Assessment of the Probabilities of Failures and Dam Reliability

Frédéric Laugier (EDF) and Laurent Peyras (INRAE)

INRAE
EDF

Principles and steps of a Risk Analysis Study

❶ Functional Analysis

⇒ Determination of the functions of a dam and of their components

❷ Failure Modes Analysis

⇒ Determination of the failure modes of dam components

❸ Modeling the failure scenarios

⇒ Connexion of the failure modes

❹ Assessment of the Risk

⇒ Determination of the probability of the scenarios and their consequences

❺ Risk Reduction

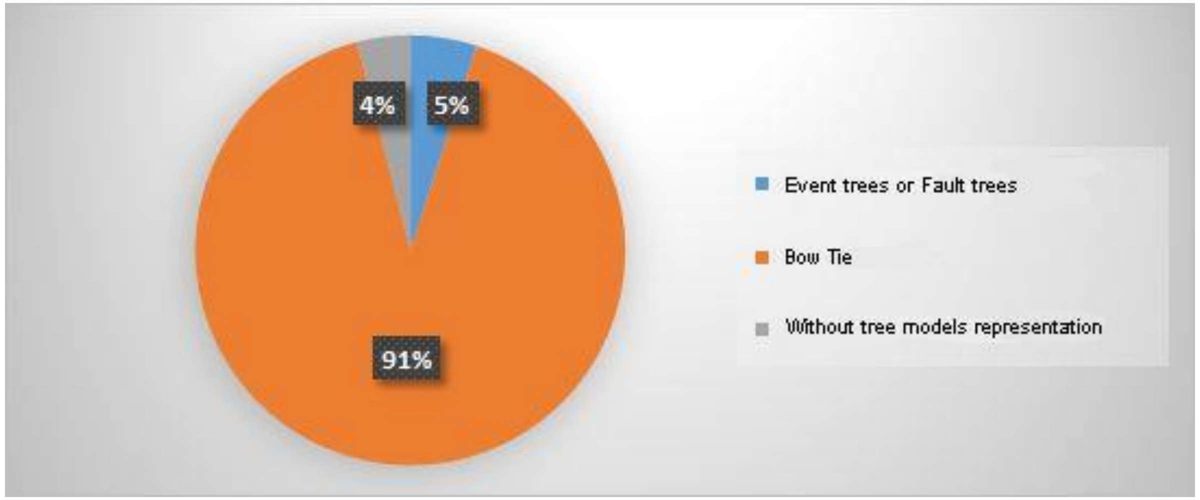
INRAE

EDF

Cfbr comité français des barrages et réservoirs

Assessment of the probabilities for the failure scenarios

- For a Quantitative assessment
  - ETA: Event Tree Analysis Method
- For a Semi Quantitative assessment
  - FTA: Fault Tree Analysis Method
  - BTA: Bow Tie Analysis Method



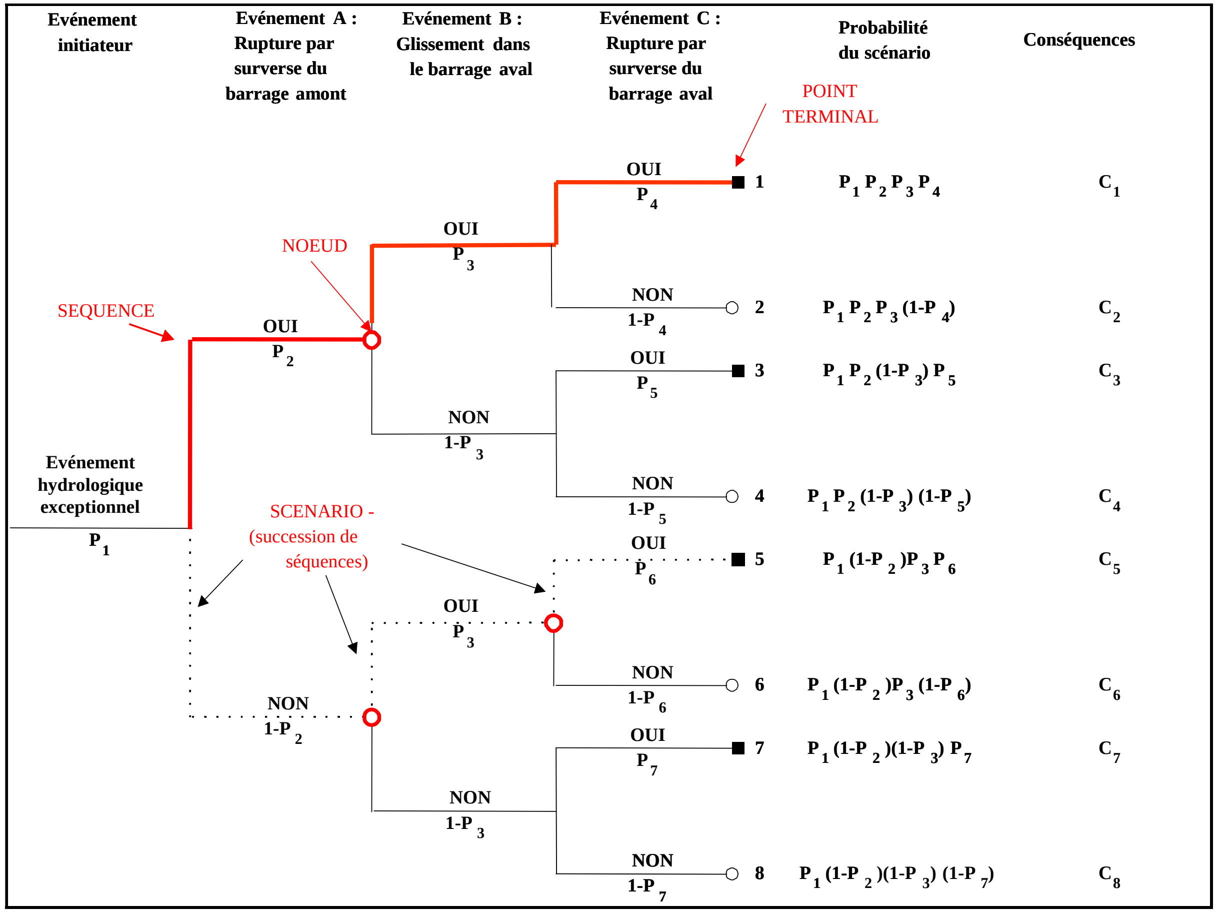
Assessment of the probabilities for the failure scenarios

- For a Quantitative assessment
  - ETA: Event Tree Analysis Method

- For a Semi Quantitative assessment
  - FTA: Fault Tree Analysis Method
  - BTA: Bow Tie Analysis Method

Quantitative Assessment with ETA

- Principles:
  - Determine the probabilities for each failure modes of the Event Tree considered
  - By multiplication of the elementary probabilities, determining the global probability of the scenario/ETA



$P_1 = P(IE)$

$P_2 = P(A \mid IE)$

$P_3 = P(B \mid A \text{ and } IE)$

$P_4 = P(C \mid B \text{ and } A \text{ and } IE)$

$P_{scenario} = P_1 \times P_2 \times P_3 \times P_4$

Failure Modes Probabilities Assessment

- Three ways to assess Failure Modes Probabilities:
  - Probabilistic assessment:
    - For natural hazards as Floods, Hydrology, Earthquakes
    - The intensity of the natural hazard action is linked to a probability
  - Frequency assessment:
    - Technological Failure Modes can be linked to frequencies
  - Expert Judgment Assessment:
    - Used when Probabilistic and Frequency assessments are not possible

Probabilistic Assessment

- Assessment of Natural Hazards:
  - Probabilistic Models for Hydrology: Intensity of Floods matches with annual probabilities
    - *Example*:
    - Design Flood for Dam: 1’000 years flood to 10’000 years flood depending on the size of the dam
  - Probabilistic Models for Earthquakes: Intensity of Earthquakes matches with annual probabilities
    - *Examples*:
    - Annual probability for Operating Basic Earthquake:
➔ 475 years earthquake
    - Annual probability for Maximum Design Earthquake:
➔ 5’000 years earthquake

Frequency assessment

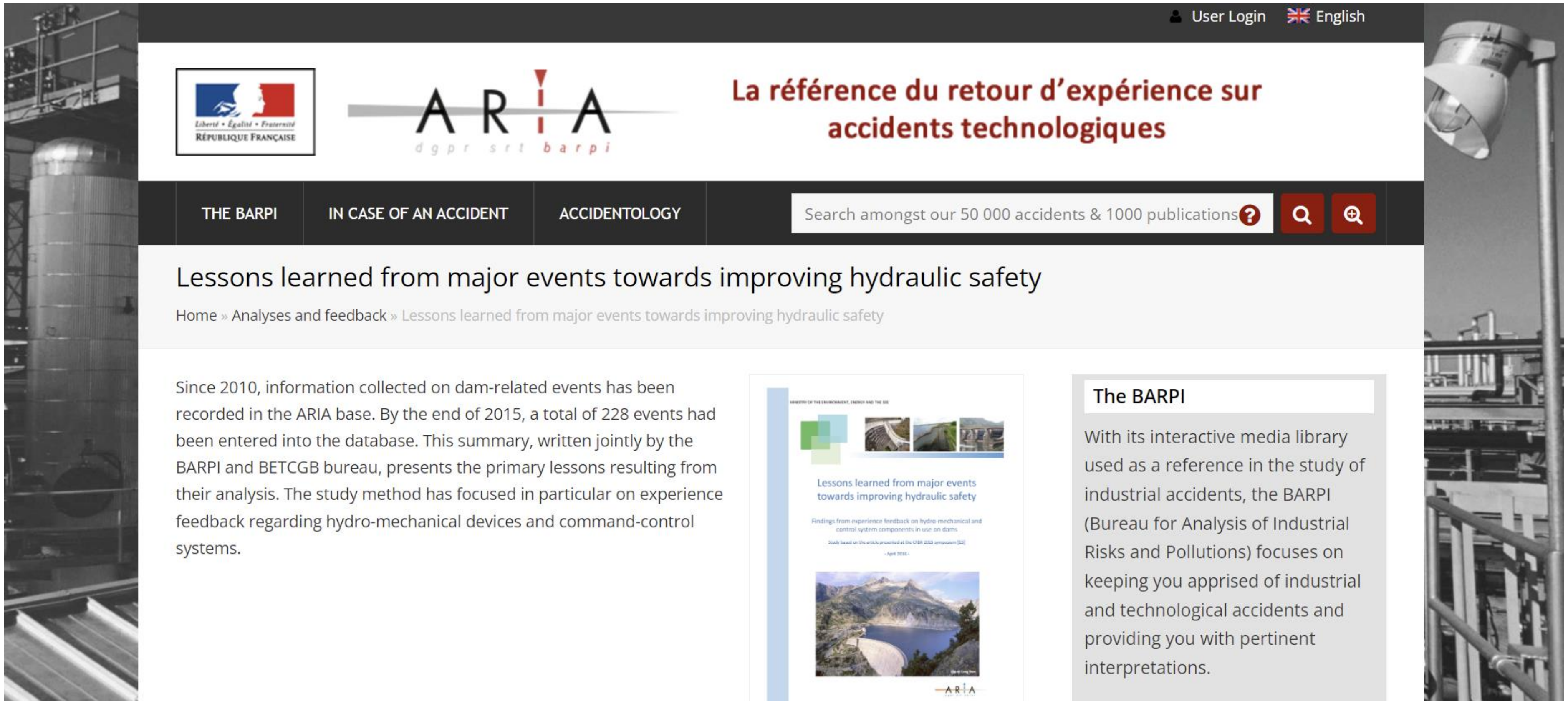
- Principle: assess the frequencies of the failure modes of the components, supported by feedback

➔ Rate of Failure = $\dfrac{\text{Number of Failures of a Component}}{\text{Number of utilization of this component}}$

- Components concerned
  - Electro-mechanical systems: gates, outlet, emergency commands
  - Monitoring systems
  - Human failures

Frequency assessment

- Frequency assessment based on feedback – Interest to use specific database
  - French Ministry of Environment database on incidents/accidents – *ARIA Database*
  - Operators have to declare all the incidents/accidents related to their dam

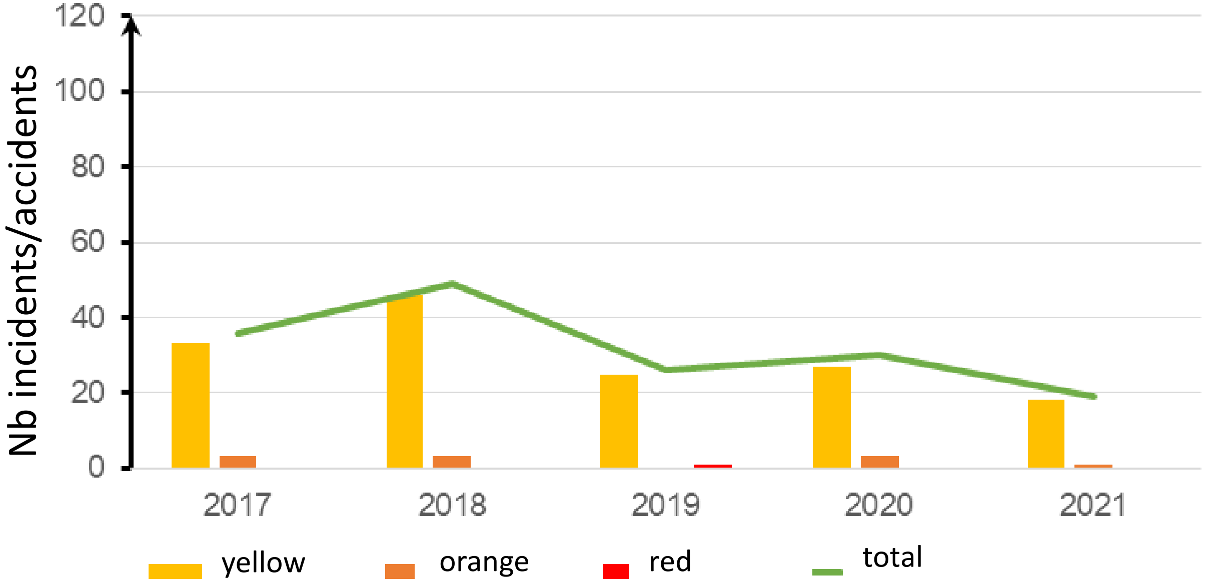


https://www.aria.developpement-durable.gouv.fr/le-barpi/la-base-de-donnees-aria/

comité français des **barrages** et **réservoirs**

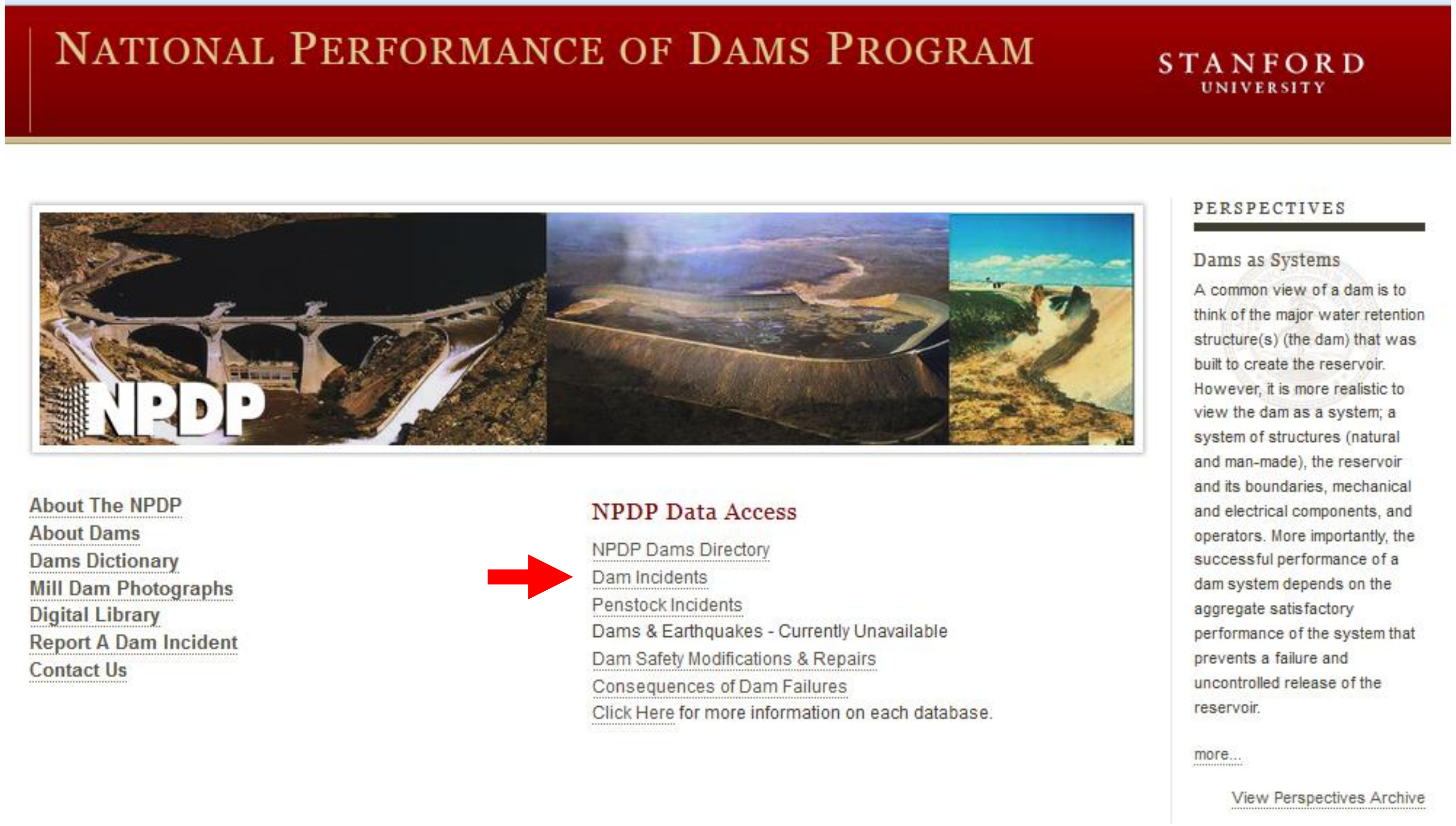
Frequency assessment

- Frequency assessment based on feedback – Interest to use specific database
  - 3 levels of incidents/accidents depending on the severity
    - **RED:** death or serious injury to persons - Major damage to hydraulic structures
    - **ORANGE:** endangering people without sustaining serious injuries - Significant damage to hydraulic structures
    - YELLOW: causing difficulties for people or minor damage outside the installation
  - Some frequency data can be available for some failure modes of dam components



Frequency assessment

- Frequency assessment based on feedback – Interest to use specific database
  - Major operators and owners have often their own database on incidents in France
  - NPDP: National Performance of Dams Program – Standford University



http://npdp.stanford.edu/

INRAE
EDF
Cfbr comité français des barrages et réservoirs

Expert Judgment based Assessment

- Principle: some failure modes cannot be assessed by probabilistic analysis or frequency analysis
because probabilistic laws or data are not available

➔ probabilities assessment based on expert judgment

- Specific Working Group to provide probabilities assessment based on expert judgment
  - Engineers of various disciplines: Civil Engineering, Hydrology, Hydraulic, electromecanic
  - The operator and the owner of the dam
  - Working group leaded by an risk analysis engineer or an risk analysis analyst

Expert Judgment based Assessment

- Specific Tables based on Expert Judgment to assess probabilities
- Expert Judgment non correct to assess very low probabilities ($< 10^{-3}$)

Verbal Description	Probability Equivalent	Low	High
virtually impossible	0.01	0.00	0.05
very unlikely	0.10	0.02	0.15
unlikely	0.15	0.04	0.45
fairly unlikely, rather unlikely	0.25	0.02	0.75
fair chance, toss-up	0.50	0.25	0.85
usually, good chance, probable, likely	0.75	0.25	0.95
quite likely	0.80	0.30	0.99
very likely, very probably	0.90	0.75	0.99
virtually certain	0.99	0.90	1.00

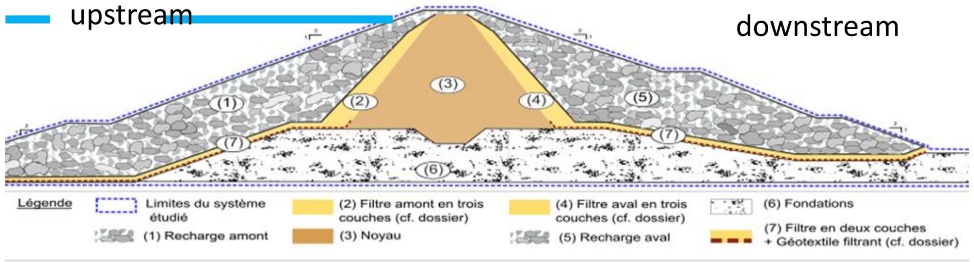
[Vick 1997]

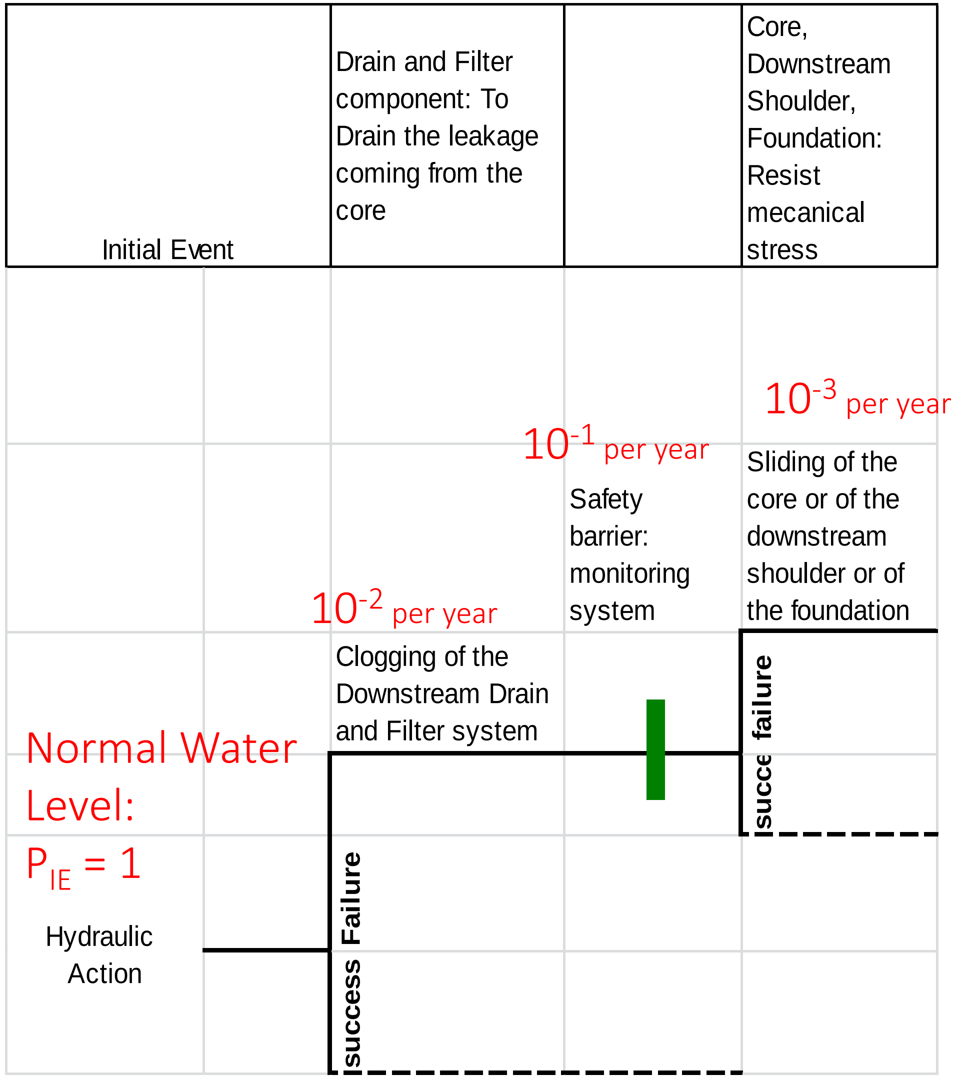
Appréciation experte de la probabilité d'occurrence	Traitement quantitatif des dires d'experts
« très probable »	0,60
« probable »	0,40
« moyennement probable »	0,20
« peu probable »	0,10
« très peu probable »	0,01
« extrêmement peu probable »	0,001

[INRAE 2010]

Example 1: Quantitative Assessment with ETA

Scenario of increase of pore pressure in the core or in the foundation in an embankment dam - Clogging of the filter





Total scenario:

$P = 10^{-6}$ per year

➔ Completely impossible

Example 2: Quantitative Assessment with ETA

Scenario of overtopping linked to inadequate hydraulic capacity

Initiating Event		Spillway : Pass the flood Ti	Downstream fill : Resist external erosion	Probabilities Consequences
			1/10	Probability : **p=10^{-6}** Flood wave : 2 500 m^3/s
		1/10	Erosion of downstream fill : Creation of breach around spillway chute	
1/10 000		Failure of spillway system : loss (or unsufficiency) of spillway capacity		
Flood Ti				

Total scenario:
P = 10^{-6} per year

➔ Completely impossible

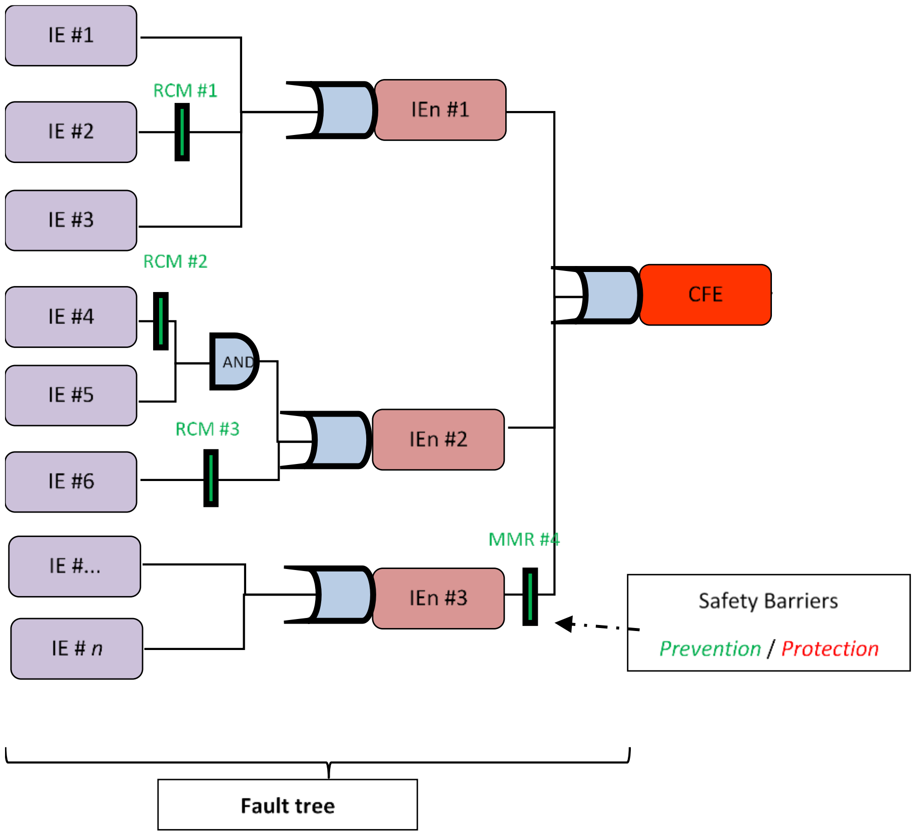
Assessment of the probabilities for the failure scenarios

- For a Quantitative assessment
  - ETA: Event Tree Analysis Method

- For a Semi Quantitative assessment
  - FTA: Fault Tree Analysis Method
  - BTA: Bow Tie Analysis Method

Semi-Quantitative Assessment with Fault Tree Analysis or the Bow Tie Analysis

to estimate the annual probability of occurrence of the feared event or final event of a Fault Tree / Bow Tie tree



Input Data Necessary for the semi-quantitative assesssment

1. Initial Event: IE

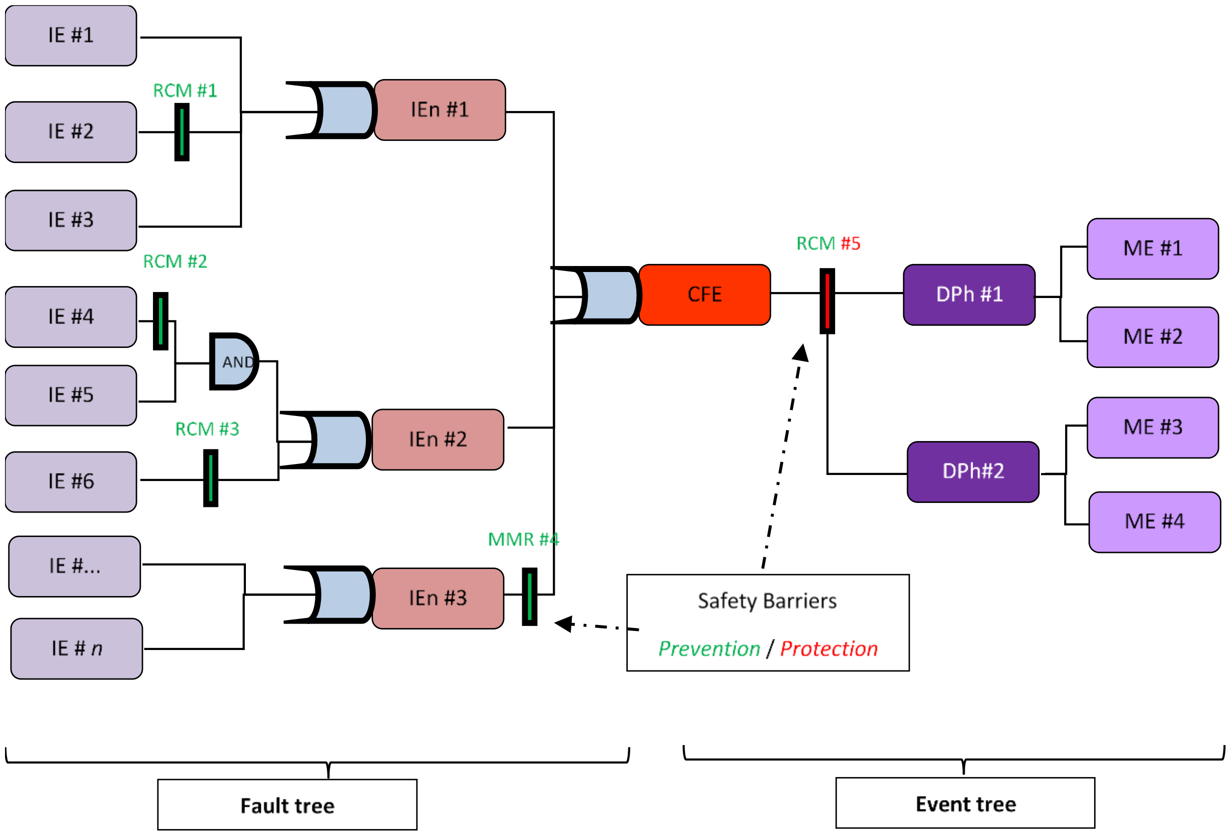
2. Safety Barriers or Risk Control Measure: RCM (prevention/Protection)

3. Intermediate Event: EIn

➔ *4. Central Feared Event of Final Event: CFE*

Semi-Quantitative Assessment with Fault Tree Analysis or the Bow Tie Analysis

to estimate the annual probability of occurrence of the feared event or final event of a Fault Tree / Bow Tie tree



Input Data Necessary for the semi-quantitative assesssment

1. Initial Event: IE

2. Safety Barriers or Risk Control Measure: RCM (prevention/Protection)

3. Intermediate Event: EIn

➔ *4. Central Feared Event of Final Event: CFE*

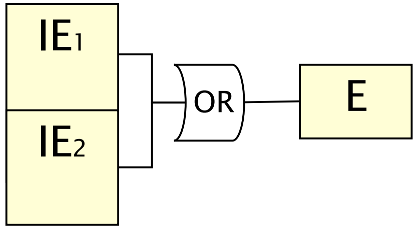
Semi-quantitative analysis of probabilities

French Practice – Regulation of october 2005

Probability Scale	**E**	**D**	**C**	**B**	**A**
Qualitative (if number of installations and feedback are sufficient)	"Possible event, but extremely improbables : *is not impossible considering current knowledge, but not experienced worldwide during a large number of installation.years*	"very improbables event": *already occured in the industry sector, but corrective actions were taken which significantly reduced the probability of occurrence*	"improbables event": *similar event already occured in the industry sector or in this type or organization worldwide, but no corrective actions were taken which significantly reduced the probability of occurrence*	"probables event": *already occured or can occur during life duration of the installation*	"current event": *already occured or can occur several times during life duration of the installation, in spite of risk reduction measures*
Semi-quantitative	This scale is intermediate between qualitative and quantitative scales, and enables to take into account risk reduction measures				
Quantitative (by unit and by year)	10^{-5}	10^{-4}	10^{-3}	10^{-2}	

Aggregation Rules for semi-quantitative assessment with FTA or BTA

GATE « OR »



Two Independent Events IE $_{1\ \text{or}\ 2}$

- **Quantitative Analysis**

$$E_{\text{gate OR}} = \sum_{i=1}^{n} IE_i$$

Total probability is the sum of the individual probabilities of the independent events

- **Semi-Quantitative Analysis**

Probability Class (E) ~ minimum (probability class (IE_1), probability class (IE_2))

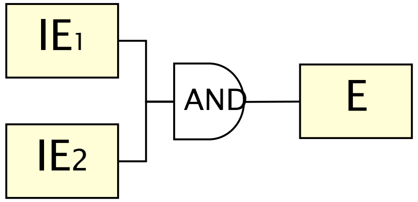
OR	A	B	C	D	E
A	A	A	A	A	A
B	A	B	B	B	B
C	A	**B**	C	C	C
D	A	B	C	D	D
E	A	B	C	D	E

➔ *the lowest occurrence prevails according to the matrix*

➔ *Note that aggregation rules are not imposed by the Authorities*
This table is an example of what could be used based on existing recommandations for the industry sector (Ineris)

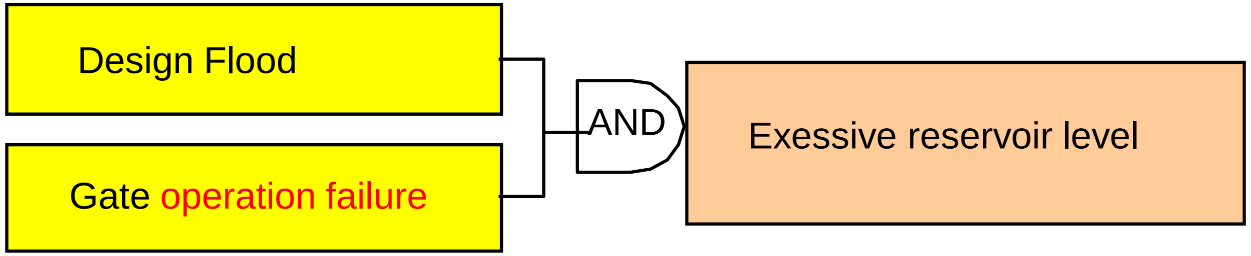
Aggregation Rules for semi-quantitative assessment with FTA or BTA

GATE« AND »



Two Independent Events IE $_{1 \text{ or } 2}$

Example:



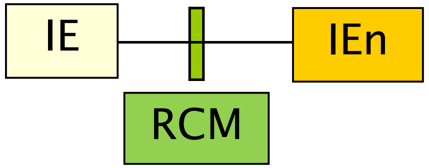
- **Quantitative Analysis** Prob. (E) = Prob. (IE_1) x Prob. (IE_2)
- **Semi-Quantitative Analysis** Probability Class (E) ~ minimum (probability class (IE1), Probability class (IE2)) – 1. class

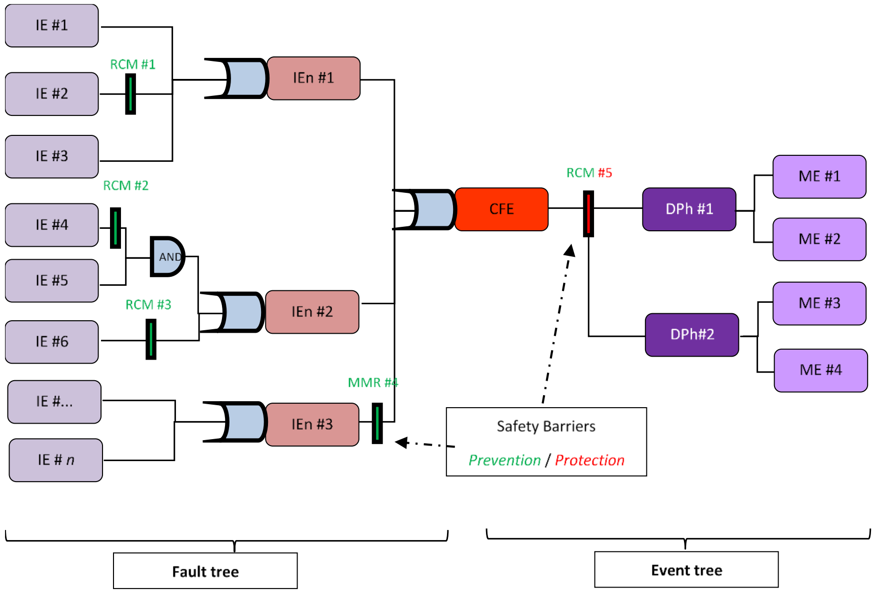
AND	A	B	C	D	E
A	B	C	D	E	E
B	C	C	D	E	E
C	D	**D**	D	E	E
D	E	E	E	E	E
E	E	E	E	E	E

➔ *Note that aggregation rules are not imposed by the Authorities*
This table is an example of what could be used based on existing recommandations for the industry sector (Ineris)

Rules for semi-quantitative assessment with FTA or BTA

Prevention Safety Barriers or Risk Control Measure (RCM) applied to an Intermediate Event



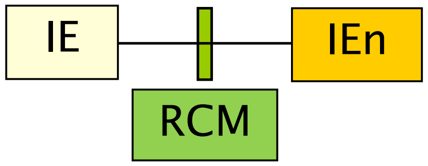


- ❑ Safety Barriers or Risk Control Measure: taking into account with a Level of Confidence (LC)
  - ❑ Prevention barrier
  - ❑ Protection barrier
- ❑ Level of Confidence ⇔ risk reduction factor
  LC/RRF are discrete for Semi-Quantitative Analysis or continuous for Quantitative Analysis

INRAE
EDF

Rules for semi-quantitative assessment with FTA or BTA

Safety Barriers or Risk Control Measure (RMC) :



=> Criterias to be observed

- **Independence** with the event and with the other barriers carrying out the same safety function.

  Example: if the event under assessment is "operator error", the operator cannot be a barrier. On the other hand, a second operator acting as a controller (= control task) would be able to catch the drift and be considered as a barrier

- **Effectiveness** of the barrier

  => depends on many parameters and to assess it, we study its design, availability, accessibility and resistance to specific constraints, etc.

- **Response time,** when this is relevant

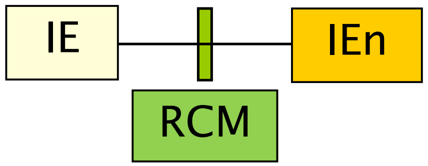
  (for example, it takes into account gate opening times, the time it takes an operator to reach the site, etc.). It must match the kinetics of the event on which the barrier is meant to act

- **Testability/maintainability** for technical barriers

  including training/audit/exercises for human barriers.

Rules for semi-quantitative assessment with FTA or BTA

Safety Barriers or Risk Control Measure (RMC) applied to an Intermediate Event



- **Quantitative Analysis** Prob. (IEn) = Prob. (IE) x Prob. (RMC | IE)

- **Semi-Quantitative Analysis** Probability Class (IEn) = Probability Class (IE)+ LC (LC =1 or 2)

LC = Level of Confidence ⇔ risk reduction factor

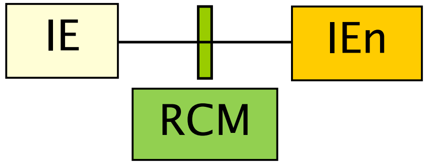
LC are discrete for Semi-Quantitative Analysis
=> from level "1" (lowest level) to level"2" (highest level)
LC determine a risk reduction factor (1 : 1/10, 2 : 1/100)

➔ *Most of the time LC=1 is chosen*

INRAE
EDF

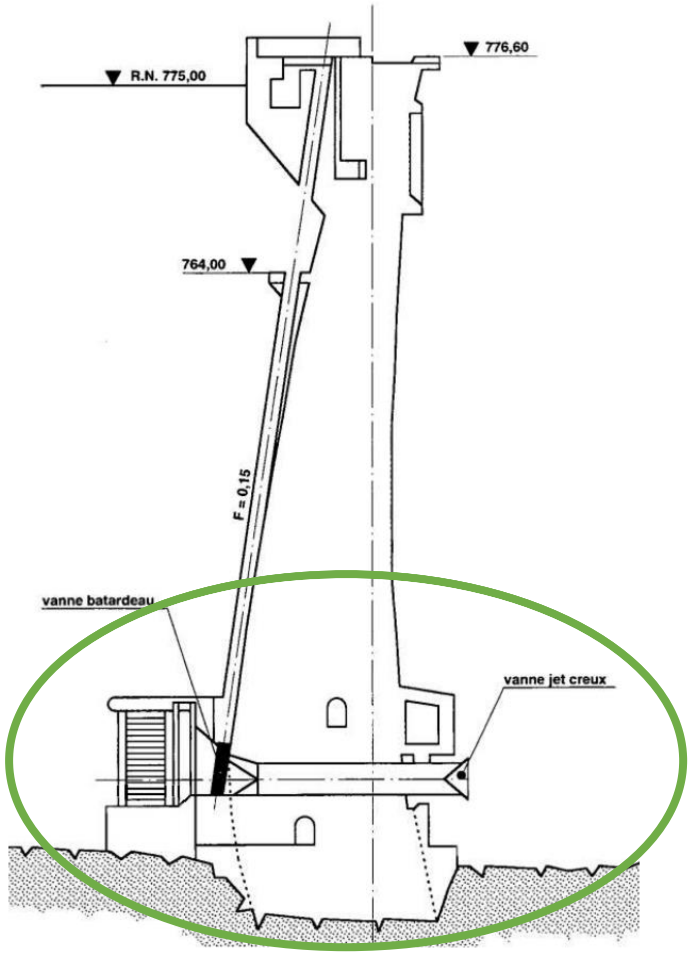
Rules for semi-quantitative assessment with FTA or BTA

Examples of Safety Barriers or Risk Control Measure (RMC) applied to an Intermediate Event



- **Decreasing Réservoirs Safety level**

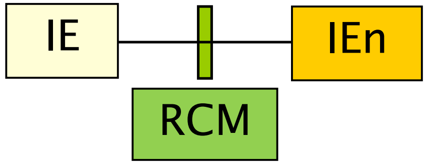
Using Bottom Outlets



INRAE
EDF

Rules for semi-quantitative assessment with FTA or BTA

Examples of Safety Barriers or Risk Control Measure (RMC) applied to an Intermediate Event



- **Human operation (repair)**

  In case of Scada/automation misoperation

- **Use of emergency energy supply**

  In case of electrical supply failure (general and back up)

Rules for semi-quantitative assessment with FTA or BTA

Particular case – Taking into account the human factor

Two families of events linked to human factor :

- Inappropriate actions
  - A clearly identified deviation, error of interpretation or execution,
  - Or an omission on the part of an individual (or a team)
    that occurs in the context of an activity and a given work situation
  - Includes non-technical factors (organizational, social, human, contextual, individual or collective)
  - Assessing 4 criteria that are questioned separately: [LAROUZEE 2015]
    - The operators' skill
    - The complexity of the task to be accomplished
    - The work situation (conditions for carrying out an operation)
    - The capacity for auto-correction

INRAE
EDF

Rules for semi-quantitative assessment with FTA or BTA

Particular case – Taking into account the human factor

Two families of events linked to human factor :

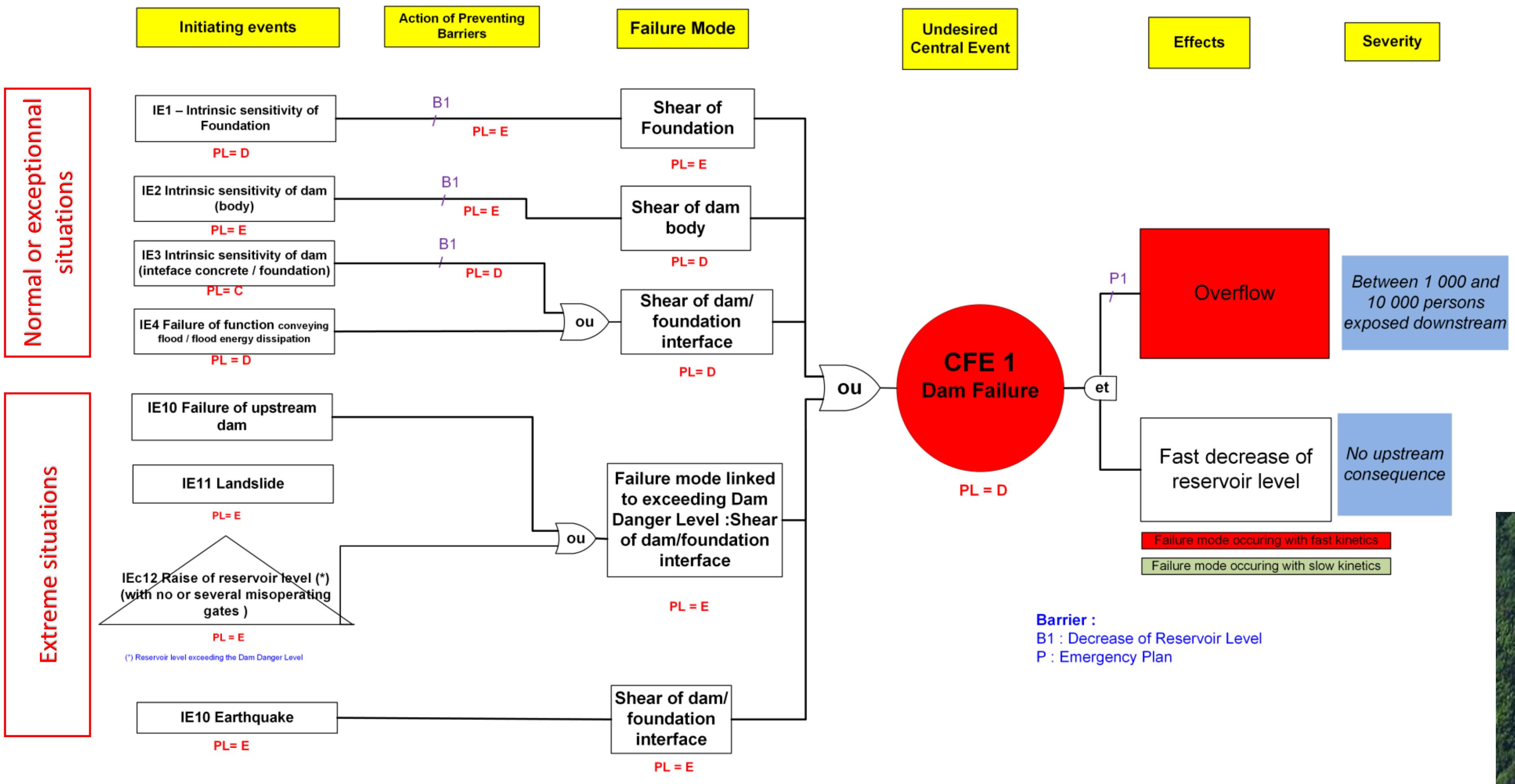
- Inappropriate actions
  - ➢ A clearly identified deviation, error of interpretation or execution,
  - ➢ Or an omission on the part of an individual (or a team)

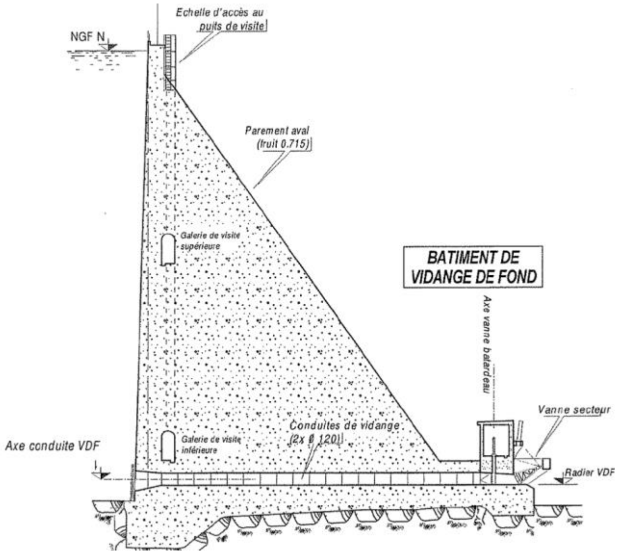
    that occurs in the context of an activity and a given work situation
  - ➢ Includes non-technical factors (organizational, social, human, contextual, individual or collective)
  - ➢ Assessing 4 criteria that are questioned separately: [LAROUZEE 2015]
    - The operators' skill
    - The complexity of the task to be accomplished
    - The work situation (conditions for carrying out an operation)
    - The capacity for auto-correction
- Human failure
  - ➢ Unintentional interruption of an activity that is in progress or expected, linked to the "intrinsic reliability" of one or several participants
  - ➢ Generally considered independent of the organization

    For example: fainting, traffic accident..

Example 1: Semi-Quantitative Assessment with BTA

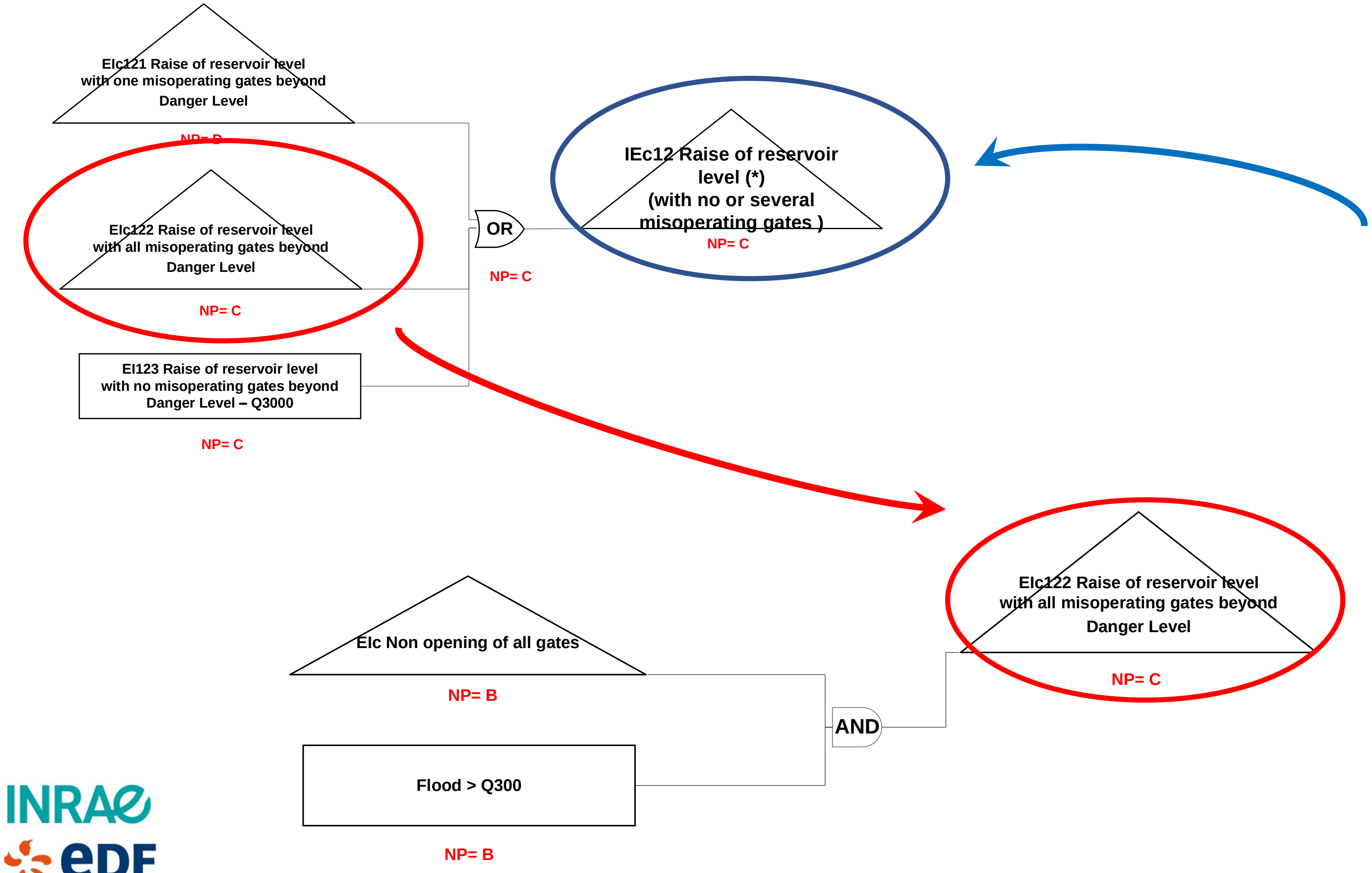
Scenarios leading to the Central Feared Event “Dam Failure” for a gravity dam

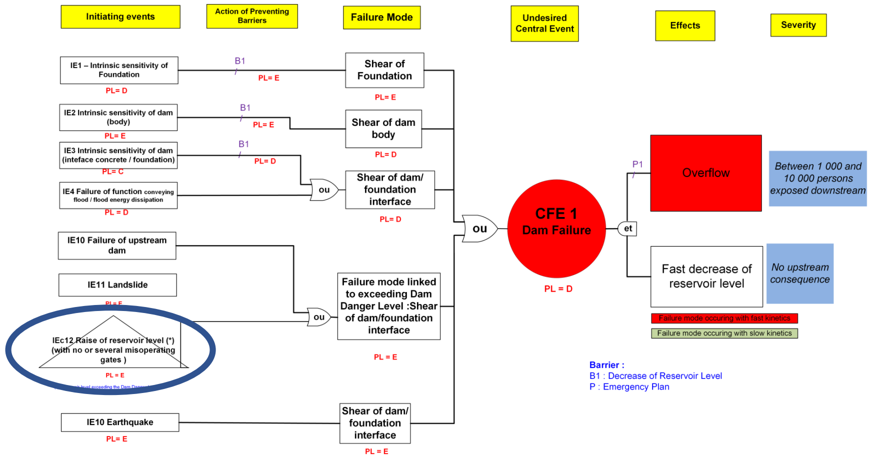




Example 1: Semi-Quantitative Assessment with BTA

Scenarios leading to the Central Feared Event “Dam Failure” for a gravity dam

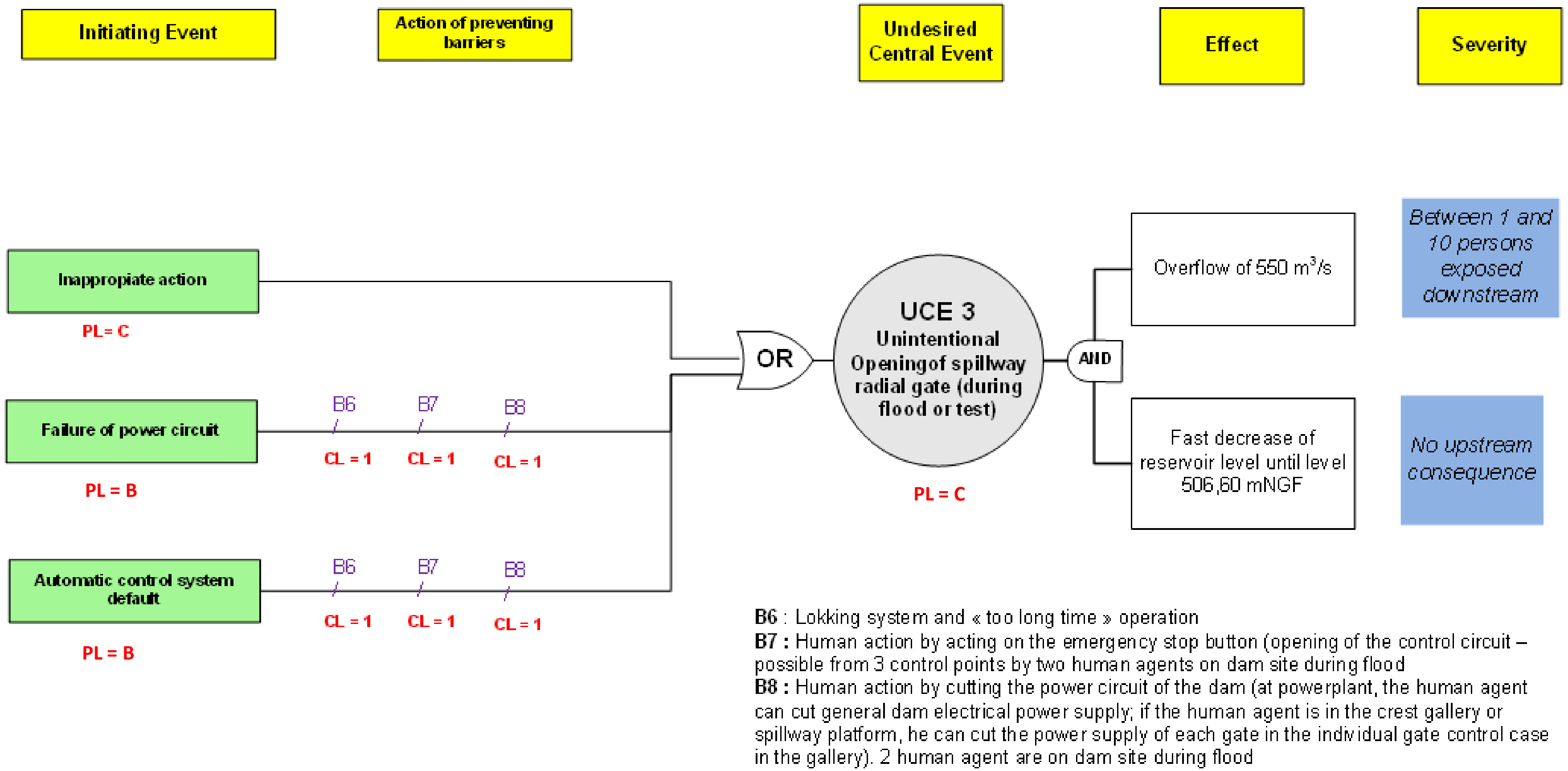




INRAE
EDF

Example 2: Semi-Quantitative Assessment with BTA

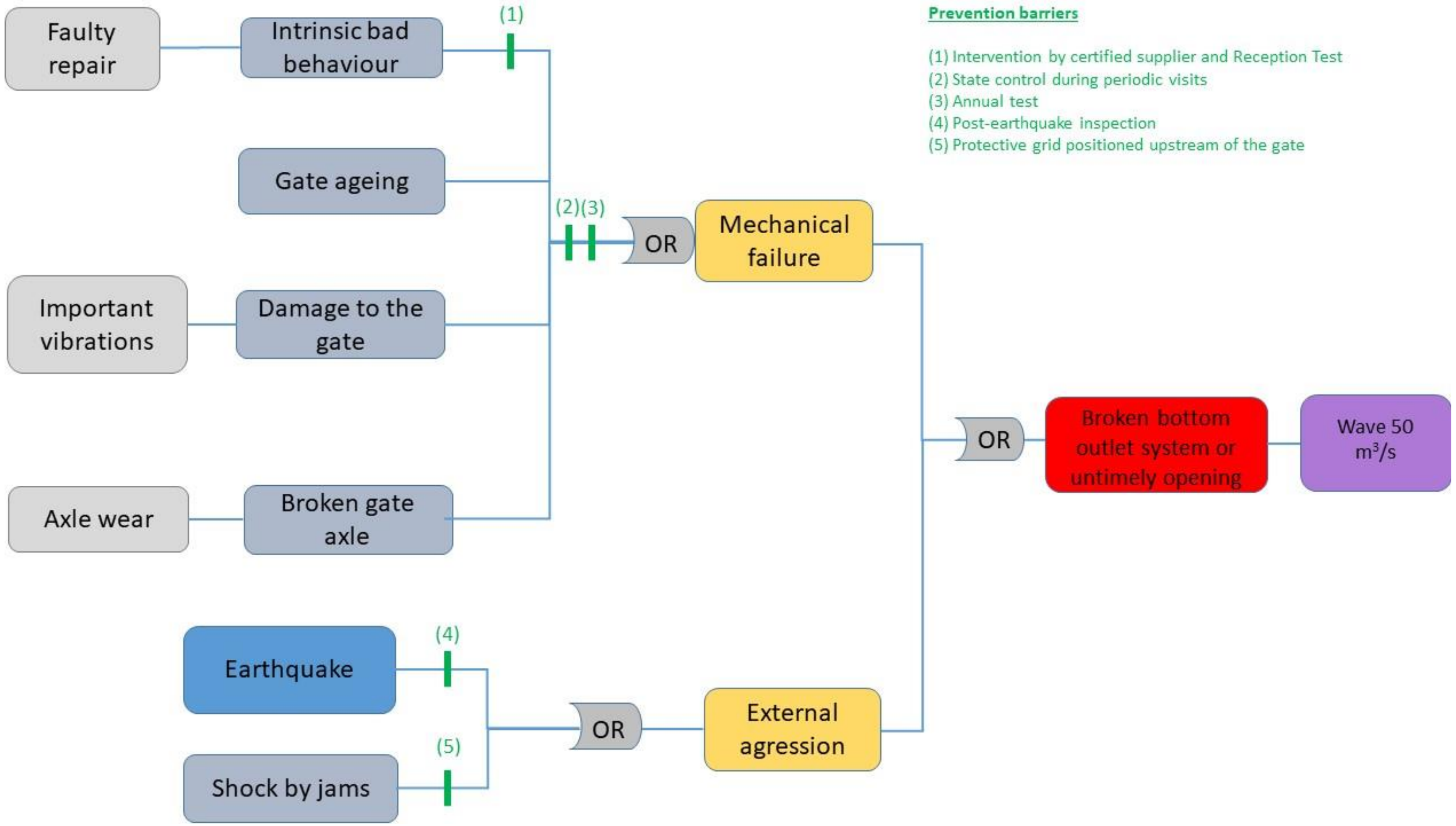
Scenarios leading to the Central Feared Event "Unintentionnal opening of spillway radial gate (during flood or test)"



When not during trial test or flood period, the gate is confined and electrically unplugged. It can not open without energy

Example 3: Semi-Quantitative Assessment with BTA

Scenarios leading to the Central Feared Event “Bottom Outlet failure”



Summary of risk assessment

- Event Tree analysis: for a Quantitative Risk Analysis Assessment
  - Need to proceed to an extensive Functional Analysis and a Failure Mode Analysis, to provide the completeness and the independence for the failure modes
  - quantitative Risk Analysis Assessment justified for specific structures (canals, canal embankments, etc.)
  - Various measurements of the probabilities related to failure modes:
    - Probabilistic: for natural hazards
    - Frequency: technological failure modes
    - Expert judgment based: failure modes with low data, human failures

- Fault Tree Analysis or Bow Tie Analysis: for a Semi-Quantitative Risk Analysis Assessment
  - Relative simplicity of implementation: need to proceed to light Functional Analysis and Failure Mode Analysis, as PRA
  - Based on expertise and working group for the FTA for the rating of events / barriers / level of confidence
  - A tool that is well adapted to the reality of the field of dams where structures have unique characters
  - In practice, the approach the most used in France

INRAE
EDF

comité français des barrages et réservoirs