FMECA of the Ajaure Dam - A Methodology Stydy

M. BARTSCH, SwedPower AB, Stockholm, Sweden

SYNOPSIS. In 1998 Vattenfall decided to introduce the use of risk analysis in dam safety in Sweden, by issuing two pilot studies on the Seitevare and Ajaure embankment dams. The objective of these studies was to demonstrate methods to be applied for risk analysis on dams. SwedPower performed the Ajaure study in collaboration with BC Hydro International. Incorporated into this assignment were also a number of technical investigations in order to improve the knowledge base of the dam.

In 2000-2001 a second study was performed focusing on development of the application of FMEA/FMECA and other available methods and on staff training, while still relying on the information gathered during the 1998-1999 study. This “Methodology” study is summarised in this document.

The initial step of the FMECA of the Ajaure Facility was to set up a system model and break it down into subsystems and components by the use of block diagrams. The component failure modes their root causes and effects were analysed and documented using fault trees and pathway diagrams. The FMEA was extended to an FMECA for a few components to demonstrate the proposed technique for criticality analysis. The analysis was summarised in FMECA tables complemented by more extensive component data sheets.

The study concludes that the FMECA framework provides a suitable framework for working with dam safety issues at dams. Other methods, such as, functional modelling, pathway diagrams, event and fault tree analysis should be integrated as considered necessary with regard to the characteristics of the sub-system at hand. In fact, coupling of various methods can be looked upon as a promising direction for further development in the area.

It is envisaged that studies of this type will be performed for a limited number of dams in the Vattenfall portfolio.

Long-term benefits and performance of dams. Thomas Telford, London, 2004

LONG-TERM BENEFITS AND PERFORMANCE OF DAMS

BACKGROUND

General

Ajaure is a high consequence dam according to the Swedish dam safety guidelines. The 50 m high rock-fill dam is situated in the upper part of Ume River and was constructed 1964 to 1967. The dam has exhibited a number of unanticipated performance characteristics since construction, which include progressive horizontal downstream deformation, and overtopping of the spillway walls. Also, with regard to a revision of the Inflow Design Flood it has been concluded that Ajaure at present has insufficient spillway or surcharge capacity. Therefore the decision has been taken to raise the dam, which also would be beneficial for dams downstream. (The design of the raising of the dam has been performed in parallel to the risk analysis and is presented in the adjacent paper by A Nilsson and I Ekstrom, SwedPower.)

The dam owner Vattenfall (the former State Power Board) decided to consider the issues within a risk management framework and sought the assistance of BC Hydro International (BCHIL). BCHIL assisted Vattenfall and SwedPower (consulting engineers within the Vattenfall Group) by providing guidance on the application of a version of its evolving failure modes and effects analysis (FMEA) process to the Ajaure Dam risk management issue.

A preliminary FMECA was performed in1998-1999. The study included some technical investigations in order to improve the knowledge base of the dam. The present study performed in 2000-2001 relies on the information gathered during the first study. Focus has instead been on methodology and staff training issues. BCHIL was again sub-contracted by SwedPower to provide assistance to accomplish this Methodology Study.

The Ajaure assignment was one part of a two-part initiative by Vattenfall to introduce the use of risk analysis in the dam safety discipline in Sweden.

Problem Characterisation and Method of Problem Analysis

The task has been to characterise and evaluate the risk posed by Ajaure Dam with the view to develop a safety management system, which demonstrates that the risks are being effectively controlled. The risk characterisation process should permit the identification of the relative contribution of different hazards and deficiencies to the overall risk. The process should also permit the assessment of the changes in risk profile associated with modifications to the dam and/or risk reduction alternatives.
Essentially this project involves:

- a methodical approach to hazard and risk identification and their characterisation;

- modelling the ways in which hazards may be realised with resulting harm;
- identification of how the hazard sequence might be arrested or the effects mitigated.

In principle, the risk can be characterised in a relative sense in terms of a criticality index comprised of three indices that reflect the potential for a failure mode to initiate, the sequence progressing to failure; and the consequences of failure. Also, and again in principle, uncertainty can be characterised by assigning ranges to the indices instead of individual values as appropriate.

Objectives

An important objective in Vattenfall authorising a second risk based analysis for Ajaure Facility is further training of its engineering staff (SwedPower) in emerging methodologies. Another focus of the FMECA analysis of Ajaure Dam is characterisation and evaluation of the risks that have been identified in the Ajaure SEED by monitoring and surveillance and through operating experience.

FMEA, general

Failure Modes and Effects Analysis (FMEA) is a method of analysis whereby the effects or consequences of individual component failure modes are systematically identified and analysed. While the actual analysis is inductive, i.e. is based on the question "*What happens if a component or element fails?*", it is first necessary to 'break the dam system down' into its individual components or elements. Once the system has been de-aggregated the failure modes of each of the fundamental elements can be identified.

Once the failure modes and/or root causes have been identified, the effects of the failure mode on other components of the subsystem and on the system as a whole are systematically identified. The analysis is usually descriptive and information is normally presented in tabular and/or spreadsheet form. FMEA clearly relates component failure modes and their causative factors to the effects on the system and presents them in an easily readable format. A thorough understanding of the system under analysis is essential prior to undertaking an FMEA.

APPLICATION OF FMEA AND FMECA ON AJAURE FACILITY

General

The application on the Ajaure facility comprised the parts where the principles of FMEA were the primary focus of the study.

- The FMEA, in which the facility was broken down and analysed in a structured manner
- The FMECA, in which criticality ratings were assessed for a few components, and
- Derivation of global failure modes related to the Water Retaining Structures, the Discharge Facilities and the Spillway Gate Control.

FMEA process

General
In this application the FMEA process can be said to consist of three basic parts:

- System and subsystem breakdown
- Component details
- Failure modes and effects

The FMEA process was extended to FMECA by adding a fourth part:

- Criticality ratings and criticality index

The analysis has been documented on FMECA worksheets, where each of the four basic parts listed above is found as column headings. Under the heading "System and subsystem details" the functional subsystems were broken down into their physical parts, i.e. from subsystems stepwise down to components.

Under the heading "Component details" the design function(s), the design and performance parameters and the performance details have been listed. For each component the design parameters that characterise its performance have been identified. Input has been collected from designers and design data. The next step has been to collect information on the performance details with the intent to map out the design and construction adequacy. Important input has been gathered from the SEED report, performance records and complementary investigations.

In the third section with the heading "Failure modes and effects" the first step was to list the functional failure modes for each component. Here the failure mode of a design function is identical to the loss of the design function. Fault trees have been used to document the relation between root causes and the failure mode.

For each primary failure mode the potential failure sequences, i.e. the pathways to dam breach, have been explored. Also the possibilities to stop the failure sequence from progressing all the way to dam breach, the ultimate effect, have been documented.

As described above the FMEA findings are documented in FMEA tables in a worksheet format. More exhaustive information on each component is compiled in a "component data sheet". On the component data sheet each of the headings are identical to those of the FMEA table are listed. To illustrate the failure sequences graphical pathways showing the chain of events from component failure mode to dam failure are included. Fault trees have been used to illustrate the interrelationships of root causes to component failure modes.

FMEA application to the Ajaure dam

In a system context the Ajaure facility belongs to the "Super System" of Ume River. Upstream of Ajaure the systems of Överuman Regulation Dam and Klippen Power station are situated. Downstream Ajaure there are 14 hydropower facilities, of which the Gardiken Facility is situated immediately downstream. This is illustrated in Figure 1 below.

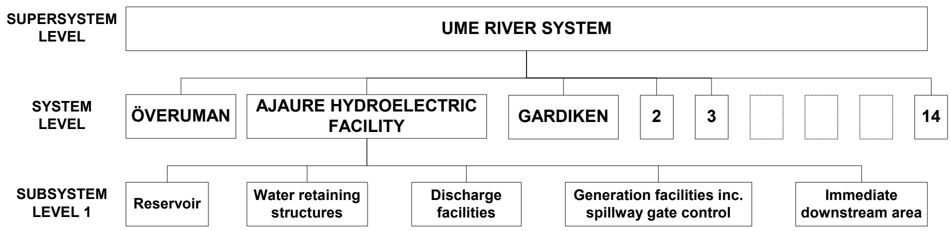


Figure 1. Logical Model of Supersystem, System and Subsystem Level 1

The function of the Ajaure facility (global system) was defined as to "retain water in the reservoir with control of the outflows". It's ability to generate power has been omitted from the study. The motivation is that the focus has been purely on dam safety. As an effect of this the study of the Subsystem Generation facilities has been limited to the Spillway Gate Control.

The "global system" failure mode to be analysed has been defined as "dam breach and release of reservoir water". Component failure modes that cannot initiate a sequence of events that may lead to dam breach have not been covered in this analysis.

In the FMEA the Ajaure facility was broken down into five principal sub-systems; Water Retaining Structures, Discharge Facilities, Spillway Gate Control, Reservoir and Immediate Downstream Area. The focus of the analysis was on the first three subsystems. Since they have great differences regarding their structure (continuous versus discrete components, man made versus geological formations, etc) and functioning (continuous loading

versus work on demand, etc) slight differences in the methodology have been used for the three subsystems.
Spatial and functional models were developed to facilitate the analysis, see example in Figures 2 and 3.

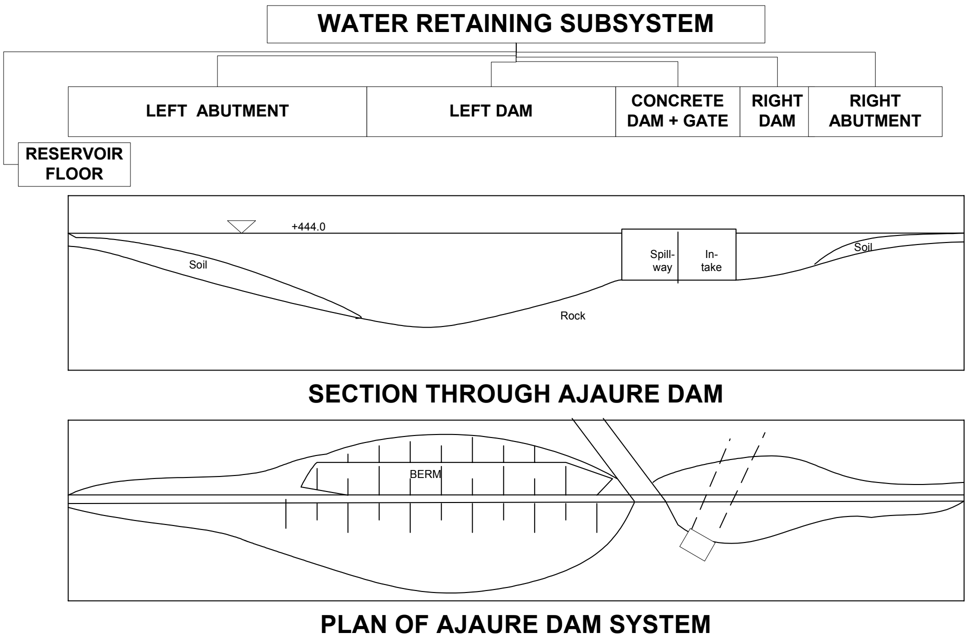
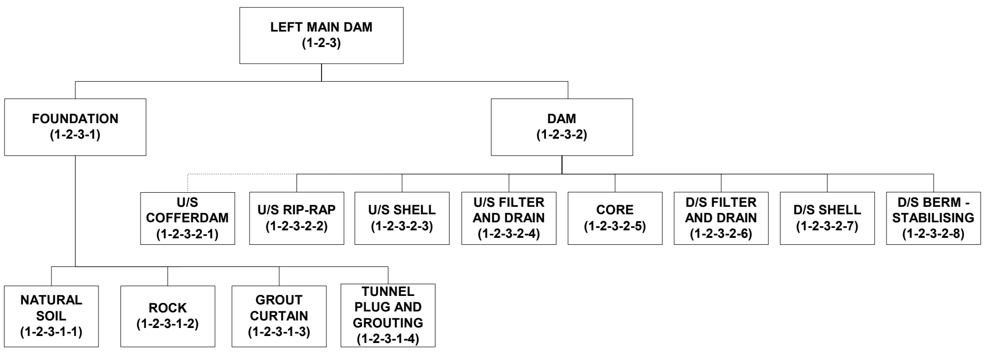


Figure 2. Plan and section of the Ajaure Dam



Block diagram of the component level of the Left Main Dam

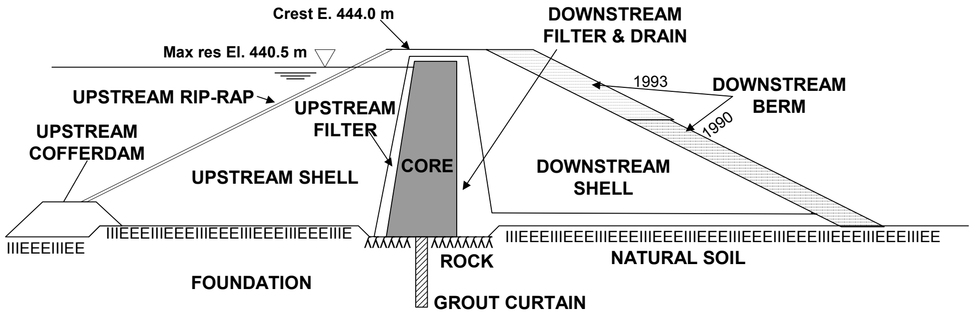


Figure 3. Spatial Model of Left Main Dam

The subsystems were broken down to the component level. Detailed component data sheets including pathway diagrams for identified failure sequences were elaborated for a number of components. Such a sheet for the downstream shell is summarised in Figure 4.

Primary Function (1)
P1: Provide structural support for core and D/S filter.
Design/performance parameters
Compressive strength, shear strength, Los Angeles-value, rock type, specific weight – not specified in design but investigated due to malperformance
Material and construction specifications, see Chapter 4. The rock fill consists of schists and gneiss with a high content of mica.
Performance details
During the second half of the 1980's, it was established that section 0/640 of the left embankment dam was moving abnormally in horizontal downstream direction….etc.
Functional Failure Mode
Failure to provide structural support for core (loss of structural integrity of D/S shell)
Immediate Effects
Deformation of core
Failure Sequence - Pathway Diagram

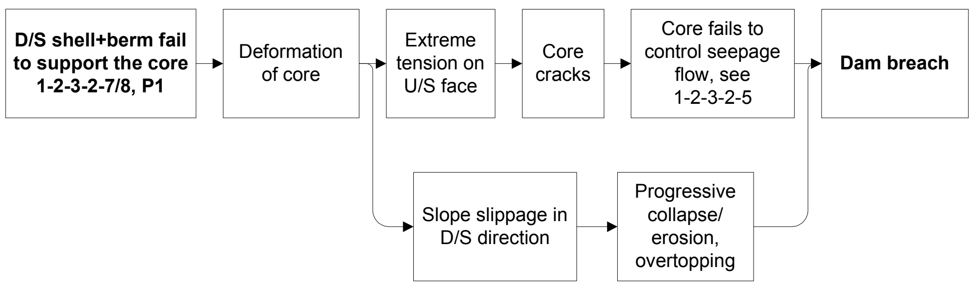


Figure 4. Summary of the Component Data Sheet for the D/S Shell

The design function of the subsystem "Water retaining structures" has been defined as to "retain water in the Ajaure reservoir with a controlled (small) seepage flow and with controlled discharges as required". Every element that has significance in making the system act as a continuous water barrier has been considered to be part of the water retaining structures. However the study was limited to one of the subsystems, the “Left Main Dam”. Further, gaps in the present knowledge of the mechanics of the functioning of embankment dams and in the available information on site specific data such as material properties and performance characteristics render this case study is primarily a demonstration of how the principles of the FMEA methodology can be applied.

The design function of the subsystem "Discharge facilities" has been defined as to "convey water in a safe way from the upstream reservoir, through the dam, and to the river downstream of the dam". All elements of significance in making the system perform the spillway function are included in the sub-system.

The design function of subsystem “Spillway Gate Control” has been defined as to “be able to activate spillway gates in a controlled manner given a requirement to pass flows”. Every element that has significance in making the system activation of the spillway gates possible has been considered to be part of the spillway gate control. The system components can be grouped in three overall aspects of the spillway gate control, for which functional models were developed

- Information flow and means of activation
- Power supply for spillway gate motors
- Power supply for measuring equipment, remote control, and station control equipment

The availability in many systems is influenced by human intervention (such as design, operation, test, maintenance etc.). There is therefore a logical connection between human reliability and technical reliability. Both human and technical availability is also determined from factors that lie outside the direct work situation. The organisation design is such an overall context and has therefore both direct and indirect influence on the basis for human and technical availability.

FMECA process

The FMEA process has been extended to FMECA by addition to the FMEA tabulation of:

- Criticality ratings and criticality index

The criticality analysis allows us to rank the importance of the failure modes by assigning criticality indices for the probability of occurrence of failure and the severity of the failure consequences. Here a qualitative approach, that does not require detailed frequency data, has been chosen. A relative index scale with five steps 1-5 has been put up. Here a set of three criticality indices has been assigned for each failure mode. They represent:

- Failure mode initiation - the potential for the failure mode to occur
- Failure sequence progression - the potential for the failure sequence to progress to ultimate failure
- Failure consequences - the severity of the consequences caused by ultimate failure.

Based on the three "criticality indices" a risk index has been calculated by multiplying them together. This risk index can be used to rank the potential failure modes according to the combined influence of their index of vulnerability and the severity of their failure consequences.

However, in order to cover differences in component function "demand" a fourth column has been added to provide context to the "criticality indices, e.g.:

- Event likelihood - frequency (1/year) of event that requires the component to function.

The process of assigning criticality indices involves weighing of evidence that supports a postulated failure mode (hypothesis) against evidence that contradicts the postulated hypothesis. Where the available information/evidence is incomplete a range has been assigned to the index. A wide range indicates that there are large uncertainties in the analysis due to lack of information/evidence. Here it is important to point out that a high number does not necessarily mean than that there is a weakness in the dam. It may also mean that there is a great lack of knowledge about the phenomenon in question, suggesting actions such as further investigations and/or a continued analysis. The "weight of evidence" explaining and motivating the assigned criticality indices has been documented.

Global Failure Modes

In the FMEA the system has been broken down into manageable bits and analysed. As an extension of the FMEA, an attempt is made to put the bits back together again, and return to the overall function of the Ajaure facility. This is done by working backwards in the pathways to failure, from dam breach towards the component failure modes. The end-branches (just before dam breach) of the pathways to failure interfaces with a global failure mode. Grouping together of the pathways' end-branches results in a few principal types of global failure modes, with connection to the three primary subsystems:

- Failure by slope instability, crest collapse and leakage/internal erosion, originating from deficiencies in the left main dam in the water retaining structures

- Erosional failure of D/S slope, originating from unsafe passage of discharge flow past the dam, initiated by deficiencies in the Discharge facilities or the Spillway gate control
- Overtopping, originating from failure to control the reservoir water level by discharge, due to deficiencies in the Discharge facilities or the Spillway gate control

For the identified global failure modes the global pathways, or when more appropriate the global fault trees, have been derived from the pathways used to model the effects of the component failure modes.

CONCLUSIONS AND LESSONS LEARNED

The training component of the SwedPower staff is deemed to have been successful, regarding methodologies with regard to risk analysis of dams, as well as training in sound engineering practices in general.

The applied FMEA methodology is regarded to provide a suitable framework for working with safety issues at dams. However, FMEA do not provide a stand-alone method or procedure but other methods such as pathway diagrams and fault tree analysis should be integrated in the application. Further development of the coupling of various methods and the criticality analysis would be beneficial to make the application more straightforward.

The elaboration of global failure modes provides a means of joining the results from the more disciplinary analysis of the various sub-systems. The global failure mode diagrams serve as logical maps displaying the relationship between various component functions and their role along the failure pathways.

The criticality ratings provide insights into what the engineers consider to be the principal issues concerning seriousness of issues and extent of uncertainty. The outputs from the criticality analysis process serve well as a basis for reasoning concerning the management of the risks.

Another conclusion is that complementary technical investigations providing site-specific data are often required to make the FMEA meaningful.