MINISTRY OF THE ENVIRONMENT, ENERGY AND THE SEA

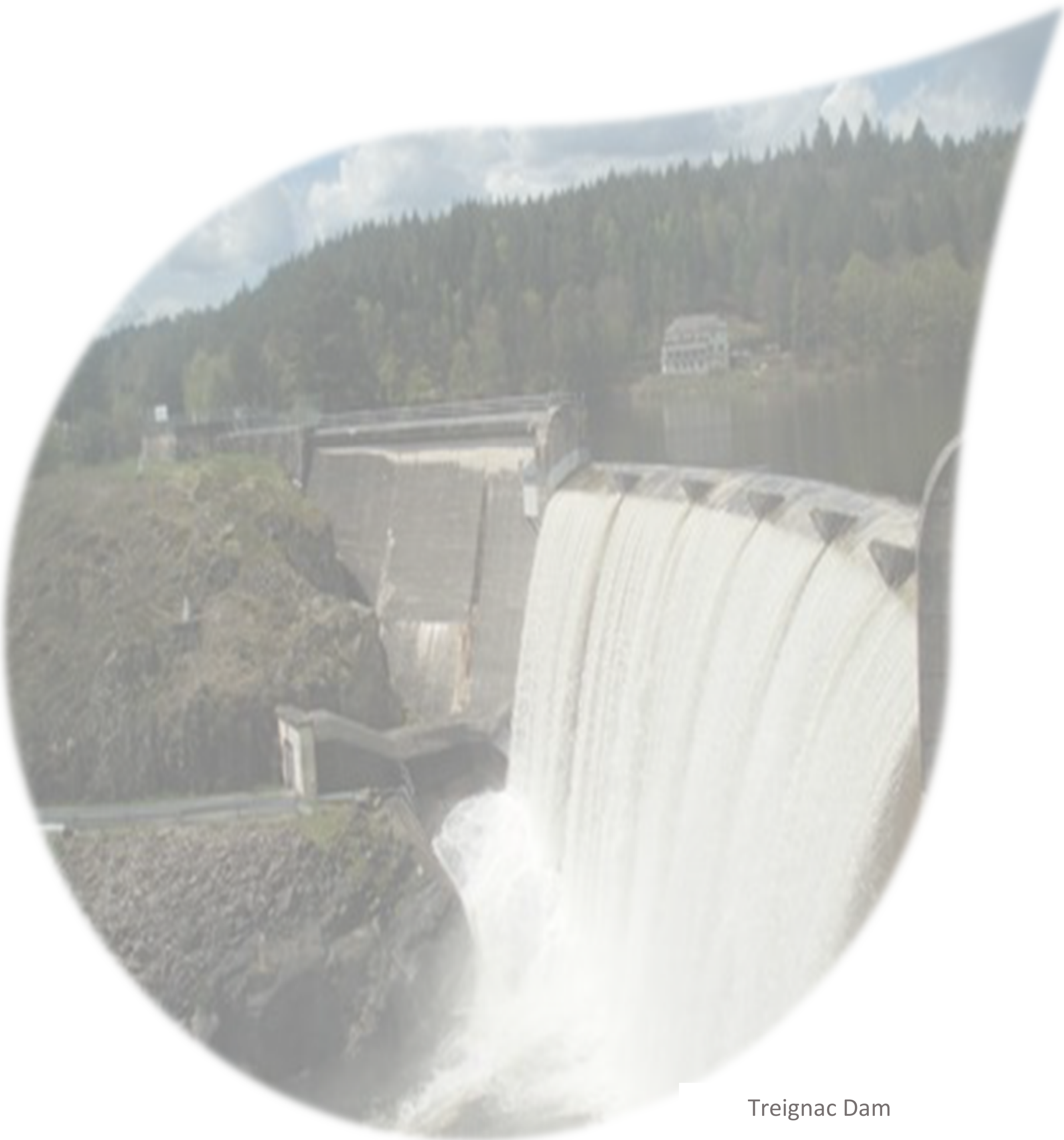
Lessons learned from major events towards improving hydraulic safety

Findings from experience feedback on hydro-mechanical and control system components in use on dams

Study based on the article presented at the CFBR 2015 symposium [15]

- April 2016 -

ARIA
dgpr srt barpi



Treignac Dam

Contents

Abstract 4
Introduction 5
1. Generating and sharing experience feedback 5
1.1 Whether accident or incident, all events must be taken into consideration 5
1.2 Control systems and hydro-mechanical devices: Analysing weak signals 6
1.3 Causal analysis 6
2. Feedback from valve-operated structures and control systems 7
2.1 No probabilistic use of quantitative information 7
2.2 Result of the global database analysis 7
2.3 Experience feedback specific to control systems and hydro-mechanical devices 11
3. Sample events 15
3.1 ARIA 43703 - 2013 - Automated controls - Works 16
3.2 ARIA 44915 - 2014 - Automated controls - Testing 17
3.3 ARIA 44554 - 2013 - Automated controls - Works 18
3.4 ARIA 46064 - 2014 - Valve - Flooding 19
Conclusion 20
APPENDICES 21
A.1 The EIHS and HSP regulatory framework 21
- EIHS 21
- HSP 21
A.2 Lessons and perspectives drawn from the EIHS-HSP data collection campaign 22
A.3 The "ARIA" base: Analysis, Research and Information on Accidents 23
References and quotes 25

Abstract

The sharing and use of information and/or lessons drawn from analyses of incidents and accidents constitute the building blocks of a continuous process aimed at improving risk prevention. The order issued on 21 May 2010 requires facility owners to declare key events involving hydraulic safety (EIHS) along with, for all class A and B dams, the set of hydraulic safety precursors (HSP). A causal analysis must then be performed to finalise all such declarations "on the spot".

Since July 2010, the information collated on dam-related events, notably that contained in the EIHS datasheets, has been recorded in the ARIA database (analysis, research and information on accidents). Consulting this base, accessible to the general public via the site www.aria.developpement-durable.gouv.fr, provides aspects of experience feedback from technological accidents along with event summaries.

By the end of 2015, ARIA had catalogued a total of 356 events occurring at both French and foreign facilities. While this database has not been designed for any statistical purpose (due to its reduced sample size and insufficient representativeness), it still allows for the universal sharing of lessons learned from accident analyses. Now that the system has been up and running for a few years, an analysis of information listed in the database, as well as records held by the bureau specialised in large dam engineering and control (BETCGB), may be undertaken in order to present a qualitative and quantitative overview of the available experience feedback, in particular regarding hydro-mechanical devices and command-control systems implemented on dams.

By means of a few examples, focusing specifically on automated controls and hydro-mechanical systems, it becomes possible to demonstrate how an experience feedback analysis exposes the deep-rooted causes of an operational malfunction.

Saint-Marc Dam

Introduction

To assess the robustness and relevance of rules in effect for designing and operating dams, or those applied following an event, the analysis of accidents and incidents occurring at hydraulic structures is regularly emphasised across the profession, in giving rise to a steady stream of publications. Bulletins 99 and 109 [1] of the International Commission On Large Dams (ICOLD) are commonly cited in published safety reports. More recently, the symposium organised by the French Committee on Dams and Reservoirs (CFBR) in 2011, addressing safety reports, featured a presentation of France's regulatory regime for recording key hydraulic safety events and hydraulic safety precursors (HSP) [2].

In light of the risks at hand, it is very fortunate that accidents remain highly infrequent. Each structure is typically involved in just a few incidents. Any assessment must rely on lessons drawn from cumulative feedback covering the greatest number of similar structures and facilities, whether in France or abroad. For this reason, similarities cannot be restricted to the type of structure but instead must encompass all functional components or elements, coupled with the mode of organisation, specifically as regards the fields of control technology and hydro-mechanical systems.

This effort presumes ease of access to information regarding a large number of events and an experience feedback that enables selecting those cases whose similarities make for meaningful lessons. Each dam is in fact a prototype, a unique outcome from the use of varied techniques, with combinations of diverse equipment and technologies. Compiling worldwide statistical data alone (even if correlated with a list of accidents or incidents), yet without conducting a targeted analysis, falls short of its objective [3]. Such an observation becomes even clearer for specific devices like dam valves or control systems (from a broader perspective).

The causes of a technological accident may be multi-fold, often prompting analyses (in particular those carried out by the BARPI Office assigned to analyse industrial risks and pollution) of: technical causes (e.g. equipment failure, flawed design), human and organisational causes (e.g. human error, inadequate training, weak organisation), and natural causes (e.g. lightning, flooding, extreme cold). Acts of malicious intent can also result in accidents of a serious nature, especially given that such acts are seldom incorporated into risk analyses and safety reports.

1. Generating and sharing experience feedback

1.1 Whether accident or incident, all events must be taken into consideration

The term "accident" is commonly defined as any event leading to serious consequences for either property or people, whereas "incident" refers to any event not causing serious physical consequences. With respect to dams, it is also possible to limit the use of "accident" to structural failures. Accordingly, ICOLD's publications typically refer to major dam breaks or accidents occurring when the dam is being filled or else during construction.


Malpasset Dam

Accident scenarios are not necessarily the outcome of a single cause, but rather a series of physical, organisational or human mishaps that, taken individually, might be of no concern. All events, regardless of whether or not their consequences are serious, contribute to an experience feedback that serves to improve safety.

1.2 Control systems and hydro-mechanical devices: Analysing weak signals

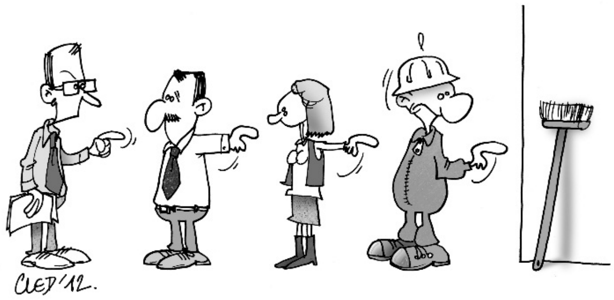
When not accompanied by flooding, the failure of a safety device will not systematically create problems. For example, an outage of electrical power to flood control facilities, should they not need to be operated, has no adverse consequences. It is still worthwhile however to study this malfunction; experience feedback can easily be applied to flood conditions. The risk of device failure becomes more acute in cases of major flooding, which tax the operating system to a much greater extent.

Moreover, for dams built to resist exceptional high waters, it makes sense that only a small number of serious events due to safety mechanism failure have ever been observed. Findings by the U.S. National Research Council (1983) estimated at 2% the number of embankment dams experiencing accidents due to valve malfunction [4]. Similarly, ICOLD demonstrated that an accident typically results from a combination of breakdowns involving several material and organisational barriers [5].

It has thus become necessary to focus on inconsequential events or on smaller dams. These investigations help raise overall dam safety. Efforts expended on analysing these weak signals give momentum to safety improvement campaigns and build organisational resilience.

1.3 Causal analysis

Analysing the origin of an event in the aim of preventing its recurrence requires, as a starting point, refusing to consider the event as the outcome of a set of unfortunate circumstances. Only in-depth analyses yield measures capable of remediating a situation over the long run. Such analyses entail a systematic and well-organised approach that, under ideal conditions, leads to adopting the most appropriate set of corrective measures. It is essential herein not to find fault or assign blame.



Many approaches available today are aimed at explaining an event after the fact [13]. An event must be considered in all its ramifications, as a series of superimposed layers. While the top layers are accessible to visual inspection, an analysis is needed to penetrate into the lower depths and, in so doing, may succeed in exposing disturbances (or initial causes) as well as more deep-rooted causes. It is essential to always distinguish one from the other.

Disturbances designate the set of direct malfunctions contributing to the event under study; they are accessible upon simple observation. From the outset, deep-rooted causes can be seen as breakdowns of the socio-technical system in which the accident took place and tend to involve aspects related to human, as well as organisational and managerial, factors. Examining deep-rooted causes means being able to identify the factors inherent in system operations (e.g. structural failures of defence barriers) that created the accident-prone working conditions. This desire for a detailed understanding necessarily directs the analysis towards: more collective aspects (collaboration, communication), workplace organisation, management practices and task prioritisation, while not overlooking the physical and mental state of facility personnel plus the social and technical work environment.

The method employed by BARPI [6] is intended to highlight both surface disturbances and deep-rooted causes. The examples below offer typical disturbances:

- physical defects;
- external aggression (including weather-related events);
- human intervention, as characterised by the failure to complete required actions or by actions carried out that were not required.

An identification of disturbances exposes the source of installation malfunction, in addition to shedding light on the event sequence, yet this step fails to explain the why. The series of deep-rooted causes explored by BARPI include:

- technicians' working conditions, e.g. training and certification, adequacy of workplace ergonomics;
- risk management, e.g. shortcomings in risk identification, inappropriate choice of facilities (as regards their design or materials), flawed organisation of controls, lack of safety culture;
- unanticipated factors, e.g. malicious intent, hazardous phenomena unknown to the dam operator when conducting the risk analysis.

The regulatory regime governing EIHS, the protocol for recording hazardous events and the tools available for their interpretation (i.e. the ARIA database) will be presented in detail in the Appendix.

2. Feedback from valve-operated structures and control systems

The results provided below are based on events whose information has been properly analysed. Depending on the type of event, study sample sizes may vary. The percentages listed therefore are indicative of relative occurrence rates but are not statistically significant.

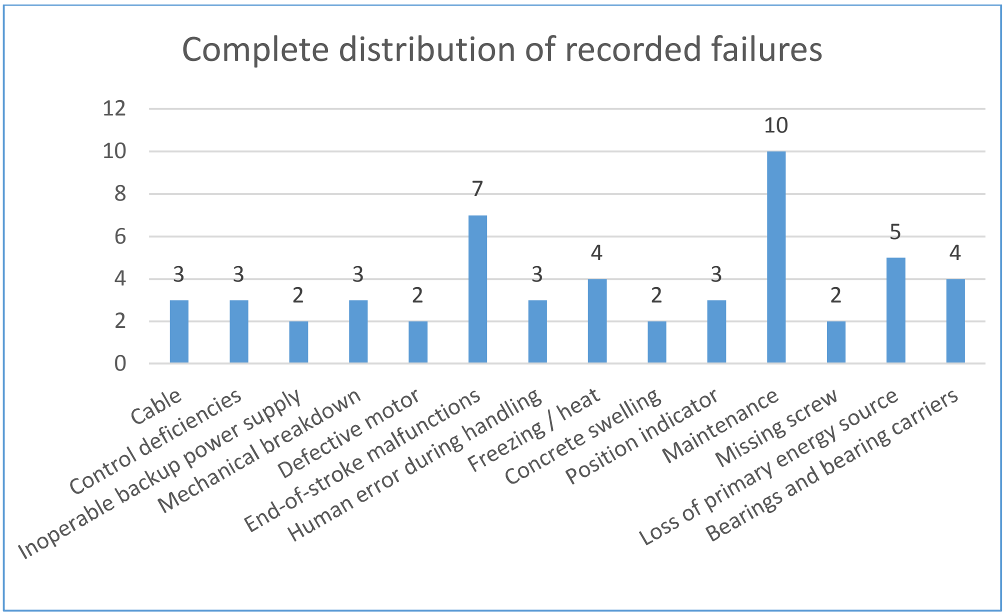
2.1 No probabilistic use of quantitative information

Our research has led to presenting a quantitative description of the events studied. A warning must be issued against any statistical interpretation of the data. It would be erroneous to establish probabilistic laws in assuming some kind of similarity among the failure modes of each subset.

- On the one hand, extending the laws observed on just the structures studied to the full set of facilities would constitute, by neglecting the inevitable biases inherent in the composition of these non-exhaustive databases, an ill-advised approach.
- On the other hand, such an approach would overlook the diversity in designs, operating procedures and loads imposed on both the dams and their facilities. The same device, depending on the layout of the structure where it is installed, its immediate environment, and its maintenance, monitoring and operating conditions, may behave completely differently [3].

2.2 Result of the global database analysis

Along the same lines as accident scenarios targeting gravity dams [8] or dam foundations [9], an analysis of incidents involving hydro-mechanical devices was the topic of various CFBR publications during the 1990's [10], as well as a more recent paper [11]. In foreign countries, ICOLD's recently issued recommendations regarding spillway gate reliability, based on Hobbs' research (2003) analysing some 60 incidents related to valves, indicate a statistical breakdown of the fields involved (see Fig. 4). It is worth noting that in his analysis, Hobbs explicitly cited human factors. Consultation of the ARIA base as well as databases compiled by BETCGB, whose contents will be presented below, yield similar analyses and underscore the importance of the fields of specialisation governing control systems and hydro-mechanical devices in the observed and recorded events.



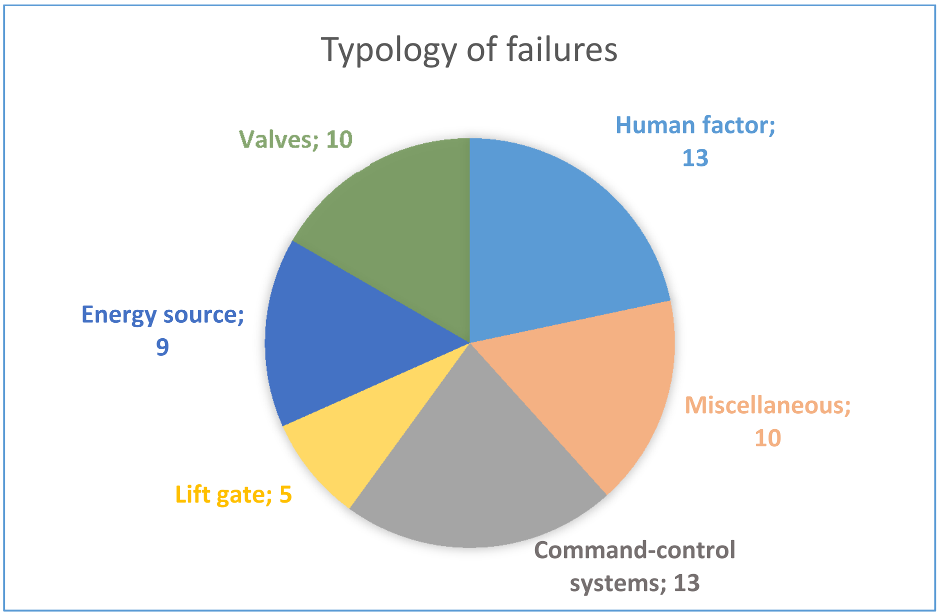


Figure 2: Type of failure according to Hobbs, based on 60 events involving valves: Breakdown and typology

2.2.1 ARIA: Experience feedback from dams

As regards the selection criteria mentioned above, it can apparently be concluded that out of the 228 events pertaining to dams, 211 point to hydraulic safety issues. Several hazardous phenomena may be at play during a single event. Their occurrence rates are shown in Figure 3.

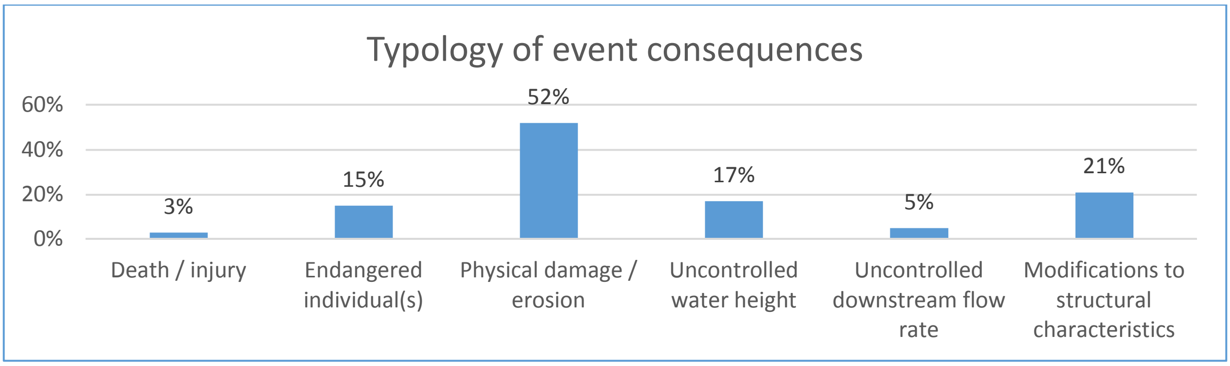


Figure 3: ARIA base - Consequences of EIHS events

A full third of the events involve a deficiency in assessing the upstream water height, enabling the "water retention" function or controlling the release of flow with the potential to activate hydro-mechanical devices or control systems.

Out of the 228 recorded events, 179 resulted in an EIHS declaration, as intended in the administrative order promulgated on 21 May 2010. The selected ratings have still not been added to the database, even for the initial cases input. Table 1 shows that 77% of all EIHS entered into ARIA with a level indication were assigned a yellow rating.

Selected EIHS level	Number of accidents	Percentage (out of total recorded)
Yellow	113	77%
Orange	32	22%
Red	2	1%

Table 1: ARIA base - EIHS rating

As discussed above, the causal analysis of an accident may comprise various degrees of investigation. Identifying the initial causes, or disturbances, is the step most frequently carried out. Out of the 228 cases studied, 192 events were associated with at least one disturbance identified in the base. The reporting of deep-rooted causes does not systematically appear in the sources utilised by BARPI. Some however have been connected with 135 events of the 228 recorded in the base (see Table 2). Several deep-rooted causes may lie at the origin of a single hazardous phenomenon.

Deep-rooted causes	Number of accidents	Percentage (out of total recorded)
Human factors, including:	2	1%
- behavioural traits (negligence, distraction, poor technique, lack of rigour, etc.)	2	1%
Unanticipated factors, including:	4	3%
- malicious intent	2	1%
- unknown phenomenon when the accident occurred	1	1%

Organisational factors, including:	180	
- technicians' working conditions, relative to:	26	19%
* task organisation and supervision	18	13%
* procedures and guidelines	5	4%
* personnel training and certification	2	1%
* poor ergonomics	1	1%
- risk management, relative to:	154	
* execution of controls	29	21%
* choice of equipment and processes	15	11%
* risk identification	15	11%
* inadequate experience feedback	14	10%
* lack of a proper safety culture	8	6%
* ineffective communication	6	4%

Table 2: ARIA base - Deep-rooted causes

2.2.2 The BETCGB accident database

BETCGB operates an observatory to record accidents (dam failures and serious accidents listed in categories F1 and F2, and in A1, A2 and A3 as intended by the ICOLD Commission [1]) occurring in France and worldwide. This media and technical-driven observatory, which relies on published experience feedback and information disseminated via ICOLD, has helped build an accident database that currently spans 706 events from 57 countries over the period 1799-2014.

Given the means of data collection, the amount of knowledge derived from the accident scenarios obviously varies from one accident to the next, ranging from very basic (with at least the date, place and type of structure, accounting for 77% of all cases) to a precise analysis of the causes, notably in cases where the accident has yielded a scientific paper. This database cannot aspire to being either exhaustive or statistically representative to any great extent with respect to global accident trends.

An analysis of this database serves to qualitatively position the importance of command-control systems and hydro-mechanical devices as causes of the various failure scenarios (Fig. 4).

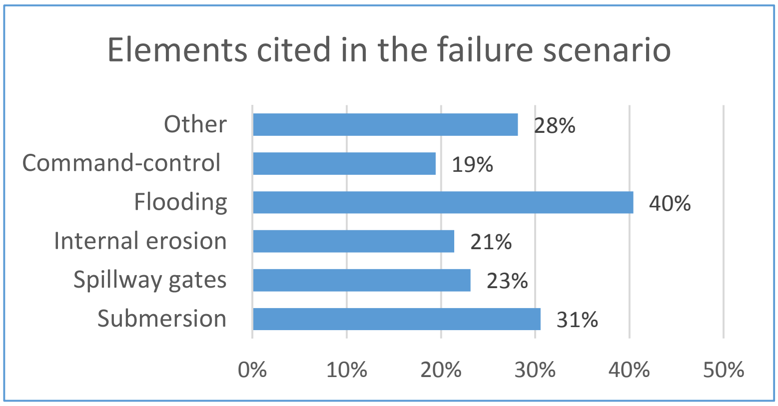


Figure 4: BETCGB base (454 events) - Accident recordings cited in the given failure scenarios

While it comes as no surprise that floods and submersions are identified as the initial causes of accident scenarios (which is only logical since 77% of the accidents listed in this database pertain to embankment dams), the mentions of hydro-mechanical devices and their control systems remain fairly widespread in the scenarios recorded, i.e. cited in nearly 20% of all events. In practically 40% of these cases, the accident occurs during a flood situation.

It can be observed that for 27 cases out of the 194 failures during flooding (14%) and moreover for 33 cases of the 140 dam failures due to submersion (23%), the accident scenarios point to deficient flood control facilities. This proportion turns out to be sizeable when considering that a large majority of structures only feature passive spillway gates. As an example, the proportion of passive spillway gates ranges between 54% and 77% for French structures authorised to be run as a concession [12].

In comparison, a summary of the risk analyses conducted within the scope of dam safety reports written in France has identified defective valves or control systems [14] as the critical initiating event in 15% of all cases.

2.2.3 The BETCGB incident database

This base is populated by events that did not lead to failure, i.e. primarily the EIHS and HSP collected since 2006, along with events known to BETCGB through the execution of its support missions. Events included in the base have also been extracted from scientific publications. The number of events listed is limited by the collection and processing capacity, notably when introducing older events, thus preventing compilation of a database incorporating every single event known by the authorities.

The work completed to date has however made it possible to record nearly 400 events (involving 36 countries, with 95% occurring this century), composed for the most part by EIHS (20%) and HSP (40%). In building this database, preference has been given to input related to hydro-mechanical devices or control systems, thus introducing statistical bias into the database representation of these events.

Out of the some 200 EIHS declared since 2008, as reviewed by BETCGB, 70 events contain at least one mention of a hydro-mechanical device or control system parameter, thus accounting for some 30% of all event declarations. This proportion becomes much higher when considering events that have triggered an HSP declaration, since out of the 153 HSP analysed, 19% pertain to an event involving hydro-mechanical devices, 20% cite energy supply, 56% indicate automated controls / control systems, and 5% point to monitoring devices. An analysis of the accident scenarios based on these weak signals using control system equipment or hydro-mechanical devices is thus of major interest.

2.3 Experience feedback specific to control systems and hydro-mechanical devices

2.3.1 The BETCGB accident database

An analysis of this database according to the layout proposed by ICOLD [1] makes it possible to ascribe the origin of failure in 21% of the cases with ancillary structures, more specifically those incorporating valves and control systems. Figure 5 provides a breakdown of the various factors behind the causes cited. The malfunction of flood discharge systems is the leading cause listed.

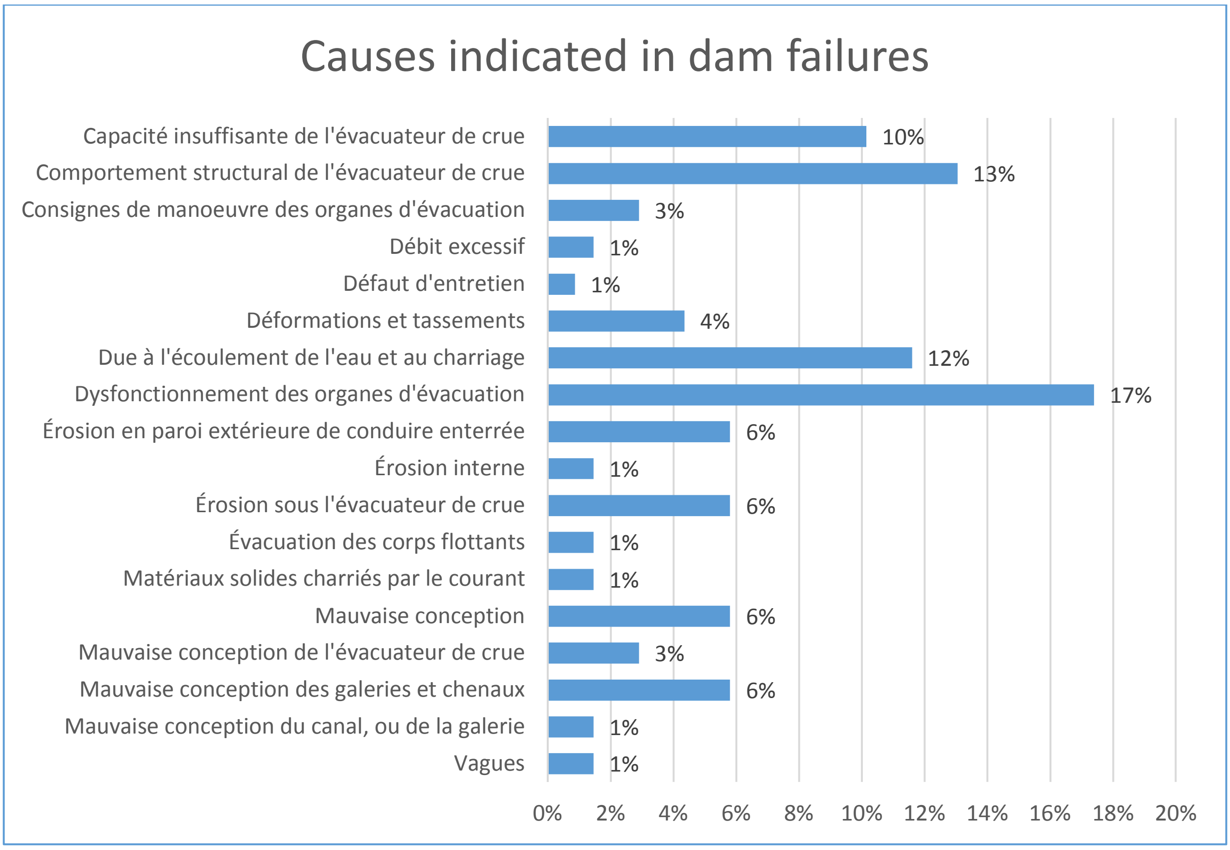


Figure 5: BETCGB base (69 events) - Primary trigger affecting ancillary structures involved in dam failures

2.3.2 The BETCGB incident base

For the first level of analysis, it is worthwhile to expose for each event the primary dedicated functional unit. For the needs of this study, we have introduced a simple analytical breakdown focusing respectively on the hydro-mechanical devices, power supply and control system components (Fig. 6).

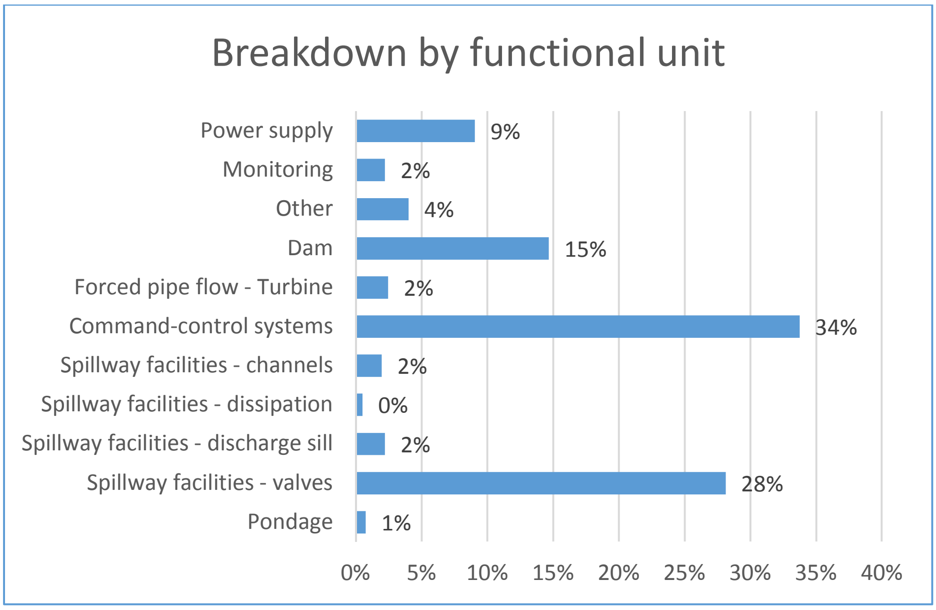


Figure 6: BETCGB base (405 events) - Breakdown by functional unit

As regards the hydro-mechanical devices, it can be observed (Fig. 7) that the kinematic chain unit as well as actuators and safety / protection systems (e.g. torque limiter) account for the major share of total events recorded. For comparative purposes, all functional units have been depicted in this chart.

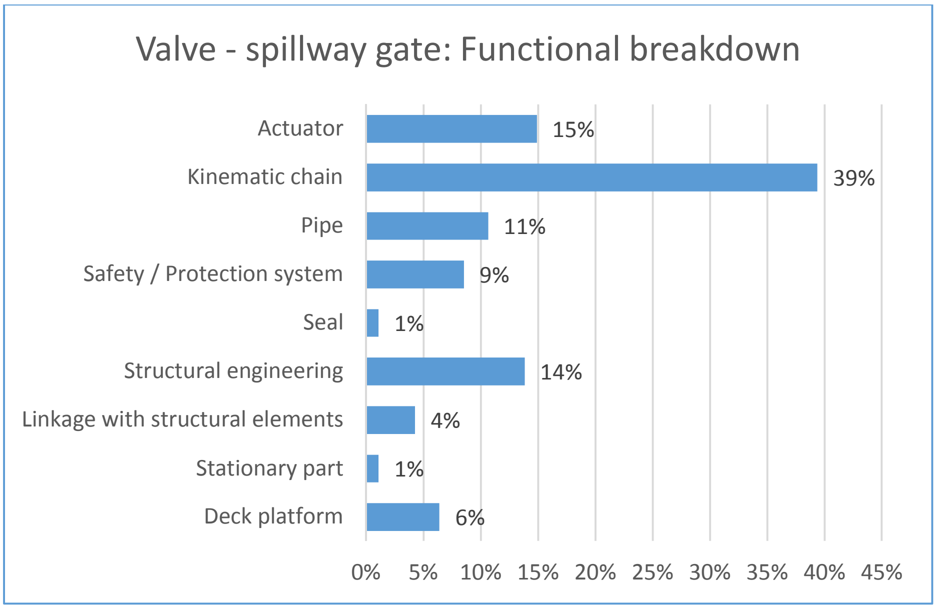


Figure 7: BETCGB base (96 events) - Functional breakdown of events involving valves and spillway gates

Provided the sample is sufficiently large, it is possible to sharpen the functional distinction. As an example, with respect to deficiencies found in the kinematic chain, the components cited were: hydraulic jacks (6 cases), mechanical jacks (2 cases), pushrods (1 case), the hydraulic processing circuit (6 cases), mechanisms (3 cases), cables (3 cases), valve fasteners (3 cases), Galle handling chains (1 case), butterfly valve mechanisms (2 cases), and valve bearing tracks (1 case). This breakdown is quite distinct from that produced by the 1998 CFBR study [10] conducted on an independent sample of 28 cases of spillway gate malfunctions, divided as follows: hydraulic handling system (3) / sensor (1) / hydraulic and mechanical jack (2) / safety feature (1) / handling synchronisation tree (3) / mechanism (2) / Galle chain (8) / cables (2) / pushrods (3) / connections (2). This breakdown clearly demonstrates the potential for considerable bias that would pre-empt any probabilistic interpretation drawn on such a small-sized sample. In most cases (16), a design flaw has been exposed, while the other major causes identified consisted of maintenance or design issues.

As regards actuators, deficiencies in hydraulic plants (6 cases) and float-based handling (6 cases) are indeed widespread. Counterweight systems, heat engines and electrical motors are also cited (1 case).

With control systems, the functional unit responsible for generating the most events recorded in the accident base would be programmable controllers (Fig. 8). Let's also point out that the propensity to add instrumentation and automated controls in order to prevent human error does not protect against all hazards. Sensors (position and measurement of a watercourse), as well as safety / protection devices, are also involved in a significant proportion of incidents. Nonetheless, this area of investigation remains somewhat understated in the risk analyses conducted as part of safety reports.

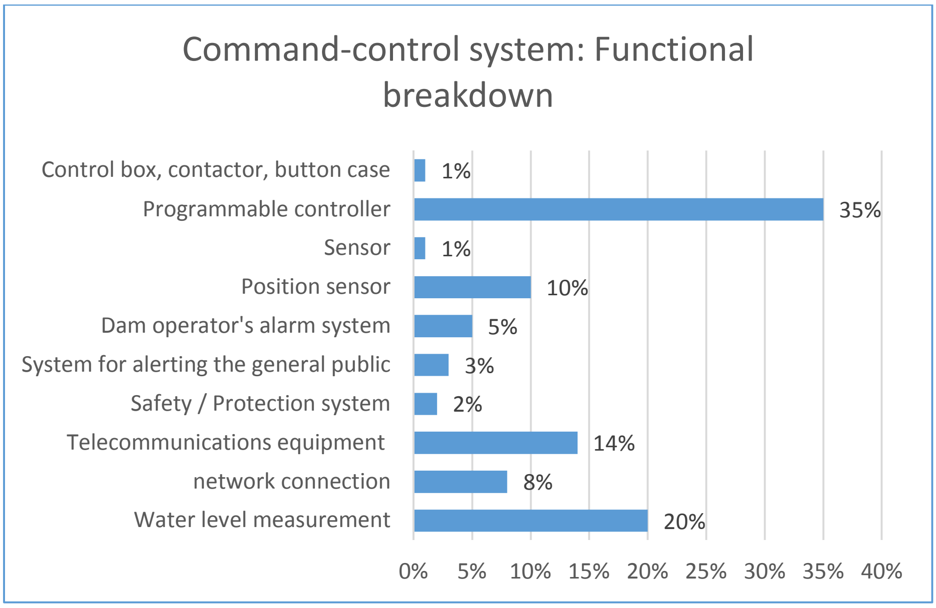


Fig. 8: BETCGB base (99 events) - Functional breakdown of events with automated controls or control systems

Energy supply: The majority of recorded events pertain to energy sources, whether as a primary source or backup (Fig. 10). In many cases, backup energy sources are found to fail during testing or maintenance situations.

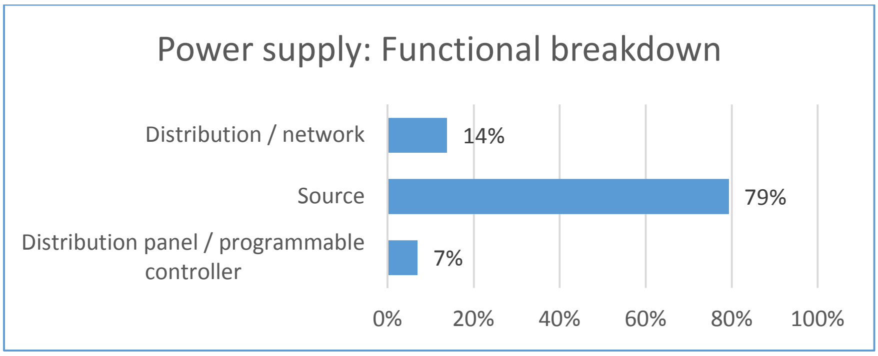


Figure 9: BETCGB base (29 events) - Functional breakdown of events involving power supply

Physical defects stand out as the leading disturbance cited in the failure scenarios specific to hydro-mechanical devices and control systems (Fig. 10). The limited depth of analysis performed on the recorded events prevents establishing any statistical summary of the initial causes of incidents listed in the base. From a qualitative standpoint, organisational factors may be hypothesised in many cases. Subpar maintenance (56 cases), faulty design (77 cases), ineffective organisation and procedural guidelines (19 cases), and human error though much less frequently (10 cases), have been cited.

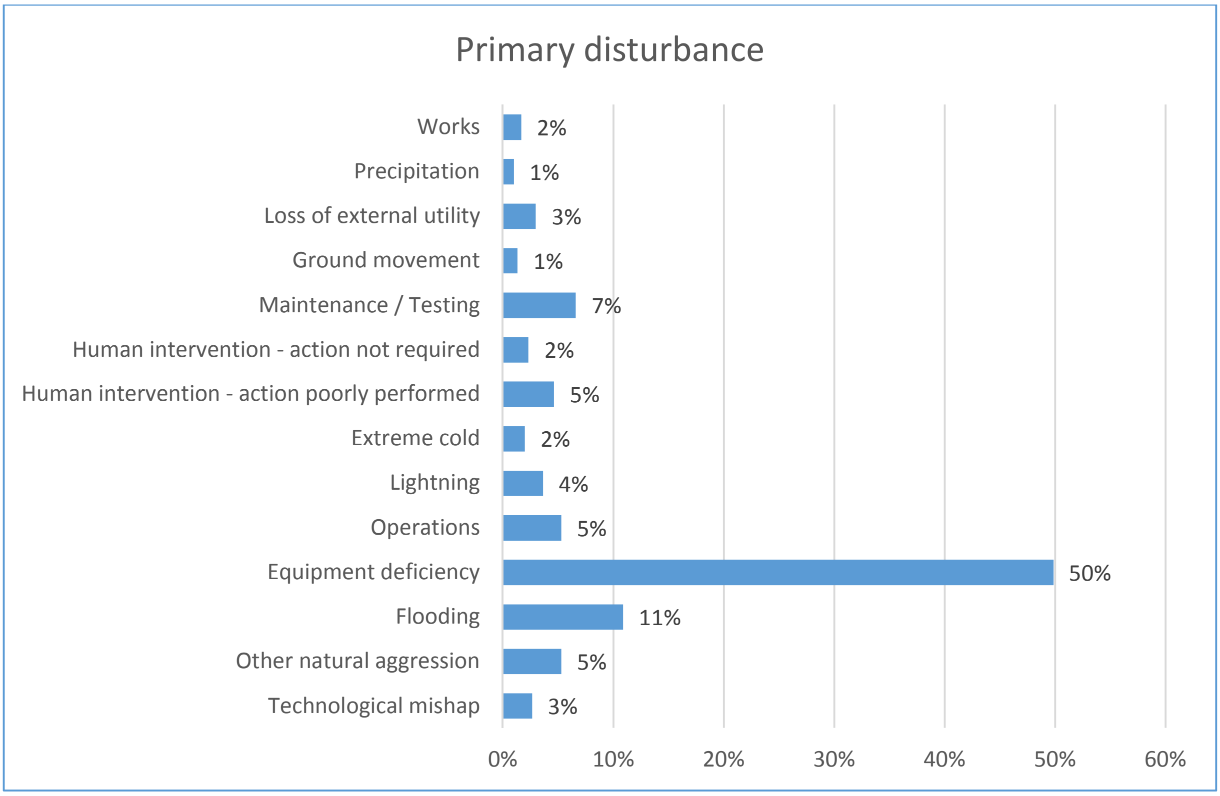


Figure 10: BETCGB base (303 events) - Disturbances linked to events correlated with the failure of hydro-mechanical devices or control systems

3. Sample events

For four recent events recorded in the ARIA base that specifically cite the area of control systems and hydro-mechanical devices, Figures 11 through 14 provide, in conjunction with the available summary, a graphical representation of the event, illustrating the analytical process aimed at showcasing the deep-rooted causes of these incidents. Let's note that the experience feedback of an event affecting operations at a class "D" dam (Fig. 13) can easily be transposed to larger dams.

3.1 ARIA 43703 - 2013 - Automated controls - Works

An outage in the 90-kV external power supply occurred at 12:30 am on a dam site. The electricity production unit automatically switched off and an alarm notified the dam operator. Due to ongoing works, the structure's vertical lift gates were locked in the closed position and the automatic (float-activated) check valve was sealed off: all flow was being discharged via the central check valve. The two position coders of the dam's central check valve, powered by the same source without a backup, had become unresponsive and the programmable controller could no longer regulate pondage.

Upon the operator's arrival around 1 am, the water level was 15 cm above the highest water level (HWL), hence reaching the zone triggering the backup controller (tripping the central check valve and gates on the locked-out valves). The operator lowered the central check valve into manual mode and, by 1:30 am, had brought the water level back to its highest normal elevation. The hydroelectric plant was subsequently restarted.

Following this accident, the risk analysis dedicated to the works phase was updated to include a systematic lowering of the central check valve at the end of each day. Moreover, the control unit assigned to hydraulic facilities requested the operator to build a comprehensive strategy applicable to its command-control system (with all devices requiring backup, common failure modes adopted across the coders and other equipment, etc.).

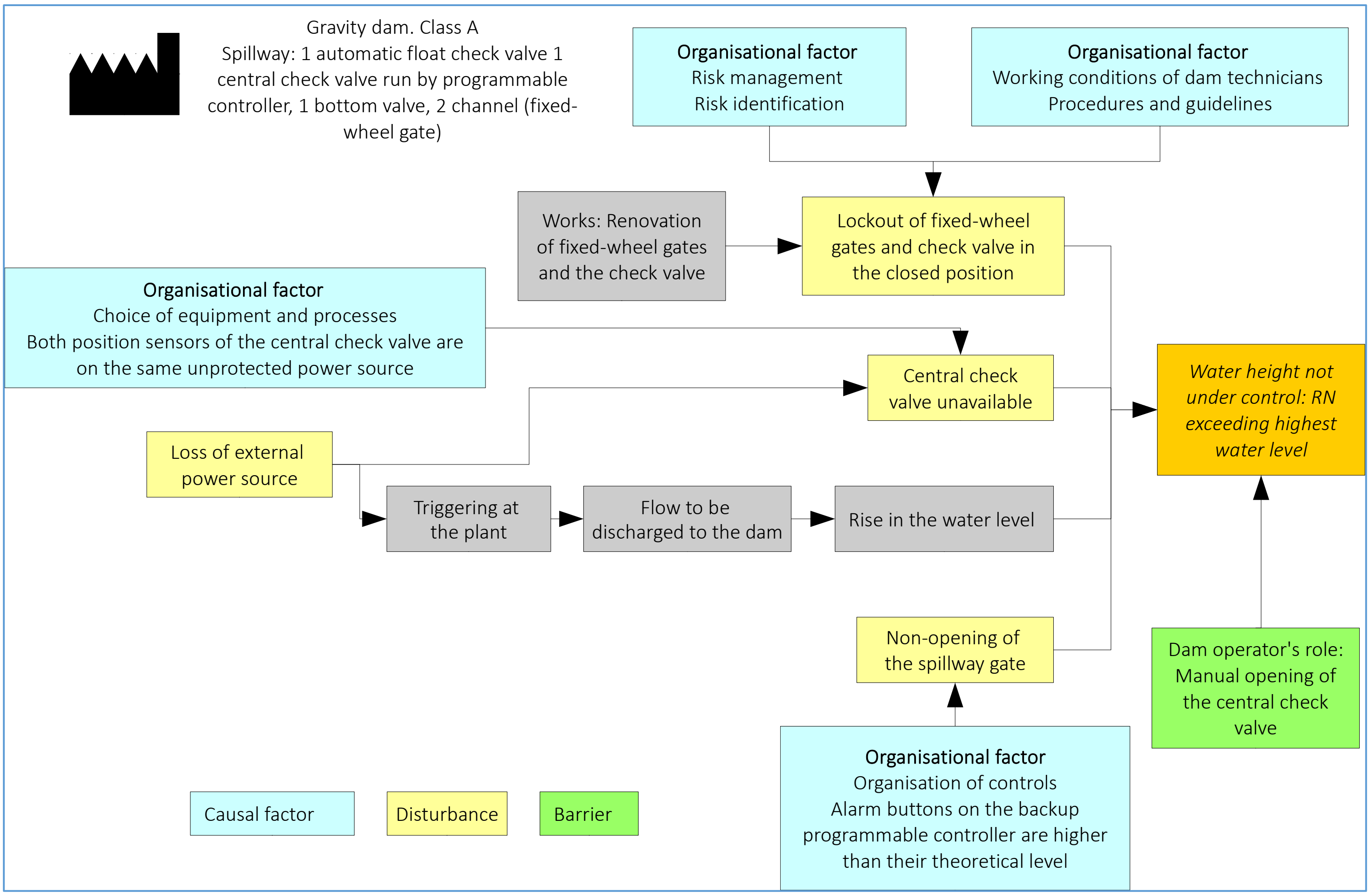


Figure 11: ARIA database record 43703

3.2 ARIA 44915 - 2014 - Automated controls - Testing

Two employees were conducting performance tests adjacent to a telecommunications cable connecting a dam to a hydroelectric plant. Poor handling had caused an outage on the dam's continuous 48-V power line and shut down the connection between programmable controllers (loss of power to the modems). The dam's main controller was neutralised, and the valves could no longer be operated. The water rose and spilled out above the dam's valves. The water level remained below the HWL mark (519.50 m, NGF reference). Notified by an alarm, an on-call technician visited the site and manually opened the valves.

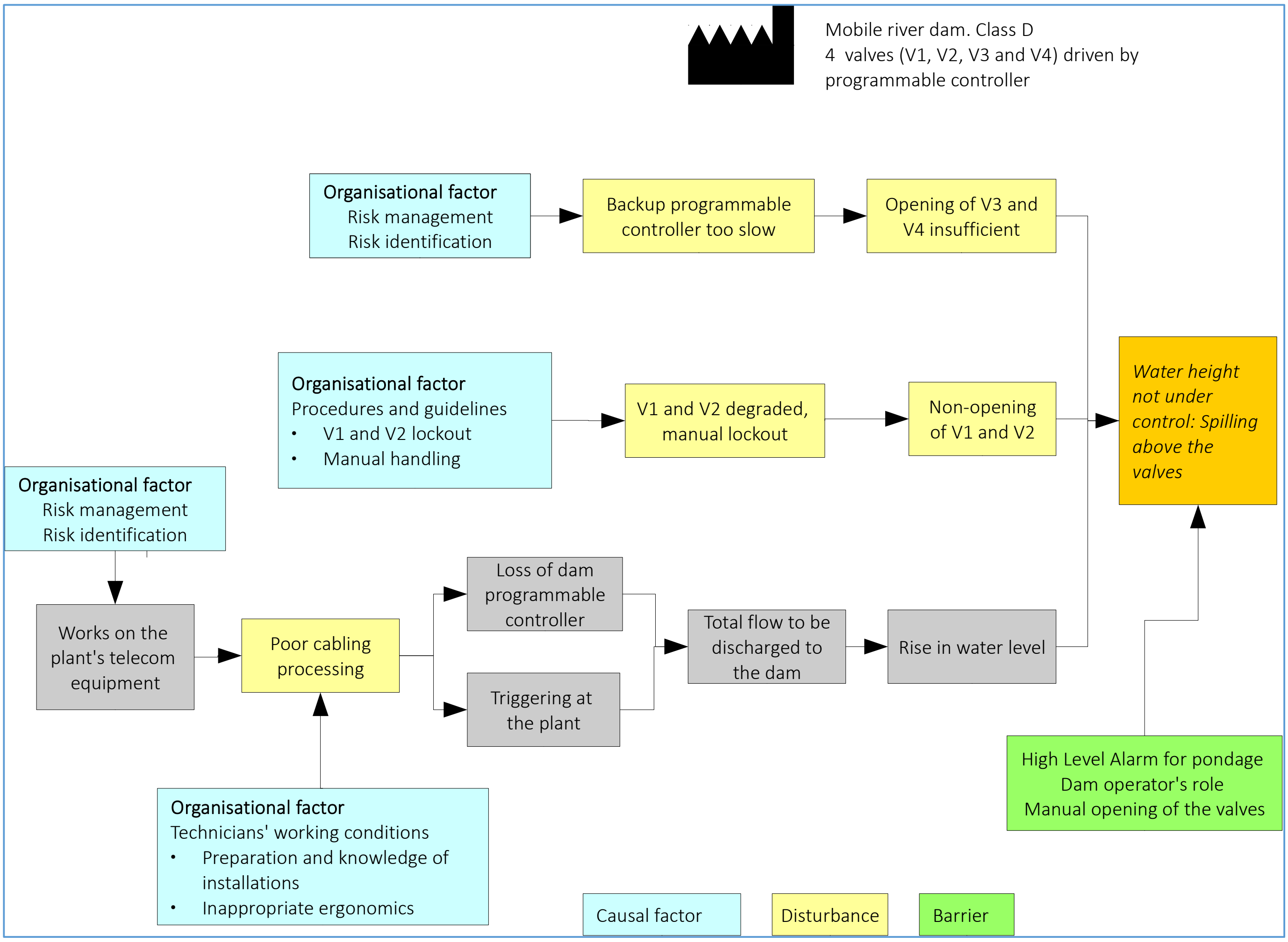


Figure 12: ARIA database record 44915

3.3 ARIA 44554 - 2013 - Automated controls - Works

While RHINE River flow was fluctuating around the saturation rate over its piped portion (i.e. Alsace's Grand Canal), a dam operator was carrying out certification tests on the facility's new programmable controller. Should the canal's saturation flow rate be exceeded, the controller was expected to route some of the water to the OLD RHINE branch by activating the flood discharge valves.

On two occasions that afternoon, the threshold requiring opening of these valves was reached. At 11:45 am, flow in the OLD RHINE suddenly jumped by 600 m^3/s, causing a 1.75 m rise in water level downstream of the dam. The valves closed again at 12:40 pm. At 3:23, a second abrupt boost to flow rate, by 470 m^3/s this time, triggered a 1.46-m rise in the downstream level. This wave endangered 3 people who had just gained access, in violation of restrictions, to a small island 300 m downstream of the dam. One of them reached the German side of the riverbank and alerted authorities. German and French rescuers searched, in relying on helicopters and divers, for the two other victims, who were found safe and sound on the French side at 5 pm. The dam operator reactivated the former regulation controller, with ensuing variations in water surges being significantly lower.

The operator's analysis pointed to organisational breakdowns in defining flow regulation settings in the new controller: the risk analysis conducted prior to this replacement focused on controlling the dam's upstream water height and failed to adequately address control measures on flow channelled into the OLD RHINE branch.

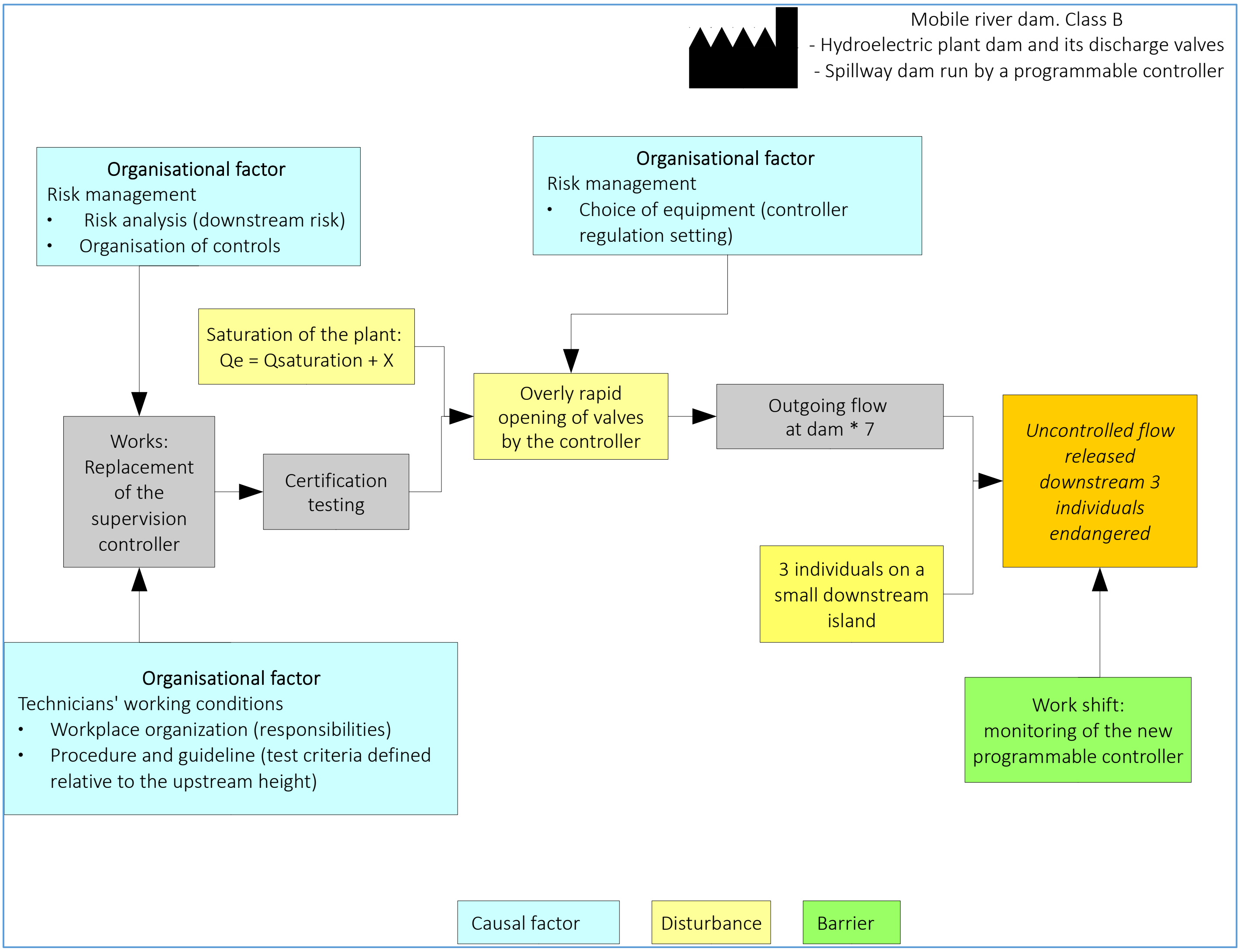


Figure 13: ARIA database record 44554

3.4 ARIA 46064 - 2014 - Valve - Flooding

During a flood episode, the automatic flood discharge check valve on a dam failed to lower. The pondage rose to 22 cm above its normal level. The origin of this malfunction was quickly identified. The entry grating of the check valve's counterweight chamber had been obstructed by leaves, and the filling of this chamber triggered the check valve opening and water discharge. The dam operator cleaned the grating, which immediately enabled lowering the valve and dropping the pondage level.

Subsequent to this event, the operator scheduled a visual inspection of this grating every autumn, i.e. during the season when water level rises and leaves fall.

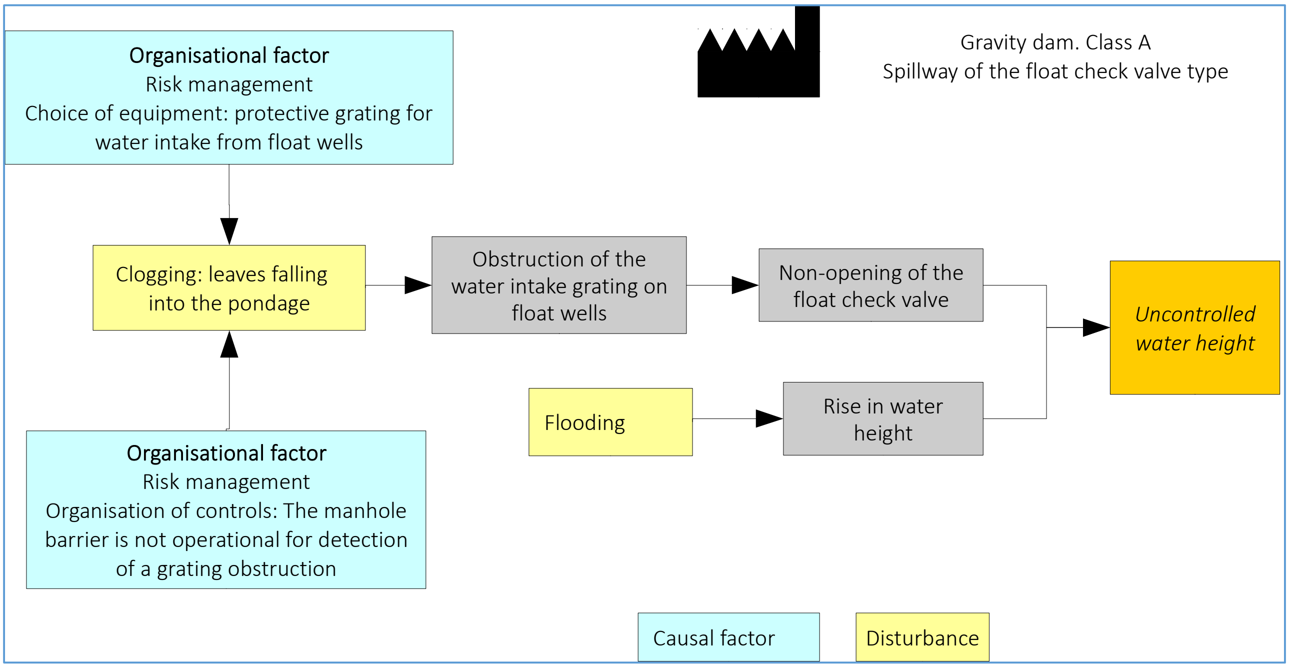


Figure 14: ARIA database record 46064

Conclusion

Implementation of the EIHS-HSP protocol has made it possible to record and document a large number of events, in turn offering valuable experience feedback. Accessible to all via the ARIA database, these events for the most part relate to the functional aspects of hydro-mechanical devices and control systems. To draw the most instruction from this body of feedback, all actors need to be involved.

For starters, the commitment from dam operators is critical. The sharing and dissemination of feedback will be even more helpful when the event has been described and analysed in fuller detail, thus providing insight on both the initial and deep-rooted causes of the various accident scenarios.

Analysing the accidents and incidents that have occurred is a key to sharing the lessons learned. The various risk prevention actors are thus in a position to better understand, act and address the potential accident scenarios applicable to each facility. Furthermore, such analysis serves to stimulate a collective drive towards instituting a safety culture and transmitting the experience acquired.

Control units also play a vital role in this effort. They must convince dam operators of the benefit gained by showing transparency regarding the lessons drawn from each accident. Their mission includes supporting the dam operator when analysing causes and defining the set of preventative and corrective measures. At its core, this strategy also emphasises positive feedback, more specifically the successful risk control measures.

APPENDICES

A.1 The EIHS and HSP regulatory framework

The collection of accident-related information in France regarding hydraulic structures did not begin solely with publication of the Ministerial order on 21 May 2010 [7]. Internal measures implemented by major facility operators also merit mention. The practical measures adopted by the administration, by virtue of the circular dated 23 July 2006, had already led to declaring EIHS for dams categorised under a concessionary regime. Subsequent to an assessment of this data collection process performed by a working group assembled by the DGPR Risk Prevention Directorate, the programme was extended to dams authorised by the 2010 order, with this legislation being broadened to encompass HSP as well.

- EIHS

The 21 May 2010 Ministerial order imposes declaring as an EIHS event any accident or incident concerning classified dams[1] "*relative to an operations-based action, the structure's intrinsic behaviour or a malfunction of one of its components, whenever such events feature at least one of the following consequences: compromised individual safety (accident, exposure to danger or difficulty); property damage (including the riverbed, riverbanks and pondage) or damage to hydraulic structures; plus for dams, modification to operating procedures or hydraulic characteristics (water level, etc.).*"

- HSP

The HSP declaration requirement, according to the definition established in the 21 May 2010 order, is stated as follows: "*Precursor events or trends capable of creating an impact in terms of hydraulic safety. Applicable herein are malfunctions tied to 'safety barrier deficiencies', as identified in a safety report, capable of deteriorating safety functions of the type that 'retain water', 'control pondage levels upstream of the structure' or 'regulate the flows released downstream'. Above all, the HSP are intended to add to the database and facilitate production and critical interpretation of the statistical accident study required in all dam safety reports.*"

HSP declarations are thus focused on communicating events that have not resulted in major consequences (hence not classified as an EIHS), yet still involve key structural components or functions for controlling risks. HSP events might entail events that, under different circumstances (e.g. accompanied by a flood), could have led to serious consequences.

Regulations have been aimed at strengthening the HSP declaration obligation by requiring production of a safety report that formalises a risk analysis for class A and B dams, while identifying for each accident scenario the corresponding safety barriers. Evaluating a sizeable number of safety reports or HSP declarations written by various authors entails great diversity when formalising risk analyses, hence when defining the notion of barrier and its composition.

[1] As intended in the decree promulgated on 11th December 2007 relative to the safety of hydraulic structures, as well as in Article R214-112 of the Environmental Code.

A.2 Lessons and perspectives drawn from the EIHS-HSP data collection campaign

This collection of events relies on a process whereby facility managers file declarations to administrative authorities, producing rankings on a risk magnitude scale, along with exchanges to allow conducting a causal analysis, which depending on event complexity may necessitate investigations by the facility manager. The feedback collection process is effectively described in Figure 1. Once the administration becomes aware of an event, a recording is input into the ARIA base by BARPI, in coordination with the BETCGB.

PSH and EIHS declaration timetables:

Events must be written up in a declaration even more quickly should the consequences prove to be more serious: immediately for red-coded EIHS; as fast as possible and no later than one week for orange EIHS; within a month for yellow EIHS. The PSH need to be declared no less frequently than once a year and are to be accompanied by a causal analysis.

A 2009 EIHS working group devised a declaration template [2] that provides the bases of event declaration and paves the way to analysing the relevant circumstances, consequences and functional fields, in addition to seeking lessons. This template is now widely used and has yielded an initial categorisation of the fundamental event circumstances and causes. The declaration immediately following an event is unable, in many cases, to set forth an adequate analysis of the event's deep-rooted causes. The first event communication step, which is basically descriptive, must therefore be accompanied by a second analytical step to establish with certainty both the initial (disturbances) and deep-rooted causes.

With respect to the EIHS declared until now, it is rare to find that subsequent analyses specifying the deep-rooted causes of an incident are also being formalised and transmitted to administrative authorities. Consequently, EIHS declarations basically remain, for the time being, descriptive and focused on the defects of installations' hardware components. The causal analysis and description of corrective measures provide material that in most cases can only be partially documented, by conveying the elements known at the time of filing the declaration. A few cases however have undergone additional analyses.

A large number of events do not directly fault the dam's hydraulic safety: such cases pertain most often to encountering personal risks as part of an installation's normal operations. This finding speaks to the history of the EIHS initiative, which was launched as a means of public communication in emergency situations and as an instructional aid regarding the hazards downstream of hydraulic installations. These events, while improving the assessment of downstream risks (i.e. a major issue relative to human safety), often merely contribute limited information in terms of accident scenarios capable of affecting the structure.

In 2015, the BETCGB analysed a collection of HSP from 2013 submitted by control unit staff. The extreme variability of the contents and events included in this analysis prevented the inclusion of all these events into the ARIA base. Generally speaking, an analysis of declarations suggests that the quality of descriptions and, even more so, of analyses has been considerably degraded in comparison with the EIHS declarations, by being confined to just the observed physical defect. Identification of the potential consequences and the most dreaded accident scenarios is not at all systematic. The scope of these declarations varies widely from one facility manager to the next, due to the divergence in interpretation of the notion of safety barrier or loss of safety barrier, as well as to the heterogeneity inherent in risk analyses conducted as part of safety reports.

Since 2010, nearly 200 EIHS have been declared. Extension of this initiative to include the set of authorised structures has not actually led to a greater number of declarations, which have remained steady in the vicinity of forty a year. The majority (54%) of declared EIHS pertain to structures run as a concession. The collection process, still in its infancy, has experienced difficulties in recirculating information; either the events have not been declared or their transmission to control authorities and then to technical support teams is still not fully operational. It is logical to infer that HSP declarations span a significantly larger number of events than the EIHS.

As regards both EIHS and HSP, the first years after the programme's launch exposed a reflex to narrow identification to just the physical causes. Inspections carried out by control technicians can provide the opportunity to further the analysis of events observed by adding robustness to experience feedback.

A.3 The "ARIA" base: Analysis, Research and Information on Accidents

The website www.aria.developpement-durable.gouv.fr offers access to BARPI's various outputs. This site also hosts the ARIA database, the core tool for harnessing experience feedback with 47,000 event entries spanning a broad spectrum of industrial activities. Both professionals and the general public alike are free to consult this base using the custom search engine. To promote information sharing, the anonymity principle is applied to all accidents listed in the various publications. Only the municipality name is communicated, so as to enable searches based on geographic criteria.

Events may be searched in the ARIA base in a number of ways. Several filters are proposed. The main filter serves to define the broadest criteria. The search proceeds by date, period or place; it is possible to focus a search on hydraulic structures by selecting this field under the "Type of event" tab. Another search criterion may be compromised hydraulic safety, by selecting this field under the "Phenomenon" tab. Once a criterion has been checked, a more precise search can be performed by selecting the "EIHS" field. This step narrows the search results to just those events associated with an EIHS declaration, as intended in the 21 May 2010 decree. The secondary filters introduce additional criteria, i.e.: keyword (found or not found) in the summary; and human, environmental or economic consequences ("consequences" tab). Moreover, it is possible to solely examine those events triggered by certain families of initial or deep-rooted causes.

The ARIA base was originally designed to collate information on industrial accidents, especially for activities falling within the classified facilities codification. To ensure generating as broad an experience feedback as possible in the field of hydraulics, the scope of ARIA's input includes events that have given rise to an EIHS or HSP declaration, as well as those satisfying the criteria and awaiting declaration. Undeclared events, e.g. occurring abroad or on a structure beyond the "Water Law" designation, that still offer applicable experience feedback have also been added.

Information sources are quite diverse. Control units focus first and foremost on accident causes from the standpoint of prevention at the source. First responders prefer a chronology of the facts and contribute valuable lessons regarding the kinetics of how a loss occurs and the response difficulties encountered. Moreover, the media's aim is to reflect society's viewpoint on the event.

References and quotes

[1] CIGB Bulletin 99 - Bulletin 109.

[2] Brandon E., Rival F. (2010). Apports de l'analyse des événements importants pour la sureté hydraulique (EISH) dans les études de dangers de barrages. *CFBR / AFEID Symposium: "Dam Safety Report Practices*", 28-29 November 2011, Lyon.

[3] Laloux S., Castel Y., Boubée D. (2011), Analyse de risques : Comment faire quand la statistique ne suffit plus, *CFBR / AFEID Symposium: "Dam Safety Report Practices*", 28-29 November 2011, Lyon.

[4] Lewin J., Ballard G., Bowles D.S. (2003) Spillway gate reliability in the context of overall dam failure risk. *USSD Annual Lecture 2003*.

[5] Dam Safety Committee, New South Wales - Reliability of spillway flow control systems - June 2010.

[6] Eury S-P., Rival F., Robache A. (2014). ARIA 3 : Identifier les causes profondes des accidents industriels par une modélisation graphique. *J. Math. Phys, 33, 308-330*.

[7] Ministerial order promulgated 21 May 2010 defining the scale of risk magnitude for events or trends relative to dams or dykes or their operations, and jeopardising or potentially jeopardising the safety of people or property, and stipulating the conditions for their déclaration; French Republic Official Journal, issued dated 11 June 2010.

[8] Deroo L., Jimenez B., Note sur l'accidentologie des barrages poids. *CFBR / AFEID Symposium: "Dam Safety Report Practices*", 28-29 November 2011, Lyon.

[9] Fry J.J., Couriveau J.R., Lévèque L. (2015), Typologie des incidents d'érosion interne dans les fondations de barrage. *CFBR*.

[10] Bister D. (1998), Synthèse du groupe de travail CFGB sur la sécurité des barrages et évacuateurs en service lors des crues. *CFGB Symposium*, 1998.

[11] Feuillas D., Fiabilisation des évacuateurs de crues (EVC) du parc de la CNR, *CFBR-SHF Symposium: "Design and operations of Spillway Gates*", 20-21 January 2009, Lyon.

[12] Cottin L. (2009), Les évacuateurs de crues des barrages hydroélectriques concédés ; vue synthétique du parc (2009), *CFBR-SHF Symposium: "Design and operations of Spillway Gates*", 20-21 January 2009, Lyon.

[13] Bulletin ICSI issue no. 2014 04 : FHOS l'analyse approfondie d'évènement. Working group on "Improving the incident analysis process" - Les Cahiers de la Sécurité Industrielle

[14] Prevot G., Schriqui C., Cloix R., Dieudonné S., Mériaux P., La vantellerie et le contrôle commande dans les livrables réglementaires : la vision des services de contrôles et de leur appui technique, *CFBR Symposium: "Gates, control systems, telecommunications and power supply for safer dams"*, 2-3 December 2015, Chambery.

[15] Gastaud C., Gauthier A., Enseignements tirés des événements importants pour la sûreté hydraulique (EISH) et éléments de retour d'expérience (REX) sur les organes hydromécaniques et de contrôle commande des barrages, *CFBR Symposium: "Gates, control systems, telecommunications and power supply for safer dams"*, 2-3 December 2015, Chambery.

TECHNOLOGICAL ACCIDENTS ONLINE

Safety and transparency are two legitimate demands being imposed by our society.

As such, since June 2001, the website www.aria.developpement-durable.gouv.fr hosted by the Ministry of the Environment, Energy and the See has been proposing to both professionals and the general public many lessons drawn from analyses of technological accidents. The main headings of this site are presented in both French and English.

Under the general headings, site visitors have the opportunity to: consult a plethora of information, e.g. on governmental action; access extensive extracts from the ARIA base; and discover the presentation of the European scale of industrial accidents; learn about the index relative to hazardous substances released in order to complement "on-the-spot reporting" in the event of an accident or incident. The description of accidents, as the raw material of any feedback-driven approach, makes up a significant portion of the site's resources: event sequencing, consequences, sources, circumstances, identified or assumed causes, actions taken, and lessons learned.

Some 100 detailed and illustrated technical datasheets present the accidents selected to benefit from their lessons. Many analyses by theme or industrial sector are also available. The heading dedicated to technical recommendations is broken down by various topics, e.g.: fine chemistry, pyrotechnics, surface treatment, silos, tyre warehouses, hot work permitting, waste processing, and material handling.

A multicriteria search pulls up information on accidents that occurred in France or abroad. The site www.aria.developpement-durable.gouv.fr is continually being expanded. For now, some 47,000 accident entries appear online, while new thematic analyses are regularly uploaded.

The summaries of all events presented are available on the following website:
www.aria.developpement-durable.gouv.fr

BARPI (Bureau of Risk and Industrial Pollution Analysis)
5 place Jules Ferry
69006 Lyon
Phone: +33 (0)4 26 28 62 00

BETCGB (Bureau of the Technical and Control Committee on Large Dams)
44 avenue Marcelin Berthelot
38030 Grenoble Cedex 02
Phone: +33 (0)4 78 62 50 50

Department of Technological Risks
Division of Natural and Hydraulic Risks
Risk Prevention Directorate
Ministry of the Environment, Energy and the See
Tour Sequoia
92055 La Défense Cedex
Phone: +33 (0)1 40 81 21 22

Coordination:
Annie NORMAND, Christian VEIDIG (BARPI)
Authors:
Clément GASTAUD (BETCGB)
Annelaure GAUTHIER (BARPI)

Picture credits: BETCGB

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère
de l'Environnement,
de l'Énergie
et de la Mer