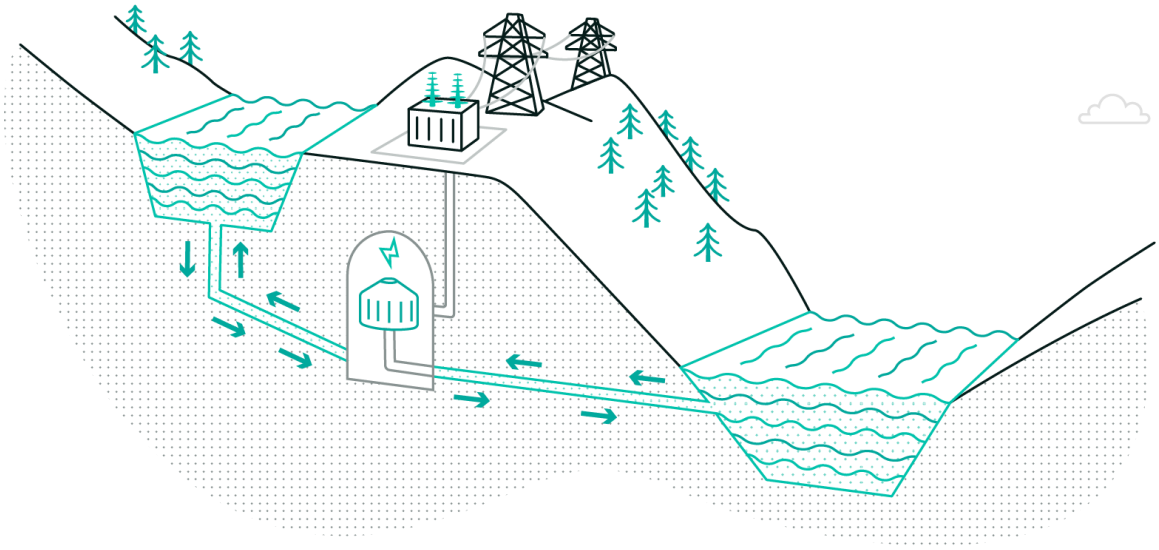
BRITISH HYDROPOWER ASSOCIATION

Pumped Storage Hydropower

Reservoir Safety - UK Technical Guidance



Authors & Editorial

This technical guidance is a collaboration between All Reservoir Panel Engineers (ARPE) and experts across the hydropower industry, mainly with reference to UK power stations and pumped storage hydro (PSH) projects in development. The work was coordinated by the British Hydropower Association to be hosted on the website with opportunities for further updates as PSH projects develop.

Tom Clegg – Fichtner Consulting Engineers

Tom is the Head of Hydropower for Fichtner, a mechanical engineer with over 15 years of experience in the sector working initially on run of river schemes during the feed in tariff period. He is currently providing technical support and project management services on a number of UK pumped storage projects in development. Tom holds a master's degree in mechanical engineering with renewable energy from the University of Edinburgh, is a chartered engineer with the Institute of Mechanical Engineers and is a certified functional safety engineer (SIS) with TÜV Rheinland.

Joao Correia – Bechtel

Joao is Chartered Civil Engineer and member of the Supervising Engineers panel with over 20 years' experience in the design and construction of hydropower, irrigation, water supply and flood control projects.

Currently, and for the past 2 years, he has been working as a Dams and Hydropower Engineer at Bechtel working on FEED studies, ECI processes, and proposals for the construction of hydro and pump storage projects in the UK, Balkans, North America and Australia.

Werner Delport – Thames Water

Werner is a Civil Engineer with over ten years' experience in the dams and reservoirs industry, including dam design, dam safety evaluations, quantitative risk assessments, investigations, and construction supervision in the UK and overseas. He is appointed as a Reservoir Supervising Engineer under the Reservoirs Act 1975 and currently works at Thames Water as Reservoir Safety Manager within the Reservoir Safety Team.

Russ Digby – KGAL

Russ has over 40 years post-graduate experience in the design of hydraulic steel structures, including aspects such as mechanical, electrical, oil hydraulic and reliability engineering. He has previously worked for specialist M&E contractors (Biwater Hydropower) and has now worked for KGAL Consulting Engineers Ltd, specialist water control gate consultants, for the last 27 years. Russ has written and presented technical papers and workshops at conferences around the world. He is the UK representative on the Hydromechanical Equipment Committee of ICOLD.

John Foster – Mott MacDonald

John is a Fellow of the Institution of Civil Engineers and an All-Reservoirs Panel Engineer (ARPE) with over 20 years at Mott MacDonald working on dam construction and reservoir safety projects worldwide for irrigation, water supply and energy markets. He has recently supported the outline design of UK pumped hydro schemes, undertaking a de facto Construction Engineer role under the Reservoirs Act.

Stuart King – SSE

Stuart has worked in the dams and reservoir industry for almost 30 years, first employed at Babtie Group/Jacobs Babtie working in the dams and reservoir team, gaining significant experience with asset management, remedial works on existing structures, hydrology, flooding and water resource. For the last 18 years he has been employed by SSE Renewables to manage reservoir safety on their portfolio of reservoirs. He has been a Supervising Engineer under the Reservoirs Act for over 20 years.

Guy Mason – Statkraft

Guy has over 20 years' experience working in consultancy, construction, and operations worldwide. His current role is as a dam expert for the Norwegian state-owned company Statkraft, who are Europe's largest generator of renewable energy. He is responsible for managing their dam safety programmes in Albania, Germany, India, Türkiye and the United Kingdom. He is a member of the team developing the Loch Na Cathrach pumped-storage hydroelectric project in the Scottish Highlands, which will provide 500MW capacity and is scheduled for commission in 2030.

Peter Mason – Damsolve

Peter has a BSc in Civil Engineering and MSc and PhD degrees in the Applied Hydraulics of Spillways. He has over 50 years' experience of working on major international dam & hydropower projects in Africa, Asia, Europe and North and South America and on Expert Advisory Panels in Africa, Europe, Asia and North America. He has authored over 100 technical papers on all aspects of dams and hydropower. He is a Fellow of the Institution of Civil Engineers, a member of various National and International Committees and Panels and past Chairman of the British Dam Society.

Anthea Peters – Arup

Reservoirs (Scotland) Act, 2011. She has 30 years' experience of earthfill, rockfill and concrete dam structures. She is a highly experienced dam engineer specialising in dam safety and hydraulic design and has extensive experience of delivering reservoir safety schemes and dam safety specialist studies, including risk assessment.

Anthea has been the technical lead on a number of high profile large, raised reservoir schemes, most recently as the design lead for the restoration of Todd brook reservoir and Loch Kemp PSH scheme and has undertaken technical due diligence reviews for PSH schemes internationally.

Louise Shaw – Stillwater Associates

Louise is a Chartered Civil Engineer and Supervising Engineer with more than 18 years of experience maintaining hydro power stations in the UK. These range from run of river schemes in Scotland to pure hydro schemes supplied from reservoirs and pumped storage hydro in Wales with the oldest infrastructure dating from 1905. Louise currently works as a Supervising Engineer for reservoirs.

Tom Wanner – Stillwater Associates

Tom is a chartered civil engineer and an All-Reservoirs Panel Engineer with over 25 years of experience in the civil, geotechnical and hydraulic engineering fields with expertise in earth, rockfill and concrete dam design, risk assessment, dam filter assessment, geotechnical investigation, hydropower, hydraulic structures and construction supervision. Tom is currently undertaking reservoir panel engineer roles on several new hydropower projects in Scotland and

Wales and provides panel engineer support for a major existing hydropower scheme in Wales comprising several large dams.

Bryn Williams – First Hydro Company (Engie)
Bryn is a Chartered Civil Engineer and a Reservoirs Act 1975 Section 12 Supervising Engineer. He joined the company in 2001 and became the Company Civil Engineer in 2008. He is responsible for the safe operation of the pumped storage reservoirs of Dinorwig and Ffestiniog Power Stations and is part of the asset management team with remit extending to monitoring, surveillance and maintenance of the associated tunnels, penstocks, shafts, caverns and structures.

Kate Gilmartin – British Hydropower Association
Kate Gilmartin is Chief Executive of the British Hydropower Association, leading the organisation's work to advance hydropower and pumped storage across the UK. She advises government, regulators and industry on energy policy, infrastructure investment, resilience and water management, championing hydropower's contribution to a secure, low-carbon electricity system.

Further editorial work by:

- Jonathan Cox – AECOM
- Matt Hill

Contents

Glossary **9**
Executive Summary **12**
Preamble and Purpose **14**
Context and Formation of the Working Group *14*
Scope and Intent of the Guidance *14*
Legislative and Regulatory Context for new build pumped storage hydropower *15*
Introduction to Pumped Storage Risk Management *15*
Status and Use of this Document *15*
Introduction **17**
1. Chapter 1: Types of Pumped Storage Hydropower **18**
1.1. An overview *18*
1.2. Types of pumped storage hydropower *18*
1.2.1. Open-loop pumped storage 20
1.2.2. Closed-loop pumped storage 21
1.3. Types of power station *22*
1.3.1. Hydraulic and turbine configurations 22
1.3.2. Types of dam 23
2. Chapter 2: Reservoir Inflows and Outlet Works **24**
2.1. Introduction *24*
2.2. Upper reservoirs *24*
2.3. Lower reservoirs *24*
2.4. Criteria for the design and sizing of principal outlet works *25*
2.5. Natural floods for spillway design *27*
3. Chapter 3: Spillways **29**
3.1. Introduction *29*
3.2. Upper reservoirs *29*
3.3. Lower reservoirs *31*
3.4. Spillway design *32*
3.5. Legal requirements and guidance *33*
3.6. Managed overflow of the dam structure *34*
3.7. Energy Dissipation Structures *34*
3.8. User Guidance *35*
4. Chapter 4: Drawdown Works and Requirements **36**
4.1. Introduction *36*
4.2. Dam types *36*
4.3. Current UK Guidance *37*
4.4. Embankment Dams *37*
4.5. Concrete dams *38*
4.6. Rockfill dams with an impermeable upstream face *40*
4.7. Recommendations *40*
4.8. Facilities for drawdown *40*
4.8.1. Power station and hydraulic waterways 41
4.8.2. Compensation outlets 41
4.8.3. Gated Spillways 42
4.8.4. Dedicated Low-level Outlets 42
4.9. Control of Incoming Inflows *43*
4.10. Legal Requirements and Guidance (UK) *43*
4.11. International Context and Good Practice *44*

4.12. Testing of the drawdown system ... *44*
5. Chapter 5: First Filling of the Upper Reservoir ... **46**
5.1. Introduction ... *46*
5.2. Filling of upper reservoir ... *46*
5.3. First filling plan ... *46*
5.4. First filling within the construction and commissioning programme ... *47*
6. Chapter 6: Downstream Releases and Consequences ... **48**
6.1. Introduction ... *48*
6.2. Risk to life and public safety ... *49*
6.3. Impact on downstream infrastructure and property ... *50*
6.4. Environmental consequences ... *50*
6.5. Invasive and non-native species risk ... *50*
6.6. Permitting and regulatory compliance ... *51*
6.7. International context and good practice ... ***Error! Bookmark not defined.***
6.8. Testing of a drawdown system ... ***Error! Bookmark not defined.***
6.9. Duration of downstream releases ... *51*
6.10. Acceptable levels of damage ... *52*
6.11. Mitigation ... *53*
7. Chapter 7: Operational Considerations ... **55**
7.1. Design Narrative/Statement ... *55*
7.2. Operational Considerations ... *55*
7.3. First filling ... *56*
7.4. Timing of inspections ... *58*
7.5. Staffing and Maintenance ... *59*
7.6. Water management ... *60*
7.7. Energy Management ... *61*
7.8. Longer term use of Reservoir ... *61*
7.9. Securing Critical National Infrastructure ... *62*
8. Chapter 8: Control Systems ... **63**
8.1. Introduction ... *63*
8.2. Control System Architecture ... *63*
8.3. Instrumentation ... *66*
8.4. Communication ... *67*
8.5. Redundancy ... *68*
8.6. Alarm and Trip Functions ... *69*
8.7. Cyber Security ... *70*
8.8. Remote Operation ... *70*
8.9. Example protection function – Reservoir High Level ... *71*
9. Chapter 9: Functional Safety ... **73**
9.1. Introduction ... *73*
9.2. Relevance ... *74*
9.3. Human Factors ... *74*
10. Chapter 10: Risk ... **76**
10.1. Risk Assessment – Example approach ... *77*
10.1.1. Selecting the appropriate level of risk assessment ... 78
10.1.2. The approach ... 79
10.2. Process Safety Risk studies ... *84*
11. Conclusion ... **87**
12. Appendix A – Overview of Reservoir Legislation by Jurisdiction ... **88**
12.1. England and Wales ... *88*
12.2. Scotland ... *88*
12.3. Northern Ireland ... *88*
Appendix B: Case Studies ... **90**

12.4. Turkey's Nest *90*
12.4.1. Taum Sauk Dam Failure: Instrumentation, Freeboard Management, and Failure Mechanisms in Lined Reservoirs 90
12.5. Dinorwig – a case study *92*
13. References 93
13.1. UK Legislation, Policy and Regulatory Guidance *93*
13.2. Reservoir Safety, Engineering and Risk Management *93*
13.3. Risk and Functional Safety Standards *94*
13.4. Pumped Storage Hydropower: Industry Evidence and Analysis *94*
13.5. Case Studies and International Experience *94*
13.6. Community, Workforce and Wider System Context *95*
13.7. Events and Expert Evidence *95*

Glossary

Abnormal Operation: Operating conditions outside normal parameters but not representing immediate failure, typically requiring monitoring or intervention.
ALARP (As Low As Reasonably Practicable): A principle used in risk management whereby risks are reduced to a level where further reduction would require disproportionate cost, time, or effort relative to the benefit gained.
Cavitation: The formation and collapse of vapour bubbles in a liquid due to local pressure reduction, which can cause damage to hydraulic structures and equipment.
Closed-Loop System: A pumped storage configuration where both reservoirs are largely isolated from natural watercourses, with limited natural inflows.
COMAH (Control of Major Accident Hazards Regulations): UK regulations aimed at preventing and mitigating major accidents involving dangerous substances, requiring operators to identify risks and implement appropriate control measures.
Consequence: The outcome or impact resulting from a failure event, including effects on people, infrastructure, and the environment.
Control System: The integrated system of sensors, logic, and actuators used to monitor and manage plant operation and reservoir behaviour.
Design Flood Level (DFL): The water level associated with a defined flood event used for design purposes, typically including allowances for wave action and operational uncertainty.
Drawdown: The controlled lowering of reservoir water level through outlets, spillways, or generation systems, typically for operational, maintenance, or emergency purposes.
DSEAR (Dangerous Substances and Explosive Atmospheres Regulations 2002): UK regulations governing the safe use and control of substances that could cause fire or explosion, including requirements for risk assessment and mitigation.
EPC (Engineering, Procurement and Construction): A project delivery model in which a contractor is responsible for the design, procurement, construction, and commissioning of a facility.
FAT (Factory Acceptance Test): Testing of equipment or systems at the manufacturer's facility prior to delivery to verify that they meet specified design and performance requirements.
Fail-safe: A design principle whereby a system defaults to a safe condition in the event of failure, loss of power, or loss of control signal.
FEED (Front-End Engineering Design): An early-stage engineering phase used to develop project scope, design basis, and cost estimates to a level sufficient for investment decision-making.
Freeboard: The vertical distance between the maximum operating water level (or design flood level) and the crest of the dam, providing a margin to prevent overtopping under abnormal conditions.
FSA (Functional Safety Assessment): A systematic and independent review undertaken to confirm that a system meets the required functional safety standards and safety integrity levels.
FSMP (Functional Safety Management Plan): A structured document describing how functional safety will be managed throughout the lifecycle of a system, including responsibilities, processes, and verification activities.
HAZID (Hazard Identification Study): A structured process used early in project development to identify potential hazards and their causes, typically through facilitated workshops.

HAZOP (Hazard and Operability Study): A detailed, systematic review of a system or process to identify deviations from design intent, their causes, and potential consequences.
Hazard: A condition or situation with the potential to cause harm to people, infrastructure, or the environment.
HS0, HS1, etc. (Hazard Study 0, 1, etc.): Stages within a structured hazard study process, typically progressing from high-level concept review (HS0) to detailed design review (HS2/HS3).
Human Factors: The consideration of human interaction with systems, including decision-making, workload, interface design, and potential for error.
IPL (Independent Protection Layer): A safeguard that is independent of other layers and capable of preventing or mitigating a hazardous event, typically used within risk assessment frameworks such as LOPA.
LOPA (Layer of Protection Analysis): A semi-quantitative risk assessment method used to evaluate whether sufficient independent protection layers exist to reduce risk to an acceptable level.
Low-Level Outlet: An outlet located at or near the base of a reservoir, typically used for drawdown or emergency release.
Maximum Water Level (MWL): The highest water level expected during normal or specified operational conditions, excluding extreme or emergency events.
Mitigation: Measures implemented to reduce the likelihood or consequences of a hazard.
Open-Loop System: A pumped storage configuration where one or both reservoirs are connected to natural watercourses and subject to natural inflows.
Operational Cycle (Cycling): The repeated filling and emptying of a reservoir as part of normal pumped storage operation.
Operational Envelope: The range of conditions within which a system is intended to operate safely and effectively.
Overflowing Flow: (Relatively) steady state flow over the crest or top of the dam, arising from the water level in the reservoir being above the crest or top of the dam, as a result of the water inflow being greater than that which can be accommodated by the spillway.
Overtopping Flow: Intermittent flows over the crest or top of the dam created solely by the run-up of waves not being contained by the available freeboard.
PMSP (Process Safety Management Plan): A framework outlining how process safety risks will be managed, including procedures, responsibilities, and monitoring arrangements.
Principal Outlet: A controlled outlet used to regulate reservoir levels under normal operating conditions.
Pumped Inflow: Water transferred into a reservoir through pumping operations, often at rates significantly exceeding natural inflows.
Redundancy: The provision of multiple independent components or systems performing the same function to improve reliability and reduce the likelihood of failure.
SIF (Safety Instrumented Function): A specific safety function implemented by a safety instrumented system to detect a hazardous condition and take action to prevent or mitigate it.
SIL (Safety Integrity Level): A measure of the reliability required for a safety function, expressed as discrete levels (e.g. SIL 1 to SIL 4), relating to the probability of failure on demand.
Single Point of Failure: A component or system whose failure would result in loss of a critical function without backup or mitigation.

SIS (Safety Instrumented System): A system comprising sensors, logic solvers, and final elements that performs one or more safety instrumented functions.
SRS (Safety Requirements Specification): A document that defines the required performance and functionality of safety systems, including safety integrity levels and operational requirements.
System Dependency: The reliance of one system or function on the availability or performance of another (e.g. drawdown dependent on grid connection).
System State: The operating condition of the scheme at a given time, including reservoir levels, plant status, and control system availability.
Time to Failure: The time between initiation of a failure mechanism and the occurrence of a critical outcome.
Time to Intervention: The period available between detection of a developing condition and the point at which intervention is no longer effective.
Upper Reservoir: The higher elevation storage reservoir in a pumped storage scheme, typically subject to rapid filling and drawdown cycles.
Lower Reservoir: The lower elevation reservoir in a pumped storage scheme, which may be naturally fed, modified, or purpose-built.

Executive Summary

This guidance document provides a structured, risk-informed framework to support reservoir safety considerations for pumped storage hydropower (PSH) schemes in the UK. Developed by industry experts, it responds to the growing pipeline of PSH projects and recognises that existing reservoir safety practices, largely developed for passive, naturally fed reservoirs, do not fully address the operational complexity and risk profile of modern pumped storage systems. The document is not intended to be prescriptive, nor does it introduce new regulatory requirements. Instead, it is designed to inform professional judgement and support project teams as they refine designs over the coming years within the existing legislative framework.

A central theme throughout the guidance is the distinction between natural and operational risks. In PSH schemes, pumped inflows can exceed natural inflows by several orders of magnitude, meaning that key risks often arise from system operation, control failures, or human factors rather than extreme weather alone. As such, the document promotes a proportionate, risk-based approach aligned with the principle of reducing risks to “as low as reasonably practicable” (ALARP), supported by clear documentation of design intent and operational assumptions.

The role and necessity of spillways is a key area of focus. For upper reservoirs, spillway requirements are typically governed not by natural flood events but by the potential for over-pumping and control system failure. The guidance highlights that “adequate fail-safe provision” may be achieved through a combination of passive infrastructure, operational controls, and storage allowances, rather than relying solely on traditional spillway design standards. For lower reservoirs, spillway design remains more closely aligned with conventional flood hydrology, though the interaction with generation flows must be considered. Across both cases, the document emphasises the importance of balancing risk, cost, and downstream consequences, and of clearly justifying design decisions to support future inspection and regulatory review.

Drawdown capability is identified as another critical safety function, particularly in emergency scenarios where rapid lowering of reservoir levels may prevent dam failure or reduce its consequences. The guidance builds on existing UK drawdown standards but introduces additional considerations specific to PSH schemes, including frequent cycling, varied dam types, and reliance on operational systems. It outlines the need to assess appropriate drawdown rates based on dam characteristics, inflows, and downstream impacts, and to consider multiple drawdown pathways such as power waterways, low-level outlets, and spillway systems. Importantly, it recognises that system availability, grid connection, and operational constraints may affect drawdown reliability, reinforcing the need for redundancy and robust planning.

Control systems are presented as a fundamental component of PSH safety, reflecting their central role in managing water levels, flows, and operational states. The guidance discusses system architecture, instrumentation, redundancy, alarm functions, and cybersecurity, highlighting the need for reliable, fail-safe design. Given the dependence on automation and remote operation, it also underscores the importance of integrating human factors and ensuring that operators are supported by clear procedures and well-designed interfaces. Control systems are not treated in isolation but as part of a broader, layered safety approach alongside civil and hydraulic measures.

Finally, the document adopts a comprehensive approach to risk management methodologies. It encourages the use of structured tools such as risk assessments, event trees, and hazard studies (e.g., HAZOP), combined with ALARP-based decision-making. The guidance stresses that risk evaluation should consider both likelihood and consequence, including time available for intervention and the effectiveness of mitigation measures. It also highlights the need to account for downstream impacts, on communities, infrastructure, and the environment, and to ensure that these are incorporated into both design and operational planning.

In summary, this guidance provides a coherent framework for addressing the unique safety challenges of pumped storage hydropower. While not directive or legally binding, it offers practical, experience-based insights to support consistent and well-reasoned decision-making. Its application is intended to evolve alongside the sector, helping designers, engineers, and operators to develop safe, resilient PSH schemes in an increasingly complex energy landscape.

Preamble and Purpose

This document has been developed by a specialist Working Group of engineers and practitioners with extensive experience in the design, operation, regulation, and inspection of pumped storage hydropower schemes. The work has been convened and curated by the British Hydropower Association in response to a growing recognition that existing reservoir safety guidance does not always adequately reflect the distinctive characteristics and risks associated with modern pumped storage developments.

The purpose of this guidance is to support proportionate, risk-based decision-making for PSH reservoirs within the existing UK reservoir safety framework. It is intended to complement established legislation, standards, and guidance, and to assist construction engineers, inspecting engineers, designers, owners, and regulators in exercising informed professional judgement where pumped storage schemes raise issues not fully addressed by conventional reservoir safety practice. The guidance reflects current practice at the time of publication and should be read alongside prevailing statutory and technical guidance.

Context and Formation of the Working Group

Interest in pumped storage hydropower in the UK has increased significantly in recent years, driven by the need for long-duration energy storage to support a low-carbon electricity system. Many proposed schemes involve new reservoir configurations, high installed pumping capacities, rapid operational cycling, and a strong dependence on control and automation systems. Members of the Working Group observed that these features can give rise to safety considerations that differ in important respects from those associated with traditional impounding reservoirs. In particular, the group identified a need for clearer guidance on the management of man-made inflows and outflows, the interaction between civil and control-system safeguards, and the application of risk-based principles to spillway provision, drawdown capability, and operational decision-making.

The Working Group was therefore established to examine these issues collectively, drawing on UK and international experience, and to develop practical guidance that reflects current good practice while recognising the need for professional judgement on a scheme-by-scheme basis.

Scope and Intent of the Guidance

This guidance seeks to capture and articulate the key reservoir safety considerations that are specific to pumped storage hydropower, including:

- The distinction between natural flood risks, and risks arising from pumping and operational failures;
- The role of control systems, automation, and human factors in preventing or initiating hazardous conditions;
- The application of ALARP principles to spillway provision, drawdown arrangements, and downstream consequences;
- The importance of documenting design and operational rationale to support future inspection and lifecycle management;
- The need to consider time-dependent behaviour, duration of releases, and opportunities for intervention.

Parts of this guidance are not necessarily applicable for smaller pumped inflows for example when they are less than a PMF inflow for a category A dam.

The guidance does not prescribe design solutions or numerical standards. Instead, it provides a structured framework to help practitioners identify relevant hazards, assess risk in a proportionate manner, and demonstrate that risks have been reduced to a level that is as low as reasonably practicable 'ALARP'.

Legislative and Regulatory Context for new build pumped storage hydropower

Pumped storage hydropower schemes in the UK are subject to the same statutory reservoir safety regime as other large, raised reservoirs, (see Appendix A) and associated legislation. In addition, they must comply with wider health and safety, environmental, and planning requirements.

This guidance is written within that existing legislative framework. It recognises the continuing relevance of established reservoir safety standards and Environmental Enforcement Agencies guidance, while acknowledging that these documents were largely developed with passive, naturally fed reservoirs in mind. The guidance therefore focuses on areas where pumped storage schemes may warrant additional consideration or a different emphasis, particularly where operational controls and man-made flows play a central role in risk management.

Introduction to Pumped Storage Risk Management

Risk management for pumped storage reservoirs differs in emphasis from that for conventional reservoirs. While natural inflows and extreme flood events remain important considerations, the pumped inflow can be several orders of magnitude greater than any naturally arising flow. Therefore, many of the most significant risks in PSH schemes arise from operational scenarios, including control-system failures, human error, loss of grid connection, or abnormal plant behaviour. Effective safety management therefore depends on the interaction of multiple layers of protection, including civil design, hydraulic capacity, control systems, operational procedures, and organisational competence. This guidance adopts a risk-based approach that considers both the likelihood and consequences of hazardous events, and that recognises the time available for detection, intervention, and response.

Throughout the document, emphasis is placed on understanding how risks are controlled in practice, how assumptions are recorded and maintained over the life of the scheme, and how future engineers and operators can be supported in making informed decisions as systems, standards, and operating contexts evolve.

Status and Use of this Document

This guidance represents the collective view of the Working Group at the time of publication. It is intended to inform and support professional judgement rather than to serve as a regulatory instrument. Users are expected to apply the principles set out here in a manner that is proportionate to the scale, complexity, and potential consequences of individual schemes.

The BHA intends that this document will evolve over time as further experience is gained from new pumped storage developments in the UK and internationally. Feedback from users is therefore welcomed and will be considered in future updates.

Introduction

All reservoirs built in the UK and retaining more than a designated volume of water are required to be designed and constructed under the supervision of a Construction Engineer as defined in the Reservoir Act appropriate to the country concerned. It should be noted that England, Scotland, Wales and Northern Ireland each have their own Reservoirs Act legislation. A high-level comparison of legislative arrangements is provided in Appendix A. Moreover, 2 years after the Construction Certificate for a reservoir has been issued, it must be inspected by an appropriate Inspecting Engineer, independent of the original design and construction. They have the power to make recommendations *in the interests of safety*, if there are matters with which they are concerned.

There is a limited supply of suitably qualified Construction and Inspecting Engineers in the UK and most of those will have had their primary experience based on inspecting water supply and irrigation reservoirs. Hydropower reservoirs, with large diameter tunnels, penstocks and gates, are very much the exception and those featuring pumped storage even more so. Pumped storage projects involve the regular transfer of large water volumes between reservoirs generally over a short space of time.

Pumped inflow and natural inflow are both design considerations. These should be considered in a manner that assures safety and requires considerable judgement from the engineers involved and so reduces the potential for differences of opinion between the Construction Engineer and later Inspecting Engineers. The need for a reference to outline and discuss the various factors involved, and so to perhaps also encourage a consistency of approach, was the genesis of this report.

As the report took shape it was clear that many factors were linked not only to reservoir safety as defined in the various Reservoirs Acts, but also to the overall operational safety of pumped storage schemes in general. These include particular levels of safety evaluation for mechanical and electrical works as well as the often slightly different approaches adopted for the design of civil construction. Therefore, these are also explored in the report in order to give a central reference to those involved whilst at the same time providing links to other sources where relevant.

1. Chapter 1: Types of Pumped Storage Hydropower

1.1. An overview

For national electricity grids such as those in the UK, the demand at any one time has to match an equivalent amount of generation. But at times, generation may take place when there is no demand for that energy. The first pumped storage power stations were built to support nuclear generation's inability to reduce output quickly overnight. Second generation pumped storage were built to avoid inefficient coal burning.

More recently, pumped storage power stations support variability of wind and solar generation. In such cases, intermittent generators have to be shut down and that potential energy is lost, unless it can be stored. This is exactly what pumped hydropower does. Serving as a dynamic energy storage solution, pumped storage hydro involves two reservoirs at different elevations. During periods of low energy demand, surplus electricity is used to pump water up to the higher reservoir.

When demand increases, that stored water is released, generating electricity. There is an overall loss of energy in this process, typically in the order of 25%, but this is acceptable where it provides flexibility and makes available a greater amount of stored energy from renewable and other sources, that would otherwise be lost. In the UK this fluctuation in demand is reflected in power prices. Price fluctuations occur daily but there is also a seasonal aspect with long, cold nights increasing demand and hence prices.

The four existing PSH power stations in the UK were built to store overnight nuclear power generation but with the rise in wind and solar power generation, the UK now needs far greater storage, notably to avoid the curtailment of wind power. Today the four existing UK schemes have a combined output of 2.8 GW/24 GWh representing around 5% of the energy storage the UK will need to achieve net-zero by 2050. They are summarised in Table 1.

Table 1: Existing pumped storage hydro schemes in the UK (as at 2026)

Scheme	Completion Date	Capacity	Upper Reservoir Vol. Mm^3	Owner
Ffestiniog N. Wales	1963	360 MW 1.3 GWh	2.2	Engie
Cruachan Loch Awe, Scotland	1965	440 MW 4.5 GWh	11.3	Drax
Foyers Loch Ness, Scotland	1974	300 MW 6.4 GWh	13.6	SSE Renewables
Dinorwig N. Wales	1983	1,700 MW 9.1 GWh	9.0	Engie

1.2. Types of pumped storage hydropower

There are two main types of PSH scheme. An open-loop scheme means that at least one of the reservoirs (usually the lower one) is connected to a body of natural water which is also capable of receiving flows from other sources. For example, where the lower reservoir comprises a river

or large lake which is also fed by a natural catchment. A closed-loop scheme comprises two reservoirs that are not connected to any natural water body and the same water is simply re-circulated. Regardless of the type of scheme, there will always be an element of natural inflow. For Cruachan in Scotland, rainwater into the upper-reservoir catchment area (see Figure 1) allows the station to generate around 10% of its annual electricity without pumping. Utilising nearby catchments, there can be a number of catchment tunnels that bring water into the reservoir.



Figure 1: Cruachan's upper reservoir, Argyll & Bute, Scotland

The amount of energy in megawatt hours (MWh) that a PSH project can store will depend on the size and height difference between the two reservoirs and the time over which water is pumped. As already noted, due to general system losses, only about 75- 80% of that stored energy will subsequently be available for generation on its release through turbines. The amount of electrical power that can be generated at any one time will depend on the size and capacity of the installed turbines in terms of megawatts (MW). It may be appropriate to generate more MW for a short duration or less MW for longer. This will be an economic decision based on installation costs and system demand.

For example, a facility with two reservoirs 5,000 M^3, and with a 500 m height difference between them, might typically provide a capacity of 3 MW and would store up to 3.5 MWh of electricity. At the opposite end of the scale the Fengning PSH Station in China has twelve 300 MW reversible turbines and can produce 40 GWh of energy storage over 11 hours. Its combined reservoirs hold 110 million m^3 of water and the station could power approximately 20 million homes[12].

[1] IHA PSH webpage

1.2.1.Open-loop pumped storage

In an open-loop system, the lower reservoir will typically have a natural outflow into a river or a large natural lake. Europe's largest pumped hydro station is Grand Maison in France which uses the Verney Dam, naturally supplied by rivers, as the lower reservoir. While there are no PSH plants in the UK with direct connection to large river systems, the Foyers power station on Loch Ness and Cruachan on Loch Awe use expansive natural lakes as their lower reservoirs with downstream connection to the sea. A typical arrangement for an open-loop PSH scheme is shown in Figure 2.

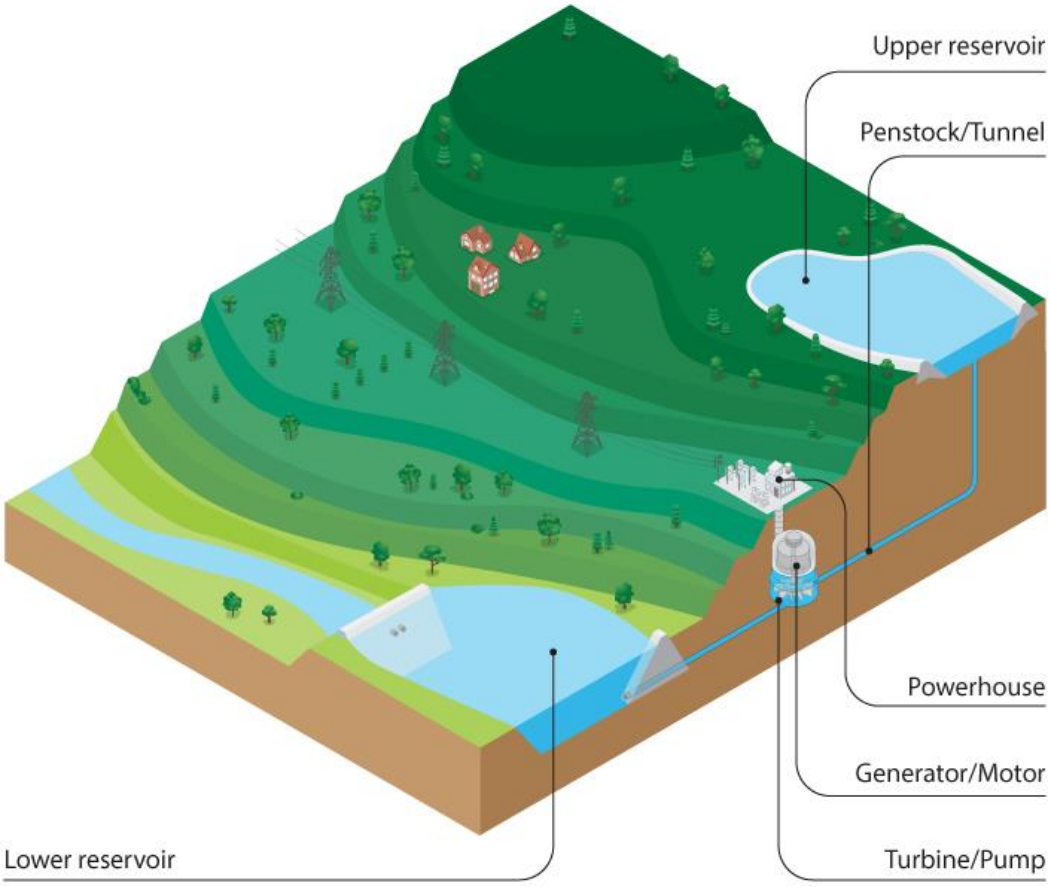


Figure 2: Example of an open-loop pumped storage hydropower scheme
Diagram courtesy of the International Hydropower Association

A primary concern for an open loop system, and for a closed loop system where the lower reservoir is significantly larger than the upper one, is the risk of over-pumping into the upper reservoir. This in turn could lead to the upper reservoir breaching. Other important aspects are the use and scale of natural water bodies as well as any impact on biodiversity. Migratory fish such as salmon entering lower reservoirs could also be a defining factor of an open-loop system. Around the world, PSH plants are bespoke and built according to the constraints of the topography and hydrology. As such, layouts will vary, with water volumes, inflows and outflows depending on system characteristics and demand.

1.2.2.Closed-loop pumped storage

An 'off river' pumped storage site produces power from water pumped to an upper reservoir without a significant natural inflow. For the purposes of Figure 2, a closed-loop system would not have a river flowing from the lower reservoir. The Goldisthal Pumped Storage plant in Germany is one of Europe's largest closed-loop systems.

In the UK, the Dinorwig PSH scheme is effectively a closed-loop system. Dinorwig's lower reservoir, Llyn Peris is a natural, glacial lake whilst Marchlyn Mawr, the upper reservoir was artificially created. The Upper Reservoir on the north side of Elidir Mountain has only a small catchment with minimal inflow that has little overall impact on the availability of storage capacity for energy generation.

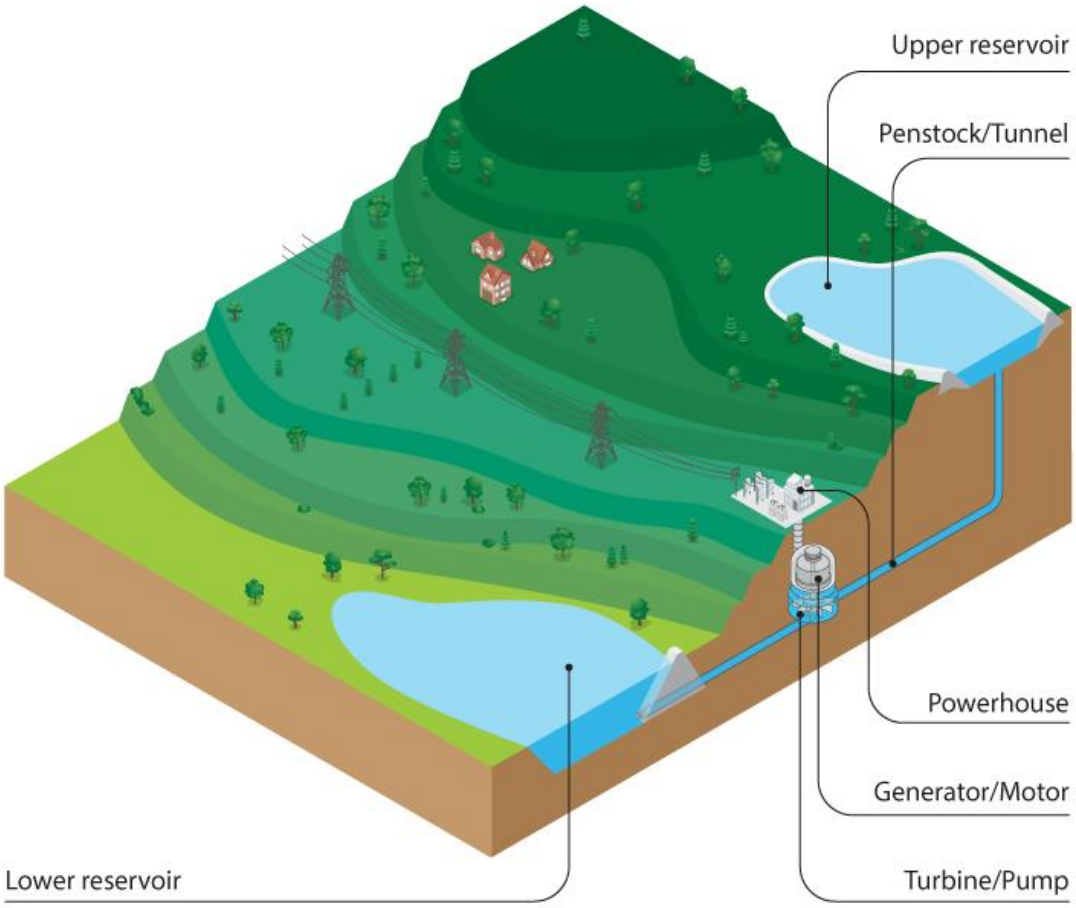


Figure 3: Example of a closed -loop pumped storage hydropower scheme
Diagram courtesy of the International Hydropower Association

The lower reservoir was constructed by forming a 4m high rockfill embankment to enlarge the existing Llyn Peris lake on the Afon Nant Peris river. To maximise operational storage, flow from the Afon Nant Peris river is diverted around Llyn Peris by means of a 2.2 km long, 6.25 m high x 6 m wide diversion tunnel that discharges to Llyn Padarn, downstream.

Despite the Nant Peris diversion structure, there is a significant inflow from Llyn Peris's immediate catchment that cannot be diverted, as well as infiltration under Afon y Bala dam

from Padarn to Peris when Peris is low. To stop this inflow reducing the usable volume in the closed-loop, there is an arrangement of bypass pipes through the Afon y Bala dam, at a level of 102.5m OD that allows surplus water to be shed from the system when Llyn Peris is above this level. Flood flows exceeding the bypass capacity are evacuated via a gated spillway at 106.25m OD with three 5.25m wide x 2.75 m high automatically operating "Bascule" tilt gates. The dam is designed to be over-toppable in extreme floods.

1.3. Types of power station

The power station or power-house element of any PSH scheme houses the rotating machinery, i.e.: the pumps, turbines and generators or combined pump-turbines. Power stations typically fall into three categories; shaft power stations built adjacent to the lower reservoir, surface powerhouse which is built in an open excavation and underground power stations within caverns. Although the former two may seem easier and less expensive to construct, in practice costs will be affected by various factors. These include the topography and geology of the site as well as the elevation or "setting" required for pumping. The specific speed of the units also has a major bearing on the setting level with faster units requiring much deeper setting levels than slower units. Slower units are larger in size and cost more so there is a trade-off to be analysed when deciding on the type of powerhouse structure. Pumps will generally need to be set at an elevation some way below that of the lower reservoir in order to avoid cavitation. This may be more easily achieved with an underground arrangement than a surface one. Again, there are no hard and fast rules, and each project will need to be evaluated on its own merits with costs, both for construction and for future operation and maintenance generally being the deciding factors. In the UK, both types of power station exist, with the Ffestiniog and Foyers PSH schemes both featuring shaft power stations and with Cruachan and Dinorwig turbine halls both being underground.

1.3.1.Hydraulic and turbine configurations

PSH schemes can employ either separate pump and turbine units or combined pump-turbine units able to reverse their function. There are two main categories of pump-turbine and the choice between the two may have implications for operational safety and reliability.

Fixed speed pump-turbines operate at a constant fixed speed and employ simple electrical control. Hydraulic responses are predictable, but pumping power consumption is binary and not controllable, shutdown and start-up times may also be relatively slow. Variable speed pump turbines use power electronics for flexible control particularly of pumping power consumption. However, the greater precision and efficiency of control and dependency on complex control system and on power-electronics reliability. The power converters also impose a notable efficiency penalty.

Where multiple units are installed, designers should consider how combined operation affects reservoir level change rates, freeboard margins, and "time-to-react" for alarms and shutdowns (refer also to Chapter 7 – Operational Considerations).

1.3.2. Types of Dams

Whilst various types of dams may be associated with PSH schemes, the most common dam types are likely to be those associated with hard rock foundations able to withstand rapid water level changes. These in turn are a feature of the mountainous regions most suited to PSH schemes and where significant head differences can occur over relatively short distances. Thus, while the form of dam selected will depend on topography, geology, and available materials, the most common types used or proposed for PSH tend to be those shown in Table 2.

Table 2: Likely types of dams at PSH schemes

Dam Type	Typical Characteristics
Concrete (mass gravity, buttress or arch)	Suitable for narrow valleys and good rock foundations. Can incorporate spillways.
Roller Compacted Concrete (mass gravity)	Suitable for good rock foundations. Can incorporate spillways.
Concrete Faced Rockfill (CFRD)	Economical for wide valleys. Impermeable upstream face. Needs separate spillway.
Asphalt Faced Rockfill (AFRD)	Similar to CFRD dams but with a more flexible (asphalt) facing. Needs separate spillway.
Clay Core Embankment	Not recommended for PSH schemes, due to the effects of rapid drawdown, but may be used for lower reservoirs with natural inflows. If used at the lower reservoir, the water level range would need to be relatively modest. Needs separate spillway.

These types of dams, their characteristics and other considerations are expanded further in Chapter 4: Drawdown Requirements.

2. Chapter 2: Reservoir Inflows and Outlet Works

2.1. Introduction

The role of a reservoir, as the name implies, is to "reserve" or store water. This implies that there must be a source of water feeding into the reservoir and also some means of extracting it via outlet works. In conventional reservoirs, both inflows and outflows can take a variety of forms, but a particular feature of the upper and lower pump storage hydro reservoirs in a typical PSH scheme is the high volumes of artificially pumped water regularly exchanged between them. The likely differences between the resulting upper and lower reservoirs are explained below.

2.2. Upper reservoirs

PSH upper reservoirs are typically artificial impoundments sited at the highest practical altitude in mountainous or hilly regions. Natural inflows from rainfall and/or snowfall directly onto the reservoir will occur but there is unlikely to be significant inflow from local hillside runoff. By far the major inflow is likely to be pumped inflow from the lower reservoir via pumps or pump-turbines.

The inlet works feeding the pumped water into the reservoir will also comprise the main outlets from the upper reservoir and serve to feed water back to the lower reservoir via turbine-generators.

In addition to this, separate spillway overflow works may be provided to safeguard the dam and reservoir in the event of continuous over pumping when the reservoir is full. A low-level drawdown facility might also be provided to lower the upper reservoir in an emergency should that not be possible directly via the power station.

2.3. Lower reservoirs

PSH lower reservoirs are typically created by using, and possibly enlarging, existing natural bodies of water in the valleys of mountainous or hilly regions. Inflows into such water bodies could comprise:

- Direct rainfall or snowfall onto the reservoir
- Rainfall and/or snowfall runoff from the reservoir catchment
- Artificial diversions from other catchments
- Generation outflows from the upper catchment

Associated outlet works may comprise:

- Intakes to pump water to the upper reservoir
- A flood spillway
- A low-level reservoir draw-down facility
- A compensation water outlet

In practice some of the works may be combined to give dual functions. For example, the low-level draw-down facility may also be used for compensation releases.

Detailed discussion of likely spillway and draw-down work requirements are given in Chapter 3 and Chapter 4 respectively. The remainder of this Chapter will discuss background aspects relevant to one or other, or to both.

2.4. Criteria for the design and sizing of principal outlet works

Arguably, the main outlet for both upper and lower reservoirs in a PSH scheme is that which supplies the power station in either pumping or generation mode. Because the flows are reversible these will operate as either outlets or inlets at any one time. The sizing of these works will be wholly related to the flows required for generation and pumping. These in turn will be defined to meet wholly commercial objectives. However, any spillway will also have to accommodate natural flood events, especially in the case of the lower reservoir. Emergency drawdown works will be sized according to appropriate UK guidance for large, raised reservoirs. In fact, it can be reasonably argued that both spillways and emergency drawdown works will be designed to meet the hydraulic requirements whilst also complying with legislation, given that they will be defined by either a Construction Engineer or an Inspecting Engineer appointed under the appropriate UK Reservoirs Act.

As noted in the Introduction to this Guide, all reservoirs built in the UK and retaining more than a designated volume of water, are required to be designed and constructed under the supervision of a Construction Engineer as defined in the Reservoirs Act appropriate to the country concerned. See Appendix A for detail on legislation in each country. Moreover, 2 years after the Construction Certificate for a reservoir has been issued, it must be inspected by an appropriate Inspecting Engineer who is independent of the original design and construction, but who can make recommendations that could require modification to the original works if there are matters with which they are concerned. This situation will continue throughout the life of the scheme as the reservoirs in question continue to be inspected at recurring intervals of not greater than 10 years.

When the scheme is operating in generation mode, the water supply outlet in the upper reservoir will need to be sufficiently submerged to avoid the development of upstream vortices. Even so, some anti-vortex arrangements may also be needed. The same applies in the case of the water supply outlet in the lower reservoir when the scheme is operating in pumping mode.

Given the likely depths of submergence, it may be possible to use these works for the occasional drawdown of the upper and/or lower reservoirs. Whether such an arrangement can also be assumed to apply in case of emergency is subjective. For example, it would not be available if the main machines were on a maintenance outage or if the grid connection was unavailable for any reason. If the station is out of action due to planned maintenance, then the owner can lower the upper reservoir to a low level prior to embarking on the outage. This greatly reduces the risk for the upper reservoir and enables the bottom outlet to be sized reasonably. The same argument could also apply to the lower reservoir.

A Construction and/or Inspecting Engineer may therefore consider it appropriate to at least partially duplicate the ability to draw down either reservoir, with entirely separate, dedicated facilities. Any such decision should be clearly recorded by the Construction Engineer, with background reasons, for the use and benefit of subsequent Inspecting Engineers.

A similar dilemma occurs when it comes to considering the use of the pumping and generating works to accommodate flood events or to prevent either dam over-topping and failing. The dilemma stems from the different levels of risk which are considered acceptable for PSH operational purposes and the levels of risk for which large, raised reservoirs in the UK are required to be designed against failure. This is illustrated by the levels of risk shown in the tables below.

Table 3 gives necessary levels of risk reduction for a specific Safety Instrumented Function or "SIF" in terms of a Safety Integrity Level or "SIL" as stated in BS EN 61511-1, which is further explored and amplified in Chapter 9 . Table 4 is taken from the 4th edition of the ICE publication *Floods and Reservoir Safety* (FRS). This uses a standards-based approach and defines the levels of natural flood risk for which spillways should be sized according to downstream hazard or consequence category. Comparison between these two tables, gives a view of how risk levels are applied in practice using the two different approaches.

Table 3: Necessary Level of Risk Reduction by Safety Integrity Level value

Safety Integrity Level	Level of Risk Reduction (Low Demand Mode)
1	10 to 100
2	100 to 1,000
3	1,000 to 10,000
4	10,000 to 100,000

Table 4: Design flood requirements by downstream hazard category

Category	Safety Check Flood	Design Flood	Downstream Hazard or Consequence
A	Prob. Max	1:10,000	Loss of life in a community
B	1:10,000	1:1,000	Isolated loss of life and/or extensive damage (i.e. loss of major infrastructure)
C	1:1,000	1:150	Negligible risk to life and limited damage
D	1:150	1:150	No apparent loss of life and very limited additional damage

In Table 4 the design flood is that which must be discharged under normal conditions with an acceptable freeboard safety margin. The safety check flood is the inflow beyond which the safety of the dam cannot be assured.

While the levels of risk implied by these tables are similar, it should be noted that PSH schemes are operationally complex, which can limit SIL compliance. For example, it will be noted in Chapter 9 that an aspirational SIL value of 2 is considered operationally reasonable for an example PSH scheme. However, this would not meet the level of risk required for a Category A reservoir according to Table 4.

2.5. Natural floods for spillway design

In the middle of the 20th Century there was a general consensus among hydrologists to derive extreme floods by the statistical analysis of rainfall data coupled with rainfall-runoff modelling. This assumed that rainfall was essentially random or stochastic and meant that predictions for the future could be based on probability theory. It implied that with enough data one could calculate, for example, the risk of 1:1,000 or even a 1:10,000 event.

However, estimating such extreme probabilities needs a lot of data and prior to 1960 there were just 600 stations in the UK with typical record lengths of 50 years and so approximately 30,000 station years of data. To achieve the size of dataset needed for estimating extreme probabilities more gauging stations were added in the UK. A further 6,000 stations were added in 1961. This meant that analyses for the 1975 UK *Flood Studies Report* (FSR) were able to claim a database of 96,000 station years. However, it should be remembered that two-thirds of that, about 60,000 station years, covered a period of only 10 years.

More data was added subsequently and when the FSR was replaced in 1999 in the UK by the *Flood Estimation Handbook* (FEH) studies were based on 151,245 station years. Unfortunately, problems emerged with using the FEH for extreme floods (greater than a 1:1,000 probability) and this led to both the FSR and FEH methods being used in parallel for a while, with of course appropriate guidance. The matter was subsequently resolved by further studies at the UK Centre for Ecology & Hydrology (CEH). These studies resulted in refined values for the 1:100, 1:1,000 and 1:10,000-year storm events.

However, it is important to remember that the rainfall database on which all this is based is still heavily weighted over the period between about 1960 and 2000. In other words, it is more of a spatial record than an extensive time history. So, while we usually talk about a 1:1,000-year event, what we really mean is a 1:1,000 annualised probability of the event occurring based on a limited and relatively recent record. This of course remains valid if the climate is static. But in recent years there have been concerns that climatic change could increase both extreme storm values and also affect their frequency of occurrence. This also applies to Probable Maximum Storm estimation which, at the time of writing, is subject to further study and which is based on climatic factors rather than statistical analyses of historic records.

Once the design storm has been established or calculated using the above data it is necessary to convert that into catchment run-off and river flow. This is handled in the UK by the FEH web-based service run by the CEH. This provides the rainfall model outputs needed as well as all the necessary catchment descriptors. The matter is conveniently summarized in the ICE publication *Reservoir Management* (2019), Chapter 3 which notes that,

"*The FEH catchment descriptors include catchment area, mean drainage path length and slope, mean altitude and the standard percentage runoff from soil types. The rainfall database holds model depth duration frequency relationships for every 1 km Ordnance Survey grid point in the UK. When this is combined with the model parameters estimated from catchment descriptors, FEH methods can produce estimated flood flows and hydrographs for a point on any water cost in the UK".*

For preliminary planning purposes, use can be made of a rapid assessment method. This first appeared in the *Flood Studies Report* (1975) and is repeated in the ICE *Floods and Reservoir Safety* (2015). It gives a formula for the peak probable maximum flood (Qm) as:

$$Qm = 0.454\ A^{0.937}\ S_{1085}{}^{0.328}\ SAAR^{0.319}$$

Where:

A = catchment area (km^2)

S_{1085} = the mean slope between the altitudes at 10% and 85% of the main stream length

SAAR = standardized annual average rainfall 1941-1970 (mm)

The various long period floods can then be approximated as a factor of Qm where: -

The 1:10,000 probability flood = 0.5 Qm

The 1:1,000 probability flood = 0.3 Qm

The 1:150 probability flood = 0.2 Qm

However, it should be stressed that while these approximations are useful for order-of-magnitude planning, any final design should be based on the web based FEH method available through CEH and also the work done by a Hydrologist or someone with appropriate hydrological training.

3. Chapter 3: Spillways

3.1. Introduction

This chapter is intended to provide guidance on designing the works necessary to accommodate inflows into either the upper or lower reservoirs that are in excess of operational requirements. In the upper reservoir, these are likely to be dominated by over-pumping. In the lower reservoir, they are likely to be dominated by natural flood inflows. The chapter considers the need for a spillway and how one should be sized and operated. The guidance is based on relevant UK and overseas guidance and the experiences of the working group.

3.2. Upper reservoirs

As noted in earlier chapters, PSH scheme upper reservoirs are likely to have little to no direct catchment or be very large relative to the natural direct catchment. The assessment of natural inflows and associated flood routing is therefore not likely to be the driving criteria for spillway requirements. It is more likely to be based on the capacity and management of the pumped inflow. The ICE's guide *Floods and Reservoir Safety,* 4th Edition (FRS) provides the principal UK design reference for appropriately sizing the works required for the safe impoundment and conveyance of flood flows. The guidance also includes reference to reservoirs without direct catchments, which is relevant to the majority of PSH scheme upper reservoirs. The guidance requires that:

"Adequate fail-safe provision exists that the inflow cannot continue to the point of overflowing the embankment (unless overflowing is allowed for in the design)."

Consideration will need to be made at an early project stage as to how "adequate fail-safe provision" will be achieved. This may include provision of a passive spillway arrangement, additional storage allowances, consideration and reliance on control systems, or a combination of these.

In FRS there are two approaches to reservoir safety with regard to floods (and by implication excess inflows in general). One is a standards-based approach where the required level of protection is derived and defined based solely on a categorisation of downstream damage potential or hazard. The requirements for this approach are summarised in Table 4. However, in recent years the UK reservoir industry has moved towards an alternative risk-based approach, where the risk and consequence of dam failure due to floods are assessed and the tolerability of that risk evaluated. In that event, the risk of failure due to floods is reduced to 'As Low As Reasonably Practicable' (ALARP).

If the reservoir poses no risk to life, property or the environment, then the systems provided should be to an appropriate level to protect against harm to the owner's reputation and to generally ensure the ability for continued operations and the fulfilment of any licensing conditions. Also, consideration around the insurance requirements and the potential loss of income that would result from a major incident at any part of the PSH system. The cost of a passive spillway or other automated control systems should be considered within this context.

Even for “natural” flood events, some damage may occur to natural watercourses, especially when the flood is large and exceptional. It is therefore often uneconomic to provide a downstream waterway from the dam which is sufficiently large to convey all potential natural flood outflows. Some downstream damage associated with such discharges may therefore be considered tolerable. However, a PSH scheme spillway may not be designed to pass a natural event, but a man-made discharge many times larger than that which the natural environment has experienced. It may also occur outside natural seasonal variance. Therefore, the impact from such releases should be carefully considered and downstream protection or mitigation incorporated as appropriate. Such man-made releases are also arguably outside the standards-based approach of FRS and so call for risk-based methods to be employed.

In deciding if a spillway is required and for what capacity it should be designed, consideration should therefore be given to the magnitude of the over-pumping; the impact of any discharge on the downstream receptors and the proportionality of any safety works in relation to the risk they cause. The risk posed to the downstream receptors will need to be quantified, noting that this will not only consider loss of life, but may also include environmental and heritage receptors.

The test should therefore be as to whether “*adequate fail-safe provision*” has been provided and whether the residual risk can be considered ALARP. Whether or not a spillway is required and its capacity should be discussed and agreed with the Construction Engineer as early as possible in the project life cycle and documented clearly within a design statement to accompany eventual certification by the Construction Engineer. The designer and Construction Engineer should also clearly document the decisions taken and the reasons for doing so, so future Inspecting Engineers have sight of this and can be appropriately informed.

The potential exists for future Inspecting Engineers to regard the original design as insufficient for the associated risk to public safety. This may be due to personal experience, to guidance changes and/or influence from future related events including changes to downstream land use. The inclusion at the design stage of a robust method of allowing water to pass safely from the reservoir would reduce the risk of enhanced provisions being required later.

In considering the approach to upper reservoir spillway provision at PSH schemes it may also be useful to consider the approaches taken to date at existing UK facilities, both constructed and planned. There are currently, as of the Guide’s publication date, four operational pumped storage plants within the UK and a further major scheme where consent has been granted. They are summarised in Table 5 below.

In addition, it is worth noting that following the failure of the upper reservoir of the Taum Sauk PSH scheme in the USA (see Case Study), that country's standard is now to require provision of an unregulated spillway equivalent to the full pumping capacity of the scheme.

Table 5: Upper Reservoir Spillway Provision at UK PSH schemes

Power plant and upper reservoir	Date of construction	Spillway provision?	Spillway design parameters
Ffestiniog PS Stwlan Dam	1963	Yes	Over-pumping from all 4 pumps plus Probable Maximum Flood at the same time
Cruachan PS	1965	Yes	Full pumped inflow
Foyers PS Loch Mhor	1974	Yes	Capable of passing the full pumped design inflow, or safety case flood outflow, but not at the same time
Dinorwig PS Marchlyn Mawr	1983	Yes	PMF only (7 m^3/s), compared to 300 m^3/s pumped inflow. The lack of spillway capacity was justified by a generous freeboard and effective control system
Coire Glas (design stage)	Not yet constructed	Yes	Full pumped inflow capacity planned – at current design stage.

3.3. Lower reservoirs

As mentioned previously, the ICE's guide, *Floods and Reservoir Safety* (FRS) provides the principal design reference for defining the capacity requirements for the safe impoundment and conveyance of flood flows based either on a standards-based downstream hazard classification or on a risk-based approach. The requirements of the standards-based approach are summarised in Table 4.

For example, for the standards-based approach and where a reservoir poses potential harm to people in a community (Category A as defined in FRS) then a proportionate level of protection would be 'no damage or loss of life against a 1 in 10,000-year event'. But this would be coupled with the safety of the dam being assured up to the Probable Maximum Flood (PMF). The design provided should be expected to provide that level of protection reliably over the foreseeable life of the reservoir asset. Reasonable maintenance and reconstruction might be expected and suitable provision to enable this should be considered throughout the design cycle.

The FRS guidance recommends not only appropriate flood inflow conditions but also associated freeboard depths and acceptable wave overtopping rates. As this would be considered recommended guidance for decisions on freeboard allowance and overflow provision, it is suggested that any deviations from that guidance require clear explanation so that future Inspecting Engineers understand the decision process and may therefore be less likely to instruct significant and costly later changes. However, it should be noted that the FRS Guide is based on the current typical reservoir stock in the UK which are generally impounding reservoirs

formed of earth embankment dams with the majority of the inflow coming from direct and indirect catchments and therefore linked to rainfall.

As noted in Chapter 2, PSH lower reservoirs are typically created by using, and possibly enlarging, existing natural bodies of water in the valleys of mountainous or hilly regions. Inflows into such water bodies could comprise:

- Direct rainfall or snowfall onto the reservoir.
- Rainfall and/or snowfall runoff from the reservoir catchment.
- Artificial diversions from other catchments.
- Generation outflows from the upper catchment.

Apart from generation inflows, the remaining inflows are typical of most or many UK reservoirs. The required spillway capacity is then defined by customary natural inflow assessments, as discussed briefly at the end of Chapter 2 and using FRS guidance. Inflows from other indirect catchments are treated separately and whether they are included will depend on whether they are controlled or uncontrolled. In the case of controlled inflows from other indirect catchments, it is customary practice to assume that they would be closed off at times of flood or that their potential contribution is limited by the capacity of their conveyancing works.

In the case of PSH schemes it is reasonable to assume that generation could be paused or at least limited during times of exceptional natural flood inflows to any lower reservoir. It is therefore recommended that the spillway capacity for any lower reservoir is defined mainly by naturally occurring events, or that it is defined by some limited generation outflow coupled with the naturally occurring "design flood" for the reservoir. In the case of the more onerous natural "survival flood" this guide suggests that it is assumed generation has ceased.

However, during design development, it will be up to the Designer, the Owner and the Construction Engineer to agree and confirm such a major decision. The Owner or Operator may have opinions from an operational, safety, or reputational standpoint and may choose to adopt even more onerous conditions also reflecting considerations of additional storage allowance and/or reliability of control systems. In any event, the background to the design decision must be recorded in a design basis document which can accompany any future Construction Engineer's certification.

3.4. Spillway design

Spillways come in a variety of forms and geometries. At their simplest they might comprise only an overspill weir, usually in the form of a concrete crest to discharge downstream. The weir crest may be straight or circular, as in the case of a bell-mouth spillway or it may be artificially extended geometrically as in the case of a labyrinth. However, perhaps the biggest differentiation in terms of the intake works for a spillway is whether it is controlled (i.e. gated) or uncontrolled (i.e. ungated).

An ungated spillway is the simplest arrangement and offers arguably the best reliability, as it does not rely on any mechanical or electrical control works. However, it may require the dam crest to be at a significantly higher elevation than the spillway crest. As the incoming flood increases, the level in the reservoir will increase, putting water into storage. This will continue until the required design head over the weir is reached for peak discharge purposes. One

advantage of this is that water going into storage reduces the peak outflow requirement compared to the peak flood inflow. The disadvantage, as noted, is that the dam crest may need to be significantly higher than the overspill crest in order to contain the raised reservoir level. This increases the height, volume and therefore the cost of the dam. Getting the right balance between weir length and increased dam height must be done by economic optimisation.

On a gated crest, as the name implies, the water is retained by a gate sitting on the crest. This means that the volume above the spillway crest can be used for permanent storage rather than only filling at times of flood. In other words, greater reservoir storage for the same height dam is possible by using gates.

A good guide to spillway options in the UK is provided by the ICE publication *Reservoir Management* (2019). In practice, the majority of UK reservoirs are used for water supply in one form or another, and their spillways tend to be ungated. Hydropower reservoirs on the other hand, often do feature gated spillways for possibly two reasons. Firstly, maximising available head is important for hydropower generation and, secondly the availability of nearby power stations ensures the availability of adequate operation and maintenance staff to service the gates.

The design of spillway gates is a specialised field, but good guidance can be obtained by publications such as *Hydraulic Gates and Valves* (Lewin 1995) and *Design of Hydraulic Gates* (Erbiste2014).

3.5. Legal requirements and guidance

It should be emphasised that spillway works comprise three key elements and that under the English and Welsh Reservoirs Acts, the Inspecting Engineer is legally obliged to report their opinion on their adequacy. The three elements are:

- The spillway headworks or intake;
- The downstream conveyancing channel or conduit taking the flow to a point safely downstream of the dam;
- Downstream energy dissipation works designed to dissipate the kinetic energy of the flow before it is released further downstream into any natural channel or water body.

Within 2 years of a new reservoir receiving its final certificate by a Construction Engineer it is required to be inspected by a qualified Inspecting Engineer who has not been involved in the original construction. Further inspections will take place throughout the life of the plant at intervals not exceeding 10 years.

The Inspecting Engineer is required to present a report in a certain format and commenting on certain aspects. The aspects on which they are legally obliged to comment and give their opinion are not stated in the Reservoirs Act itself but instead in accompanying Statutory Instrument SI 2013 No. 1677. This states that Inspecting Engineers' reports must be written according to Schedule 5 of SI 1677, which lists:

- item (v) as "Findings as to the adequacy and condition of the waste weir or overflow and any channels connected with it" and
- item (vi) as "Findings as to the adequacy of the margin between dam(s), reservoir walls or embankment level and overflow level".

Similar advice in the Scottish Act is provided but as guidance rather than as a statutory requirement. The fact that the opinion of the Inspecting Engineer carries with it the legal power to demand change if considered necessary, emphasises the importance of treating all these aspects with due care, caution and recorded justification at the time of the original design.

A flood risk assessment may be required as part of the planning process if it is possible for the lower reservoir overflow to produce greater discharges than would naturally be expected downstream, i.e. where there is a chance of an additional flow to the naturally occurring flood flow. This could be the situation where any of the following exist:

- Operational discharge when lower reservoir is spilling;
- Gated spillway;
- In-direct catchments.

3.6. Managed overflow of the dam structure

While spillways are generally provided and sized to prevent dam overflowing and failure, there are some arrangements where overflowing of the dam may be acceptable. These are typically non erodible structures, such as concrete or masonry dams, or embankment dams specifically designed and protected for overtopping (such as some flood storage embankments). In this context, rockfill embankments are expected to survive higher volumes of wave overtopping flows than earth embankment dams, but washout of rockfill or its foundation cannot be ruled out and that could lead to the loss of structural support to the watertight element. Even where the dam form could be overtopped, it will still require a structural stability analysis against the risk of development of failure modes, such as scour at the downstream toe. A spillway could be sized to accommodate any natural inflows, or a proportion of the pumped inflow, whilst the dam structure is designed to be resilient to overflows during a full pumped inflow event.

3.7. Energy Dissipation Structures

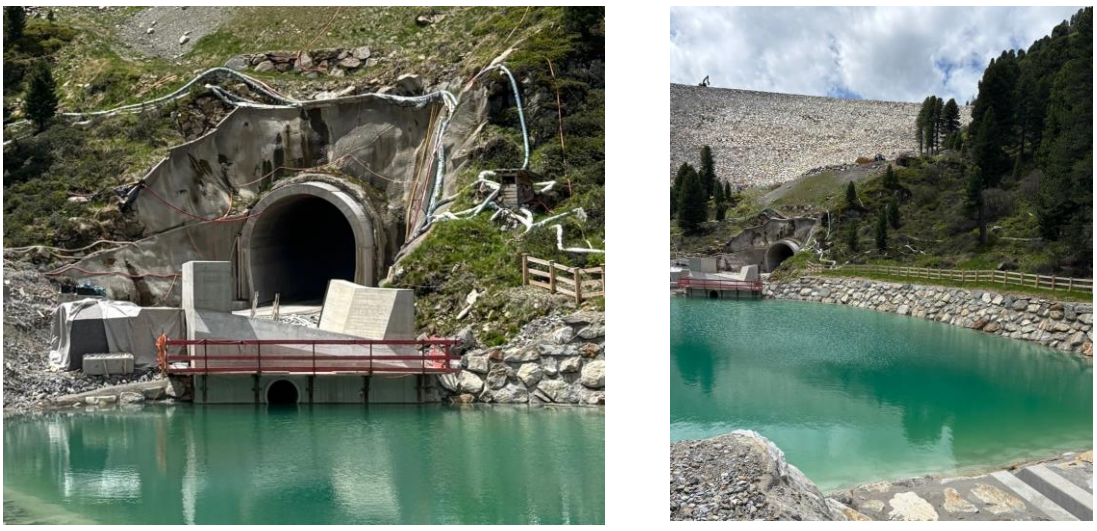


Figure 4: Kuhtai Project, TIWAG, Austria (courtesy of Tim Montagu, BHA ETIP Hydropower, May 2025)

This structure shows an energy dissipation ramp and pond where water plumes into the air, losing energy before continuing downhill via a man-made ‘mountain stream’ designed with twists and boulders to further reduce water flow and energy.

Level with the bottom of the dam wall of the upper reservoir, is the outlet for the spillway rated for 40 Cumecs or about 40% of the pumped inflow.

3.8. User Guidance

The following flow chart has been prepared to assist readers by showing the process of determining the requirement for a spillway and the considerations to be made both in design and risk mitigation.

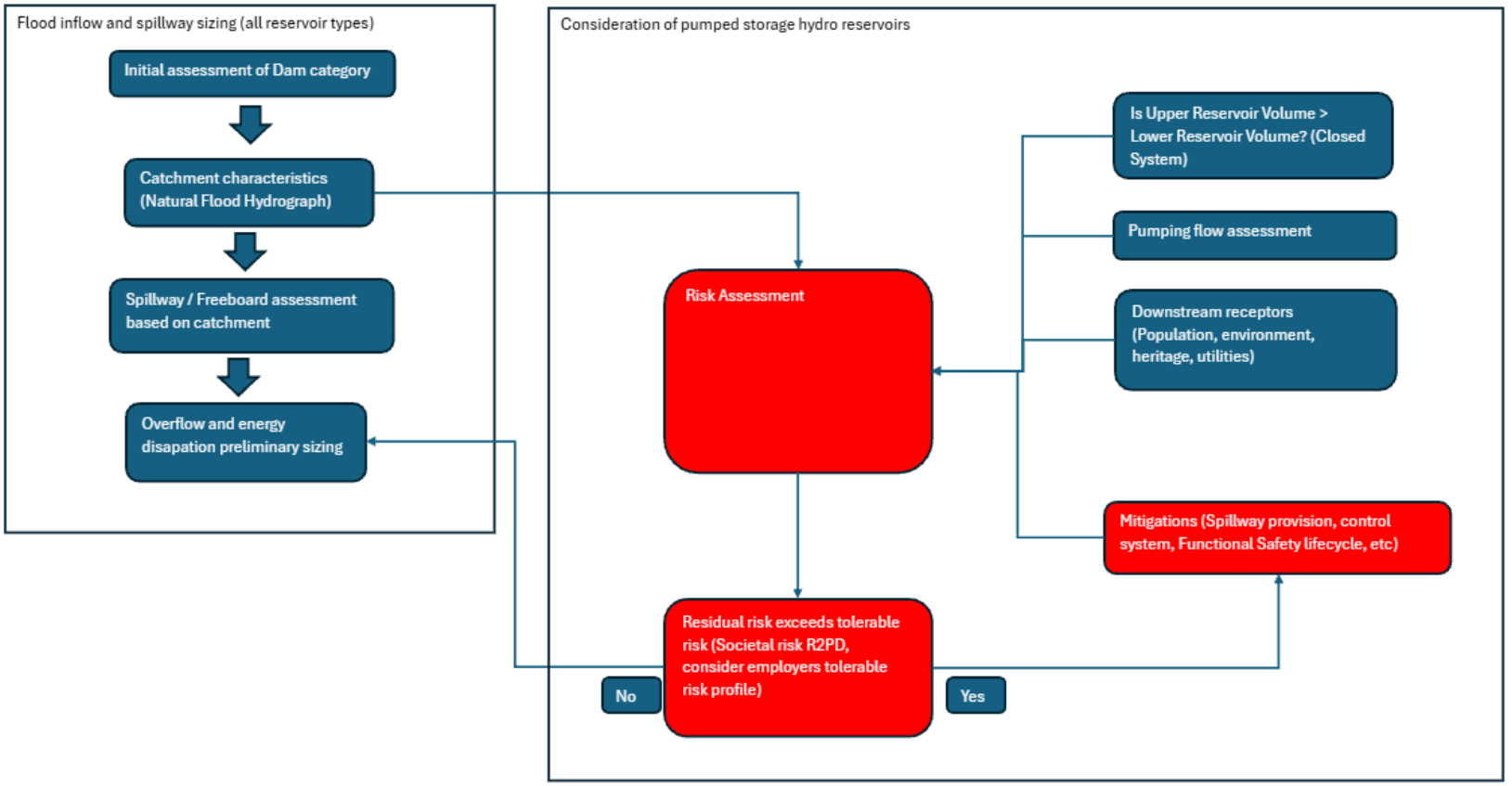


Figure 5: Chart depicting process of determining the requirement for a spillway

4. Chapter 4: Drawdown Works and Requirements

4.1. Introduction

Over and above the ability to pass surplus water at times of flood inflow, it is accepted as modern practice to provide a facility to lower the reservoir in the event of an emergency and hence reduce the likelihood of dam failure and the catastrophic dam outflow that this would produce.

This chapter provides guidance relating to such drawdown requirements for reservoirs that form part of PSH schemes. Whilst current guidance exists for the drawdown of reservoirs in the United Kingdom, this chapter provides additional considerations that are specific to the types of dams and arrangements that are more common on PSH schemes. These considerations should be addressed when assessing the drawdown requirements of an existing PSH scheme, or at the early stages of any new scheme.

The rate of drawdown of both the upper and lower (if present) reservoirs in a PSH scheme should be considered during normal operation, emergency conditions, maintenance, first filling, commissioning and valve testing. This rate, the facilities available to undertake the drawdown, and the associated downstream consequences, are discussed further below.

4.2. Dam types

Whilst the type of dams that may be associated with PSH schemes can vary, the most common dam types are likely to be those associated with hard rock foundations and were given in Table 2. Table 6 builds on that to summarise some reservoir safety conditions relevant to rapid reservoir level change that may be associated with emergency drawdown.

Table 6: Types of PSH dams and associated safety issues

Dam Type	Typical Characteristics
Concrete (all types, including RCC construction)	Low permeability and resistant to over-topping. Care needed to avoid structural cracking. Generally tolerant to rapid loading and unloading.
Concrete Faced Rockfill (CFRD)	Sensitive to face deformation, plinth joint leakage and settlement under cyclic loading. Set drawdown limits
Asphalt Faced Rockfill (AFRD)	As for CFRD dams but face sensitive to temperature change cracking. Face inspection access vital
Clay Core Embankment with earth fill shoulders*	Vulnerable to rapid drawdown, less preferable for large drawdown PSH. Follow EA/Defra 2017 drawdown guidance

Notes:
Slope stability of the reservoir rim should also be considered in relation to rapid drawdown.
*Acceptable factors of safety for embankment design may be higher due to cyclic loading.

The nature of PSH operation will subject the PSH dams to rapid and frequent reservoir level changes. This repeated cycling increases the importance of deformation monitoring, joint detailing, and material fatigue assessment compared with conventional water-supply reservoirs.

Whilst up-to-date drawdown guidance exists for UK reservoirs (EA/Defra 2017), that guidance is more relevant to embankment dams rather than the type of dams listed above. This is discussed further in the following sections, and additional guidance is provided for consideration.

4.3. Current UK Guidance

In an emergency situation there may be the need to lower the water level in a reservoir in order to reduce the loading on the dam and potentially prevent a breach of the dam. It is therefore essential that there is a fully functioning drawdown facility of sufficient capacity to draw the reservoir level down to an appropriate level and at an appropriate rate. Detailed drawdown guidance was published in 2017 by the Environment Agency / Defra in the *Guide to Drawdown Capacity for Reservoir Safety and Emergency Planning* (reference SC130001/V01), referred to as the 'drawdown guide' in the following sections.

According to the drawdown guide, the consideration of an appropriate reservoir drawdown rate is based on:

- Basic recommended standard (Section 6.3 of the guide)
- Vulnerability of the dam to rapid failure through internal erosion (embankment dams)
- Other factors (Section 6.5 of the guide)
- Precedent practice (Section 6.6 of the guide)

The drawdown guide also provides guidance on options for mitigating against insufficient drawdown capacity in Section 8. Mitigation would generally only apply to existing schemes and not new schemes. Mitigation includes options such as early detection of potential failure modes reduction of the likelihood of a particular failure mode through remedial works. Section 8 of the drawdown guide also provides guidance on evaluating mitigation options and assessing whether the cost of implementing a particular option is warranted by the reduction in risk it would achieve.

4.4. Embankment Dams

The basic recommended minimum drawdown rates as a percentage of reservoir height (H) are provided in Table 6.2 of the drawdown guide for the following dam types:

- homogeneous embankments
- zoned (clay core) embankments
- rockfill dams with a clay core

Table 7: Guide to drawdown capacity for reservoir safety and emergency planning, Source - Environment Agency / Defra, 2017 (reference SC130001/V01)

Dam category (Note 1)	Recommended minimum rate (Note 2)	Upper cap on practical drawdown rate (Note 3)
A (Note 4)	5% H/day (Note 5)	1 m/day

B	3% H/day (Note 5)	0.6 m/day
C or D (Note 6)	2% H/day	0.3 m/day

Notes

1. The dam category is defined in *Floods and Reservoir Safety (ICE, 2015)* based on the potential risk to life and downstream damage if the dam were to fail. Category C dams are those where there would be negligible risk to life, and category D dams are those where no loss of life could be foreseen.
2. The rates are based on drawing the reservoir down from top water level.
3. The cap is considered justifiable on the basis that higher dams tend to conform to higher standards of design, construction and general management; but where this is not considered the case, then it may be appropriate to raise the cap.
4. Category A dams are those "where a breach could endanger lives in a community". For particularly large communities (e.g. where the likely loss of life (LLoL) exceeds 100 people), consideration could be given to increasing the recommended rates to drawdown from that shown above.
5. For low height dams where there is a risk to life, the drawdown rate should be a minimum of 300 mm/day unless there are alternative emergency actions which can be implemented to mitigate the risk.
6. For category C or D dams, the recommended standard is based on protecting the value of the dam as an asset and avoiding potential reputational losses associated with dam failure. Departure from the recommended standard could be considered if these potential losses can be tolerated.

The focus of the drawdown guide, and the above recommended minimum drawdown rates, is on embankment dams. This included consideration of embankment dams with thin clay cores, steep slopes and no filters. Modern embankment dams would be expected to mitigate much of these factors.
As a result, the main failure modes that drive the specified drawdown rates relate to internal erosion and overtopping-type erosion. The drawdown guide is therefore considered to be appropriate to apply to embankment dams associated with PSH schemes.

The types of failure modes associated with embankment dams generally do not apply to other dam types such as concrete dams, and rockfill dams with some form of upstream impermeable barrier. For this reason, there is some guidance within the drawdown guide for 'other dam types', but the focus is on concrete and masonry dams.

It should also be noted that the drivers for dam failure, based on loading from the reservoir are subtly different between embankments and concrete dams. For example, it is normally accepted that the driving head for seepage and internal erosion in an embankment will be governed by reservoir head at the point of consideration. A 30% reduction in that head will give a similar 30% reduction in seepage driving head. However concrete dams tend to fail by sliding and the linear load on the dam is proportional to the square of the reservoir head. Thus, a 30% drop in reservoir head gives a 51% drop in load on the dam body. The total load reduction is even greater if the associated drop in lateral load is taken into account.

4.5. Concrete dams

For concrete dams, such as Ffestiniog (see Figure 6), the drawdown guide states (p. 62) that 'assuming the dam is still standing and therefore factors of safety for stability must be greater than 1.0 at that time, the purpose of drawdown should be to prevent water levels from rising

and to also bring about a lowering of water levels, but such a lowering could be relatively gradual.
Therefore, the purpose of drawdown for concrete and masonry dams is to:

- remove the load from the dam to ensure an increase in the factor of safety for stability;
- facilitate investigation and repair works;
- provide a buffer to absorb floods without water levels rising sufficiently to cause a failure mode to be triggered.

In the very worst outcome, the intervention of drawdown may at least reduce the consequences of failure by reducing the volume of water released in a breach.'



Figure 6: Ffestiniog PSH upper reservoir, Wales

The drawdown guide goes on to state the following to achieve this:
'The installed drawdown rate, D_I, and time to empty the top third of the reservoir volume, $T_{33\%}$, should be determined in the same way as for embankment dams following the guidance in Sections 3 to 5 of this guide. However, because the minimum recommended drawdown rates are less for concrete and masonry dams, the allowance for reservoir inflows is more likely to be a key factor in achieving drawdown and it is therefore even more important to carry out sensitivity studies for higher-than-average inflows.'

The *Engineering Guide to the Safety of Concrete and Masonry Dam Structures in the UK*, Report 148 (CIRIA 1996) notes that concrete and masonry dams are less likely to require a rapid drawdown when compared to embankment dams. However, the guide suggests that it is important that the top 10% of the reservoir should be able to be emptied 'reasonably quickly'. The guide also suggests a rate of 1 /m per day under 'average' inflow conditions (i.e., presumably the Q_{50}).

It is also useful and informative to look elsewhere for specific relevant guidance in the case of concrete dams. French and some US guidance generally give a recommended time for a 50% reduction in reservoir volume. This is similar to the drawdown guide's $T_{33\%}$. The maximum time for this reduction generally ranges from 7 to 8 days in the various guidance. This reduction in volume equates to around a 2.6% to 3% reduction in reservoir water depth per day.

4.6. Rockfill dams with an impermeable upstream face

The drawdown guide does not provide any specific guidance relating to rockfill dams with an impermeable upstream face such as CFRD or AFRD dams. However, these types of dams are also likely to be founded on hard rock foundations, and the embankments would not typically be susceptible to internal erosion. It is therefore suggested here that the drawdown rates associated with concrete dams, as detailed above, should also apply to these dam types. In the unusual case where a CFRD or AFRD dam is founded on soft foundations, the drawdown guide should be referred to by applying the guidance for embankment dams.

4.7. Recommendations

In summary, for earth-fill type embankment dams it is recommended that consideration be given to the adoption of the requirements of the drawdown guide where relevant for PSH schemes.

For concrete (including RCC), masonry, CFRD or AFRD dams it is recommended that the following points are considered:

- A drawdown rate of 3.0% height per day with Q_{50} inflow and compare this against the current UK concrete dam guidance of a minimum of 1 m/day.
- Consideration should also be made of the longer-term drawdown rate, as the initial drawdown rate, ensuring a reduction of 30% of the maximum reservoir water height (T33%) in 7-8 days with Q_{50} inflow.

The above assumes that all pumping and/or generation has been stopped prior to the drawdown commencing. The above should be considered for Category A and B reservoirs (current categorisation), which are the more likely categories when considering new PSH schemes that are likely to involve large volumes of water stored in reservoirs in elevated regions with some impact to lives on failure. More relaxed rates of drawdown could be considered for Category C and D reservoirs based on the drawdown guide and/or risk-based assessments.

For schemes where more than one dam type exists on the same reservoir, the drawdown rates for each dam type should be assessed and the most conservative drawdown rate should apply.

4.8. Facilities for drawdown

Methods of drawdown to meet the required drawdown rates for the upper and lower reservoirs include using:

1. The power waterways;
2. Any compensation outlets;
3. Any gated spillways;
4. Dedicated low level drawdown facilities.

They are discussed below under those headings.

4.8.1. Power station and hydraulic waterways

As noted in a previous chapter, the power waterway intakes in both upper and lower reservoirs will be sited at a low level to suppress vortices. They are therefore ideally suited to be perhaps the quickest way to draw down reservoir levels. They can also lend themselves to providing or assisting with any emergency drawdown requirements, provided they are available. In the case of the lower reservoir, that would require the system to be in pumping mode. In the case of the upper reservoir, it would need to be in generation mode.

However, whether such a use is intended would need to be decided at the time the works are designed and recorded in the appropriate operation manuals. Even if such usage is not intended, an operator may decide to use the power waterways for such a use in the case of an emergency. In either case, this requires careful consideration of a number of factors and risks including:

- The likelihood of the power station being available in an emergency;
- The grid having the capacity to accept generation so as to drawdown the upper reservoir and/or provide power for pumping to drawdown the lower reservoir;
- The likelihood of a power cut preventing generation or pumping;
- Periods of outage for maintenance;
- That the required drawdown level is still within the operating range of the pump/turbine unit;
- The lower reservoir must have sufficient capacity to absorb the discharged water;
- The upper reservoir must have sufficient capacity to absorb the pumped water.

The provision of multiple independent waterways and units, with independent isolation may only suit very specific site layouts. It would have the additional benefit of allowing a significant outage of part of the system whilst maintaining operation of one or more other sections. However, this will have no benefit if the grid is not available.

The issue of availability of the plant during planned maintenance outages can be mitigated by lowering the reservoir levels using the power station in advance of any significant outage. This however does not allow for unplanned outages / emergent work or power cuts preventing use of the Power Station to draw down the reservoir in an emergency.

4.8.2. Compensation outlets

Compensation flows are used to compensate for loss of natural residual flows and potential loss of habitat. For this reason, they may still be required for upper reservoirs with minimal catchments and hence minimal natural runoff. However, they are likely to be required for lower reservoirs.

There may be more than one dam at a reservoir, and if these impound across an existing watercourse then there may be a requirement to provide compensation at each dam. The compensation facilities could be considered to be included in the drawdown capacity of the reservoir.

These are likely to be sized to pass the minimum compensation flow at minimum reservoir levels, however at higher levels the capacity is likely to be greater, a control valve could be used to avoid releasing compensation above required levels. In addition, they could be oversized to provide additional flow capacity, up to the maximum considered allowable for that watercourse, so reducing the requirement for drawdown outlets on other watercourses.

4.8.3.Gated Spillways

As noted in previous discussions, it is likely that any spillway works associated with upper reservoirs and designed to accommodate emergency over pumping, are likely to be simple ungated weirs. However, in the case of lower reservoirs, possibly based on enlarging an existing reservoir, there is much precedent in the UK for hydro schemes to feature gated, surface spillways. These tend to be radial, vertical lift or drum gates operating on overspill crests set a few metres below top reservoir level.

Such gates also tend to have a significant capacity, based as they are for dealing with flood flows. As such their operation can be a very effective way of rapidly lowering the reservoir by a few metres. As we have seen from earlier sections, this can be particularly effective in reducing the load on concrete and rockfill embankment dams and so improving their security.

4.8.4. Dedicated Low-level Outlets

A low-level outlet should be located near the lowest point in the dam to allow the reservoir to be emptied in an emergency, or to allow maintenance to be undertaken. It could be designed and located solely for this purpose, placed within any construction phase water diversion or access structure through the dam, and may have other associated functions such as passing compensation flow.

Some schemes may have multiple dams. Incorporating all drawdown facilities in only one of the dams may reduce the reservoir safety risks associated with drawdown facilities to that dam. There may however be other benefits in including drawdown provision in some of the other dams, particularly if there is a requirement to have outlets for other purposes.

When designing the layout of the works, reference can be made to the guidance in Dams and Reservoir Conduits, Inspection, Monitoring, Investigation, Maintenance and Repair, CIRIA C743 (2015) and Pipework, Valves and Associated Equipment in Dams, CIRIA C789.

The following should be considered:

- Impact/risks to the dam - Pipework placed within conduits, location of conduit in the dam structure e.g., within the foundation, tunnelled around or below the dam;
- Upstream control and/or isolation;
- The design of the low-level outlet gate or valve should take into account the infrequent operational requirement and also that the gate or valve must work reliably when called upon to do so, given its inherent dam safety function;
- Access and provision for inspection, maintenance and testing of pipework, gates, valves and any associated control system infrastructure;

- Pipework and associated equipment designed for significant variation in head, and any requirements for control of discharge flows;
- Risk of blockage of inlet, screening arrangement;
- Additional functions. Inability to isolate for repair or maintenance if compensation flows to be maintained, requiring alternative means of passing compensation;
- The ability to wet test the system over the full range of the reservoir. Full wet testing may be constrained due to the impact on downstream receptors, and this should be considered. Current guidance is to fully operate valves and gates over their full range under full head if possible.

In an ideal situation it would be possible to provide a low-level draw down outlet that could drawdown and completely empty the reservoir at the required rate in an emergency. However, there may be a number of restrictions that limit the capacity of the low-level outlet, resulting in this facility not being able to provide the desired rate of drawdown. It may be possible to augment drawdown through other methods and operational rules for example:

- There may be other outlets such as compensation flow outlets at the dam. If these are separate from the drawdown system the contribution from these outlets could also be included;
- As already noted, if the power station is available, this will almost always be the quickest method to drawdown the reservoir. However, the power station may not always be available due to planned outages, unplanned / emergent works, or power outages. Some consideration and risk assessment could be undertaken to provide some allowance that the power station can contribute to the drawdown;
- If there are large direct or indirect catchments contributing to reservoir inflows, can these be managed to reduce inflow, so increasing the rate at which drawdown facilities can lower the reservoir.

4.9. Control of Incoming Inflows

Over and above providing reservoir drawdown facilities, in an emergency it will also be ideal to restrict any unnecessary flows from entering the reservoir. For example, this might be from adjacent indirect attachments or other supply facilities.

If there are any incoming indirect catchment inflows to the reservoir, for example transfer via tunnel or pipeline from another catchment, then these should be provided with a means of isolation to allow the inflow to the reservoir to be stopped. If there is a significant incoming direct catchment to the reservoir then it may be possible to divert some of the flow around the reservoir using a bypass channel or similar arrangement.

4.10. Legal Requirements and Guidance (UK)

As stated previously, within 2 years of a new reservoir receiving its final certificate by a Construction Engineer it is required to be inspected by a qualified Inspecting Engineer who has not been involved in the original construction. Further Inspections will take place throughout the life of the plant at intervals not exceeding 10 years.

The Inspecting Engineer is required to present a report in a certain format and comment on certain aspects. The aspects on which the Inspecting Engineer is legally obliged to comment and give their opinion are not in the Reservoirs Act itself but rather, are in accompanying Statutory Instrument SI 2013 No. 1677. This states that Inspecting Engineers' reports must be prepared according to Schedule 5 of SI 1677, which lists item (viii) as:

"Findings as to the efficiency of the scour pipe or discharge culvert or other means of lowering the level of the water in, and any means of controlling the inflow of water to, the reservoir."

Similar advice in the Scottish Act is provided, but as guidance, rather than as a statutory requirement. The fact that the opinion of the Inspecting Engineer carries with it the legal power to demand change if considered necessary, emphasises the importance of treating this aspect with due care, caution and recorded justification at the time of the original design.

4.11. International Context and Good Practice

Globally there is growing recognition of the need to consider operational drawdowns in reservoir safety planning. In jurisdictions such as the United States, Canada and parts of Europe, drawdown testing that involves high flows is increasingly incorporated into risk assessments. These regions place a strong emphasis on maintaining ecological flow conditions and protecting downstream communities even during emergency operations.

In countries like Austria, Norway and Switzerland, environmental assessments are required for planned drawdowns, and operational strategies are developed to minimise disruption. The use of flow monitoring, alert systems, and public communications is also more prevalent, contributing to a more proactive and transparent approach to risk management.

4.12. Testing of the drawdown system

The required capacity of the low-level outlet will be governed by the required drawdown rate. However, the capacity that can be released may be limited by the downstream capacity of the river channel and the risks to people, infrastructure, the environment and cultural heritage sites. In a reservoir safety emergency, some impact on receptors may be considered acceptable, for example erosion damage of the watercourse. This would not be the case for normal operations, which would include wet testing of the system.

It may be possible to demonstrate that the overall system operates by releasing smaller flows under the following scenarios:

- If there is more than one dam, then there may be more than one drawdown system, one at each dam, providing water diversion facilities during construction, compensation flow and sized to provide additional drawdown capacity;
- Providing multiple outlets on each drawdown system so that these can be tested individually, for example one pipe through the dam distributing through a manifold to two or more control valves;
- Fully testing outlets at lower reservoir levels to reduce discharges to prove the valve operates over its full range and then part testing valves at high reservoir levels to prove they operate at maximum head thereby limiting outflow;

- Providing isolation gates or valves to allow control valves and gates to be fully tested in dry and partly tested wet conditions.

During first filling of the reservoir the power station may not have been commissioned and so the low-level outlet may be the only means of drawdown. The following should be considered in the commissioning sequencing, due to the possibility of pumps being commissioned separately to the turbines:

- The means of drawdown to have been tested and commissioned “dry” before first filling and “wet” as soon as possible once filling commences;
- Testing at regular intervals during the first filling to confirm operation with increasing head.
- Closure of the construction diversion

5. Chapter 5: First Filling of the Upper Reservoir

5.1. Introduction

Most of the new schemes being planned in the UK use an existing loch or reservoir as the lower reservoir and propose the construction of a new upper reservoir. Dams are at a higher risk of failure during construction and first filling, or in the initial years of reservoir operation. Design, construction, and/or material deficiencies of a new dam may become apparent during the first filling. For example, excess leakage or seepage, cracking, and erosion are often noted when the reservoir is raised to new levels for the first time. The initial filling of a reservoir is the first test that the dam will perform the function for which it was designed. A carefully managed first filling plan is crucial to the future success of a dam.

5.2. Filling of upper reservoir

The following arrangements are possible for the upper reservoir of a new PSH scheme:

- Impounding reservoir with a sufficiently sized catchment to fill the reservoir;
- Non-impounding reservoir that relies on pumped flows for the reservoir's first filling;
- Impounding reservoirs with relatively small catchments that could take a long period of time to fill only with natural inflows.

The new schemes currently being planned in the UK are generally considering long duration storage and the upper reservoirs tend to have relatively large storage capacities when compared with runoff flows. For these types of schemes, pumping from the lower reservoir is likely to be required to completely fill the upper reservoir.

5.3. First filling plan

In the UK, the first filling plan is defined by the Construction Engineer in the Preliminary Certificate(s). The first filling plan can impose filling rates, restricted reservoir water levels ("specified level") together with other measures such as a monitoring/surveillance programme.

The dam will be equipped with instrumentation to monitor the behaviour of the dam and its foundation when subjected to the applied loading conditions. Checks of the readings and analysis of the data are required during construction, operation and during the first filling of the reservoir to understand the dam behaviour, detect trends and signs of abnormal behaviour that would prompt some actions. Due to the cyclic, rapid and large reservoir level fluctuations during normal operation, it may be prudent to also include the early stages of operation in the first filling plan where the dam will be kept under strict surveillance.

The first filling plan may also impose a minimum period that the reservoir needs to be kept full under strict surveillance before it can start being used for energy generation/storage. The upper intakes/outlets will be able to convey water in and out of the upper reservoir once the turbines are operational. However, if the first filling relies on runoff flow, even partially, then other outlets will be required to maintain the filling rates and to hold the reservoir level to the level specified in the Preliminary Certificate.

This requirement justifies the need to have a low-level outlet in the upper reservoir. Note that the capacity of the low-level outlet for this scenario does not necessarily need to match the

rates for emergency drawdown, but it will need to have sufficient capacity to discharge flood flows without significantly increasing the specified restricted level. In the US and other countries that follow the same practice, a capacity to pass the flood with a return period of five times the duration of the filling period is generally used. If the first filling is aided by a separate pump system and/or the Pump Turbine Units (PTU) then the filling process should also be planned, controlled and closely monitored. A low-level outlet may not be necessary if the PTU has been commissioned with low reservoir levels and the system is available to control the filling rate and, if required, quickly draw down the reservoir by operating the PTU in turbine mode.



Figure 7: Marchlyn Mawr – the upper reservoir for Dinorwig, North Wales

5.4. First filling within the construction and commissioning programme

New schemes take several years to plan, design and build and therefore it is critical that, after the commissioning and handover, the scheme and the upper reservoir can be operated without restrictions to maximise revenue.

The commissioning of the PTU will always sit in the critical path of new schemes and if the upper reservoir relies either totally, or partially, on the pumped flows, then commissioning of the PTU cannot be detached from the first filling of the reservoir. Therefore, there are two important aspects to consider in relation to the first filling:

1. The need to have sufficient water in the upper reservoir to commission the first PTU, noting that the preference is to start the commissioning in turbine mode. Note that the availability

of water in the lower reservoir also needs to be considered as it will be required to enable filling of the upper reservoir.
2. Following commissioning of all PTUs and handover of the scheme to the operator, it is important that the reservoir can be operated at full capacity with no restricted levels.

It is very important to develop a draft first filling plan during the early stages of the project so that the requirements of the plan can be considered in the design and incorporated into the construction/commissioning programmes of new schemes. This will help to manage expectations and justify the prioritisation of the reservoir works which will enable early first filling. The first filling could either be via runoff flows from the natural catchment or pumped flows. This will minimise risks of having to operate the scheme with restrictions on the reservoir levels following commissioning of the PTU.

6. Chapter 6: Downstream Releases and Consequences

6.1. Introduction

Releases from the lower reservoirs of a PSH scheme can include those from floods, from excess generation, for compensation purposes and from drawdown facilities. Where the lower reservoir is a new construction the downstream consequences of all such releases would need to be assessed. Where the lower reservoir already exists, it is likely that such aspects will have already been largely addressed. However, in the case of an upper reservoir, construction is likely to be new and as we have seen from previous chapters, there exists the risk of releasing significant over-pumping flows onto areas with minimal natural flow. New drawdown facilities at such a facility would have a similar capability. In all such cases, the potential for downstream consequences means that drawdown activities must be carefully planned and managed to protect downstream receptors including the public, infrastructure, and the environment.

This section addresses the downstream consequences associated with both unplanned over-pumping releases and drawdown activities in PSH schemes, considering both emergency drawdown events and routine drawdown testing. While differing in urgency, each scenario can have a range of consequences for downstream receptors. These consequences may result from rapid changes in flow, degradation of water quality, or the unintentional release of invasive species.

This section examines the key risks associated with drawdown operations and outlines measures to mitigate those risks through appropriate design, planning and operational practices.

In the case of upper reservoir emergency spillways, passive spillway systems and channels are anticipated to be able to convey the discharge to a point where there is no risk of damage to the dam. From this point, the flow could be discharged overland or within another form of structure. The decision on how to pass flow should follow ALARP principles and be based on adequate assessment of risk to the downstream catchment. This assessment will consider the impact on people, economic activity, the environment, and cultural heritage. The assessment should also consider the duration of overtopping as consequences of an emergency release will also be time dependent. If an over-pumping situation has occurred, it is likely that there has been a failure with the operating and control systems. The spillway may safeguard the dam from

complete failure, but it is possible that major damage to downstream receptors could occur due to an unintentional release via the spillway. The owner could face claims for damages, legal action, prosecution from SEPA / EA. Therefore, it is suggested that multiple levels of protection are considered, for example, water level monitoring or auto-ramp down of pumps. This process should be clearly documented and should be included with the reservoir records, so that it is available to future Inspecting Engineers.

Where flows are passed overland and no formal channel will be constructed, a hydraulic model should be developed using a Digital Elevation Model i.e., LiDAR, to confirm flow paths. This model will then be used to identify potential flood receptors between the spillway and receiving waterbody and develop appropriate mitigation measures. Whether or not the receiving waterbody forms the lower reservoir, it is important that the owners, authorities or agencies associated with the waterbody are consulted, as they will be key stakeholders, and will need to agree to any works required on their assets, i.e., upgrade of existing spillways etc. An assessment must be carried out on the receiving waterbody to determine if the flow of water released during operation of the spillway can be safely passed, contained and/or attenuated. Assessment of the receiving waterbody should consider the effect of receiving such inflows in isolation, i.e. not combined with a flood event, but with the starting water level in the receiving waterbody at Top Water Level (TWL). This approach is similar to that taken when considering a dam breach on an upper reservoir in a cascade.

If works are required, ALARP principles should be applied and be proportionate to the consequence of the receiving waterbody overtopping or breaching. It will be the responsibility of the PSH scheme developer to undertake these assessments and cover the cost of any upgrade works. With or without upgrade works, the developer should aim to maintain the current annual failure probability of the receiving waterbody.

6.2. Risk to life and public safety

Drawdowns and/or unplanned over-pumping releases that lead to high-volume discharges pose a significant risk to life and public safety, especially in emergency scenarios where rapid releases may overwhelm the capacity of downstream watercourses or discharge structures. The resulting flooding can occur with little warning, posing threats to downstream residents, recreational users, and emergency responders. In PSH schemes, particularly those located in upland areas, the high head and storage capacity can lead to sudden and intense surges of flow downstream when drawdown facilities are operated. Even during routine safety testing, similar hazards may arise if flow control systems fail or discharges are not managed appropriately.

Therefore, the risk to life and public safety needs to be considered during the design stage for all PSH schemes. Detailed hydraulic modelling should be undertaken to simulate potential drawdown discharges and their downstream impacts, including identification of vulnerable receptors such as residential areas, critical infrastructure, and recreational sites. This modelling would inform design modifications, such as the inclusion of energy dissipation structures, staged outlet controls, or flow attenuation measures, to mitigate rapid flow releases and reduce flood risk.

In England, Reservoir Undertakers are legally required to prepare on-site emergency flood plans for their large-raised Reservoirs. These plans are primarily aimed at preventing, controlling and

mitigating an uncontrolled release of water due to a dam breach or structural failure of the reservoir. Although not a requirement to be included in emergency plans, it is considered good practice for Undertakers to consider safe discharge methods within their emergency planning, taking into account the protection of life, critical infrastructure, and the environment downstream.

6.3. Impact on downstream infrastructure and property

High-intensity discharges during drawdown activities can pose a threat to downstream infrastructure such as bridges, culverts, road embankments, utility crossings etc. These structures may experience hydraulic loads exceeding their design capacity, leading to risks of overtopping, structural failure, scour, or erosion. Such impacts are more pronounced in confined or partially obstructed channels, where flow acceleration and turbulence increase vulnerability.

Mitigating these risks requires early and accurate hydraulic modelling to predict peak discharge rates, flow duration, and the response of downstream systems. Models should incorporate a range of scenarios, including partial blockages and equipment malfunctions. Downstream infrastructure at risk should be assessed for resilience under these conditions. Where needed, protective works such as energy dissipation structures, erosion control measures, or channel modifications can be integrated into the design. Flow control systems should be designed to allow staged or throttled release, if possible, thereby reducing the hydraulic impact on downstream assets.

6.4. Environmental consequences

Abrupt or sustained changes in flow conditions resulting from drawdown can have significant ecological consequences. Aquatic and riparian habitats may be disrupted by flow velocities that disturb substrates, displace fish and invertebrates, or damage vegetation. Where reservoir water is drawn from deep or stratified zones, discharges may introduce water that is colder, oxygen-depleted, or nutrient-rich, affecting downstream water quality and ecological health.

To address these issues, pre-drawdown ecological assessments are essential to establish baseline conditions and identify sensitive habitats. Drawdowns should be planned to minimise ecological shock, employing staged releases or limiting drawdown rate where possible. Monitoring of dissolved oxygen, temperature, and turbidity during and after the event can help inform operational decisions and guide recovery efforts. Environmental off-site mitigation should be considered - to prevent or minimise ecological harm.

6.5. Invasive and non-native species risk

Drawdowns have the potential to spread invasive non-native species (INNS) by mobilising viable organisms present in sediment, vegetation, or on infrastructure. These organisms may be carried downstream and colonise previously unaffected ecosystems, particularly where drawdown flows reach new catchments or ecologically sensitive areas. PSH schemes, due to their scale and inter-basin transfer potential, are particularly susceptible to this risk.

To mitigate the spread of INNS, biosecurity risk assessments should be undertaken prior to any drawdown. These should evaluate the likelihood of species transfer and identify containment

measures where appropriate. Where necessary, operational procedures should include protocols for inspecting and cleaning infrastructure, and for monitoring post-drawdown environments for signs of new introductions. Where risks are identified, reservoir operators should follow the guidance set out by the GB Non-Native Species Secretariat and ensure that all actions align with current legal requirements under the *Invasive Alien Species (Enforcement and Permitting) Order 2019* in England and Wales, and EU Regulation on *Invasive Alien Species (Regulation (EU) 1143/2014)* in Scotland.

6.6. Permitting and regulatory compliance

Drawdown activities that involve significant discharges to watercourses are regulated under the *Environmental Permitting Regulations* (EPR) 2016 in England and Wales, and the *Water Environment (Controlled Activities)* (Scotland) Regulations 2011 (as amended). Permits may be required where discharges alter the volume, velocity, temperature, or quality of receiving waters. Even if discharges appear benign, regulatory approval is often needed to ensure cumulative or long-term impacts are addressed.
Reservoir undertakers must liaise with regulators well in advance of planned drawdowns to determine permitting requirements and provide supporting documentation such as discharge estimates, water quality data, and mitigation strategies.

Emergency drawdowns carried out to prevent immediate risks to life or infrastructure may proceed without prior authorisation; however, operators may still be required to notify regulators retrospectively and provide a rationale for the actions taken. It is good practice to include permitting considerations in emergency planning, with pre-agreed contingency measures to streamline regulatory engagement when time is critical.

6.7. Duration of downstream releases

The duration of an overtopping event will depend on the cause of the release and in the case of an unintended release, the redundancy of any instrumentation and/or reaction time of personnel. It may therefore be necessary to undertake a risk assessment or simple flowchart type analysis, depending on the project stage. At an early stage a range of scenarios could be considered (e.g., 1, 6, 12 and 24 hours), which may help the operator decide how to set their maximum response time. The upper limit may be defined by the capacity of the lower reservoir and therefore this should be considered in determining the range of scenarios to be tested.

Pumped hydropower sites are typically locally operated in the UK, but future facilities could be remotely operated. They will be monitored through on-site instrumentation, likely to be real-time monitoring. Control systems are considered in detail in Chapter 8 in this guidance note, but consideration should be given to the potential for failures of instruments, alarms, power supplies and/or communications between instruments and end user.

In the event of an error or failure of the control system, CCTV or automatic system shutdown, the facility would require human interaction to manually close off the pumped inflow. For PSH there should be a requirement that the emergency response plan provides detail on how an over-pumping failure will be managed. The response time for any human interaction will need to account for alarm; reaction time; travel time and then operational action to isolate the inflow.

In the event of an external hazard, such as major flooding or a seismic event the failure of the pumps to shut down, or failure of alarms/ instrumentation could coincide with personnel being prevented from reaching the site or being needed elsewhere. This may be an example of double jeopardy, however, is an example of a plausible scenario that should be considered. It is suggested that during the design stage of a scheme, scenarios are tested using risk assessment or similar, to map potential scenarios and that this is used to inform decisions on the duration of overtopping to be integrated into the design.

6.8. Acceptable levels of damage

Any mitigation measures identified should be tested against ALARP principles, to ensure that they are proportional and that any residual damage is acceptable. The Guide to Risk Assessment for Reservoir Safety (RARS) includes advice on undertaking a qualitative (Tier 1) assessment, which could be used to better qualify what an acceptable level of damage would be. Section 5.2 of the guide explores the consequences of failure and considers the risk to people, economic activity, the environment and cultural heritage. By applying the high-level matrices within the guide, the designer can determine an overall consequence class for the asset and consider the benefit of any mitigation measures which may be considered.

By applying sections 5.2 and 5.3 of RARS to a series of different durations of overtopping, an assessment of the tolerability of a duration can be assessed. The designer may find that this provides some clarity between a tolerable or unacceptable duration and could be used as the basis of a decision on acceptable limits for overtopping duration.



Figure 8: Cruachan turbine hall: 4 x 110MW reversible Francis turbines can move 200m^3 / sec.

6.9. Mitigation

The mitigation for any planned or unplanned releases will depend on the sensitivity of any downstream receptors. For example, should a discharge pass safely along a downstream valley which can accommodate that flow without environmental damage and with no downstream receptors or human life at risk, then the mitigation would be much less onerous than the flow passing through an environmentally sensitive environment, or a residential or culturally sensitive location.

- ***Environmental damage*** should be considered with regard to the duration of overtopping, as a short duration event may be acceptable in terms of minor damage, compared to a longer duration which causes more erosion or habitat loss.
- ***Risk to human life*** would slightly depend on the duration, with a very short duration discharge potentially attenuating along the valley and resulting in minimal damage. However, once a duration is reached where flows would pass much further downstream, the impacts would be more widespread, and the severity of the consequences would increase.
- ***Damage to property or cultural heritage*** may be affected by the duration of the event and as with environmental damage, the affected property or heritage asset may be able to withstand a shorter event with only minimal damage.

Mitigation measures will depend on the size of discharge and the duration of overtopping as well as the sensitivity of the downstream receptors.

In the case of over-pumping, the simplest mitigation may be to consider a safety margin between the highest water level alarm and the spillway level, in order to accommodate an agreed duration of over-pumping. This would ensure an over-pumping 'buffer' before spilling but would of course come with an additional construction height cost penalty, which would have to be assessed and evaluated at the design stage.

Should this option not be feasible or proportionate, further mitigation measures should be considered. These can be grouped into:

- measures associated with the operation of the reservoir;
- measures to protect the downstream receptors or minimise the impact on them;
- a combination of both.

Other mitigation measures could include:

1. Multiple reservoir level sensors with independent communication routes
2. CCTV pointing at the overflow so the operator can see in real time what is happening
3. Manned facilities

An energy dissipation structure as seen in Figure 4 will reduce flow velocities at the exit of either the low-level outlet or spillway and such provision should be regarded as best practice, however this may not be sufficient to fully protect the downstream receptors.

An emergency plan for incident management at any large, raised reservoir will also be required. In England, this is now a statutory requirement, whereas in Scotland and Wales this is still considered best practice and most reservoir owners will have prepared one. Due to the potential scale and impact of an over-pumping event and also of drawdown releases, it is

advisable that both scenarios are considered in the on-site and off-site plans. Any emergency planning should consider a range of scenarios, including the risk of access to the site being restricted, with alternative access routes planned in advance.

7. Chapter 7: Operational Considerations

7.1. Design Narrative/Statement

Given the many considerations in the design of a pumped storage hydro scheme and associated reservoirs it is easy for the detail and reasons behind the final, as built, structures to be "lost". The Construction Engineer, in collaboration with the design team for the reservoirs, should clearly set out the design intentions for the final structure(s). This may best be detailed in a design basis report attached to the Reservoirs Act 1975: Certificate of Efficient Execution but, if not, should be in a document available for the lifetime of the dam structures. The Reservoirs Act is an ideal framework for this information to be recorded. It should include (but not be limited to) design constraints, design considerations, planning restrictions, factors of safety and any critical design assumptions for operational processes. It is also a fundamental requirement of Construction Design and Management Regulations (2015).

This information will be fundamental for refurbishment and upgrades to the power station in the future and to allow reviews of the safety processes as required. It should be updated as frequently as necessary for operational process changes, refurbishments or upgrades that change how the reservoirs are operated or maintained. Finally, at some stage the reservoir and structures will need to be decommissioned, and that generation of engineers will be grateful to have this valuable information available.

7.2. Operational Considerations

Pumped storage reservoirs can be filled quickly, far in excess of natural inflow, and in most cases exceeding Probable Maximum Flood flow. Some pumped storage reservoirs have been designed to be fully impermeable to avoid the erosion and instability that can occur due to rapid emptying and filling. Water with high concentrations of silt can cause problems to power station operators, reservoir water is normally used for cooling water, fire main supply and to supply water to pressurise seals. Turbine moving parts have labyrinth seals to prevent leakage, small diameter pipework for pressure measurement and control sensors and alarms. All are liable to fouling with silt.

Cavitation on turbine blades is also a consideration; silt in high concentrations can cause erosion, which may then initiate further damage through cavitation, caused by localised low pressure across the runner blades. Fully impermeable upper reservoir designs allow more locations for development; however, for economic reasons, when a natural valley is present, full coverage of the natural ground is not undertaken. In these cases, the designer may need to consider features to prevent silt as follows:

- Prevention of landslip from rapid drawdown of natural slopes;
- Wave rip-rap;
- Removal of superficial deposits near intakes;
- Allowance for unused 'dead' water storage below the intake sill of the power station intake to accommodate settled silt;
- Removal or covering of peat susceptible to drying and floating.

The requirement for spillways is discussed elsewhere in this document; however, the size of pump in relation to the volume and surface area of the reservoir should be a design consideration. The current pumped storage reservoirs in the UK were designed to be pumped

full in a window of time between around midnight and dawn. Future designs may have a faster rate of rise resulting in less time to react to prevent overflowing. Even if a spillway is provided to accommodate pump flow, the very high flow rate of a pump being released into a small catchment can be dangerous. The freeboard provided between different alarms and trip mechanisms and eventual spilling, alongside dam overtopping should have the rate of filling taken into consideration. The 'time-to-react' should be subject to risk assessment but the following should be included in the assessment:

- Number of people at risk downstream;
- Whether the control room is local or remote and the number of people on duty;
- Shutdown sequence time (multiple unit power stations may have hard wired delays built into the sequence to avoid stress to the power network meaning that pumps will continue to operate even after a shutdown signal has been received);
- Control initiation and sequencing is becoming partially or fully automated without the need for manned operational control rooms (remote or local) and machine learning or artificial intelligence may be introduced.

7.3. First filling

The first filling of impounded valleys, if possible, should be done after a period of natural inflow from the catchment area. Dam construction should be completed in advance of main works completion to allow for a 'dead' volume to be stored. This reduces the erosion and silt caused by pumping. Filling will be undertaken by pumps or pump turbines to pump water; however, designs may require dedicated first filling pumps for the waterways and the "dead" volume of the upper reservoir. In these instances, the first filling pumps should be used first to reduce the amount of silt disturbance on first filling and allow controlled watering up of the waterways and avoid damage to the pump turbines. Reservoirs may have river compensation arrangements or catchment capture incorporated into the design, these should be utilised, or limited in the case of compensation, to improve the initial filling to create an effective 'dead' volume. Nearby rivers or natural lakes should also be considered for extraction, if reasonably practicable.

The nature of pumped storage allows for rapid lowering of reservoirs in the event of problems arising such as excessive leakage during filling; however, initial filling to create a 'dead' volume may give an opportunity to evaluate performance and undertake remedial work in advance of the main filling.

The PSH commissioning engineers should consult with the Construction Engineer to ensure that their sequence of work is compatible with safe first filling. Generators that would normally be available to empty the reservoir in an emergency may not have been commissioned fully even if the pumps are. Commissioning engineers may also want to undertake tests, such as overspeed, and valve and gate closures. The Commissioning Engineers should consult the Construction Engineer before making any changes to the operation of the reservoir.

7.4. Ancillary structures

Pumped storage reservoirs will incorporate large diameter pipes or tunnels and other ancillary features that may raise doubts as to where the reservoir ends. The Reservoirs Act excludes mines and canals but is silent on pumped storage tunnels.
Within the Guide to the Reservoirs Act 1975 (2014), the section describing common types of reservoirs includes the following relevant statements:

- *Ancillary structures form part of the reservoir and must be supervised and inspected along with the main impounding structure.*
- *The extent of the inflow and outflow conduits considered to be part of the reservoir should be considered as the limit at which failure of a pressurised conduit would pose no risk to the safe operation of the reservoir.*
- *The point at which infrastructure does not form part of a reservoir is determined by where its function is not relied upon for safe reservoir operation. For example, if pipework beyond the dam toe is relied upon for emergency drawdown provision or drainage monitoring, then all pipework upstream of the outlet providing free discharge shall be considered part of the dam, even if it extends well beyond the dam footprint.*

The above statements imply that a conduit is not considered part of the reservoir if its failure would not affect the 'safe operation' of the reservoir; however, it misses the significance of the size of the conduit as most reservoirs will have relatively small sized conduits, compared to pumped storage tunnels. Therefore, in ascertaining the extent of the 'reservoir', the first factor that should be decided is whether the failure of an ancillary structure would cause an uncontrolled release of a sufficient volume that it could have an impact downstream analogous to a reservoir breach.

The second factor to be reviewed in the decision to include an ancillary structure is the consideration of the stored volume of the reservoir. The Act defines the stored volume as being that which can be released above lowest natural adjoining ground level. A tunnel may lead from a reservoir and emerge further downstream where it could fail *above natural ground level* thus emptying the reservoir towards a downstream community. Again, the failure scenario must be of sufficient volume that it meets the threshold of the Act, it is uncontrolled and should consider the consequence of the breach on the inundated area downstream.
Some pumped storage power stations include surge ponds.

A third factor, uniquely applicable to these features, is the consideration of a temporarily stored volume of water. Ancillary works of this kind are not capable of storing water in the same way as conventional reservoirs, as the water exits at the same rate as it entered; however, they do fall under the remit of the Act as they are "*designed or used for collecting water and storing water*". In addition, the Act, as it was originally written, calculated the volume of a reservoir up to the sill of an overflow implying that a flood rise volume was excluded, an anomaly for flood storage reservoirs corrected by Statutory Instrument 2013 No. 1677. This SI states that the top water level is defined as:

> *2(1)(c) In the case of a reservoir designed for the purpose of holding back floodwater, the maximum level to which floodwater may be stored during any flood event exclusive of any provision of overflow*

Although the above was not written for pumped storage surge ponds, the similarity is clear.
At Dinorwig Power Station, the upper reservoir has a 9m diameter 1600m long tunnel that terminates at a surge pond structure. A failure at the adjoining construction tunnel plug, could

qualify as ‘lowest adjoining natural ground level’. The tunnel and pond arrangement then lead to a shaft and tunnel system that supplies water to the individual turbines where there are another construction tunnel plug and six large diameter valves. The next qualifying ‘lowest adjoining ground level’ in this system is the tunnel entrance to the underground works at the shore of the lower reservoir.

At Dinorwig Power Station, a decision was made to register the upper reservoir as one asset under the Act, and the surge pond structure as a separate asset. The plug at the lower end of the system was considered for registration but was rejected by the first Inspecting Engineer appointed under the Act. The plug adjoining the surge pond was ignored, and the surge pond included on the basis that, in a surge scenario, it could temporarily store water above the threshold volume. It is worth noting, however, that the Engineer expressed doubts that it met the criteria as written in the Act. At Dinorwig Power Station, the limit of the upper reservoir has been set at the headgates controlling water flow to the 1,600m long tunnel; the surge pond is registered separately, and the remaining system is excluded. At Ffestiniog, the limits are given as the headgates at the reservoir intake.

The Construction Engineer appointed under section 6 of the Act may decide on the inclusion or exclusion of ancillary works early in the design process based on the best available information at that time. These early decisions may be difficult to justify by future Inspecting Engineers. For this reason, it is important that the functional safety of any gate, valve or turbine involved in controlling a release and movement of water is understood early in the power station’s design process so that the reservoir limits are defined appropriately to ensure public safety. A comprehensive record of the decision process and justification for the extents of the reservoir should be made and saved with the reservoir record for future reference.



Figure 9: Surge Pond at Dinorwig (courtesy of Bryn Williams, First Hydro)

7.5. Timing of inspections

The Reservoirs Act 1975 requires the appointment of a Construction Engineer during the dam build phase. Most conventional impounding reservoirs would be under their supervision until

the reservoir is at least filled enough for them to be satisfied with the performance. The Act requires an independent inspection within two years of the Construction Engineer's final certification, after which the new Engineer will decide on the frequency of inspection. The frequency of visits is the Inspecting Engineer's prerogative. In some circumstances, they may decide to sanction inspection before the minimum 10 years until they were satisfied with the performance. It is not unusual for the minimum 10 years to apply to pumped storage reservoirs; the ability to empty the reservoir quickly and safely balances the increased burden of daily emptying and filling.

Supervising Engineers are appointed after the issue of the Final Certificate by the Construction Engineer, and although not required by the Act, it is usual for a Supervising Engineer to be familiarising themselves with the dam before issue. Afterwards, the frequency of visits should be recommended in the report appended to the final certificate. Frequent visits may be recommended initially; weekly visits are not unusual in the first few months, and thereafter, every month or quarterly. It is important to note that the Construction Engineer, in the case of pumped storage reservoirs, will be able to witness many cycles of emptying and filling, and is therefore better placed to judge the ongoing requirement for future inspections than would normally be the case.
The use of dam surveys over the full cycle of empty to full reservoir will yield information which can be checked against design criteria and expected structural movement.

7.6. Staffing and Maintenance

Pumped storage reservoirs are unusual in that they are subjected to many hundred times the number of cycles of conventional reservoirs, which may only have one cycle per year for drinking water supply. Not all dams are the same, but settlement, in some cases, is proportional to the number of cycles. Damage to water retaining elements may be more pronounced and more regular dimensional monitoring and instrumentation readings are required to predict future maintenance and repair.

Critical to the ongoing safe operation of the reservoir is the maintenance of the alarm and shutdown system. This should be tested regularly and elements that contribute to its continuing health, should be subject to scrutiny. Crest settlement, where it reduces the margin between alarms and overtopping, should either be restored or the alarm levels changed accordingly. Any blockages or threats to the correct operability, e.g., debris to intake chambers, should be cleared immediately. Any change or compromised system should be subject to a 'Control of Change' procedure, and all staff should receive training in system maintenance awareness including the implications of failure.

During prolonged maintenance periods, the reservoir may be held at the same level and gates or valves considered to be 'appurtenant works to the reservoir, closed. These gates or valves will then function as elements keeping the reservoir water from escaping. The Construction Engineer will normally include any 'appurtenant works' in the report appended to the final certificate. Appurtenant works are features that, in the opinion of the Engineer, form part of the reservoir. The Guide to the Reservoirs Act 1975 contains the following:

'The extent of the inflow and outflow conduits considered to be part of the reservoir should be considered to be the limit at which failure of a pressurised conduit would pose no risk to the safe operation of the reservoir'.

The main gates or valves of the supply tunnel, pipe or conduit leading from the reservoir should therefore be considered to be part of the reservoir by the Construction Engineer and subsequent Inspecting Engineers. The inclusion of any features beyond these is subject to the judgement of the Construction Engineer.

Staffing levels and maintenance will vary over the life of the reservoir, as will the operational framework. It is certain that staff will change during the lifetime of the PSH; to ensure that the dangers of maloperation are understood, staff training and familiarisation of operational systems will need to be renewed periodically. This also applies to contractors, where the maintenance is outsourced, who may not have detailed knowledge of the reservoir and its safety systems.

PSH have the ability to adjust their generating and pumping output by algorithm, this has the benefit to the Grid Operator of matching supply to demand automatically. This is done by measuring the frequency of the National Grid; reducing frequency indicates an increasing demand, and generators can automatically increase output. In pump mode, this introduces the risk of output not being in the control of an operator, but automated. Decreased coal generation and increasing wind, has created a demand for generator inertia (the ability to absorb sudden grid variations through the angular momentum of the generator), meaning that frequency-initiated generation and pumping has become a more important feature of PSH.

The Reservoirs Act's Inspecting Engineer should understand these processes for each of the reservoirs and make risk-based judgments on the level of supervision required in the interest of public safety.

7.7. Water management

Pumped storage Reservoirs can be closed loop or partially closed systems that are not part of a natural river catchment or are only partially part of one.

Foyers and Cruachan have lower lochs that are part of substantial natural systems that, due to their size, vary in height by a small amount and therefore, abstraction limitations aside, are not difficult to manage from the point of view of the impact on the power operator. Ffestiniog has a lower reservoir that has a significant catchment compared to its volume, whereas Dinorwig has a lower reservoir created by impoundment of a valley whose catchment is largely diverted to prevent it flowing into it. Foyers has an upper reservoir with a relatively large natural catchment, whereas Cruachan has a very small catchment but with a catchment-capture element from an adjoining valley, whereas Dinorwig and Ffestiniog upper reservoirs have very small natural catchments with corresponding very low inflow.

In each case above, the operators will balance the incoming water to either lower or upper reservoir and act according to their specific circumstance. The operators of Cruachan and Foyers may decide, for example, to avoid pumping to their fullest extent if the incoming catchment yield is expected to be high. Dinorwig, a near-closed loop system, requires any direct rainfall and

groundwater infiltration into the lower reservoir to be spilled to allow sufficient space for generating. At Ffestiniog, the lower reservoir's catchment must be continuously discharged to avoid curtailment of generation. Although presently absent in the UK, reservoirs where the floor and upstream water retaining elements are continuous and leakage or infiltration is very small, evaporation may be the dominant factor, in which case, supplementation from a nearby watercourse may be necessary.

New pumped storage reservoirs will have their own unique features needing a specific water management plan which should include normal and abnormal conditions (e.g. pumping during an extreme flood event) and cases of maloperation (e.g. actions required if pumping has continued beyond automated shutdown levels and the switches have failed to initiate a trip).

7.8. Energy Management

PSH are traded from energy trading centres usually situated remotely. Traders buy and sell the energy as GWh and may become detached from the reality of what this means in water level. Traders will utilise the energy fully with little or no margin for error, and in the process of multiple trades, find that the GWh to be delivered differs from their target.

The control and instrumentation engineer should make the Construction Engineer aware of any delays in the shutdown sequence so that the buffer zone is not breached. They should monitor the accuracy of their stored energy delivery so that they can make a judgement on whether the buffer zone is adequate.

The Construction Engineer and subsequent Inspecting Engineers should also be mindful of any changes in the PSH over its lifetime and how this affects water level. As the PSH ages, the traders may decrease their GWh target, and if a generator is refurbished, restoring efficiency, increase their GWh.

7.9. Longer term use of Reservoir

Existing pumped storage power stations were designed for long service life, nominally an 80-year life, with major replanting at 40 years. There was no clear strategy for what would happen at 80 years but it's likely that another replanting, with perhaps extensive civil works would be undertaken at that time, assuming that there is a continuing requirement for pumped storage. If not, the reservoir may be re-purposed for conventional hydroelectric power or drinking water supply. The Inspecting Engineer should consider the implications of the power station turbines not being available with a possible reduced rapid drawdown capability with the usual water level management system also unavailable. For example, a larger capacity emergency drawdown may be required if the power station is decommissioned.

Any future change in the management of the reservoir should prompt the Supervising Engineer to call a section 10 inspection under the Reservoirs Act early. The Inspecting Engineer should then reconsider the new management requirements of the reservoir.

7.10. Securing Critical National Infrastructure

This section aims to consider aspects of the physical security of a site and the associated electricity infrastructure. A full appraisal would require a stand-alone paper and likely involve engagement with the National Protective Security Authority, the Department of Energy Security and Net Zero, the National Energy Systems Operator, the National Cyber Security Centre, Ofgem and the Ministry of Defence. When Dinorwig was built in 1983, the MoD took a keen interest in how the upper reservoir could be damaged by sabotage. At the time, the IRA represented the threat of such actions and whilst today there is no specific threat to inland UK energy assets, the design of new energy infrastructure should consider how to safeguard equipment and the impact on the electricity grid of a power station being disabled by malicious activity from third parties.

The UK's transmission lines, sub-stations and other energy infrastructure are relatively open to attack on the basis that it is impossible to secure all equipment. Security agencies operate on an intelligence-led basis, understanding a likely threat rather than protecting assets from a range of possible threats. However, it should be feasible to design infrastructure at minimal extra costs, that increases security from sabotage. Such measures could include:

Physical Security:

- High fences around the upper reservoir and key infrastructure;
- Cameras with both day and night vision enabled and AI-enabled alert systems;
- Lighting triggered by movement within the secure fenced area;
- Access roads – designed to make the approach difficult undetected;
- Limit access points with security personnel, ID checks, and biometric scanning;
- Underground substations and protected control systems;
- Embankment dams offer the best protection from blast impact.

Surveillance and Emergency Response:

- 'Pattern of life' monitoring, what is normal? How close can hillwalkers get?
- Random security patrols to demonstrate presence and monitor activity;
- No-fly drone areas for threat reduction and to spot unusual activity;
- Community engagement – ensuring they know how to report unusual activity;
- Emergency response training – for site staff and communities.

It is understandable that the design of new PSH projects may not satisfy all security arrangements, but acknowledging a potential weakness through improved physical security, surveillance and emergency response planning is important risk mitigation for such critical national infrastructure.

8. Chapter 8: Control Systems

8.1. Introduction

This chapter is intended to introduce and outline control systems and functional safety considerations for pumped storage hydropower stations. It is intended to draw attention to key considerations which could influence on-reservoir safety. Where appropriate, existing standards and guidance are referred to for further information. For a robust and reliable control system, suitably qualified and experienced individuals must be responsible for the design, manufacture, installation, commissioning and operational phase maintenance and upgrading that make up the lifecycle of the control system. Any control system should be implemented with thorough testing during manufacturing and commissioning stage then ongoing testing as part of operative training.

8.2. Control System Architecture

Modern pumped storage facilities use sophisticated Distributed Control Systems (DCS) which provide a central point for automatic operation of the plant, protection functions to initiate a plant shutdown in the event of abnormal operation and collect and record all operational data and alarms. The DCS system has several advantages over a traditional centralised control system such as Supervisory Control and Data Acquisition system (SCADA). The DCS platform is engineered with redundancy at its core, infrastructure such as controllers, power supplies and networking switches will all be redundant to tolerate failure of individual components and minimise downtime. Sensitive components such as the controllers will be installed in climate-controlled server rooms away from the potentially hazardous process areas which reduces the potential for premature failures and corresponding system outages.
A DCS is structured to provide several layers in a hierarchy which is simplified into the diagram shown below.

The levels in Figure 10 can be described as follows:

- Level 4 and 5 depict the enterprise level systems which can be considered as the administrative networks (information technology (IT)) associated with the plant used for business and management purposes.
- The Demilitarized zone provides a hardware and software cyber security barrier between the enterprise network (IT network) and the operational technology (OT) zone.
- Level 3 (operations support) provides the operations support level where engineering and analysis functions can be performed to evaluate plant operation and amend automation routines.
- Level 2 (supervisory control) is the main operator interface with the operator workstations allowing for full monitoring and control of the plant from a single workstation.
- Level 1 (control devices) are the plant controllers which contain the processors which run the software prepared for control of the plant.
- Level 0 (field devices) for all equipment in the process areas such as instrumentation, analogue and digital communication cables, input/output PLC cards, panels, valves and actuators responsible for adjusting and changing process parameters.

Depending on the performance requirements a further independent safety control system (or Safety Instrumented System or SIS) may be necessary to deliver the required reliability for critical functions. The specification and engineering of such a system may be defined and assured by adhering to existing standards as are introduced in the following sections. Components of the Safety Instrumented System (SIS) have a “Mission Time” which defines their useful life. This is stated in the relevant Safety Manual which the manufacturer provides. Once the Mission Time is exceeded, the relevant component must be replaced. The maximum duration typically quoted would be 20 years, but other components are quoted at lesser durations such as 5-15 years.

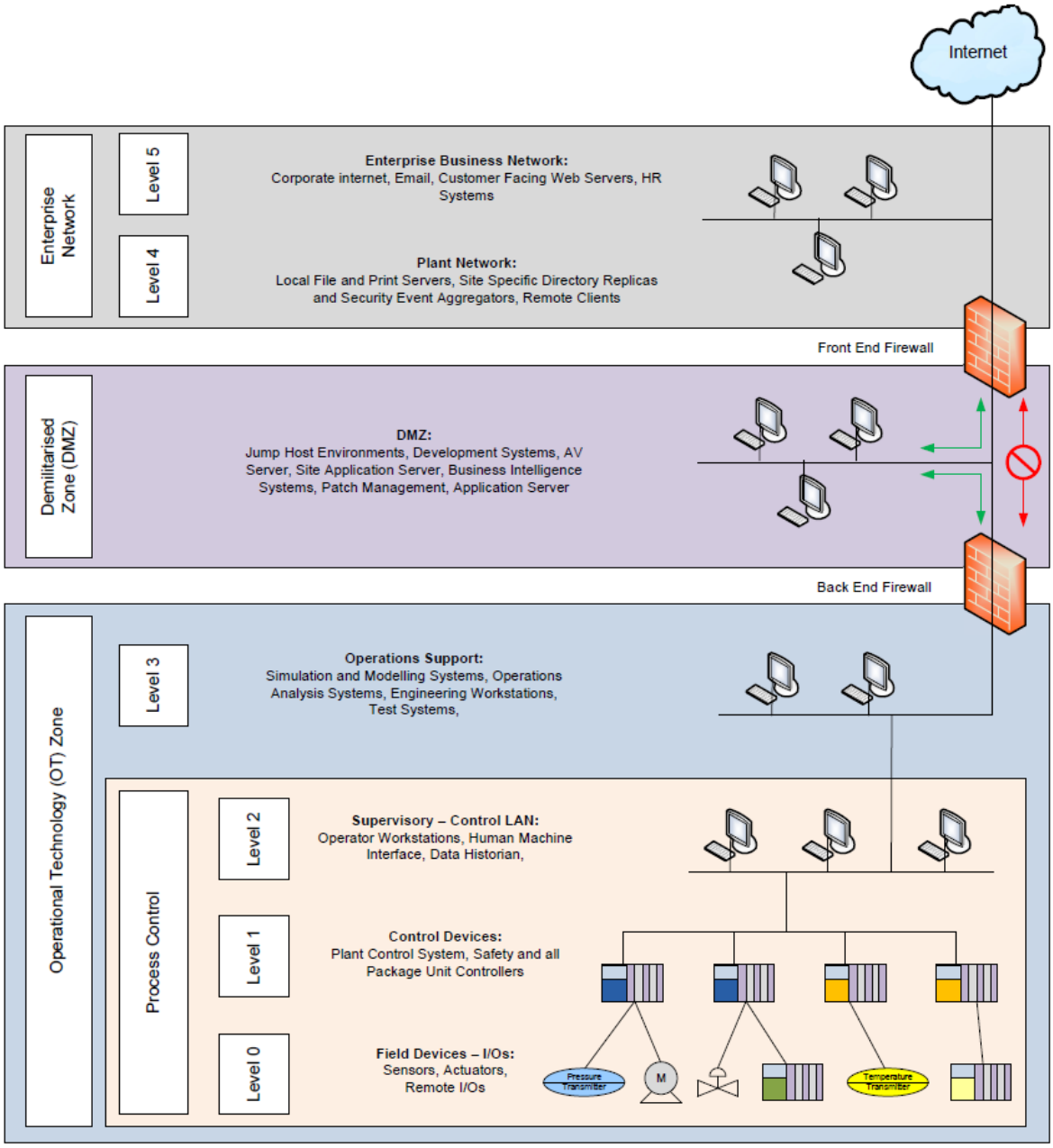


Figure 10: Plant control system architecture (Source: Fichtner Consulting Engineers)

Original Equipment Manufacturers (OEMs), as part of their scope of supply will normally specify and design the DCS to provide the automatic control and monitoring of their supplied equipment. Considerations of availability and reliability need to be defined to ensure that the system delivers an appropriate level of redundancy with robust and reliable technology. The DCS hardware and software architecture provides the potential to segment the layers of the hierarchy and incorporate redundant elements to improve availability and reliability of the control system. Depending on the performance requirements a further independent safety control system may be necessary to deliver the required reliability for critical functions. The specification and engineering of such a system may be defined and assured by adhering to existing standards as are introduced in the following sections.

8.3. Instrumentation

It is strongly recommended that a structured, multi-systems approach is used to select instrumentation for control systems in water conveyance projects such as Pumped Storage Hydropower. The first steps should identify the functional requirements of the water conveyance and specify the focus and boundaries of a specific and detailed examination to determine the need for instrumentation.

Later steps describe the process and basic principles for conducting Hazard and Operability (HAZOp) and Failure Mode and Effects Analyses (FMEA). The output from these analyses is used to determine the instrumentation and monitoring requirements of the systems associated with the water conveyance. **Error! Reference source not found.**Figure 11 provides an overview of the process.

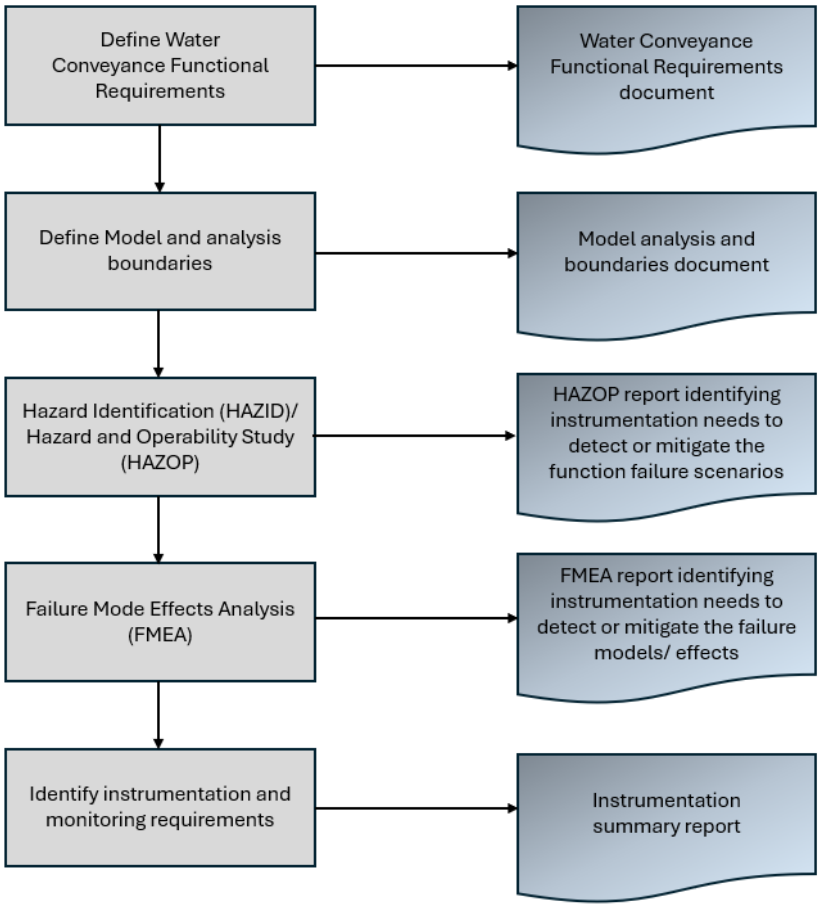


Figure 11: Overall Process: Assessment and Outputs

The HAZOP process will provide a clear understanding of the hazards and potential operability problems associated with the system, contained within the pre-defined boundaries. The functional requirements themselves will then be used as a tool to identify the scenarios and consequences where they are not met and to further highlight any safeguards, including instrumentation needs. The emphasis will be on instrumentation needs to safeguard the initiation of operation as well as feedback requirements that the required operation has been performed.

The FMEA will identify the boundaries, relationships, dependencies, and interfaces, defined in the earlier analysis. The associated designs of each of the sub-systems will be broken down into their constituent elements so that the failure modes and their effects can be identified. The functional requirements will be used to define the design intent of each sub-system/element. The potential mitigation and means of detection will be identified that will highlight the specific instrumentation needs.

Instrumentation needs will be identified via both the HAZOP study where these are safeguards against the scenarios, as well as the FMEA where these provide mitigation and detection against the failure modes for each subsystem/constituent elements.

The collated instrument list will be further assessed in a FMEA study to identify the failure mode of each instrument type and depending on its design intent, and the degree of criticality, establish the requirements for enhanced resilience (i.e. redundancy), that would need to be considered in the design process. Consideration of the architectural requirements dictated by a functional safety standard such as BS EN 61511 may also require specific levels of redundancy in control system components such as instrumentation.

The final stage will summarise the instrumentation needs identified in the previous step and examine the various options for instrument types that could be used to satisfy the specific requirements for each application.

On a more general note, there are several points relating to the use of instrumentation that should always be considered:

- The use of alternative or different technologies is considered to represent best practice when trying to monitor water levels (e.g., radar, ultrasonic, pressure transducer) such that the possibility of common cause failure will be removed.
- Similarly, the use of diverse technological solutions for measuring process metrics is highly recommended.
- Whatever the variable being monitored, the use of redundant instruments is also considered to represent best practice in that the failure of one unit will not prevent the control system from continuing to operate, thus allowing time for the failed unit to be replaced.
- The location of the installed device is also critically important, as the device could be adversely affected by eddies, crossflows or other disruptions such as maloperation or sabotage.
- CCTV should be used as a further means of observation for operators in the control room and remotely. While such information cannot be interfaced directly into a control system, it provides a means of visually verifying the status of the plant and plausibility of reported readings.
- There needs to be regular scheduled maintenance and calibration of these devices if they are crucial to the overall reliability of the control system.

8.4. Communication

Modes of communication can be used to transmit and receive information, whether that be voice or data traffic. In the specific instance of control systems for water conveyance systems, we are most interested in “signal” data traffic (e.g. from remote sensors), particularly as that relates to the acquisition, interpretation and usage of that data.

In the vast majority of cases, the connection between remote sensors and the control system (which could be a PLC or relay-logic based system) will be hard wired. This is conventional technology and utilises copper-cored cables that are both readily available and cost-effective.

Modern trends may lead to the increased use of fibre optic cables as the amount of data that can be transmitted is far in excess of the copper-cored cable alternative. The risk of electromagnetic interference (EMI) is also significantly reduced with the use of fibre optic cables. However, the cost will be greater than a copper-cored cable equivalent. Consider also the additional equipment necessary in signal converters, Fibre Optic modules, switches etc all having an impact on the overall reliability of the system.

In remote locations, the use of wireless or radio communications may be the only viable alternative available. These means of communication may be more vulnerable to loss of signal, interference, the risk of interception/corruption and the loss of operating power. For these reasons, it is essential to consider diversity in cable routing in the design phase to ensure redundancy and safeguard availability.

8.5. Redundancy

The aim of a control system is to automate a process, mitigate a danger or to give warning. Redundancy is the ability to maintain these functions if one or more failures occur, allowing the system to be made safe automatically or allowing an operator to take alternative action. Designed redundancy should provide numerous ways to detect and avoid the dangerous occurrence.

Reservoirs may be located in remote and mountainous locations where access is difficult. Economic reservoir design would not normally have two independent access routes to the dam, and ducts would usually follow the same path. A robust redundant design would have more than one communication route between reservoir and control system, these should have enough separation that the same event cannot compromise all functions. Events could be a catastrophic flood washing away cable ducts buried in roadways, a landslip, a building fire, intentional malign actions or accidental damage by an excavator.

Level transducers and float switches should be multi-channelled and be doubled through alternative independent controllers. Systems dependent on mains electrical supply should have battery backup systems typically Uninterrupted Power Supply (UPS) or emergency generators and any loss of power communicated to the operator so that action can be taken to restore the redundancy.

A redundant design should also make use of different methods of determining the same information. For example, water level transducers (such as pressure transducers), could be supplemented by above water level ultrasonic level transducers and CCTV. Whatever the type of level transducer, attention must be given to the housing of the sensing elements. Submerged pressure transducers will require protection from water borne sources that could result in damage. Float switches set at water levels that trigger warnings and water levels that trigger emergency action will supplement the reservoir water level sensing equipment. Float switches should be treated as binary devices; either ‘off’ or ‘on’ and will have their own inherent

reliability. For cross-checking purposes, indirect measurement of reservoir level from penstock pressure instrumentation readings can be used. Note that the raw static pressure measured from a hydraulic tapping into the waterway will need to be corrected to take account of velocity head and head losses both of which are dependent on the operating status of the station at any moment. Further, such data is only applicable if the waterway isolating gates are open.
If, through the process of risk assessment, the control function is determined to require a particular level of performance then it is classified as a Safety Instrumented Function (SIF). As a result, a minimum level of fault tolerance and redundancy may be necessary, and this is specified in the relevant functional safety standards such as BS EN 61511. This topic is further introduced in Chapter 9 – Functional Safety.

In specifying redundancy, a specific voting logic can be defined. For critical measurements a two out of three ('2oo3') might be considered the minimum appropriate. This would require two out of three tolerance measurements to necessitate a trip i.e., immediate shutdown of the process into a safe state. This provides redundancy in that one instrument could fail and the plant would not trip, reducing the number of spurious trips and improving availability of the station. Designed redundancy must not be relied upon on as a means to reduce maintenance, as a justification to delay replacing faulty equipment or to reduce supervision and surveillance by trained operators. System testing must be designed to reveal hidden failures to ensure that the designed redundancy is maintained. Functional testing must be 'end to end' (i.e. instrument to actuator) and with all individual elements tested.

8.6. Alarm and Trip Functions

The status of all inputs to the control system can be evaluated against defined thresholds and limits to generate alarms or trips for the protection of the plant. The designer, in preparing the design, will specify the limits of the acceptable operating window for a piece of equipment or process. Configurable within the software of the control system are various thresholds which can trigger alerts to the operator of an abnormality within the plant. For a lower threshold, an alarm notification can be sent to the operator workstation to indicate that the process has deviated from an acceptable operating value; this is commonly set to a value outside of the normal operating window but not at a level where harm or damage may occur for prolonged periods of operation. For a higher threshold, continuous or prolonged operation may generate damage or harm, and functions are configured which will take automatic actions to correct the process or bring it into a safe state.

A well rationalised alarm management system is an important deliverable in any control installation or upgrade to ensure the operator is not overloaded with information. Care must be taken to classify and commission alarms so that severity is clear, and the volume of alarms is manageable for the operator. Standards such as EEMUA 191 provide guidance on alarm rationalisation and appropriate volumes of alarms for efficient operator response. Frequent spurious alarms can erode the operator's trust in the protective function and may result in lack of action in the event of a serious incident.

Modern control systems allow prioritisation of alarms which segregate alarms into specific categories according to the severity of the consequences. The priority of these alarms would ascend according to the potential consequence with the highest priority reserved for the highest consequence alarms. In such a distribution there should be a low number of alarms assigned the

most severe category for ease of recognition by the operator; these represent the most critical faults the system can encounter and require urgent action. For example, a fault on a minor auxiliary system not required for operation of the plant may be assigned a low priority and appear as such on the alarm management system. However, a potentially dangerous deviation alarm notification would be assigned the highest priority for the immediate attention of the operator.

8.7. Cyber Security

Remote connectivity to power stations has become a necessity for remote monitoring and dispatch and support from technology providers. While this gives benefits for the availability of the station to those with an interest in its operation it also provides a potential attack vector for malicious intent.

As the control system is responsible for the safe operation of the plant, its reliable operation is essential, and it must be safeguarded from the potential of cyber-attack. Standards and guidance documentation have been developed to outline methodologies for cyber risk assessment and development of protocols and architectures to address identified risks. Technology providers are also incorporating security features into their control systems as standard practice to reduce potential for cyber-attack. It is expected that any new control system would be designed and commissioned with due consideration of cyber security risk. Standards and frameworks such as IEC 62443, National Cyber Security Centre – Cyber Assessment Framework may be utilised as part of this process alongside suitably experienced individuals.

8.8. Remote Operation

Power stations are increasingly being operated remotely. When pumped storage power stations were first developed, they were primarily for storing surplus night-time energy, the energy being released in a few peak periods during the day. Mode changes were small in number, typically a few dozen generating and pumping phases per day. Pumped storage power stations are increasingly being used to provide support to grid systems which are more dependent on intermittent power supply such as wind turbines meaning that mode changes can be very frequent. This has increased the need for grid operators to control generators remotely or automatically, some operated by algorithm. Energy storage may be bought and sold numerous times by traders before final delivery by operators, with the potential to sell more energy than is physically able to be stored in water volume.

In the future, algorithms could be replaced by machine learning. The opportunity for operators, who are able to detect a problem, may reduce due to cost and/or performance pressure. The introduction of remote operation and machine learning should be assessed to ensure that the designed-in safety measures are not compromised. Remote operators may not have an appreciation of potential consequences of their actions. Their screens, spreadsheets and calculations may display stored energy in MWh, as opposed to height of water or volume. Where control desks are remotely situated, operators must have the same information available to them as the local control. Energy traders and remote operators must have specific training to avoid system stress events, to recognise dangers and to have an awareness of their actions.

8.9. Example protection function – Reservoir High Level

The following sub-chapter is intended to provide an overview of an example safety function within a control system. It is simplified and generalised for the purposes of explaining the overall process. Details such as individual component performance, reliability and redundancy are not specified and would be determined during the design phase. Other details such as alarm and trip thresholds, time delays and hysteresis would also need to be determined by designers considering the individual characteristics of the project in question.

below illustrates an example diagram of the arrangement for detecting reservoir level and shutting down the pump/turbine units. As the focus is a reservoir high level trip, the operating scenario is the plant operating in pumping mode; the motor-generator units operating as motors and the pump-turbine units operating as pumps. This is summarised as follows.

- The reservoir level is monitored by instrumentation with redundancy and may utilise several technologies to ensure resilience in the measurement of water level.
- The instrumentation is connected to the control system via a communication link which will be determined according to the site layout and performance requirements determined during design.
- The control system will continuously monitor the reservoir levels indicated by the instrumentation.
- During pumping operation, should the water level increase above the threshold programmed within the control system, then a trip will be initiated to shut the pump-turbines down and stop pumping further water into the reservoir.
- Pump-turbine shutdown involves several actions each of which would cease pumping but are normally all done as part of the shutdown sequence. The shutdown sequence is different for an emergency shutdown compared to the normal shutdown sequence and often there is a slightly different 'fast' shutdown sequence as well:
    - Trip of the Motor-Generator circuit breaker(s) which will isolate the power supply to the motor-generator set(s) and cut shaft power to the pump-turbine(s) preventing further water being pumped into the upper reservoir.
    - Initiate closure of the main inlet valve closing the pumps connection to the reservoir.
    - Initiate closure of the guide vanes also closing the pumps connection to the reservoir.

The control system will be configured with several thresholds against which reservoir water level is compared.

- As described in Section 8.6, the first threshold exceeded by water level would only trigger a warning alarm to notify the operator that reservoir levels are approaching an unsafe level.
- If pumping is not stopped and the level continues to increase, then a first stage trip threshold would be triggered in the control system, this might follow a normal shutdown sequence where the machine is unloaded by closing the guide vanes before opening the motor-generator circuit breaker to reduce overspeed and mechanical wear compared to a full emergency shutdown.
- Further thresholds would also be configured closer to the maximum reservoir level where an emergency shutdown would initiate and result in immediate opening of the motor-generator circuit breaker in parallel to guide vane and main inlet valve closure. In comparison to a normal shutdown this would reduce the amount of water pumped into the upper reservoir.

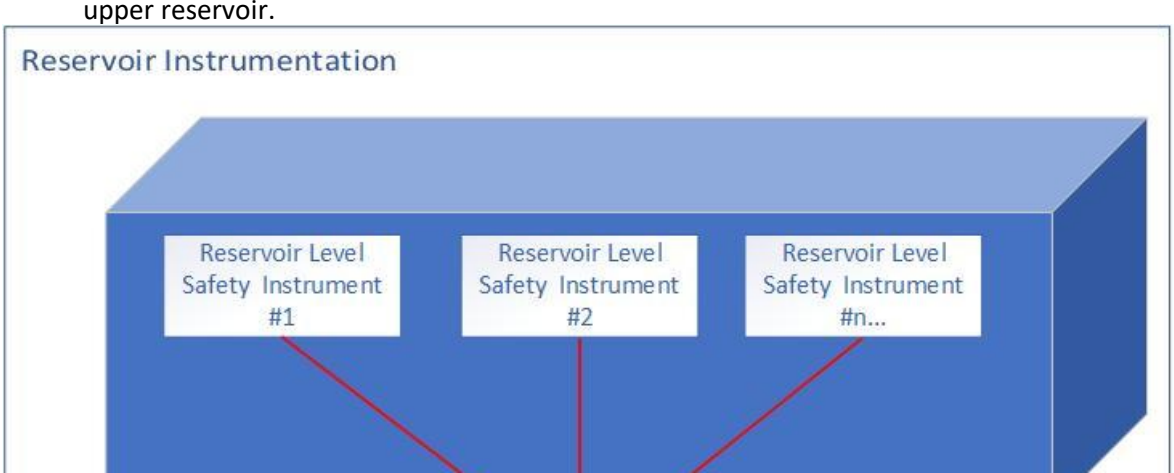


Figure 10: Example diagram of the arrangement for detecting reservoir level and shutting down the pump/turbine sets

9. Chapter 9: Functional Safety

9.1. Introduction

Functional safety involves identifying specific hazardous failures which lead to serious consequences (e.g. death) and then establishing maximum tolerable frequency targets for each mode of failure. Equipment whose failure contributes to each of these hazards is identified and usually referred to as 'safety-related'. Examples are industrial process control systems, process shutdown systems, rail signalling equipment, automotive controls, medical treatment equipment, etc. In other words, any equipment, with or without software, whose failure can contribute to a hazard is likely to be safety related.

The maximum tolerable failure rate for each hazard will lead us to an integrity target for each piece of equipment, depending upon its relative contribution to the hazard in question. These integrity targets are known as 'safety integrity levels' and are usually described by one of four discrete bands:

Table 8: Safety-integrity levels

SIL 4	Highest target and most onerous to achieve, requiring state of the art techniques
SIL 3	Less onerous than SIL 4 but still requiring the use of sophisticated design techniques
SIL 2	Requires good design and operating practice to a level not unlike ISO 9000
SIL 1	The minimum level but still implying good design practice
<SIL 1	Referred to (in IEC 61508 and other documents) as 'not-safety related' in terms of compliance

An assessment of the design, the designer's organisation and management, the operator's and the maintainer's competence and training should then be carried out in order to determine if the proposed (or existing) equipment actually meets the target SIL in question.
The steps involve:

- Setting the SIL targets;
- Capability to design for functional safety;
- Quantitative assessment;
- Qualitative assessment;
- Establishing competency;
- As low as reasonably practicable (ALARP);
- Reviewing the assessment itself.

IEC 61508 is a generic standard which deals with the above. It can be used on its own or as a basis for developing industry sector specific standards. In attempting to fill the roles of being both a global template for the development of application specific standard, and being a standard, it necessarily leaves much to the discretion and interpretation of the user. However, it should be noted that BS EN 61511 is the specific industry standard used for Process Safety, so this is probably the most relevant standard to use. It is vital to bear in mind, that no amount of assessment will lead to enhanced integrity unless the assessment process is used as a tool during the design-cycle.

9.2. Relevance

The functional safety standards provide an established approach to risk management and mitigation through the control system. Experienced individuals and organisations are already practicing and applying the concepts mentioned in Section 9.1 in other industries. A mature lifecycle for the development, implementation, operation and decommissioning of functional safety systems is in use in other process related industries for the justification of As Low as Reasonably Practicable (ALARP). The utilisation of these processes is suggested in this guidance as an appropriate route for development of new build pumped storage projects and assurance of their control systems.

9.3. Human Factors

Whenever mechanical and/or electrical devices are made and installed, their reliability will be affected by the people who made and/or installed them and by those who go on to operate and maintain them. This, and the potential effects, are recognised and routinely analysed in safety critical industries such as space flight and nuclear power generation.

In recent times, they have also been explored in terms of the reliability of spillway systems. It was the subject of an all embracing, internationally based assessment of spillway reliability, summarised in the 2016 ICE publication "Operational Safety of Dams and Reservoirs", by Hartford et al. It notes that Human Reliability Analysis (HRA) should be an important part of the overall risk-analysis process. It also notes that a number of human reliability indices have been developed by bodies such as NASA, but for the purposes of spillway gate system operation it recommends two in particular:

- **THERP** Technique for Human Error Rate Prediction;
- **ATHEANA** A Technique for Human Event Analysis.

While there are obvious ways in which human frailty can result in the incorrect or dangerous operation of directly controlled spillway gates, even automatic systems can be prone to human vulnerability. This can be through poor manufacture, installation or maintenance. It can be via a loss of corporate knowledge through inadequate resources or training. Some of the factors that can come into play are given in Table 10, but more can be envisaged.

In recent years, the failure of the Taum Sauk (Appendix B) upper reservoir was in large part due to human judgement and a loss of corporate knowledge. The failure of the spillway chute at Oroville dam also featured a loss of corporate knowledge but also under investment in inspection and maintenance as well as poor judgement during inspections.
The purpose of this Guide is not to define what is to be done or how analyses of human factors should be carried out, but simply to raise awareness that human factors should not be ignored in any detailed assessment of overall system reliability.

Examples of human factor related incidents at Pumped Storage Hydropower Projects or related works.

- Prior to the Taum Sauk PSP reservoir failure there had been a "near miss" which was not acted upon.
- Some of the operatives at the Taum Sauk PSP reservoir had not realised that the embankment was erodible, indicating either a lack of training or a loss of corporate knowledge, or both.

- At one unnamed PSP, dispatchers had twice persuaded site operatives to overrule alarm warnings and to keep pumping. Potential reservoir failure was only avoided by a cut-off on the pumps being automatically activated.
- At one unnamed PSP complete system failure sequences were not "end to end" tested because they interfered with operatives' shift work patterns.
- One factor listed in the spillway gate failure at Folsom Dam in the US was that the gates had not been inspected or exercised on a regular schedule.

Table 9: Typical factors considered in a THERP type assessment

External		
Situational characteristics	***Tasks & Equipment***	***Job & Task Instructions***
Working environment	*Long and short term memory*	*Operational procedures*
Working hours	*Feedback*	*Oral instructions*
Shift patterns	*Team structure*	*Quality of installation*
Organisational structure	*Decision making structure*	*Quality of maintenance*
Advice availability	*Information availability*	*Regularity of maintenance*
Equipment availability	*Supplier reliability*	
Recognition & rewards	*Equipment quality*	
Internal		
Psychological Stressors	***Physiological Stressors***	***Organisational***
Task speed	*Fatigue*	*Previous experience*
Stress duration	*Pain or discomfort*	*Level of training*
Monotony	*Stress duration*	*Personalities & attitudes*
Distraction	*Lack of exercise*	*Motivation*
Sensory deprivation	*Circadian rhythm disruption*	*Physical conditions*
Threat of failure/job loss	*Hunger or thirst*	*Corporate knowledge/reliability*
Motivational conflicts		*Group dynamics*

10.Chapter 10: Risk

The current approach to risk assessment for UK reservoirs is based on guidance provided in the 'Guide to risk assessment for reservoir safety management' (Report – SC090001/R2) (Defra/EA 2013). The guide presents a three-tier approach to risk assessment of reservoirs. Tier 1 is qualitative while Tiers 2 and 3 are quantitative. The Tier 1 approach is generally for use by anyone familiar with the concepts of risk assessment, whilst the Tier 2 and Tier 3 approaches are intended to be used by reservoir owners/undertakers, consulting engineers, inspecting engineers and supervising engineers who have knowledge and experience of engineering of dams and reservoirs.

Table 10: Tiered Analysis

Tier	Type of risk assessment	Description
1	Qualitative	Ranking of potential failure modes, order of magnitude likelihood and consequences estimates using a descriptive risk matrix. Optional sensitivity analysis
2	Basic quantitative	Threshold analysis using manual calculations (that is, with a basic calculator). Optional sensitivity analysis
3	Detailed quantitative	Range of levels – include system response curves, with range of initiating events (threats) using computer software for risk calculations. Ways of dealing with uncertainty range from formal sensitivity analysis to full uncertainty analysis.

Both Tier 2 and Tier 3 assessments involve the use of event trees and/or fault trees to allow the understanding and assessment of different failure modes, with detailed numerical assessment of the trees only being applied in Tier 3.

The evaluation of risk in the Guide is based on the well-established framework for risk evaluations in the UK developed by the Health and Safety Executive (HSE) called the Tolerability of Risk (TOR) (HSE 2001). It is generally used for regulating risks to society and the public in the UK that are associated with hazardous industries, but it is also used to evaluate the risks associated with reservoirs. Under the HSE TOR framework, the risks need to be reduced to be 'as low as reasonably practicable' – referred to as the ALARP principle.

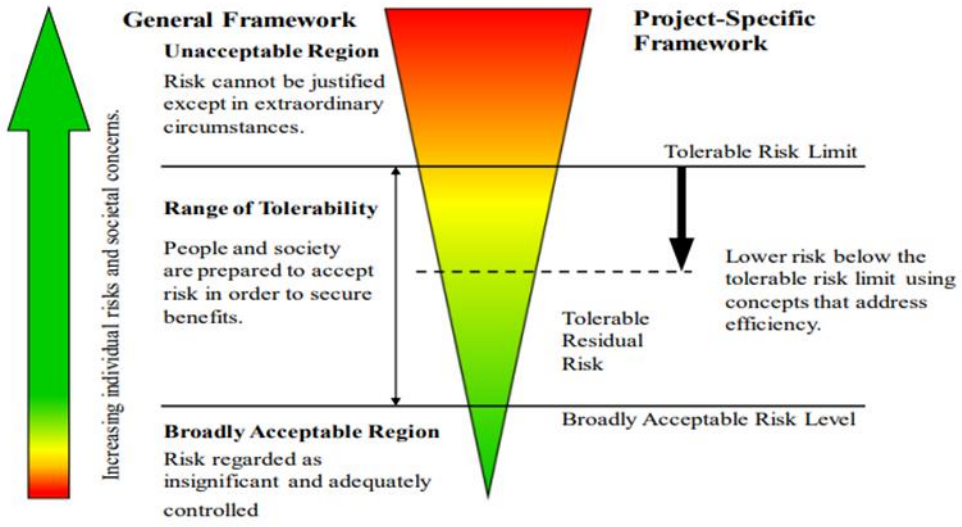


Figure 12: Tolerability of Risk Framework

The Guide states that even if a risk is in the 'range of tolerability', it should be reduced to be 'as low as reasonably practicable' (ALARP). The ALARP principle is generally satisfied when it is deemed grossly disproportionate in terms of expending resources to gain any further reduction in risk. The application of the ALARP principle therefore requires the formulation of risk control options. These could include structural measures, improved monitoring and surveillance, emergency action planning and staff training, etc.

The Guide states that the outcomes of the risk assessment can be used to:

- programme works;
- justify funding for maintenance and capital expenditure;
- prioritise and justify the urgency of works;
- identify where the largest benefits and greatest reductions in risk can be achieved.

The results can also be used to show where proposed measures are not justified, possibly because the cost of the works would be disproportionate to the potential reduction in risk.

10.1. Risk Assessment – Example approach

The following section describes a potential approach to the risk assessment of a proposed reservoir associated with a new build pumped storage hydropower scheme. The approach is based on the Guidance given in Risk Assessment for Reservoir Safety (RARS).

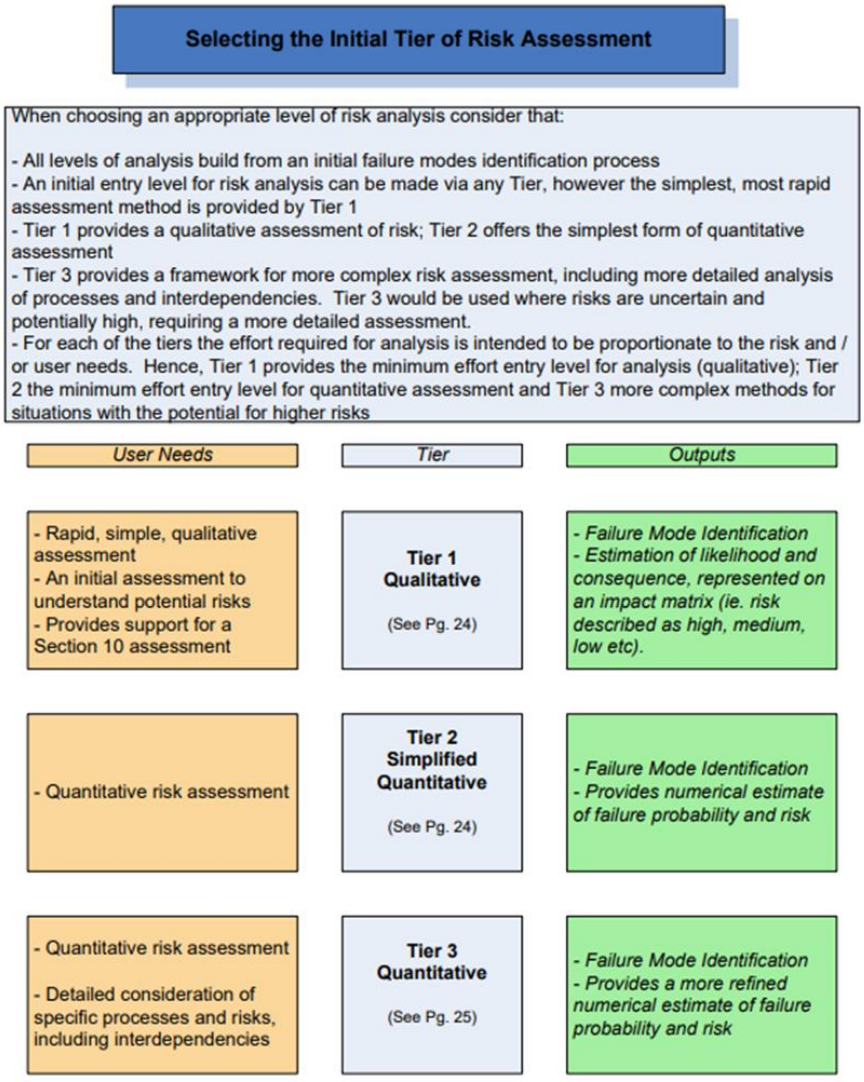


Figure 13: selection of initial Tier of Risk Assessment (taken from RARS figure 4.2)

10.1.1. Selecting the appropriate level of risk assessment

Following the matrix given in RARS and reproduced in Figure 13 above, a relevant level of risk assessment should be undertaken depending upon the project stage and therefore the information available about the dam and its operation.

At an early project stage, a Tier 1 risk assessment may be applicable. Tier 1 is a purely qualitative assessment and can be completed with minimal information. This will identify the key failure modes which may impact on concept design and steer the initial layout or components of the scheme. At a more developed project stage, perhaps FEED (Front End Engineering Design), a Tier 2 risk assessment may then be more appropriate. Following the guidance given in RARS, this follows a quantitative approach but still relies on simplified or readily available information and data, typically available during concept or outline design of a scheme. The benefit of applying a Tier 2 assessment ensures a more robust risk assessment and allows for better identification of

the key, or priority failure modes. It will also highlight where further detailed studies may be required in the later design stages, or where improvements can be made in the concept/ outline design of the scheme.

As the scheme develops to detailed design stage, more detailed or complete calculations can be used to update the findings of the Tier 2 assessment (essentially developing it to Tier 3). This results in a documented process summarising the identification and mitigation of potential risk and failure modes through the design process and aids in decisions on future management and maintenance of the asset. This is through the understanding of the key failure modes, the indicators of these developing, and the measures which can be taken to mitigate or intercept.

10.1.2. The approach

The high-level approach to risk assessment can generally follow the framework illustrated in 'Guide to risk assessment for reservoir safety management Volume 1' (Report – SC090001/R1) (Defra/EA 2013) and Figure 14 below where the approach can be applied as follows:

- **Step 1 – Risk Identification**
    - *Step 1a: Failure mode identification of reservoir and constituent dams:*
      The Guide includes a table of typical failure modes which can be readily used as a starting point; however, it is prudent to consult with an All-Reservoir Panel Engineer at this stage to ensure that all failure modes have been identified. The identified failure modes should be screened as to whether they are 'credible' and 'significant' with those identified as reaching these criteria, taken forward to the full risk assessment.
    - *Step 1b: Potential consequences:*
      The siting of the dam will result in potential consequences should the dam breach releasing an uncontrolled flow of water. As part of the risk identification, the valley or potential flow path downstream of the dam should be reviewed and potential receptors identified.
      This review can be undertaken by simply reviewing topographical mapping and satellite imagery (such as google earth) to identify possible receptors. These should include any residential or commercial properties; critical infrastructure; schools and hospitals; environmental and heritage assets. This high-level review will help to ascertain the potential impact of a breach and feed into the initial stages of the risk assessment, including being useful in scoping where more detailed breach modelling may be required.
    - *Step 1c: On the basis of the credible worst-case scenarios:*
      The assessor should then be able to determine the scope and methodology for the risk analysis (Step 2). As discussed above, the risk analysis scope and methodology need to be proportionate to the project stage and also perhaps the severity and complexity of the scenarios to be assessed, ranging from qualitative (Tier 1 in SC090001/R1) to detailed quantitative (Tier 2 or 3 in SC090001/R1).

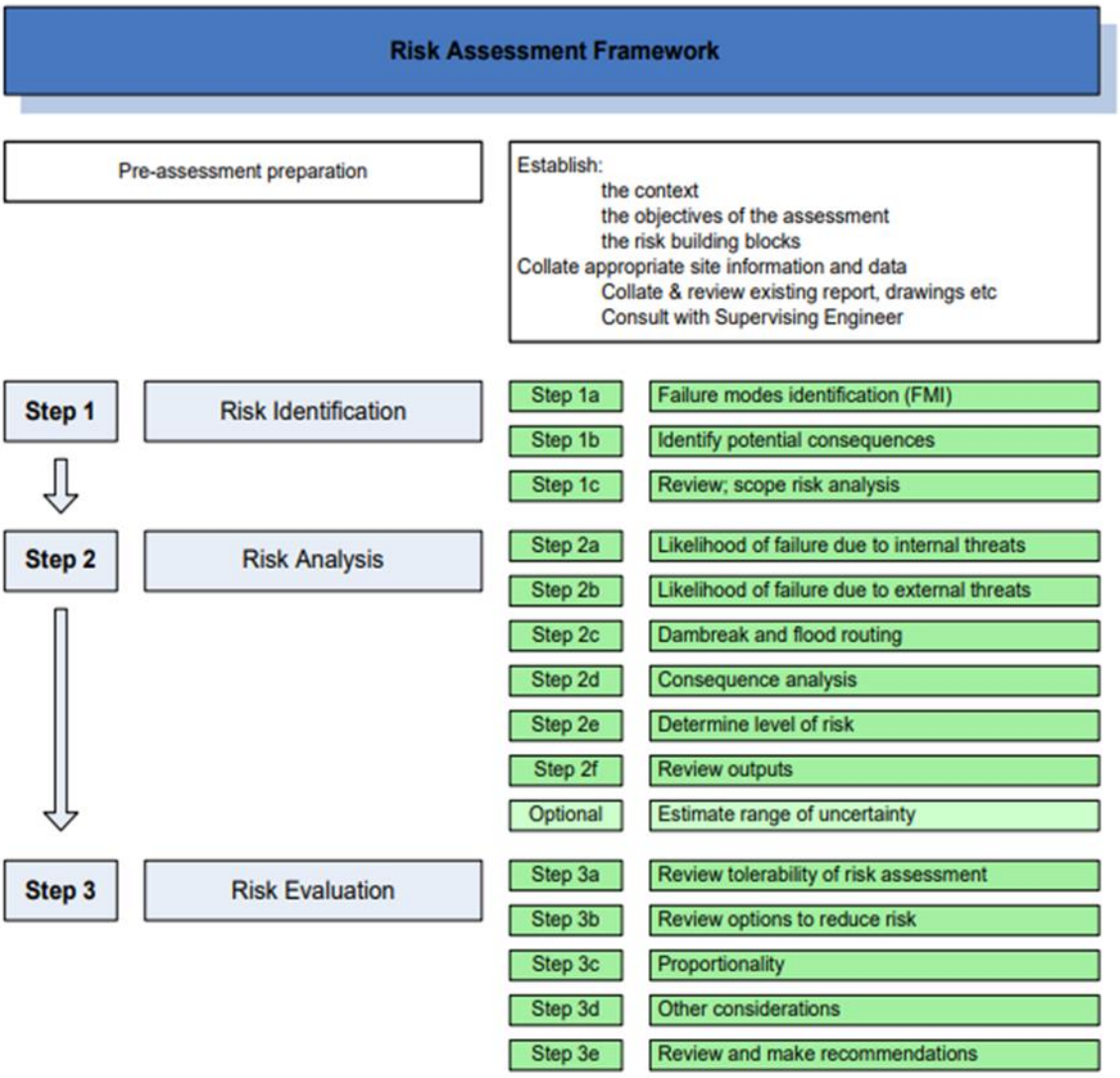


Figure 14: Risk Assessment Framework

- **Step 2 – Risk Analysis**
  - *Step 2a and 2b - The credible and significant failure modes identified in Step 1 are taken forward to the risk analysis stage:*
    The RARS Guide includes detailed worksheets which can be used as the basis for considering the likelihood of failure, with the assessment split between internal (eg internal erosion, filtering, structures passing through the dam) and external threats (eg floods, waves, seismic). Depending on the project stage, these can be based on simplified matrices (Tier 1) or more numerical (requiring information on dam dimensions, materials, foundations, etc) for Tier 2 and 3.
    The RARS worksheets are based on embankment dams and therefore if the proposed dam is of a different construction, perhaps rockfill, RCC, concrete gravity, then an event tree approach would be used, see Figure 15.
    The Guide provides further advice on applying this approach.

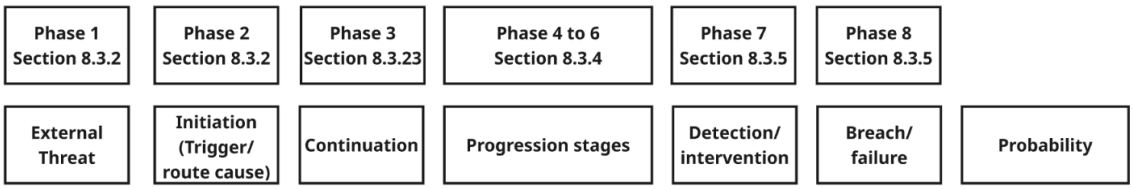


Figure 15: Event tree approach (reproduced from RARS)

It should be noted that although the event tree process is useful in representing how failure progresses from initiation through to release of the reservoir, in non-earth embankment dams, it is also more vulnerable to bias introduced by the user. The RARS Guide therefore provides a prescribed format for event trees.

The risk assessment may best be assessed in a risk workshop comprising of panel of subject matter experts, panel engineers, dam breach modellers etc. If this is not possible, then the completed assessment should be reviewed by an All-Reservoir Panel Engineer to ensure it is accurate and covers all critical failure modes. In comparison, the event tree process requires a good understanding of the engineering and behaviour of dams and should therefore be carried out in a workshop process with at least one All Reservoir Panel Engineer in attendance. Mitigations against dam breach, such as robust instrumentation, control systems and functional safety assessments can be incorporated into the event tree approach, which will give a more accurate representation of the risk of failure during operation of the asset.

- *Step 2c and 2d: Dambreak and flood routing & consequence analysis*
  The consequences of a breach of the dam must be understood to fully comprehend the severity of an identified failure mode. Depending on the project stage and Tier of risk assessment being applied, there are varied approaches to identifying consequences. At an early project stage, or a Tier 1 assessment, it may be that a simple assessment would suffice. The RARS Guide includes a high-level approach to identifying the inundation envelope and potential consequences of a dam breach, considering the height of the dam and the contours of the downstream valley. At Tier 2 and 3 stages, a more accurate breach mapping exercise would be more applicable. This would utilise 2D modelling software, digital terrain mapping and consider the development of the breach to provide a more accurate consequence assessment. It may be that different failure modes will develop at a different rate, or location and this may result in differing consequences for individual failure modes. It is therefore suggested that the failure mode scenarios, and proposed modelling approach, is discussed and agreed with an All-Reservoir Panel Engineer before commencing modelling, to ensure that the approach is applicable.

  It should also be noted that the consequence assessment is not restricted to the impact on people and property downstream of the dam, but also should reflect

environmental damage, heritage damage, impact on infrastructure and perhaps also the potential impact on public relations for the owner/ operator. breach assessment and consequence assessment will need to consider a range of flows such as natural flow, natural flood event, full pump inflow and dam breach. The dam break modelling will include a review of breach outlines, depths and velocities, also quantifying consequences (loss of life and other criteria, such as environmental damage, PR damage, as required).

- *Step 2e: Determine level of risk*
  The determination of the risk posed is given by a calculation of consequence x likelihood. At Tier 1 this can be assessed using a risk matrix, similar to that shown below in Figure 16: Example Risk Matrix (reproduced from RARS).

Likelihood of downstream flooding	Potential magnitude of consequences given downstream flooding				
	Level 0	Level 1	Level 2	Level 3	Level 4
Extreme	ALARP	ALARP	ALARP	Unacceptable	Unacceptable
Very high	Tolerable	ALARP	ALARP	ALARP	Unacceptable
High	Tolerable	Tolerable	ALARP	ALARP	ALARP
Moderate	Tolerable	Tolerable	Tolerable	RISK	ALARP
Low	Tolerable	Tolerable	Tolerable	Tolerable	ALARP
Very Low	Tolerable	Tolerable	Tolerable	Tolerable	Tolerable

Figure 16: Example Risk Matrix (reproduced from RARS)

At Tier 2 and 3 an F-n chart could be used to graphically display the risk position, see Figure 17. The chart considers the Average Societal Life Lost (ASLL) against the annual probability of dam failure to give the risk position. Boundaries of ALARP are given in RARS and based on R2P2, (HSE, 2001). To provide a more detailed view of the risk position, the annual probability of failure due to individual failure modes could be plotted against the consequence of that failure mode occurring, which may give useful input to identify where mitigation or improvements in the design should be concentrated.

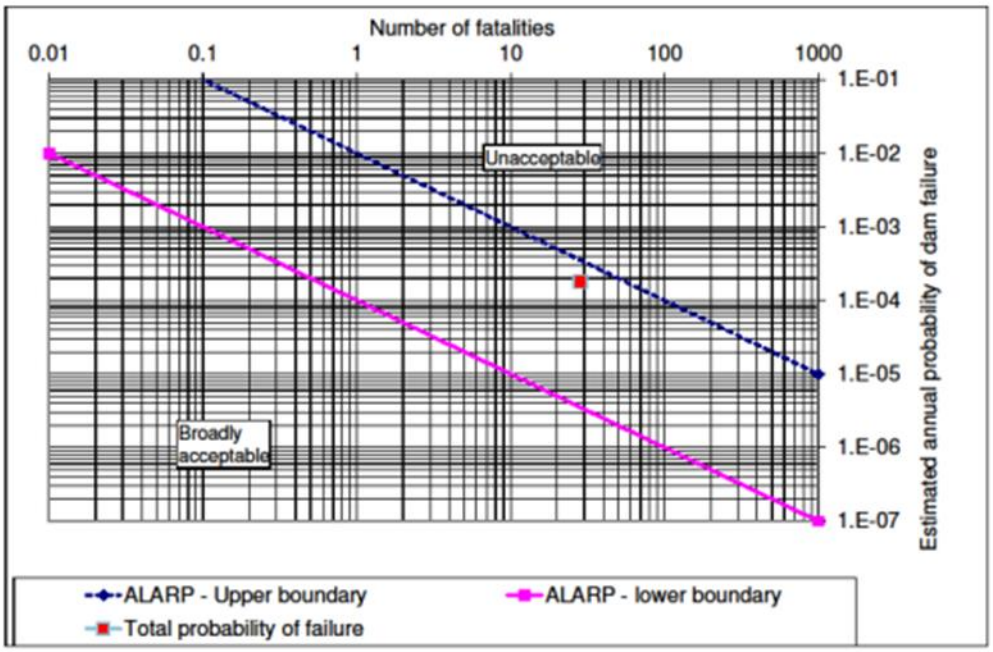


Figure 17: simple F-n chart (reproduced from RARS)

- **Step 3 – Risk Evaluation**

  At this stage there is the opportunity to evaluate the risk levels determined in Step 2 against the tolerability risk criteria set by the corporate/organisation and the All-Reservoir Panel Engineer.

  All identified risks will fall into one of the categories of Table 11.

Table 11:Three types of risk (Source: Reducing risks, protecting people; HSE's decision-making process; published 2001)

Risk colour	Risk description
Green risk	Broadly acceptable
Yellow risk	Tolerable if ALARP (TIFALARP)
Red risk	Intolerable

As far as reasonably practicable, risks should always be reduced to a broadly acceptable level. Where this is not possible, the risks should be reduced to be as low as reasonably practicable (ALARP). No risk should be left in the intolerable region without actions. Additional safeguards and their potential for further risk reduction should be identified such as the following:

- Reducing risks from flooding/overtopping - increasing spillway capacity or freeboard to dam, spillway chute or downstream channel;
- Reducing risk from internal erosion – introducing or building in a seepage monitoring system, dam geometry monitoring, phreatic surface monitoring, temperature sensing, etc. with recognised alarm trigger levels and clear emergency procedures;
- Reducing risk of instrumentation/mechanical failures - implementations of Safety Instrumented System and building in redundancies; increased frequency of inspection/monitoring/instrumentation checks and equipment maintenance item;

- Reducing risk of operational/human errors – introduction of operational system with built in safety redundancies, introduction of specific and targeted training of operating staff.

The assessment may then continue to carry out ALARP demonstrations to evaluate whether the additional safeguards, considering the time, trouble, cost, and difficulty of implementation, become grossly disproportionate to the further risk reduction achieved. Only if a mitigation measure is assessed as being proportionate should it be taken forward into the design. It is imperative that this process and consideration of mitigation measures and additional safeguards is well documented, such that future owners, operators or engineers have full visibility of the decisions made and their justification.

10.2. Process Safety Risk studies

In delivery of the process related elements of the plant the following standards and guidance would be considered applicable:

1. BS EN 61511 Functional safety – Safety instrumented systems for the process industry sector.
2. BS EN 61882 Hazard and operability studies (HAZOP studies). Application guide.
3. R2P2 2001; Reducing risks protection people - HSE's decision-making process.
4. HAZOP Guide to best Practice 3rd edition; Frank Crawley and Brian Tyler; I.Chem.E.

The block diagram in **Error! Reference source not found.** provides an overview of a typical approach to process safety activities through the project life cycle. This is aligned with general project phases and functional safety activities. Some activities may not be strictly applicable to the project under consideration. To decide which safety studies should be applied, and which should be left out, it is recommended that a Hazard Study 1 (HS1) meeting is carried out to go through a checklist of safety activities to decide which ones are applicable. This is best done at the inception stage of project planning so that the correct safety studies can be built into the project schedule.

Key studies in the project development are the Hazard Identification study (HAZID) and Hazard and Operability Study (HAZOP). These serve as key milestones in project development where designers, owner, consultants and contractors gather in a workshop format to review the design. The objective is to identify and quantify hazards and their mitigations and document actions necessary following each study. Both studies require the leadership of an experienced chair who will lead the group through the study.

The designers of the plant, operations representatives and specialist subject matter experts are required for both HAZID and HAZOP workshops. It is vital to include operators and maintainers, as their contribution is critically important in identifying all possible hazards that relate directly to the operation and maintenance of the proposed equipment. Both workshops shall be fully documented by a scribe to serve as a future record of the workshop and to ensure that actions are clearly recorded. A brief summary of each study is provided below.

- **HAZID** - Performed at the FEED stage (Front End Engineering Design – basic engineering design – approx. 10-40% design complete), using process flow diagrams (PFDs) and hazard guidewords to stimulate creative thinking to identify possible causes of significant hazards. This is a qualitative assessment. The scheme layout may be divided

into systems or sections for assessment. The outcome of the workshop will be a record of each hazard studied and an action list to be addressed in future phases of design.

- **HAZOP** - Performed during the project detailed design stage, using frozen piping and instrument diagrams (P&IDs) to identify hazards and operability problems. Guidewords are used to stimulate creative thinking about possible deviations and their effects. The HAZOP is more detailed than a HAZID. Hazard mitigations and further actions necessary to reduce risk to tolerable levels are identified. An action list is generated. Once the actions impacting design have been completed, the HAZOP can be considered complete. An initial mapping of the process safety milestones against the reservoir risk assessment milestones introduced in **Error! Reference source not found.**. Interfacing between process safety and reservoir safety studies and milestones should be integrated into the overall project schedule to ensure that necessary milestones are obeyed and the appropriate level of information and design assurance is available at each stage.

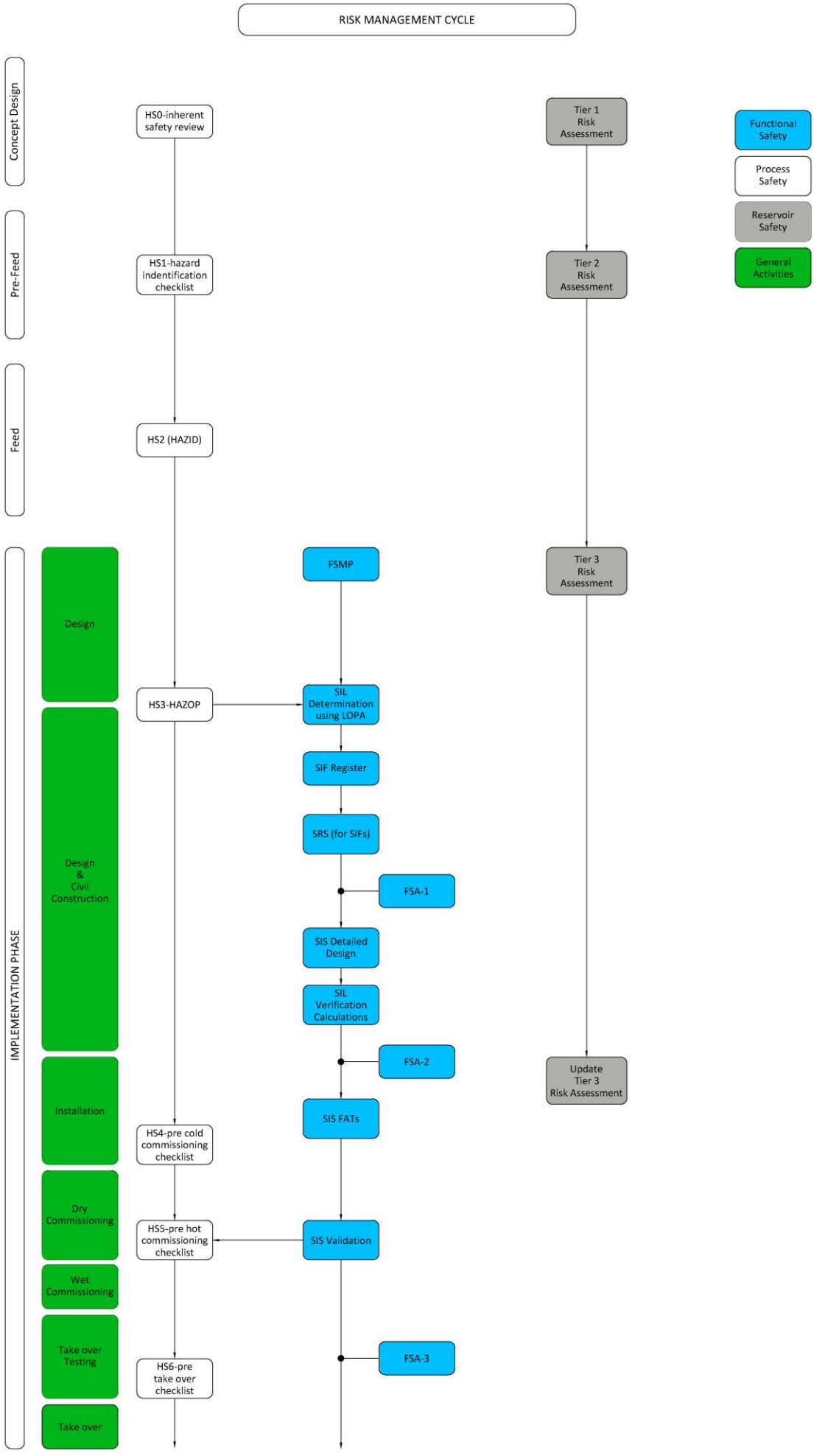


Figure 18: Process safety lifecycle

11. Conclusion

This guidance has been developed to support practitioners in considering reservoir safety within the specific context of pumped storage hydropower. It does not seek to replace existing legislation or established good practice, nor does it prescribe particular design solutions.

Instead, it provides a framework for thinking through the interactions between civil infrastructure, hydraulic behaviour, operational systems, and human factors that characterise modern pumped storage schemes. The examples and considerations presented are intended to prompt structured reflection on how hazards may arise, how systems may respond, and how safety can be managed in a proportionate and transparent manner.

The appropriate response will vary between projects. Practitioners are expected to apply professional judgement, informed by experience, site-specific conditions, and regulatory requirements. In doing so, the emphasis should remain on understanding system behaviour, recognising dependencies, and clearly articulating the basis on which decisions are made.

Ultimately, the safe delivery and operation of pumped storage schemes depend not on adherence to prescriptive rules, but on the quality of engineering judgement applied.

12. Appendix A – Overview of Reservoir Legislation by Jurisdiction

12.1. England and Wales

Primary Legislation:

Reservoirs Act 1975 (as amended by the Flood and Water Management Act, 2010)

Regulator:

Environment Agency (England)

Natural Resources Wales (Wales)

Key Features:

- Applies to large, raised reservoirs, defined as having a water storage capacity of ≥25,000 m^3 above nearest natural ground level. Note that legislation is in place to change this to 10,000 m^3 but to date (2026) this has only been enacted in Wales.
- Mandatory appointment of:
  - Construction Engineer
  - Supervising Engineer
  - Inspecting Engineer
  - These are often referred to collectively as "Qualified Civil Engineers" (QCEs) under the Act
- Statutory inspection regime (every 10-years or less if directed by an Inspecting Engineer following an inspection).
- Prescriptive compliance requirements via statutory instruments.
- Enforcement powers vested in a Regulator.

Statutory instruments and associated regulations are legally binding.

12.2. Scotland

Primary Legislation:

Reservoirs (Scotland) Act 2011

Regulator:

Scottish Environment Protection Agency (SEPA)

Key Features:

- Risk-based framework (High / Medium / Low consequence classification).
- Regulatory requirements scale with consequence category.
- Different engineer panel structures and reporting requirements.
- Greater emphasis on proportionality.
- Certain provisions are structured differently in England & Wales.

Some requirements equivalent to statutory instruments in England & Wales may operate differently or be advisory in structure under the Scottish regime.

12.3. Northern Ireland

Primary Legislation:

Reservoirs Act (Northern Ireland) 2015

Regulator:

Department for Infrastructure (DfI)

Key Considerations:

- Consequence based framework
- Relevant water storage capacity defined as ≥10,000 m³
- Transitional arrangements have applied.
- Developers should engage early with DfI to clarify applicable requirements.

Table 12: Key differences summary

Topic	England & Wales	Scotland	Northern Ireland
Governing Act	Reservoirs Act 1975	Reservoirs (Scotland) Act 2011	Reservoirs Act (NI) 2015
Framework	Risk-based	Risk-based	Consequence-based
Categories	High risk Not high risk	High risk Medium risk Low risk	High consequence Medium consequence Low consequence
Statutory Instruments	Legally binding	Structured differently to England and Wales	Jurisdiction-specific
Responsible legal entity	Undertaker	Reservoir manager	Reservoir manager
Statutory regulator	EA / NRW	SEPA	DfI

Appendix B: Case Studies

12.4. Turkey's Nest

There are several PSH schemes that have the upper reservoirs on the top of a hill formed by a perimeter (or ring) embankment. This type of reservoir is often called "Turkey's Nest" and most examples are located in Europe (Muela de Cortes, Coo-Trois-Ponts, Eggberg, Horneberg, Farmdenkopf and Waldeck, Revin, Vianden, etc), but there are also a couple of examples in US (Ludington, Rocky Mountain) and other countries.

These reservoirs do not have direct catchments and in most cases do not have spillways, relying on water level alarms to minimize the risk of over pumping. Taum Sauk was a reservoir of this type, where the alarm systems failed and the over pumping led to the failure of the embankment as explained in the case study below.

Usually, these reservoirs are lined with asphalt concrete linings or more recently also with PVC geomembranes (Gilboa and Pinnapuram) and have underdrainage system to collect and monitor seepage flows through the lining system. Automatic systems monitor the seepage flows and raise the alarm once a certain threshold value is reached.

In most cases these reservoirs do not have dedicated low levels outlets and rely on the pump turbine units for emergency drawdown. These reservoirs generally perform daily cycles, and the pump turbines are capable of entire drawdown of the reservoir in less than a day.
None of the PSH schemes in the UK have a reservoir of this type, but there are plenty of reservoirs formed by perimeter embankments in the UK, most of the reservoirs in London are of this type. These reservoirs are also fed by pumped flows and generally do have spillways. However, they need to have dedicated large capacity, low level outlets to be able to drawdown the reservoir in an emergency as their other outlets generally cannot provide the required drawdown capacity.

12.4.1. Taum Sauk Dam Failure: Instrumentation, Freeboard Management, and Failure Mechanisms in Lined Reservoirs



Figure 19: Taum Sauk, Missouri – rebuilt

During installation of a geomembrane liner within a reservoir, concerns were identified regarding potential leakage pathways associated with penetrations. To minimise this risk, reservoir level sensors were not fixed directly through the liner. Instead, a suspended mounting system was adopted, whereby sensor conduits were attached to tensioned cables anchored at the crest and toe of the embankment slope. This approach reduced liner penetrations but introduced unintended mechanical vulnerabilities.

The mounting system was under-designed for operational conditions. The conduits exhibited buoyancy and were subjected to cyclic hydraulic loading due to frequent reservoir filling and drawdown. Over time, the system became displaced, resulting in inaccurate level measurements. Specifically, recorded water levels were lower than actual levels, compromising operational control.

In response, operators adjusted the control system by reducing the upper pump set point to increase freeboard from the original 600 mm to approximately 1,200 mm. This was intended as a temporary mitigation pending permanent repair. However, the underlying instrumentation error remained unresolved.

Subsequent overtopping occurred, ultimately leading to parapet wall failure and rapid erosion of the embankment. Approximately 6 billion litres of water were released, causing significant downstream damage. Post-event analysis identified multiple contributing factors:

- **Embankment settlement:** Construction materials contained excess fines, and foundation preparation was inadequate, resulting in up to 600 mm of settlement.
- **Instrumentation failure:** Displaced sensors and lack of calibration against actual elevations led to systematic underestimation of reservoir levels.
- **Failsafe system deficiencies:** Redundant high-level sensors were incorrectly located above settled wall elevations and required simultaneous activation to trigger shutdown.
- **Lack of independent verification:** No physical or visual confirmation of water levels was undertaken.

In the absence of a spillway there was a reliance on control systems and freeboard alone, which introduced a systemic risk. This event demonstrates the importance of robust instrumentation design, validation of critical elevations, and incorporation multiple safety features in reservoir engineering.



Figure 20: Taum Sauk, Missouri – breach and downstream damage (image courtesy of fyfluiddynamics.com)

12.5. Dinorwig – a case study

A new modern pump control at a reservoir was assessed as needing a SIL 2 system. This was driven by the high number of people at risk downstream and the likelihood of the event.
The pump power main switch was required to be disengaged automatically when high water level was actuated by a float switch after the failure of the operator to intervene manually.
The system's float switches were designed to be multi channelled to protect against switch failure, and to avoid spurious signals, only activated when at least two floats operated together.
The signals were received at a programable logic controller, independent of any other system, which communicates with the remote-control system switching off power to the pump.
The lack of a truly independent signal route necessitated means of warning the operator that signals had been lost. The system was also reinforced with a control of change document system, operator training, a written procedure highlighting actions to be taken on receipt of signals, a CCTV system and additional alarms on alternative controllers. A regime of regular testing was established to test continuing operation of all the elements.

13. References

13.1. UK Legislation, Policy and Regulatory Guidance

- Department for Energy Security and Net Zero (DESNZ). *Long Duration Electricity Storage: Government Response to Consultation*. London: DESNZ, October 2024.
- Department for Energy Security and Net Zero (DESNZ) & Office of Gas and Electricity Markets (Ofgem). *Long Duration Electricity Storage: Technical Decision Document*. London: DESNZ / Ofgem, March 2025.
- Ofgem. *A Call for Input: Long Duration Electricity Storage Cap and Floor Regime*. London: Ofgem, December 2024.
- Ofgem. *Interconnector Cap and Floor Regime Handbook*. London: Ofgem, 2024. https://www.ofgem.gov.uk/publications/interconnector-cap-and-floor-regime-handbook
- UK Government. *Clean Power 2030 Action Plan*. London: HM Government, December 2024.
- UK Government. *Planning and Infrastructure Bill*. London: HM Government introduced March 2025.
- Infrastructure and Projects Authority (IPA). *Cost Estimating Guidance: A Best Practice Approach for Infrastructure Projects and Programmes*. London: IPA, 2021. https://www.gov.uk/government/publications/cost-estimating-guidance
- UK Government. *Reservoirs Act 1975 (as amended)*.
- Scottish Parliament. *Reservoirs (Scotland) Act 2011*.
- Northern Ireland Assembly. *Reservoirs Act (Northern Ireland) 2015*.
- Statutory Instrument SI 2013 No. 1677 – *The Reservoirs Act 1975 (Inspecting Engineers' Reports) (England) Regulations 2013*.

13.2. Reservoir Safety, Engineering and Risk Management

- Health and Safety Executive (HSE). *Construction (Design and Management) Regulations 2015*. https://www.legislation.gov.uk/uksi/2015/51/contents
- Health and Safety Executive (HSE). *Reducing Risks, Protecting People (R2P2)*. https://www.hse.gov.uk/risk/theory/r2p2.htm
- Health and Safety Executive (HSE). *Tolerability of Risk (TOR)*, 2001.
- Centre for Ecology & Hydrology (CEH). *Flood Estimation Handbook (FEH)* and FEH Web Service. https://fehweb.ceh.ac.uk
- Natural Environment Research Council. *Flood Studies Report (FSR)*, 1975.
- Institution of Civil Engineers (ICE). *Floods and Reservoir Safety*, 4th Edition, 2015.
- Institution of Civil Engineers (ICE). *Reservoir Management*, 2019.
- Hartford, D., et al. *Operational Safety of Dams and Reservoirs*. ICE Publishing, 2016.
- Environment Agency / Defra. *Guide to Drawdown Capacity for Reservoir Safety and Emergency Planning (SC130001/V01)*, 2017. https://www.gov.uk/government/publications/drawdown-capacity-for-reservoir-safety
- Environment Agency / Defra. *Guide to Risk Assessment for Reservoir Safety Management (SC090001/R1 & R2)*, 2013. https://www.gov.uk/government/publications/risk-assessment-for-reservoirs

- CIRIA. *Engineering Guide to the Safety of Concrete and Masonry Dam Structures in the UK (Report 148)*, 1996.
- CIRIA. *Dams and Reservoir Conduits – Inspection, Monitoring, Investigation, Maintenance and Repair (C743)*, 2015.
- CIRIA. *Pipework, Valves and Associated Equipment in Dams (C789)*. Lewin, J. (1995). *Hydraulic Gates and Valves*. Erbiste, M. (2014). *Design of Hydraulic Gates*.
- British Tunnelling Society & Association of British Insurers. *Joint Code of Practice for Risk Management of Tunnel Works*.
- National Protective Security Authority (NPSA). *Guidance on the Protection of Critical National Infrastructure*. https://www.npsa.gov.uk
- Environmental Permitting Regulations (EPR) 2016 (England & Wales).
- Water Environment (Controlled Activities) (Scotland) Regulations 2011.
- Invasive Alien Species (Enforcement and Permitting) Order 2019 (England & Wales).EU Regulation (EU) 1143/2014 on Invasive Alien Species (Scotland context).

13.3. Risk and Functional Safety Standards

- International Electrotechnical Commission (IEC). *IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*.
- International Electrotechnical Commission (IEC). *IEC 61511: Functional Safety – Safety Instrumented Systems for the Process Industry Sector*.
- British Standards Institution (BSI). *BS EN 31010: Risk Management – Risk Assessment Techniques*.
- Engineering Equipment and Materials Users Association (EEMUA). *EEMUA 191 – Alarm Systems – a Guide*.
- International Electrotechnical Commission (IEC). *IEC 62443 – Industrial Cybersecurity*
- UK National Cyber Security Centre (NCSC). *Cyber Assessment Framework*. https://www.ncsc.gov.uk

13.4. Pumped Storage Hydropower: Industry Evidence and Analysis

- British Hydropower Association (BHA). *UK Pumped Storage Hydropower Pipeline 2024*.
- Biggar Economics. *The Economic Impact of Pumped Storage Hydropower*.
- Imperial College London. *System Value of Long Duration Energy Storage in a Net Zero Electricity System*.
- Oxford Global Projects. *Major Project Performance Data and Reference Class Forecasting for PSH* (BHA Event, June 2025).
- International Hydropower Association (IHA). *World Hydropower Outlook*. https://www.hydropower.org/publications
- International Hydropower Association (IHA). *Global Alliance for Pumped Storage – Policy Toolkit*.

13.5. Case Studies and International Experience

- Snowy Hydro Limited. *Snowy 2.0 Project Information*. https://www.snowyhydro.com.au

- Federal Energy Regulatory Commission (FERC). *Engineering Guidelines for the Evaluation of Hydropower Projects*. https://www.ferc.gov
- Statkraft. *Loch na Cathrach PSH – Workforce and Skills Mapping Report*.
- SSE Renewables. *Coire Glas Pumped Storage Hydropower Project*. https://www.sserenewables.com
- Drax Group. *Cruachan Pumped Storage Expansion Project*. https://www.drax.com

13.6. Community, Workforce and Wider System Context

- Royal Society of Edinburgh, Scottish Rural Action & Community Energy Scotland. *A Strategic Approach to Community Benefits in the Energy System*, 2024.
- Scottish Government. *Community Benefits from Net Zero Energy Developments: Consultation*, 2024.
- Skills Development Scotland. *Climate Emergency Skills Action Plan*.
- GB Non-Native Species Secretariat. https://www.nonnativespecies.org

13.7. Expert Evidence

- British Hydropower Association (BHA). *Pumped Storage Hydropower: Risk, Delivery and Investment Roundtable*, London, 20 June 2025.
- British Standards Institution (BSI). BS EN 61511-1: Functional safety – Safety instrumented systems for the process industry sector – Part 1. London: BSI.
- Institution of Civil Engineers (ICE). Floods and Reservoir Safety. 4th ed. London: ICE Publishing, 2015.
- Institution of Civil Engineers (ICE). Reservoir Management. London: ICE Publishing, 2019.
- Environment Agency / Defra. Guide to Drawdown Capacity for Reservoir Safety and Emergency Planning. Report SC130001/V01. 2017.
- Environment Agency / Defra. Guide to Risk Assessment for Reservoir Safety Management: Volume 1. Report SC090001/R1. 2013.
- Environment Agency / Defra. Guide to Risk Assessment for Reservoir Safety Management. Report SC090001/R2. 2013.
- Engineering Equipment and Materials Users Association (EEMUA). EEMUA 191: Alarm Systems – A Guide to Design, Management and Procurement.
- National Cyber Security Centre (NCSC). Cyber Assessment Framework.
- GB Non-Native Species Secretariat. Guidance and resources on invasive non-native species.