ICOLD Symposium on Sustainable Development of Dams and River Basins, 24th - 27th February, 2021, New Delhi

FUNCTIONAL MODES AND FAILURE MODES: THEIR IDENTIFICATION AND ANALYSIS OF THEIR EFFECTS

DND HARTFORD
B.C. Hydro, Burnaby, BC, Canada

ABSTRACT

The forensic report into the Oroville Dam Spillway Incident drew attention to shortcomings of the current Potential Failure Mode Analysis (PFMA) processes in dealing with complex dam systems and recommended that they must be recognized and addressed. The report also recommended supplementing the PFMA by way of a Failure Modes and Effects Analysis (FMEA) or similar process for complex structures (e.g. gated spillways). The forensic report further noted that the PFMA process is considerably less structured than the FMEA techniques practiced in other industries, and has also often not provided the level of comprehensive review intended with the SEED process. The paper then proceeds to compare and contrast the essential features of FMEA and PFMA and to describe their limitations. Particular attention is paid to the philosophical, methodological and practical differences between the apparently analytically apparently equivalent FMEA and PFMA process that lead to very important differences in practice, the most important of which is that the PFMA process leads to a much greater degree on non-conservatism than FMEA.

These philosophical and methodological differences are set out and their implications are explained. The paper then proceeds to address the concern raised in the Oroville Dam Spillway Incident forensic report that the PFMA methodology does not provide the level of comprehensive review provided by the USBR's Safety Evaluation of Existing Dams methodology. The paper explains why the FMEA and the PFMA processes both lead to overstatements of the safety of dams when relied on as the basis for safety assessments - a matter that has very serious implications for dam owners and public safety. It also explains why the PFMA methodology, by virtue of its formulation leads to a much greater overstatement of the level of safety than would be the case for FMEA when applied in accordance with internationally accepted standards of (FMEA) practice. The paper then proceeds to address this problem of overstatement of the level of safety (or understatement of the level of risk) to the extent that is practicable to obtain much better estimates of dam safety than can be achieved with either methodology used in isolation.

1. INTRODUCTION

1.1 Focus

This paper is primarily concerned with the question as to whether or not available good practices for determining the safety of dams overstate the level of safety and thereby underestimate the degree of hazard and level of risk that a dam poses to the downstream public and to the dam owner. This matter of understating the level of risk should be of great concern to dam owners as unpleasant, even catastrophic outcomes cannot be ruled out.

The second focal point of this paper concerns what is meant by the term "failure mode", as currently there are two quite different definitions of a "failure mode". This difference not only creates confusion in the industry, there are related implications with respect to the overstatement of the degree of safety.

1.2 Independent Forensic Team Report on the Oroville Dam Spillway Incident

The Oroville Dam Spillway Incident and the subsequent Independent Forensic Report (IFT, 2018) was the catalyst for a more detailed examination of the question of the potential non-conservatism of contemporary dam safety assessments. The Summary of the Independent Forensic Team Report on the Oroville Dam Spillway Incident included the following recommendation: "Shortcomings of the current Potential Failure Mode Analysis (PFMA) processes in dealing with complex systems must be recognized and addressed. A critical review of these processes in dam safety practice is warranted, comparing their strengths and weaknesses with risk assessment processes used in other industries worldwide and by other federal agencies. Evolution of 'best practice' must continue by supplementing current practice with new approaches, as appropriate."

While the forensic report discussed some of the limitations of the PFMA, the critique was framed in the context of the spillway incident rather than being framed in general terms. This paper provides a more general examination of methods of failure modes analysis focusing on the strengths and limitations of these inductive approaches. However, the forensic report did make two important observations that are pertinent to a general treatment of methods of identification of failure modes and their effects. Specifically, the forensic report drew attention to the facts that:

- Failure modes are defined in a different way in PFMA as compared with FMEA.
- FMEA is a structured systematic method of analysis of the effects of individual failure modes of components and sub-systems on the overall system whereas PFMA is somewhat lacking in structure.

The forensic report concluded that the "PFMA process is less structured and is fundamentally different than techniques practiced in other industries, such as Failure Modes and Effects Analysis (FMEA)". However, as will be demonstrated below, a PFMA is a type of multi-level FMEA with two fundamentally important distinguishing features that have major influence over the comprehensiveness of the PFMA process and how it is interpreted in comparison to FMEA. In this regard, and as observed in the forensic report, PFMA cannot provide a complete and comprehensive account of all failure modes, especially for systems with any complexity. However, the problem is not restricted to PFMA, it is of a more general nature.

Thus, one key issue addressed in this paper concerns the extent to which important safety related failure modes are omitted in any of FMEA or PFMA, Event Tree Analysis or Fault Tree Analysis. The related issue pertains to the question as to how far off base might the safety assessment of a dam be?

2. VULNERABILITY

Vulnerabilities are weaknesses. It is generally accepted that the endeavor of understanding and explaining the safety of dams centers on the matter of the vulnerability of the dam and its component parts. These vulnerabilities pertain to either the physical or functional performance aspects of the dam and its components. The physical vulnerabilities of a system pertain to the "load (force) carrying" capacity relative to the "demand" placed on the installation whereas the functional vulnerabilities pertain to the possible lack of capacity of the installation to perform its "transformative" functions whereby it transforms inputs into outputs and deliver on its productive expectations.

Understanding and dealing with vulnerabilities is the essence of safety management, and dam safety is no different. In fact, the safety of dams can be largely assured by identifying and dealing with the diverse range of vulnerabilities that exist be they physical or operational when operating dams. The "Parts Count" method developed in the nuclear industry when combined with an analysis of the vulnerability of the "parts" to disturbances provides effective way of identifying and treating the vast majority of dam safety concerns. Once the readily identified and characterized issues and concerns have been addresses, methods of failure modes analysis provide a starting point for more in depth analysis of the more difficult problems.

3. MODELS

A model is a simplified representation of something that reflects some of the characteristics of the "something" in a relevant and meaningful way. Developing and analysing models of reality is a foundational principle of engineering as well as to a vast array of human endeavours. Modelling involves creating a simplified system that represents reality in a relevant and meaningful way. Often, models are created in ways that are amenable to some type of scientific analysis of the characteristics that are represented by the model. Models are essentially abstractions of reality where the degree of abstraction can be vary from being a close physical likeness, such as a scale model of a dam and reservoir, or spillway in a hydraulics laboratory, to a system of mathematical equations that computationally mimic the behavior of systems in time such as a computational fluid dynamics model of flows through a spillway. Both types of models find uses in the design and safety analysis of modern dams.

Spatial models represent the physical arrangements of a system in space. Spatial models comprise a broad spectrum ranging from scaled recreations of the physical form of a system to a dimensioned sketch of the shape of the system. Functional models represent the process that are involved in producing the products and services that are derived from the system. Reliability models such as fault trees provide qualitative representations of how real systems might fail. Event tree models provide a means of representing what might happen if a certain initial condition occurs. Dam safety analysis can involve the use of a broad cross section of model types and are often applied in an iterative way beginning with low resolution spatial models and working systematically towards more complex higher resolution functional and functional failure models.

Figure 1 presents a spatial model, and a functional model of a spillway gate.

The gate can be considered to be a "system" and the spatial model illustrates the form and spatial arrangement of the components of the system. The functional model illustrates the mechanism by which the gate opens or closes. Knowing how the system works is necessary to understand the functional modes of the system and its components.

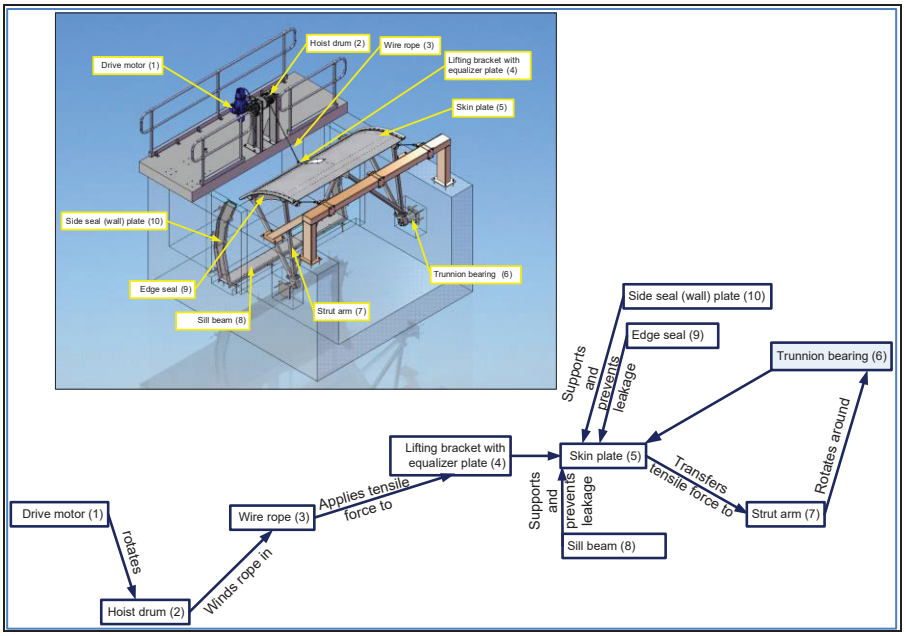

Figure 1 : Spatial Model and Functional Model of a Spillway Gate (Hartford et al., 2016).

4 MODES, FUNCTIONAL MODES AND FAILURE MODES

Before discussing failure modes in any detail, it is instructive to consider the meaning of the term "mode" as it applies first in everyday life and then in engineered systems.

- Mode (n): A state, condition, way of doing things (modus operandi), manner in which something occurs. Common uses include "flight safe" mode; mode of transport (aircraft, car, railway, etc.).
- This definition can be readily extended to describe a mode of operation: A way in which the operational states or performance objectives of the system manifest themselves.

Mode of operation: A condition or system status in which the operational functions or objectives of the system manifest themselves.

In the context of dams, water retention and water conveyance are the highest level modes of operation; at a more detailed level, the modes of operation of a spillway gate system include a) dormant mode (during the dry season); in-service mode (closed to retain water or open to pass flows); and ready mode (just prior to initiation of gate movement). Thus modes of operation which can also be termed "operational modes" can be considered in terms of how the states of operation manifest themselves. Operational modes may also be considered to be the "functional modes" but this will determined by the way the analyst defines the system and its functionality. This is important for all aspects of analysis and the way that "modes" are defined as the mode is an artefact of how the system is being modelled by the analyst to a significant degree. The definition of a functional mode follows directly along similar lines of reasoning.

Functional mode: The way that the functional state of the system is observed.

In this context of the highest level modes of operation and considering the physical states of a spillway gate, three states can be identified; closed, open, transition (from closed to open and vice versa).The functional mode of the drive motor is rotational and the functional mode of the hoist drum is to wind the lifting rope in etc. The failure modes of the components can be derived directly from the operation modes; the drive motor fails to rotate; the wire rope fails to apply the tensile force to the lifting bracket etc. The spillway gate is modelled as a system comprising 10 components which vary in functional complexity ranging from the drive motor which can be considered to be a system of some complexity in its own right for detailed performance and fault analysis, in contrast to a more elemental component such as the wire rope. However, although relatively elementary, the wire rope can considered to be a system with individual strands that may be crimped or swaged to an end fitting that attaches to the lifting bracket. The combined functions of the components can be represented in terms of the functional analysis dia-gram (FAD) illustrated in Figure 1. The functional analysis is fully coupled with the structure of the system.

In general, the modes of operation of a system may be different to the modes of operation of the components. Similarly the functional modes of a system may be different to the functional modes of the parts. The transition operational mode of the spillway gate is derived from the functional modes of the components such as the rotational mode of the motor turning the hoist drum. The corresponding functional failure modes of the spillway gate can be determined directly from the functional modes by taking the compliment of the functional mode. For example the gate transition operation mode has gate fails to move as a failure mode, similarly the functional failure mode of the drive motor is fail to rotate the hoist drum.

The details provided above are widely accepted across industry in general. However, there is some confusion in the dams industry concerning the meaning of the term "failure mode", as some practices utilise the FMEA definition of a failure mode while others use the much more recent and distinctly different PFMA definition. In this regard, it should be noted that the PFMA definition is uniquely peculiar when compared to the wider applications of these types of analyses in a wide range of industries. It also has important implications with respect to the efficiency and effectiveness of the PFMA process, and especially with respect to the questions of overstating the degree of safety and understating the degree of hazard ad risk posed by a dam.

The confusion can be traced in the case of FMEA to the somewhat vague definition of a failure mode, a problem that was compounded when the PFMA process was introduced. In some respects, one might argue that the entire matter of the definition of definition of a mode or the definition of a failure mode is simply a matter of convention, and therefore, once a definition is adopted for a particular task, then provided the term is used consistently there is nothing more to the matter. However, things are not so simple with respect to statements that are fundamental to determining the safety of the public, the survivability of an industry or the integrity of governmental oversight arrangements.

General definitions of failure modes of engineered systems whether they be dams, spacecraft or nuclear power stations follow.

1. International Electrotechnical Commission definition of a Failure Mode:- "the manner in which an item fails" (IEC, 2006)
2. International Electrotechnical Commission definition of a Failure Mode:- " manner in which failure occurs" (IEC, 2018)
3. Society of Automotive Engineers Definition of a Failure Mode:- "the way that the failure of an item occurs" (SAE, 1996)

These definitions can be contrasted with the PFMA definition of a Potential Failure Mode:- the chain of events leading to unsatisfactory performance of the dam or a portion thereof (FERC, 2005/2016). In fact, the PFMA definition of a failure mode is essentially the same as the definition of a "sequence" in Event Tree Analysis (IEC, 2010) where a "sequence" is defined as "chain of events, from initiating event through subsequent events, leading to a specific outcome". Interestingly, when discussing the US bureau of Reclamation's 1990 structured approach to probability assignment, Vick (Vick, 2002) noted as follows: "potential failure modes are identified in connection with specific features of the dam along with the types and levels of loading conditions it could experience….. The group begins by decomposing each identified failure mode into its sequence of component events".

One might argue that these definitions are open to such similar interpretations that they are synonymous. However, they are subtly and importantly different, as an item is an individual article or unit that is often part of a collection or set. The FMEA process requires that the analyst knows or can find all of the modes of failure. There is also no way of checking the analysis for completeness.

The chain of events definition of PFMA involves a distinctly different mode of analysis. The analyst must know in advance every factor or collection of factors that create the demand on the dam and reservoir system. The analyst must then be able to foresee every way that this initiating demand might play out and induce a failure state.

In formal FMEA, failure modes are not characterised in a unique way. Rather the way failure modes are characterised depends on how the system is being modelled and the level in the system that the analysis is being carried out (Figure 2). In PFMA, failure modes are uniquely defined, and, even in relatively simple systems there will be a great many of them.

Figure 2 illustrates a hierarchical arrangement of failure modes at different levels within the structure of the system. The failure modes at each level in the system structure are different, as are the functional modes. In FMEA, failure modes are fully coupled with the structure of the system in the same way as functional modes are fully coupled with the structure of the system in functional analysis. From an engineering perspective, this is how it should be outputs at one level of the system being inputs to the next highest level of the system.

Dam schemes usually comprise a large number of modules, components and elements, physical processes and procedural connections between parts, actors and activities, and often numerous interdependencies between all of the aforementioned parts and functions, each of which will have at least one and possibly several functions and their own influence over the safety of the system. A specific dam scheme will in general comprise an arrangement of modules, components and elements, processes, functions, etc. and scheme specific products and services. Such an arrangement is typically complex where each of these parts, connections, processes etc. has a purpose as determined in the design, and these purposes must be fulfilled in order for the dam scheme to deliver its products and services safely, reliably and efficiently. The purposes of the components etc. are achieved through their functionality. The functionality of the parts taken together, provide the system with its functionality. There is nothing arbitrary about the arrangement of parts, processes, etc. or their functional behaviours; they are in effect a grouping of parts that operate together for one or more common purposes.

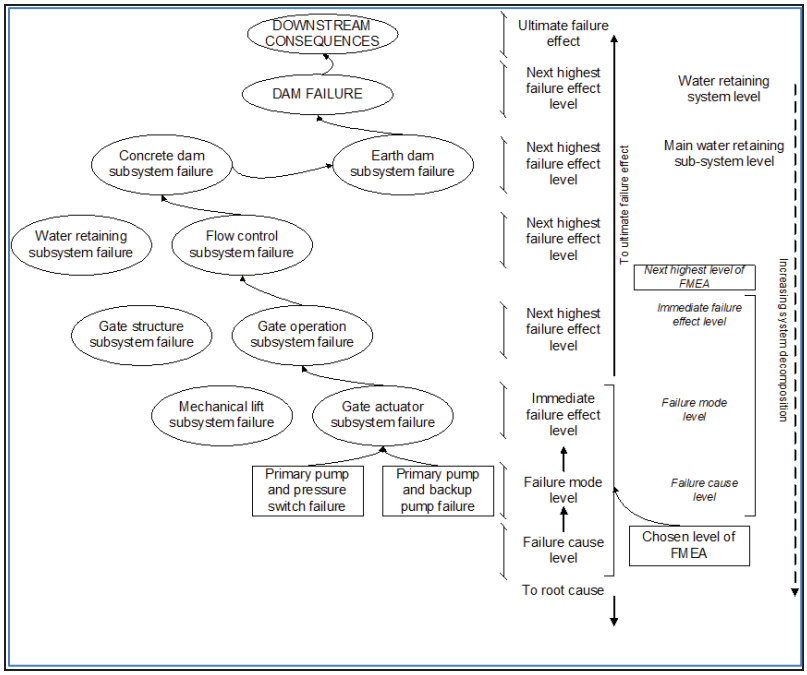

Figure 2 : Levels of failure modes in an FMEA (Hartford et al., 2004)

The hierarchical structure of a dam system is illustrated in Figure 3. The lowest part of the diagram maps directly to Figure 1, the higher levels map to a notional dam system of the type illustrated in Figure 2. Further, Figure 2 contains more than the usual cause and effect type of relationship and introduces the relationship between failure causes, failure modes and failure effects. The relationships between "failure cause – failure mode – failure effects", as illustrated in Figure 2 for the system architecture shown in Figure 3 are presented in Figure 4. A convenient identification scheme that reflects the hierarchy of the architecture is also illustrated in Figure 4. For every functional mode of operation, there will be one or more functional failure modes. For example, a motor can lose its rotational operation function in several ways. The important point is that the analyst must know all of the ways that the rotational function can be lost and these serve as inputs to the overall analysis. These abstract concepts can be readily operationalised as illustrated in Figure 1.

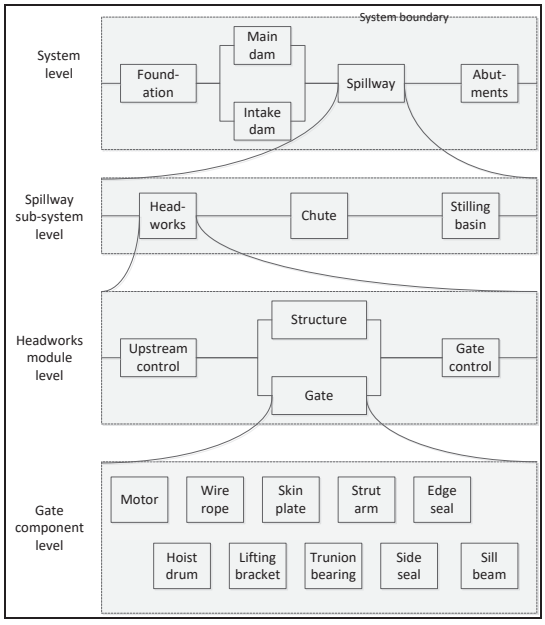

Figure 3 : Hierarchical structure of a dam

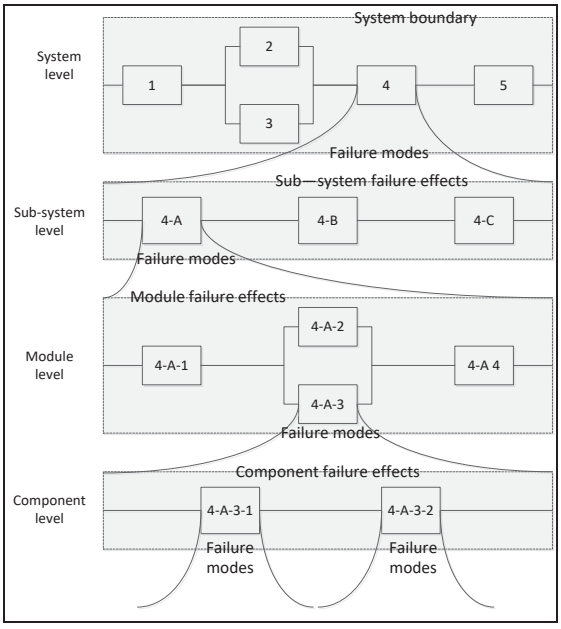

Figure 4 : Cause-mode-effect relationships system

An understanding of the system and how it works and the ability to represent the components and interactions within the system is an essential precursor to understanding and explaining how the system might fail. Thus, the primary skill required is to understand the functional nature of the system being analysed. This requires knowledge of how the system was designed and built, how system function is achieved, and how it has been and is being operated. This gives a basic appreciation of the potential weaknesses or vulnerabilities within the system and forms the basis for carrying out a failure mode-type analysis.

Given the definition of a failure mode in the PFMA process being the chain of events from initiation to failure, it follows that the PFMA process is of the same conceptual form of a multi-level FMEA. This is because it involves a subjective and way of cascading upwards through the different levels of the system that is not connected in any obvious way to the physical structure or functional arrangements of the system.

5 SYSTEM FUNCTION, SYSTEM SUCCESS AND SYSTEM FAILURE

The way a system works can be defined and explained in exact and specific ways although, the level of effort might be extremely. The way a system fails can evolve in extremely complex ways. System function is a process whereas system failure is a state, an in this regard, system function should not be confused with system success which typically concerns the efficiency of a system.

The functioning of a system can be considered from two perspectives: the various ways for the system to successfully deliver its outputs or the various ways for system to fail to deliver its outputs. Thus, there is a spectrum, bounded by total success at one extreme and complete failure at the other. Usually, there are intermediate conditions as failure and success are frequently non-binary as is the case when deterioration is ongoing (Figure 5.). Between these bounds, the system is functioning, albeit not ideally. Importantly, "functioning" includes "complete success" while excluding "complete failure". Further, it is functioning that deteriorates on the path to complete failure.

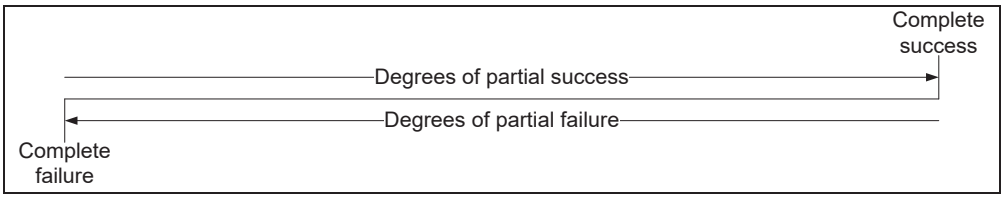

Figure 5 : Failure-Success space

In general, the relationship between success and failure is apparently simply a matter of success being the complement of failure. However, things are not quite so simple. The characteristics of success are usually described in terms of continuous variables that are not readily modelled in terms of discrete events such as "gate does not move at all". The gate might move partially or move slowly but completely. The analysis of partial failure and partial success is messy. Debates about "safe enough" in the "partial" state – which is the norm can be similarly messy, even acrimonious and include arguments concerning the "size of the gap" between success and failure. Theoretically, due to the continuous nature of the factors involved, the number of ways in which a system can fail is infinite as is the number of ways in which a system can succeed. This is stark in contrast to the number of ways the system functions – typically only 1, or a small few!

With reference to Figure 1, it is quite clear how the system works, and it only works one way. However, there many ways that the gate system can fail to function. With reference to Figure 1, there are seven of the ten components in series, each of which must perform their function in order for the gate to move at all and ten of the ten components must all function as required if the gate is to function exactly as intended by the design. Focusing only on gate movement, there are no less than 7 and up to at least 127 (27-1) possible component related reasons that the gate can fail to move.

Since in the conventional sense a mode is a discrete event, state or condition, failure modes reside at the extreme left hand end of the failure – success spectrum. If intervention to restore capability and frequency of occurrence of the loss of functionality are brought into the analysis – as they should – then the failure space is conceptually of the form illustrated in Figure 6.

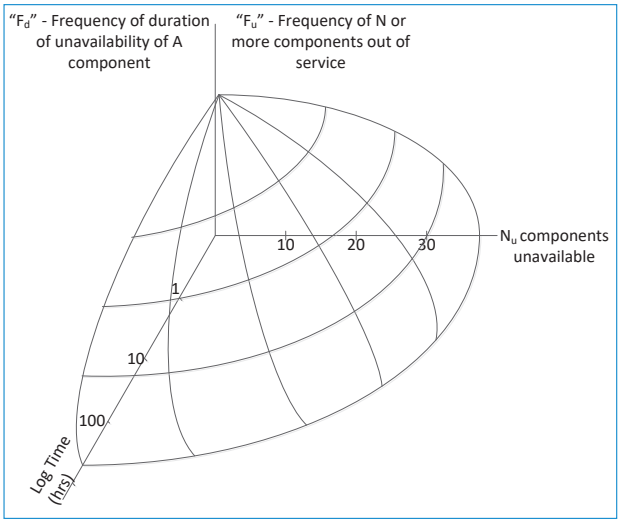

Figure 6 : Notional success and failure space considering frequency and intervention

The failure states, the number of which in practical terms is very large are within the curved surface. However, since the vertical axis is infinite in its extent, all of the remaining possible states, be they partial success or complete success, comprise the reminder of the space which is unbounded on the vertical axis. The relatively small volume of the failure states in comparison to the very large volume of success and partial success states explains why dynamic stochastic simulations are so computationally demanding. Put simply, the system resides in the non-failure volume for the vast majority of the duration of the simulation. All of this gives credence to the notion of safety being a "dynamic non-event" (adapted from Weick, 1987). Herein lies the danger, because as Weick put it, reliability is both dynamic and invisible. The same can be said of safety.

6. THE PROBLEM OF OVERSTATING THE LEVEL OF SAFETY

6.1 Limitations of FMEA

In functional analysis, the components and their functions are all identifiable. Functional failure modes can be ascribed to each component directly from the functional analysis by taking the compliment of the component function. It would appear that everything can be defines in an objective way. In fact, FMEA is very efficient when it is applied to the analysis of components that cause the failure of the entire system or of a major function of the system such as the spillway gate illustrated in Figure 1. However, and because of the quantity of different system information that needs to be accounted the analysis of complex systems, that have multiple functions involving different sets of system components, the process quickly becomes complex and tedious. Complications and errors can occur when FMEA attempts to span several levels in a hierarchical system, especially if there is redundancy or time effects. Relationships between individual and croups of failure modes cannot be effectively presented in FMEA. Further, in FMEA the main assumption is independency of failure modes. Difficulties will arise if the assumption of independence is invalid. Further, the assumption of independency may obscure a failure mode with catastrophic consequences when it is due to another failure mode, even if individually they have very low probabilities of occurrence. All of the above are reasons to restrict FMEA to one level of the system hierarchy.

6.2 Related limitations of PFMA

The definition of a failure mode in PFMA as a chain of events from initiation to unwanted outcome adds significantly to the above limitations as it involves cascading through potentially related conditions by necessity. Further, there are often a great many causal chains for one system level failure mode. This is best seen in Fault Tree Analysis where the system failure mode is defined as the top event of the fault tree, and the initiating challenges are fanned out at the bottom of the tree. Further in safety analysis, credible events can have vanishingly small probabilities of occurrence and may well be screened out in the PFMA process, whereas the so-called "incredible event" can be made up from a combination of commonly occurring lesser failures which in themselves would not lead to a system failure. In such cases it is not the frequency of each of the causative failure modes but the very low probability with which they combine.

6.3 Overstating safety and underestimating risk

These methods of failure modes analysis also suffer from the limitation of being unsuited to dealing with time effects which is important for reservoir operation and flow control. They also suffer from the limitation that only specifically identified and enumerated chains of events enter the analysis. An unforeseen or unusual combination of usual conditions that is not specifically identified and its effects analysed will be missed. It is for the above reasons amongst others that "for systems that exhibit any degree of complexity (i.e., for most systems), attempts to identify all possible system hazards or all possible component failure modes-both singly and in combination-:-become simply impossible" (NRC, 1981). This means that both FMEA and PFMA are inadequate to capture the totality of the safety problem with the result that the system will be less safe than implied by these analyses. Another worrying feature is the fact that there is no way of knowing just how much the safety of the dam has been overstated. This leads to the in-evitable conclusion that the risk will be higher than perceived and that unpleasant surprises are inevitable when performing a failure modes type of analysis.

Since it is impossible to identify all possible outcomes, dam owners are faced with the problem of explaining in advance that unpleasant surprises might occur and that with benefits of hindsight, these surprises might look to have been entirely avoidable – even obvious. This can be viewed in terms of a legalistic and philosophical question concerning whether a probabilistic progression of a sequence of events should lead to a negation of the certainty of the cause after the fact (Ale et al., 2009).

REFERENCES

Ale, BJM, Bellamy, L.J., van der Boom, R, Cooper, J, Cooke, RM, Goossens, LHJ., Hale, AR, Kurowicka, D, Morales, O. Roelen, ALC, and Spouge, J (2009). Further development of a Causal model for Air Transport Safety (CATS): Building the mathematical heart, Reliability Engineering & System Safety, Volume 94, Issue 9, September 2009, Pages 1433-1441.

FERC, Federal Energy Regulatory Commission (2005/2017). Engineering Guidelines for the Evaluation of Hydropower Projects, Chapter 14.

Hartford, DND and Baecher, GB. (2004). Risk and Uncertainty in Dam Safety. Thomas Telford.

Hartford, DND, Baecher, GB, Zielinski, PA, Patev, RC, Ascila, R & Rytters, K. (2016). Operational Safety of Dams and Reservoirs. Thomas Telford.

Independent Forensic Team (2018). Oroville Dam Spillway Incident. California Department of Water Resources (DWR).

International Electrotechnical Commission (2006-01). IEC 60812: Analysis techniques for system relia-bility – Procedure for failure mode and effects analysis (FMEA).

International Electrotechnical Commission (2010-10). Analysis techniques for dependability - Event tree analysis (ETA).

International Electrotechnical Commission (2018-08). IEC 60812: Failure modes and effects analysis (FMEA and FMECA).

NRC (1981). Fault Tree Handbook. Nuclear Regulatory Commission.

Society for Automotive Engineers (1996). Aerospace Recommended Practice: Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment.

Vick, SG. (2002). Degrees of Belief. ASCE Press.

Weick, K. (1987). Organizational Culture as a Source of High Reliability. California Management Review Vol. XXIX, No.2.