0 edition, April 2007.

[84] Lewin, Jack, Geoffrey Ballard, and David S. Bowles: *Spillway gate reliability in the context of overall dam failure risk*. In *USSD Annual Lecture, Charleston, South Carolina*, April 2003.

[85] Lichtenstein, S. and J. R. Newman: *Empirical scaling of common verbal phrases associated with numerical probabilities*. Psychonomic Science, pages 563–564, 1967.

[86] Long, Allen: *Recommended fault tree software and vendors*. http://www.fault-tree.net/software.html.

[87] Lumbroso, D.M., D. Sakamoto, W. Johnstone, A. Tagg, and B.L. Lance: *The development of a Life Safety Model to estimate the risk posed to people by dam failures and floods*. HR Wallingford, 2011.

[88] MacDonald, T.C. and J. Langridge-Monopolis: *Breaching characteristics of dam failures*. Journal of Hydraulic Engineering, ASCE, 110-5:567–586, 1984.

[89] Mc Bean, E. A., M. Fortin, J. Ding, and R. Moulton: *Adjustment factors for flood damage curves. water resources planning and management*. ASCE, 114(6):625–634, 1988.

[90] Mc Bean, Edward A., Micahel Fortin, John Ding, Ralph Moulton, Jack Gorrie, and ASCE: *Flood depth-damage curves by interview survey*. Journal of Water Resources Planning and Management, 114(6), November 1988.

[91] McClelland, D.M. and D.S. Bowles: *Estimating Life Loss for Dam Safety Risk Assesment - a Review and New Approach*. Institute for Water Resources, U.S. Army Corps of Engineers (USACE), Alexandria, VA, 2002.

[92] Melchers, Robert E.: *Structural reliability analysis and prediction*. Wiley, 1999.

[93] Messner, Frank and Volker Meyer: *Flood damage, vulnerability and risk perception - challenges for flood damage research*. Flood Risk Management: Hazards, Vulnerability and Mitigation Measures, pages 149–167, 2006.

[94] Millas, Jaime: *La riada, agravada por la rotura de la presa de tous, provoca grandes pérdidas en la agricultura, viviendas y redes viarias*. El País, October 1982.

[95] Ministerio de Fomento: *Norma de construcción sismorresistente: parte general y edificación (NCSE-02)*. REAL DECRETO 997/2002, September 2002.

[96] Ministerio de Medio Ambiente y Medio Rural y Marino: *Guía Técnica para la elaboración de los planes de emergencia de presas*. Secretaria de Estado

de Aguas y Costas. Dirección General de Obras Hidráulicas y Calidad de las Aguas. Subdirección General de Gestión del Dominio Público Hidráulico, Junio 2001.

[97] Ministerio de Medio Ambiente y Medio Rural y Marino: *Evaluación de la seguridad hidrológica de presas (suficiencia de aliviaderos) basada en riesgo. Expediente 106/RN08/02.1*, 2011.

[98] Ministerio de Obras Públicas, Transportes y Medio Ambiente: *Norma de construcción sismorresistente: parte general y edificación (NCSE-94)*. REAL DECRETO 2543/1994, December 1994.

[99] Ministry of Construction of Japan: *Outline of River Improvement Economic Research Investigation*. River Planning Section. River Department, 1996.

[100] Munger, Dale F., David S. Bowles, Douglas D. Boyer, Darryl W. Davis, David A. Margo, David A. Moser, Patrick J. Regan, and Nathan Snorteland: *Interim tolerable risk guidelines for US Army Corps of Engineers dams*. In *USSD Workshop on the future of dam safety decision making: combining standards and risk*, April 2009.

[101] Needham, Jason T., Yazmin Seda-Sanabria, and David S. Bowles: *Consequences estimation for critical infrastructures risk management*. 2009.

[102] NSW Dams Safety Committee: *Risk management policy framework for dam safety*. Technical report, New South Wales Government, August 2006.

[103] Nuclear Regulatory Commission: *Recommendations for probabilistic seismic hazard analysis: guidance on uncertainty and expert use*, 1997.

[104] Oliveri, E. and M. Santoro: *Estimation of urban structural flood damages: the case study of Palermo*. Urban Water, 2:223–234, 2000.

[105] Pérez-Arroyo, Ó., D. Sanz-Jiménez, and I. Escuder-Bueno: *Priorización de inversiones en el marco del desarrollo de un programa de seguridad complementario basado en riesgo para las presas de la confederación hidrográfica del duero*. In *VI Congreso Nacional de Ingeniería Civil*, February 2012.

[106] Quality Associates International: *Failure Mode and Effects Analysis*. http://www.quality-one.com/services/fmea.php.

[107] Reagan, Robert, Frederick Mosteller, and Cleo Youtz: *Quantitative meanings of verbal probability expressions*. Journal of applied psychology, 74(3):433, 1989.

[108] Reiter, Peter: *RESCDAM loss of life caused by dam failure, the RESCDAM LOL method and its application to Kyrkosjarvi dam in Seinajoki*. Water Consulting Ltd., 2001.

[109] Renyi, L. and L. Nan: *Flood area and damage estimation in Zhejiang, China*. Journal of Environmental Management, 66:1–8, 2002.

[110] Rowe, Gene and George Wright: *The delphi technique as a forecasting tool: issues and analysis*. International Journal of Forecasting, 15(4):353–375, 1999.

[111] Sanz, D., J.C. Bernabé, and I. Escuder: *Confección de un modelo de riesgo para la presa de castrovido*. In *IX Jornadas Españolas de Presas*, Valladolid, June 2010.

[112] Sanz-Jiménez, D, I. Escuder-Bueno, and F. Silva-Tulla: *Lecciones aprendidas a partir del análisis del riesgo cuantitativo de una presa en construcción*. In *Risk Analysis, Dam Safety, Dam Security and Critical Infrastructure Management*. Taylor & Francis Group, 2012. ISBN 978-0-415-62078-9.

[113] Sanz-Jiménez, D., I. Escuder-Bueno, and F. Silva-Tulla: *Quantitative risk analysis for a dam under construction in spain*. In *USSD Annual Meeting*, New Orleans, April 2012.

[114] Sanz-Jiménez, D, P.J. Moreno-Sánchez, J.C. Bernabé-de la Iglesia, N.E. Bueso-Suárez, Ó Pérez-Arroyo, and Serrano-L: *Programa de seguridad basado en el riesgo en la c.h. del duero*. In *Risk Analysis, Dam Safety, Dam Security and Critical Infrastructure Management*. Taylor & Francis Group, 2012. ISBN 978-0-415-62078-9.

[115] Scharffenberg, William A. and Matthew J. Fleming: *Hydrologic Modeling System HEC-HMS User's Manual*. US Army Corps of Engineers, Hydrologic Engineering Center (HEC), 3.5 edition, August 2010.

[116] Seda-Sanabria, Y., E. Matheu, and M.A. Fainberg: *Security risk assessment of dams and navigation locks*. In *Risk Analysis, Dam Safety, Dam Security and Critical Infrastructure Management*. Taylor & Francis Group, 2012. ISBN 978-0-415-62078-9.

[117] Serrano, Armando, Ignacio Escuder, Manuel G. de Membrillera, and Luis Altarejos: *iPresas: Software for risk analysis*. In *Twenty-third International Congress on Large Dams*, Brasilia, May 2009.

[118] Serrano Lombillo, A., I. Escuder Bueno, M. Gómez de Membrillera Ortuño, and L. Altarejos García: *Modelos de riesgo para la ayuda a la toma de decisiones en gestión de seguridad de presas*. In *IX Jornadas Españolas de Presas*, Valladolid, June 2010.

[119] Serrano-Lombillo, Armando: *Desarrollo de una herramienta completa de análisis y evaluación de riesgos en seguridad de presas*. PhD thesis, Universidad Politécnica de Valencia, March 2011.

[120] Serrano-Lombillo, Armando, Ignacio Escuder-Bueno, and Luis Altarejos-García: *Use of risk models for evaluation of risk reduction measures*. In *Twenty-fourth International Congress on Large Dams*, Kyoto, June 2012.

[121] Serrano-Lombillo, Armando, Ignacio Escuder-Bueno, Manuel G. de Membrillera-Ortuño, and Luis Altarejos-García: *Methodology for the calculation of annualized incremental risks in systems of dams*. Risk Analysis, 2010,

ISSN 1539-6924. http://dx.doi.org/10.1111/j.1539-6924.2010.01547.x.

[122] Silva, Francisco, T. William Lambe, and W. Allen Marr: *Probability and risk of slope failure*. December 2008.

[123] Singh, K. P. and A. Snorrason: *Sensitivity of outflow peaks and flood stages to the selection of dam breach parameters and simulation models*. Journal of hydrology, 68:295–310, 1984.

[124] Smith, D.I.: *Flood damage estimation - a review of urban stage-damage curves and loss functions*. Water SA, 20(3), Julio 1994.

[125] Soil Conservation Service: *Simplified dam-breach routing procedure*. Water Resources Publications, 1985.

[126] Solera, A., J. Paredes, and J. Andreu: *AQUATOLDMA SSD para Planificación de Cuencas*. Valencia, 2007.

[127] Stamatelatos, Michael, William Vesely, Joanne Dugan, Joseph Fragola, Joseph Minarick, and Jan Railsback: *Fault tree handbook with aerospace applications*. NASA Office of Safety and Mission Assurance, August 2002.

[128] Stewart, M.G. and R.E. Melchers: *Probabilistic Risk Assessment for Engineering Systems*. Chapman & Hall, 1997.

[129] Su, M.D., J. L. Kang, L. F. Chang, and A. S. Chen: *A grid-based GIS approach to regional flood damage assessment*. Journal of Marine Science and Technology, 13 (3):184–192, 2005.

[130] Surowiecki, James: *The wisdom of the crowds*. Doubleday, 2004, ISBN 978-0385503860.

[131] Swain, R. E., D. Bowles, and D. Ostenaa: *A framework for characterization of extreme floods for dam safety risk assessments*. Proceedings of the 1998 USCOLD Annual Lecture, Buffalo, New York, 1998.

[132] Triana Moreno, Jorge Eduardo: *Contribución a la estimación de consecuencias de fallo y rotura de presas en el contexto del análisis de riesgos*. PhD thesis, Universidad Politécnica de Valencia, Noviembre 2006.

[133] United States Department of Homeland Security: *Dams Sector. Estimating economic consequences for dam failure scenarios*, draft edition, April 2010.

[134] United States Department of Homeland Security: *Dams Sector. Estimating Loss of Life for Dam Failure Scenarios*, draft edition, April 2010.

[135] USBR: *Dam Safety Risk Analysis. Best Practices Training Manual*. United States Bureau of Reclamation in cooperation with U.S. Army Corps of Engineers, 2011.

[136] Vesely, W. E., F. F. Goldberg, N. H. Roberts, and D. F. Haasl: *Fault tree handbook*. Systems and Reliability Research Office of Nuclear Regulatory Commission, January 1981.

[137] Viljoen, M. F., L. A. du Plessis, and H. J. Booysen: *Extending flood damage assessment methodology to include sociological and environmental dimensions*. Water SA, 27(4):517–522, October 2001.

[138] Villemeur, Alain: *Reliability, Availability, Maintainability and Safety Assessment*. John Wiley & Sons Inc, December 1991. ISBN: 978-0-471-93048-8.

[139] Vrijling, J.K. and P.H.A.J.M. van Gelder: *A framework for risk evaluation*. Journal of Hazardous Materials, 43:245–261, 1995.

[140] Wahl, Tony L.: *Prediction of embankment dam breach parameters - A literature review and needs assessment*. Technical report, Dam Safety Office - U.S. Bureau of Reclamation, 1998.

[141] Wahl, Tony L.: *Uncertainty of predictions of embankment dam breach parameters*. Journal of Hydraulic Engineering, ASCE, May 2004:389–397, 2004.

[142] Walder, J.S. and J. E. O'Connor: *Methods for predicting peak discharge of floods caused by failure of natural and constructed earth dams*. Technical report, Water Resources Research, 1997.

[143] Yevjevich, Vujica: *Probability and statistics in hydrology*. Water Resources Publication, 1997.

[144] Zechner, S., C. Jöbstl, and H. Knoblauch: *SUFRI Methodology for investigation of risk awareness of the population concerned, SUFRI project, WP4, Final Report*, 2011.