HAZARDS AND FAILURE MODES MATRIX (REVISION 8, 11-03-05)

DEFINITIONS

Dam Safety Activities:

Oversight: All activities necessary for dam safety that do not require any investment in the dam or the infrastructure required for dam safety.

Activities

- Independent reviews
  - Carried out in terms of a fixed periodic schedule (3 years, 5 years, 10 years etc.)
- Surveillance
  - Continual monitoring of the performance of the dam and interpretation of the data to confirm the ongoing safety of the dam.
- Operations and maintenance oversight
  - Review and oversight of all operation and maintenance activities necessary for dam safety.
  - Supervision of testing of gates and safety critical systems.
- Emergency planning
  - Design, implementation, testing and maintenance of emergency plans
- Safety assessment
  - Development of risk management plans and justification for schedule and expenditures.
- Program management.
- Regulatory reporting.

Hazards:

Hazards can be considered to be external to the dam and reservoir system or internal to the system.

External hazards: Hazards or threats to the proper functioning of the dam that are beyond the control of the dam owner that originate outside the boundary of the dam and reservoir system.

External hazard type

- Meteorological events.
  - Floods, intense rain events (causing local erosion, landslides etc.), temperature extremes and the effects of ice, lightening strikes and wind storms.
- Seismic events.
  - Natural and those caused by economic activity such as mining or even reservoir induced seismicity. The fact that areas without active seismicity can be disturbed by distant earthquakes should not be ignored.
- Reservoir environment.
  - Includes all reservoir rim features including upstream dams, slopes around the reservoir, overhead off spillways etc. that pose a threat.
  - Reservoir environment also includes any deleterious substances, or burrowing or other animals that can effect the physical performance of the dam.
- Terrorist attacks and vandalism.
  - Including vandalism and sabotage by various groups ranging from local disaffected individuals, through domestic terrorism and international terrorism .

Internal hazard type

- Errors and omissions in the design of the dam and water conveyance structures including inadequate consideration of the performance of the reservoir rim and upstream dams.

- Construction errors or design compromises to accommodate natural or imposed deviations from the design assumptions.
- Maintenance procedure errors where maintenance requirements are not fully defined at the design stage.
- Errors and omissions in the development and maintenance of operating rules or means of verifying adequate operation (e.g. infrastructure problems with water level recorders).

The internal hazard types are further subdivided into "sources":

Internal hazard type sources

- *Water barrier:* All elements retaining or interfacing with the body of water including the main dam, any concrete spillway structure with water retaining function, saddle dams etc.
  - Spillway gates that function as water retaining subsystems form part of the water barrier.
- *Hydraulic structures*: All water conveyance structures required to direct water around or through the dam in a controlled way.
  - Typically, spillway structure, low level outlet structure and power water passages (canals and penstocks etc.)
- *Mechanical and Electrical sub-systems:* All mechanical and electrical equipment and machinery required to control the reservoir level.
  - This will include all mechanical and electrical subsystems and controls at the dam site and, in the case of remotely controlled dams, the remote control centre. The definition of the system boundary will include the boundary around the control systems.
- *Infrastructure and Plans:* The term "infrastructure" is used to describe all physical infrastructure and equipment necessary for the collection of data and information required to verify the performance adequacy of the dam. The term "plans" is used to describe all of the "non-physical" dam safety activities necessary to support dam safety, including the design, construction maintenance and implementation of all operating and safety procedures that form part of the engineering design of the dam and safety system.
  - The "infrastructure" will include all instruments and its physical supports. It will also include access roads, adits, portals etc required for siting and reading the instruments.
  - The "plans" will include all of the engineering design of all operating orders, maintenance strategies and plans, surveillance procedures and the emergency plans, all of which form part of the engineering design.
  - Plans also includes all forecasts such as inflow forecasting.
  - In general, if some form of additional infrastructure or a plan (especially if human activity is involved) is required to ensure adequate performance of the water barrier, the hydraulic structures or the mechanical/electrical system with respect to any failure mode or functional failure characteristic, then infrastructure/plans will form a hazard/failure mode pair.

Failure Modes:

A *failure mode* describes how element or component failures must occur to cause loss of the sub-system or system function. In this regard, failure modes are not unique features of the system but artefacts of how the system is modelled. Failure effects at a lower level in the system become the failure modes at the next highest level in the system. In general, the system is broken down into sub-systems to a level where there is a thorough understanding of the failure modes of the elementary sub-systems (Figure 1).

General failure mode categories have been prepared for dams and while these categories are often too general for definitive risk analysis for a dam, they are useful for comparative analysis because they are at a sufficiently generalised level to permit broad comparisons between dams and dam portfolios. At a very general level, there are two dam failure modes, dam overtopping and dam collapse.

Overtopping failure mode

- Inadequate freeboard leading to the flow of water over the crest of the dam in a manner not intended or provided for in the design, construction, maintenance and operation of the dam.

Collapse failure mode

- Inadequate internal resistance to the hydraulic forces applied to the dam, foundations and abutments while being hydraulically operated in accordance with the design intent.

Because failure modes have a physical cause, it is possible to develop general descriptions of the underlying features of the failure mode in terms of functional failure characteristics.

Dam overtopping functional failure characteristics

- *Discharge capacity exceeded:* The capacity of the dam to operate within its hydraulic design envelope is less than the design intent or current performance expectations.
- *Discharge capacity not available:* Refers to the reliability of the systems that must operate for a dam with adequate hydraulic capacity to safely pass inflows without exceeding the design envelope. The fundamental parameter is the "probability of failure on demand, given that the system is being adequately maintained and tested as required.
- *Inadequate operation:* Requires that that the operating rules have been implemented and are being followed (inadequacies in the design of the operating rules are hazards).
- *Reservoir maintenance failure:* Refers to the carrying out of all actions at the facility necessary to support dam safety. This includes performance of maintenance (debris clearing, rip-rap repair, maintenance and testing of mechanical and electrical subsystems) required to support dam safety.
- *Wave overtopping:* Reservoirs with rim stability or other concerns such as discharges from upstream dams that can be triggered by natural hazards or in the case of upstream dams, unplanned large releases. As mentioned above, reservoir rim includes upstream dams, reservoir landslides, and wind generated wave overtopping.
- *Dam Safety Management System function failure related to overtopping failure:* In BC Hydro's case, this is the function of the Office of the Director of Dam Safety and refers to the oversight, verification and corrective action procedures for hydraulic adequacy aspects of dam safety. It includes:
  - definition of dam safety requirements for hydraulic operations (operation and maintenance manuals);
  - identification and characterisation of deficiencies in hydraulic operation through routine monitoring, inspections and all surveillance activities, dam safety reviews and deficiency investigations; and;
  - the planning of risk control implementation and scheduling of dam safety improvements for hydraulic operations.

Dam collapse functional failure characteristics

- *Dam Safety Management System function failure related to dam collapse failure:* In BC Hydro's case, this is the function of the Office of the Director of Dam Safety and refers to the oversight, verification and corrective action procedures for structural adequacy aspects of dam safety. It includes:
  - definition of dam safety requirements for structural performance (performance maintenance manuals);
  - identification and characterisation of deficiencies in structural performance through routine monitoring, inspections and all surveillance activities, dam safety reviews and deficiency investigations; and;
  - planning of risk control implementation and scheduling of dam safety improvements for structural performance.
- *Liquefaction:* Seismically induced or static liquefaction of loose materials in the dam body, abutments or foundations.

- *Internal erosion:* Transport of soil particles from their natural or as-placed location in the body of the dam, abutments or foundation.
- *Deformations:* All elastic and permanent displacements that are outside the design response envelope including crest settlements due to consolidation, mass movement downstream etc. that cannot be attributed to strength deterioration due to factors such as internal erosion of crushing of material.
- *Structural weakening:* Physical deterioration of the strength of the materials in the dam body, abutments and foundations. This will include phenomena such as alkali-aggregate reaction and mechanical, chemical, temperature (freeze thaw) or radiation (UV) related deterioration.
- *Water stops and interfaces:* This relates to all elements that provide the water-retaining barrier with water tightness at joints and interfaces.
- *Pumps and drains:* All drainage systems and subsystems required to preserve stability (gravity drains, pumps etc.).

Dam collapse functional failure characteristics require careful consideration in the context of a failure modes model such as that illustrated in Figure 1, because one functional failure characteristic may or may not cause another functional failure characteristic to initiate. Note, internal erosion can also be an effect of a functional failure such as that which might occur if a water stop around a conduit fails, or a conduit bursts or an upstream water barrier (e.g. concrete face) fails permitting ingress of water into otherwise unprotected (against internal erosion) fills. Failure to maintain the reservoir through debris clearance could lead to loss of discharge capacity is another example

In general, the hazard should be coupled with the basic functional weakness of the functional failure characteristic. The idea is to identify, initiate through examination or analysis of the dam system, the vital basic condition that has to exist between the hazard and failure mode that could cause a failure sequence to progress to one of the global failure modes.

HAZARDS AND FAILURE MODES MATRIX

The interactions between hazards and failure modes can be related through a matrix representation. (Figure 2). The hazards and failure modes matrix (H&FMM) provides a simple means of summarising the considerations that, in principle must be embodied in every dam safety program. In general, hazards may be related to failure modes in different ways, including combinations of hazard contributing to an individual failure mode and individual hazards contributing to all several failure modes. It is only through understanding of the number and nature of the hazards and failure modes that must be addressed by dam safety activities that meaningful comparative analysis can be carried out. The H&FMM is a simplified representation of this understanding, but it is not the means to generate the understanding.

The most convenient way to use the matrix to identify the hazards and failure modes that must be managed at a dam is to fill out the matrix by assuming that all 104 combinations of hazards and failure modes apply, and then eliminating those that don't apply. The reasoning for the elimination of the hazard-failure mode pairs should be documented. A simple dam such as a concrete dam wedged in a narrowing canyon, and designed to operate as a weir for flood passage purposes would be expected to have a small number of hazard-failure mode pairs. On the other hand, an earthfill dam on a poor foundation with a gated spillway on a rapidly responding reservoir in a seismic area also prone to unpredictable large floods would be expected to have a large number of hazard and failure mode pairs.

Careful thought is required when de-populating the matrix as it is necessary to consider external hazards and internal hazards separately and together. As a result, a functional failure characteristic may be vulnerable to external hazards and to internal hazards and to combinations of external hazards and internal hazards that interact. Similarly, external hazards can combine such as a reservoir landslide that can occur naturally, or as triggered by a meteorological or seismic event.

The H&FMM will be used slightly differently for surveillance activities than for design reviews, dam safety reviews or deficiency investigations, in that surveillance activities comprise “proactive activities” around internal hazards and “reactive activities” for external hazards. In general, surveillance activities for the purposes of intervention will not focus on external hazards that alone exceed the design basis as in the absence of an intervention plan, any surveillance activity is for information not for active risk management. On the other hand the point at which the design basis is exceeded is fundamental to design reviews, dam safety reviews or deficiency investigations. However, while the uses may be different, the surveillance engineer should know when the design basis is exceeded even if no intervention action is to be taken.

Some examples of the thought process follow:

Considering external hazards alone initially:

1. In general, the discharge capacity can be exceeded by sufficiently large inflow events, thus exceedance of discharge capacity will be a potential failure mode albeit possibly of very low probability. The exceedance probability or the design basis exceedance event can be entered into the H-FM cell that associates meteorological hazards and the dam overtopping failure mode associated with discharge capacity exceedance.
2. A seismic event alone will not exceed the discharge capacity and the “X” is eliminated by definition.
3. Reservoir environment alone could possibly exceed the discharge capacity if there is an upstream dam with a free overflow spillway with greater capacity than the downstream dam. This is an extreme example only used for illustrative purposes.
4. Meteorological events alone can cause discharge capacity not to be available if for example the weather event exceeds the design basis of the spillway gate sub-system (i.e. an unprecedented wind event that interrupts power to or communication with the gate actuator could cause loss of gate operation).

Considering “internal hazards” alone, the following examples are illlustrative.

5. The water barrier alone cannot cause exceedance of the discharge capacity and the “X” is eliminated by definition.
6. However, a concrete water barrier with alkali-aggregate reaction could swell to the extent that the spillway gates become jammed thereby leading to the unavailability of the discharge capacity under normal inflow conditions
7. Similarly, the mechanical/electrical sub-system cannot cause exceedance of the discharge capacity and the “X” is eliminated by definition. However, problems internal to the mechanical/electrical sub-system can lead to the unavailability of the discharge capacity under normal inflow conditions

Considering “internal hazards” and “external hazards” together as follows:

8. A concrete water barrier with alkali-aggregate reaction could swell to the extent that the spillway gates become jammed thereby leading to the unavailability of the discharge capacity when required to deal with extreme inflow conditions. In such cases there would be an “X” in the Meteorological and Water barrier cells of the “discharge capacity not available” line of the matrix.
9. Similar arguments can be made about, problems internal to the mechanical/electrical sub-system can lead to the unavailability of the discharge capacity under normal inflow conditions.

Some other candidates for elimination by definition are:

10. Reservoir environment cannot cause liquefaction and the “X” is eliminated by definition as will most and usually all other hazards long the liquefaction row of the matrix.
11. On the other hand reservoir environment could cause structural weakening if combined with an internal hazard in the water barrier, if for example the structural anchors are not adequately protected against corrosion.

Elimination hazard and failure mode pairs should be done by experienced dam safety engineers who understand the features of the dam, the hazards that the dam is exposed to, the failure modes that have not been eliminated, and how the dam is intended to function. The hazard and failure mode elimination process might be carried out by the independent engineer conducting the periodic Dam Safety Reviews.

Once completed, the finalised hazards and failure modes matrix provides a template for all aspects of the safety management activities and provides an aid for the justification of dam safety expenditures.

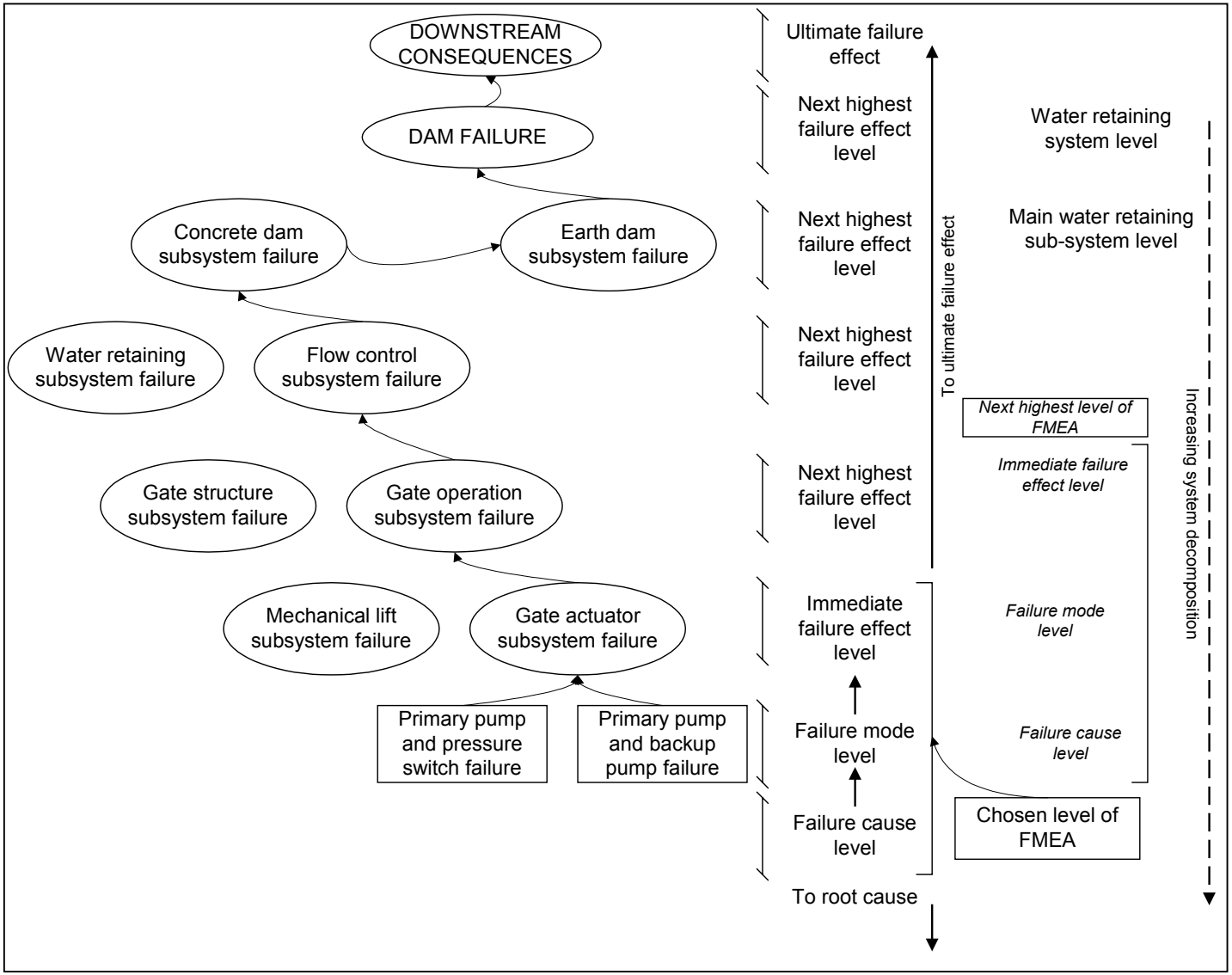

Figure 1. Hierarchical structure of Failure Modes

GLOBAL FAILURE MODES		ELEMENT AND/OR ELEMENT FUNCTION	MOST BASIC FUNCTIONAL FAILURE CHARACTERISTICS	External Hazards				Internal Hazards (Design, Construction, Maintenance, Operation)			
				Meteorological	Seismic	Reservoir Environment	Human Attack	Water barrier	Hydraulic struct.	Mech/elec	Infrastructure & Plans
DAM COLLAPSE BY OVERTOPPING (erosion or overturning)	Water elevation too high	Inadequate installed discharge capacity	Meteorological inflow > buffer + outflow capacity	X	X	X	X	X	X	X	X
			Inadequate reservoir operation (rules not followed)	X	X	X	X	X	X	X	X
		Inadequate available discharge capacity	Random functional failure on demand	X	X	X	X	X	X	X	X
			Discharge capability not maintained	X	X	X	X	X	X	X	X
		Inadequate freeboard	Excessive elevation due to landslide or U/S dam	X	X	X	X	X	X	X	X
			Wind-wave dissipation inadequate	X	X	X	X	X	X	X	X
	Institutional Failure		Dam Safety Management System (hydraulic adequacy) Function Failure	X	X	X	X	X	X	X	X
DAM COLLAPSE BY LOSS OF STRENGTH (External orinternal structural failure and weakening)			Dam Safety Management System (structural capacity) Function Failure	X	X	X	X	X	X	X	X
	Crest elevation too low	Stability under applied loads	Mass movement (external stability:- displacement, tilting, seismic resistance)	X	X	X	X	X	X	X	X
			Loss of support (foundation or abutment failure)	X	X	X	X	X	X	X	X
		Watertightness	Seepage around interfaces (abutments, foundation, water stops)	X	X	X	X	X	X	X	X
			Through dam seepage control failure (filters, drains, pumps)	X	X	X	X	X	X	X	X
		Durability/cracking	Structural weakening (internal erosion, AAR, crushing, gradual strength loss)	X	X	X	X	X	X	X	X
			Instantaneous change of state (static iquefaction, hydraulic fracture, seismic cracking)	X	X	X	X	X	X	X	X

Figure 2. Hazards and Failure Modes Matrix