Plant and Operational Safety of Hydro Power Plants

The construction of large hydropower plants involves potentially high risks for the health and lives of persons as well as for the environment. Therefore a particularly high level of safety is required for such plants. The implementation of such high safety standards in power plants begins with construction measures such as the selection of suitable material, dimensions and monitoring the quality of the individual components. Operational safety contributes essentially to the safety of the plant. This implies the safety of essential functions (e.g. shutting down safety).
Risk analysis represents the core of functional safety, forming the basis for technical and organisational measures. Examples include: redundancies in the recording of reservoir water levels or organisational measures such as regular tests e.g. shutting down tests. The safe operation of hydropower plants over decades can only be maintained by carrying out every single step constantly.

ZT Hirtenlehner

Klaus Hirtenlehner, DI
Im Stadtgut A1
4407 Steyr-Gleink
Austria
M +43 676 7750401
klaus.hirtenlehner@zt-hirtenlehner.at
www.zt-hirtenlehner.at

21.11.2012
1. Introduction

Operational safety is the technical process, in which there is no risk in the case of failure, but very high costs if the opposite occurs. Reliability of industrial processes is required in order to keep the costs down. Security is essential in industrial processes, because if it fails, not only costs are incurred, but also risk to humans and the environment.

<table>
<thead>
<tr>
<th>Definition</th>
<th>Reliability of Technical Processes</th>
<th>Safety of Technical Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All of the characteristics, which are linked to fulfil requirements under given conditions for a given period of time.</td>
<td>A technical process, in which the risk is not greater than the limit risk, a predetermined time period is required whereby persons are not allowed to enter the danger area.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Measures concerning</th>
<th></th>
<th>the occurrence of faults and failures</th>
<th>the dangerous effect of human errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reasons for Action</td>
<td>economy</td>
<td></td>
<td>approval by a regulatory agency</td>
</tr>
<tr>
<td>Methods of Verification</td>
<td>reliable calculations, plant availability</td>
<td>safety analysis</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Definition of safety and reliability (according to DIN40041 and DIN 31004)

The construction of large hydropower plants requires large investments by the operators. In most cases, the construction of such plants involves hazards, dependant on the scale of the plant and the huge volume of water stored in the reservoirs. This poses problems to the property in the affected surrounding areas, as well as to people’s health. Special requirements with regard to the construction and operation of such plants need to be met in order to reduce these hazards to justifiable risks acceptable by the general public. The term risk (Greek for cliff, danger) is defined differently in various scientific disciplines.

In general, risk is the product of the probability of occurrence of an event and its consequences. During the construction of a plant, the consequences of certain damaging events such as the breaking of a barrage are difficult or nearly impossible to control.

This article focuses on the reduction of the probability of occurrence.

During the construction of such plants the focus is therefore on the influence of the probability of occurrence of damaging events. This results in specific requirements for trades and equipment.

1. Structural measures for the main components
   - Selection of suitable material
   - Adequate strength and wear and tear resistance of components in design
   - Quality monitoring during production

2. Operational safety
   - Risk analysis / Risk evaluation
   - Functional safety
   - Safety and complementary protective measures
   - Organisational measures
2. Structural Measures for the Main Components

Inherent safety measures are the first step in the risk reduction process. They are achieved by avoiding hazards or reducing risks by a suitable choice of design features for the machine itself.

2.1. Selection of Suitable Material

Suitable materials are the basis of every technical product. Availability and price are often decisive for the choice. The selection of incorrect material can cause significant damages. The merchant ships of the early 1940s were an example of faulty design, with hulks that broke under the strain of being on the open sea. The hulk broke along the welding seams. The material failure was due to insufficient fracture toughness. The selection of material that is suitable for a specific application involves criteria that go far beyond simple material strength. The yield strength, or tensile strength, limits the mechanical load capacity of a material. It is obvious that density plays an important role in material applications in aircraft construction. The coefficient of elasticity reflects the ability of a material to resist elastic deformation or distortion. It is important to note that components which are subject to variable loads are also subject to mechanical and thermal stress. In most cases material has to prove a sufficiently high level of creep resistance. In addition, numerous other characteristics are decisive in specific applications, e.g. optical, magnetic and electrical characteristics, as well as, corrosion resistance, friction, abrasion and wear and tear.

2.2. Adequate Strength and Break-Resistant Design of Components

Limit State Design

A distinction shall be made between ultimate and serviceable limit states. One of the two categories of limit states may be omitted provided that sufficient information is verified to prove that the one is covered by the other. Limit state design shall be based upon the use of structural and load models for relevant limitations. It is stated that no limitation is to be exceeded when the following design values are used:

- material properties, or
- product properties, and
- geometrical data

The verifications shall be carried out for all relevant design situations and load cases. The design values of the action shall be conducted using the partial safety values $\gamma F$. Different load situations can be considered by the combination value $\Psi$. The design value of a material or product property will be obtained by dividing the characteristic value by a partial factor $\gamma M$.

Fatigue design

Structural members shall be designed for fatigue such that there is an acceptable level of probability that their performance will be satisfactory throughout their design life.

Fatigue assessment should be undertaken using safe life method.

Select details and stress levels which will result in a fatigue life sufficient to achieve the $\beta$ – values equal to those for ultimate limit state verifications at the end of the design service life.
<table>
<thead>
<tr>
<th>Assessment method</th>
<th>Consequence of failure</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Safe life</td>
<td>Low consequence</td>
<td>1.15</td>
</tr>
<tr>
<td></td>
<td>High consequence</td>
<td>1.35</td>
</tr>
</tbody>
</table>

Table 2: Recommended values for partial factors for fatigue strength

Modelling for nominal stresses should take into account all action effects including distortional effects and should be based on a linear elastic analysis for members and connections.

In linear damage accumulation, the basis of which are the deliberations of Palmer and Miner, the total damage is determined by a linear summation of the partial damage of each tank game. It is assumed that the damage to each part in the oscillation game is independent and does not affect each other.

2.3. Quality Monitoring during Production
The components which are used in common hydro power plants are individually produced or made in small series production. The designing engineer chooses a specific quality level for all components. To ensure that the component requirements of the designer are adhered to, test plans are required. On the basis of the relative test plan for the testing procedures, the quality of raw materials can be ensured and the monitoring of the production can be planned. These inspection plans should verify all essential features. The monitoring of quality assurance has to be carried out by independent auditors or by accredited testing institutes.

3. Operational Safety

3.1. Risk Analysis / Risk Evaluation

Risk management creates and protects value and contributes to the demonstrable achievement of objectives and improvement of performance. Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed. A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.

The risk management process should be
- an integral part of management,
- embedded in the culture and code of practices, and
- tailored to the business processes of the organization.
Risk identification
The organisation should identify sources of risk, areas of impact, events (including changes in circumstances) and their causes and their potential consequences. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.

Risk analysis
Risk analysis involves developing an understanding of the risk. Risk analysis provides an input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods.

Risk evaluation
The purpose of risk evaluation is to assist in decision making, based on the outcome of risk analysis, about which risks need to be dealt with and the priority for treatment implementation.

Risk treatment
Risk treatment involves selecting one or more options to modify risks, and to implement those options. Once implemented, treatments provide or modify the controls. Risk treatment involves a cyclical process of:
- assessing a risk treatment;
- deciding whether residual risk levels are tolerable;
- if not tolerable, generating a new risk treatment; and
- assessing the effectiveness of that treatment.

Monitoring and review

---

1 [8] Risk Management, Principles and Guidelines
Both monitoring and review should be a planned part of the risk management process and involve regular checking or surveillance.

Communication and consultation
Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.

**Example of a method of risk assessment**

To determine the risk of a technical process or of a condition detected is the combination of the frequency of an event and the resulting extent of harm.

$$ R_x = S_x \cdot H_x $$

**Probability H_x:**

- **H₁** Means very low probability of the undesired event that, in the considered processes very few adverse events are expected.
- **H₂** Means low probability of the undesired event that, in the considered processes only a few adverse events are expected.
- **H₃** High probability of the undesired event means that in the considered processes frequently adverse events are expected.
- **H₄** Very high probability of the adverse event means that in the considered processes often adverse events are often expected.

Safety-related parts of the plant are components, where malfunction and failure can create outward a hazard to human and material assets.

**Extent of harm S_x:**

- **S₁** Mild and transient effects on humans and environment.
- **S₂** Small and lasting impact on humans and environment. (Flooding which leads to an electrical short circuit.)
- **S₃** Strong and lasting impact on the environment and people. (Flooding causing undue continuous damage)
- **S₄** Strong and sustained time-critical impact on the environment and humans. (Disastrous effect, many deaths)

**Request classes R_x:**

- **R₁** No additional measures necessary.
- **R₂** Technical measures to check for faults. (Automatic monitoring of a measured value for plausibility)
- **R₃** Additional technical measurers over and above those required for R2. (Determine the necessity of redundancy with regard to the measurement value and automatic monitoring.)
- **R₄** Additional organisational measures required. (Reading of a redundant measuring device)

---

² [2] The code of practice for the maintenance of the central operation of storage dams
3.2. Functional Safety
Functional safety is part of the overall security, based on the system, which depends on the correct functioning of the safety-related system and external device risk reduction. Fail-safe is a central concept for hydro power plants. Fail Safe is the capacity of a technical system, to stay with the occurrence of a certain failure in the safe state or immediately enter another safe state.

As a guideline requirements have been developed by a working group on a number of projects that meet the criteria of large dams. Some relevant examples from the field of mechanical engineering are listed below:

- The bottom outlet is to be provided with two locking levels.
- The drives must be designed so that they can be open and closed, even under unfavourable conditions of friction.

The following basic configurations for large power plants have also been proven:

- The headwater steam must be provided with two locking levels at the beginning.
- At the higher level in the power house redundant sealing planes are often desired for instance guide vanes and spherical valves or Pelton nozzle needle and spherical valves.
- The valves in low pressure side strongly depend on the specific system configuration. Valves in the individual groups of machines are common. Some outlet structures are also equipped with redundant closures.

---

3 [2] The code of practice for the maintenance of the central operation of storage dams
3.3. Safety and Complementary Protective Measures

Safety and protective devices shall be used to protect persons and the environment whenever an inherently safe design measure does not reasonably make it possible either to remove hazards or to sufficiently reduce risks. Complementary protective measures involving additional equipment (for example, emergency stop equipment) may have to be implemented.\(^4\)

**Redundancy of components or subsystems**
In the design of safety-related parts of the machine, duplication (or redundancy) of components may be used so that, if one component fails, another component or components continue to perform the respective function(s), thereby ensuring that the safety function remains in place. In order to allow the proper action to be initiated, component failure shall be detected by automatic monitoring or by regular inspection. Diversity of design and/or technology can be used to avoid common cause failures.

**Emergency stop function**
In order to avert an emergency the following requirements are to applied in current or likely situations:

- the manual override shall be clearly identifiable, clearly visible and readily accessible;
- the hazardous process shall be stopped as quickly as possible without creating additional hazards, but if this is not possible or the risk cannot be reduced, it should be questioned whether implementation of an emergency stop function is the best solution;
- the emergency stop control shall trigger or permit the triggering of certain safeguard movements where necessary.

Once active operation of the emergency stop device has ceased following an emergency stop command, the effect of this command shall be sustained until it is reset. This reset shall be possible only at the location where the emergency stop command has been initiated. The reset of the device shall not restart the machinery, but shall only permit restarting.

In the implementation of hydropower projects, a well-known device for shutting down is the hydraulic protection. The hydraulic protection monitors operating states which are not permitted in the operation of a hydro power plant.

- To exceed the amount of permissible defecation in storage reservoir by monitoring the reservoir level.
- To exceed the maximum allowable headwater stream in the headrace tunnel between the two chambers by flow measurement with maximum value monitoring.
- Detection of major leaks or a burst pipe by comparison driving and flowing stream of water into the penstock.
- To exceed the maximum allowable pressure in the tubular track distribution pipeline of the power plant.
- Small water leaks detected in the chambers and in the powerhouse area (flood protection).

\(^4\) [10] Safety of machinery — General principles for design
3.4. Organisational Measures

It is usually not possible to minimize the risk entirely. In many cases a residual risk remains. The operator must be informed about the remaining risks. This is an essential function of the operating instructions. The residual risks should be described and the operating directives should be defined. Without an operating manual, the operator would not be able to operate a hydropower plant with an acceptable risk.

[2] The code of practice for the maintenance of the central operation of storage dams
The operation of the organisation shall be adapted to the requirements which appear in the operation manual of hydro power plants. The responsibilities must be clearly defined. The presence of qualified personnel ensures optional operational procedures. An operational centre is essential for optimum supervision and to follow the rules.

The work rules and supervision order must include the following points from a security point of view:

- description of the power plant
- management of the entire power plant (normal operation, special operations during flood events, ...)
- installed protective devices (safety-related thresholds, hydraulic protection, physical protection, ...)
- activities in response to protective devices being triggered
- regular inspection and maintenance
- measurement and assessment programmes
- clear user manuals
- organisational structure

The documentation of key operating results, the experience of operators of similar plants and the involvement of experts ensure the continual improvement of plant safety.
4. **References:**