Reliability principles for spillway gates and bottom outlets

G.M. BALLARD, Consultant, UK
J. LEWIN, Consultant, UK

SYNOPSIS. Reliability analysis of spillway gate installations, and to a lesser extent bottom outlets of reservoirs, has been increasingly used in risk assessments of dams. As a result there is now considerable collected experience of the design and operation of different types of components and systems, both qualitative and quantitative. The qualitative experience has led to general acceptance of some fundamental principles of design and operation in order to achieve good reliability. The paper discusses some of the more important principles, using examples from spillway gates which have been assessed for reliability by the authors. A common approach to attaining reliability is the provision of redundant equipment, yet the occurrence of common cause failures (CCF) – and the need to provide adequate defences against them – is less frequently considered. Attention is drawn to the types of events leading to CCFs and to some potentially effective design defences.

DESIGN

For a system that is required to have a high reliability, the design features of the system can have as much effect on the achieved reliability as the specific reliability of the individual components that comprise the system. This section briefly discusses some of the more important aspects of system design, using examples from existing spillway gate designs as illustrations.

Well Proven Equipment

Where a system is intended to perform an important safety function it is not generally appropriate to use newly developed types of equipment or technologies. The failure experience of newly developed components is limited and the failure modes of the equipment are likely to be imperfectly understood. If the equipment has not previously been used in similar applications or environments then there may be unpredicted problems which cause the component to fail in an unexpected manner. This may lead to further failures as a result of unpredicted interactions between components. Also, components based on new technology suffer from the absence of improvements which accrue as that technology matures and benefits from manufacturing and operating experience.

These factors can have a major impact where an individual component is used many times in an installation.

Long-term benefits and performance of dams. Thomas Telford, London, 2004

When updating or replacing equipment on an existing spillway gate installation, particular areas of concern include bearings and bearing materials, PLC control equipment, and lubricants.

Single Failure Criterion

A safety critical system should be designed so that, if possible, the failure of any single component will not prevent the system performing its function when required. This principle is based on the relatively high probability of a single failure occurring compared to the significantly lower probability of two or more concurrent component failures.

While this may be relatively easy to achieve with electronic, electrical and, to some extent, mechanical systems, it is more difficult or impossible to achieve with structural and civil aspects. This difference is mitigated by the respective failure characteristics of the different system types. Electronic and electrical equipment is prone to sudden failure which cannot easily be prevented by condition monitoring or preventive maintenance. Structural and some mechanical systems may be expected to exhibit failure modes which involve progressive degradation mechanisms that, in principle, should be amenable to prevention by monitoring and preventive maintenance. Therefore the single failure criterion is less critical for structural and some mechanical systems than for electronic and electrical systems.

When a component does comprise a single failure point for a system then special care has to be applied to the design, quality assurance and performance monitoring of that component. The principle of using well proven equipment becomes even more important. Equally, the ability to monitor the component to ensure continuing satisfactory performance is essential. In addition consideration should be given to the existence of any sudden failure modes that may arise for that component and how these failure modes can be mitigated by good design or operating practice.

For an existing spillway gate installation of typical design, the situation assessed against this principle may resemble the following:

- The electrical power system is partly duplicated but there are a few single failure points
- The gate control system has a number of components that are single failure points, e.g. control transformer, rectifier, limit switches, etc.
- The single brake is an example of an electro-mechanical component that mostly has degradation type failure modes but may also have sudden failure modes due to loss of electrical power
- The drive train is almost exclusively a series system, with any single component failure leading to failure of the whole system

- The gate itself is a structural system with no redundancy, as are the spillway piers and other civil structures

Judged against this principle, the design clearly has serious deficiencies.

"Fail Safe" Design

The failure of any component within the system should, if possible, move the system towards a "safe" state. For many protection systems there is a "safe" state which is acceptable and component failures should cause the system to move towards that condition.

For spillway gates the situation is significantly more complicated. The purpose of the gate is both to retain the reservoir water level and to pass the water depending on the situation that arises. Neither state – "gates open" or "gates closed" – can be considered "safe". The gate control system has some features that are used to protect the gates from damage but these may inhibit opening of the gates if they fail to operate as intended. Again there is no unambiguous "safe" state, although in a flooding emergency the requirement to open the gates may be more important than safeguarding them from damage.

A specific example involves the limit switches that control gate travel. Overtravel limits are provided to prevent equipment damage. However if one of the limit switches fail in a specific mode, open or closed depending on the logic of the control circuit, then the gate cannot be moved unless the interlock can be overridden. The other failure mode of the switch is "safe" for gate operation but may lead to equipment damage. Two alternative design strategies might be appropriate in this situation. The first would be to provide a redundant arrangement of limit switches such that no single failure would lead to either potentially "unsafe" state. The second (less preferred) would be to provide duplicated switches to prevent equipment damage, but offer an override facility which could be used if the gates need to be opened in an emergency.

Redundancy and Diversity

The main protection for any system against failure of individual components is the use of redundancy and/or diversity. Frequently this takes the form of providing two or more identical parallel lines, each of which can perform the required function on its own. Thus the electrical system on a typical spillway gate installation may have two parallel electrical feeders from the main 440V switchboard all the way through to the gate breakers. Either circuit will provide power to the hoist motors should the other fail. All that is required is a manual changeover of supply breaker on the gate control panel. An automatic changeover system could be implemented by use of

appropriate sensors if required. Further examples are the use of an alternative drive motor (not frequent in practice) should the main drive motor for a gate fail, and the provision of a standby diesel generator to maintain electrical power on failure of the commercial grid supply.

The basic effectiveness of redundancy in improving reliability performance arises because of the failure logic of such systems. If the probability of failure of either one of two duplicate channels is p, then the probability of concurrent failure of both channels is p^2, e.g. if $p=10^{-2}$ per demand for one channel then the system failure probability is $p^2=10^{-2}\times10^{-2}=10^{-4}$ per demand.

In redundant circuits the mode of operation may follow a variety of patterns depending on the exact system type and operation. Where only a single channel can operate at any one time there needs to be provision for an automatic or manual changeover to a standby channel in the event of failure of the first channel. For monitoring or control systems all channels can operate simultaneously and a voting logic can be used to determine how the various channel outputs will be used to define the system output. For example, the parallel gate limit switches are both fully operational at all times and the voting logic is that either limit switch tripping trips the hoist system. For more complex systems involving three or more parallel channels then 2 out of 3 voting arrangements can be used to reduce the occurrence of spurious control/alarm action due to component faults while maintaining a high reliability.

Identical parallel channels can be susceptible to common cause failures, so the use of diverse parallel channels should be considered. In this arrangement, both channels provide a route for the system to function but they use different equipment and/or operating methods to achieve the end result. A simple example would be the use of, say, a vane type limit switch in a parallel channel while a lever arm switch is used on the primary channel. The use of diverse equipment in redundant channels makes it less likely that multiple failures of equipment, affecting both redundant channels, will occur concurrently.

Common Cause Failure (CCF)

The use of redundancy to improve reliability relies on the fact that failure of the individual redundant channels is independent. That is, if one channel fails then the probability of failure of the other channel remains at p, the value it was before the first channel failure. This is not an unreasonable assumption and satisfactorily represents many failure events. However the assumption breaks down when the same cause, a common cause, leads to failure of multiple parallel channels.

To illustrate the effect, suppose that an individual channel has a probability of failure on demand of $p=10^{-2}$ and that p divides into two components, p_I the proportion of random failure modes and p_C the proportion of common cause failure modes. Then the failure probability for a two channel redundant system is not p^2 but $p_I^2+p_C$. If p_C is only of order 5% then the reliability of the parallel system is not 10^{-4}, assuming independent failures, but $0.95\times10^{-2}\times0.95\times10^{-2}+0.05\times10^{-2}=5.9\times10^{-4}$, that is, worse by a factor of ~6. Even if p_C is only 1% then the system failure probability is still worse by a factor of ~2 compared to the fully independent case.

Analysis of many CCF events in the past has suggested that a reasonable working estimate for p_C for a well designed redundant system is approximately 10%, and that specific CCF defence measures will be required if this proportion is to be reduced to any significant extent.

Consideration of the mechanisms that lead to common cause failure (CCF) events indicates that the two most common problems are design errors that have led to unintended interactions between channels or create common weaknesses, and operational errors – particularly in maintenance – that have instigated multiple failures. Other causes, perhaps more widely recognised, are common adverse environmental conditions and external hazards such as fire, lightning or explosion.

A typical spillway gate design is susceptible to a range of common cause failure events including environmental and external hazards, maintenance errors and design interactions. Defences against the causes of CCF events that should be considered when designing and operating systems include:

(1) Design

- Review all stages of the design with the specific target of identifying potential CCF interactions and eliminating or protecting against them
- Equipment or functional diversity such that different equipment or operating principles are used in the redundant channels
- Fail-safe design to ensure that there are no failure modes which can lead to a dangerous CCF
- Well proven equipment so that the failure modes of equipment are well understood
- Protection and segregation of redundant channels to reduce the potential for environmental or external hazards affecting multiple channels
- Derating and simplicity to ensure that equipment is not operating at the limits of its design specification and that the performance of the overall system is capable of comprehensive analysis

(2) Operations

- Comprehensive commissioning trials in order to fully verify equipment performance; comprehensive monitoring, recording and analysis of operating experience
- Ergonomic interfaces to reduce the potential for both simple operational errors and misunderstanding as to the state of the system
- Well thought out and presented procedures for all important activities
- Thorough training and regular practice in realistic exercises

(3) Maintenance and Testing

- Equipment designed to facilitate full testing of all functions without undue interference with the state of the equipment
- Well assessed and presented procedures that can act as a checklist for all relevant important actions
- Staggered maintenance of parallel channels so that redundant equipment is not maintained at the same time

Most of these features are common to the specification for the design of any reliable system, but the potential for CCFs may require special consideration. Examples from typical spillway gate installations illustrate the issues involved:

(1) Environmental CCF

Most of the equipment on a spillway was protected from the weather by sealed enclosures; electrical cables ran to and from these enclosures in steel conduits. If the seals on the enclosure are poorly designed or deteriorate with age then moisture can enter the enclosures and the cabling conduits. There was significant evidence of cable failure due to conduit corrosion and cable degradation as a result of moisture ingress. While concurrent failure of the parallel cabling on the power feeders was not thought likely, at least two factors were of concern. Firstly, the gates were typically all connected to one power feeder and the other feeder was tested infrequently, so one of the feeders could be in a failed state for a significant period of time. Secondly, the gate tests typically involved moving gates under a normal motor load, whereas in an emergency the motor currents could be significantly higher.

The defences in this case could include the following:

- Improved design of water seal; regular preventive maintenance of seals
- Gland seals on all cable entry and exits to reduce the ingress of moisture to the conduits
- Segregation of the control cabinet power feeders so that the failure of one water seal would not affect both power feeders

- Regular and staggered testing of both power feeders both electrically and operationally so that the operating state of both feeders was regularly confirmed
- Occasional testing of the motors with a dummy load that more closely represented the worst conditions of emergency use

(2) External Hazard CCF
Duplicated power feeders run in steel conduit from the 440V switchboard to the spillway gate control cabinets. The conduits run close together over extended distances, crossing structural expansion joints and metal walkways. The conduits did not appear to have any heat protection or slack when crossing structural joints, earthing of the conduits and equipment was often not to modern standards and no lightning protection was installed. If any one of the feeders was damaged due to mechanical interference, fire, seismic shearing, lightning, etc., it is probable that the other feeder would be damaged at the same time.

The defences in this case could include the following:
- Spatial segregation of the cable runs so that the two power feeders would be unlikely to suffer from the same physical event
- Improved protection of the conduits from external events
- Provision of a diverse means of operating the gates, e.g. a portable diesel driven engine that could be connected to the gate drive train

(3) Design CCF
On some spillway installations the motors drive the hoist gear train via worm reduction gearboxes. Some of these boxes, which operate at quite high speed, are small and get very hot during operation. They have breather vents, which are simply holes in the top of the boxes, and water ingress has been a recurrent problem. The water both degrades the lubrication of the gears and has led to significant problems with the shaft oil seals and bearings. Both the main drive motor for any gate and the alternative drive motor operate through identical types of worm reduction gearbox and a systematic problem with this type of box could lead to failure of both alternative drive trains. On one project 4 out of 14 gates had been tagged out for emergency use only because of degraded worm reduction boxes.

The defences in this case could include the following:
- Derating of the worm gearboxes to ensure that they operate well within their design capacity and are thus more tolerant of poor conditions
- Improved attention to environmental protection by fitting breathers with desiccant filters to reduce water ingress
- Prompt action on observed degradation so that the concurrent existence of degraded equipment can be minimised

- An alternative design of redundant motor arrangement that does not share common types of equipment

(4) Design CCF

The design of the spillway gates on some projects incorporated a gate bottom flange which would make the gate prone to severe vibration under certain opening conditions. The operators were not aware of the potential gate vibration problem and were unsure how to react to the occurrence of severe vibration. On one project where vibration had occurred it was attributed to water hammer and not thought to be significant. Continuing severe vibration could lead to failure of the gate hoisting cables or anchorage points, and possibly structural failure of the gates. The condition could affect all the gates if they had to be opened during a major emergency.

The defences include:

- Use of well proven equipment which has a recorded experience in the relevant application and environment
- Design review at project inception to identify potential weaknesses in design or operation of the equipment
- Monitoring, recording and analysis of operating experience to identify potential problems, followed by effective action to remedy them

(5) Operational CCF

In an emergency, spillway gates must be opened to prevent the dam being overtopped. Generally operational staff will receive instructions about the extent and timing of gate opening. However if communication is lost staff will be expected to open the gates themselves using a set of emergency procedures. Interviews with staff at some projects revealed that they had little understanding of these procedures, had in most cases never used them in any training or emergency exercise, and had a number of misconceptions about the correct operation of the gates. If communications were lost in a real emergency, a significant delay in opening the gates could prove critical. The performance of operational staff could affect all gates at the installation and could have breached any redundancy provisions in the design.

The defences that may be relevant to this situation include:

- Provision of clear, well presented emergency procedures and a requirement that these be practised on a regular basis
- Performance of regular emergency exercises simulating a range of emergency scenarios to which project staff must respond appropriately
- Training and certification of operating staff at all projects; regular re-certification requiring demonstration of adequate knowledge and experience

Revealed Faults

The design intent should be for any component failure to become apparent to the operators as soon as possible after it occurs. The objective is to minimise the time for which a system remains in a failed state without any repair action being initiated. For normally operating systems this requirement may be straightforward, but for protective systems operating in a standby mode it requires more consideration. The most common technique is to employ monitoring and alarm systems such that appropriate sensors will detect anomalous conditions and alert the operator.

For spillway gates much of the equipment is deactivated between tests and is therefore not amenable to monitoring. However the electrical supply systems can be monitored and alarmed, particularly where the supply to the gates is separate from the supply to the dam offices and the staff may be unaware of a power trip.

Despite the difficulty of continuous monitoring there is value in considering a monitoring system which is activated when power is applied to the gates for a test. Not all features of the gates may be exercised during testing and a monitoring system could alert the operator to potentially degraded conditions such as low oil levels, high gearbox temperatures, or high earth leakage currents which could be indicators of incipient failures. The electrical continuity of all the circuits could be checked, as could some aspects of the integrity of equipment such as limit switches, protection devices and controls.

Testing

Standby protective systems such as spillway gates may be idle for extended periods. In the absence of fault monitoring systems, component degradation and failure only becomes apparent at the time of an actual demand. Assuming that component failures occur randomly over time, the probability of the system being in a failed state increases approximately linearly with elapsed time since the last demand.

Regular testing ensures that the operability of the system is checked on a much shorter timescale and that system repair can be carried out before an actual demand on the system. An effective test programme must provide for testing all aspects of the system at appropriate intervals. The test interval should reflect the likelihood of potential failure modes, as represented by the failure rate for that part of the system. Care should be taken to ensure that the test programme examines aspects of the system that may have unrevealed failures, where components are not used on a routine basis but comprise a back-up or protection function for use only in specific situations.

With reference to a typical spillway gate installation:

- The test programme should include standby provisions such as an alternative motor arrangement
- If bypass features exist to protect against failure of, e.g., limit switches, then these should be tested regularly; similarly the correct functioning of items such as reset buttons on current overload trip should be verified
- Alternative power supplies such as diesel generators or trailer mounted emergency power supplies should be tested by operating a number of gates; where relevant, it is particularly important to test the interface arrangements for coupling the generator into the power supply circuits

OPERATION

Ergonomic Design

While spillway gate equipment is designed to operate effectively and reliably, it must also be designed to be operated easily. On installations which are manually operated, with no automatic control, the equipment and especially the control systems should reflect good ergonomic practice.

Major design elements for control systems include:

- Controls should be systematically laid out and clearly and unambiguously labelled; controls arranged on a mimic diagram of the system are often effective
- The controls should show clearly the state of the system using lights or other displays as appropriate
- If the system has interlocks, inhibits, protection etc. which can disable the system operation, the state of these should be clearly shown
- If a piece of equipment is in a failed state then this fact should be made clear to the operator by appropriate sensors/alarms/displays
- Any overrides or bypasses intended for irregular use should be protected from accidental use by appropriate means such as key operated switches
- The actual state of the equipment, rather than the state of its control element, should be shown wherever possible (a motor running light should be based on measured rpm, current drawn etc. rather than inferred just from voltage to the motor terminals)
- The operation of the controls must reflect the physical limitations of operating staff; e.g. displays should be visible and easily readable when the relevant controls are being operated, controls should be easily and comfortably accessible and well illuminated where appropriate, manual operations should be within normal manual strength limits

These features are required in order that staff can operate gates reliably, often under stressful conditions when it is easy to make slips and mistakes.

On some existing spillway gate installations the following issues arise:

- The gate controls are generally simple and the layout is therefore straightforward, but on some older plant the labels on control buttons can be illegible, causing a major problem for inexperienced staff
- The control panels may have no indication of the current state of the hoisting system; there may be no indication of electrical power to and from the breakers, no indication of power to the motor or the brake, and no indication of the position of any of the limit switches
- Gate hoist mechanisms incorporate protection systems related to the gate and the electrical equipment, but control panels often provide no information on the status of these interlocks or protective devices (if a gate, when last closed, tripped out on the overtravel limit switch it would have to be backed out using an override button until the overtravel limit switch has cleared, but the operator would have no indication of this)
- There may be no condition monitoring in the form of alarms or sensors, so the operator may have no indication of equipment failure other than lack of response from the system

Operating Procedures

All significant operating tasks, especially those performed infrequently or under stressful conditions, should have clear, well-written procedures to guide the operating staff. The procedure should be simple and straightforward, containing only essential text and diagrams.

The procedure should:

- Explain simply under what circumstances it is to be used and how the operator can determine the relevant circumstances, e.g. what readings to take, how to find them, who to communicate with, etc.
- Explain simply what it aims to achieve, e.g. why the procedure is being performed, how its success or failure can be measured, what data the operator can use to assess the procedure, etc.
- Lay out in flow sheets the sequence of actions required. At each stage the state of the equipment should be specified, with instrument readings if appropriate. References should indicate where ancillary information can be found, addressing issues such as what may go wrong during the action, how it can be identified and how to recover the situation. If there are several separate objectives these should be clearly distinguished.
- Where diagrams or graphs are required the procedure should state simply and clearly how they are to be used, what data is required as input and where it is available, what value should be read from the graph and how it should be used
- Where communications are required the procedure should identify who is the contact, how to reach him/her, what information will need to be given, and what information/instructions need to be received

- Instructions should be in large type, visible in poor light, encapsulated for use outdoors in inclement weather conditions; a copy should be kept in the action location in addition to a clearly identified central location

While much of the above may seem obvious, the authors have visited many projects where operating procedures failed to conform to these guidelines.

Training

All staff who are expected to operate the gates during an emergency should be trained and should regularly practice gate operation. They should be certified as competent to operate the gates after initial training and re-certified on a 3–5 year basis to ensure that they maintain their competence. Re-certification should be conditional on demonstrating a good level of practical experience in routine gate operations and participation in a reasonable number of emergency exercises.

Emergency exercises could vary in scope from simply practising the use of various standby facilities such as the alternative motor drive or the diesel generator, to a larger scale exercise in which a full scenario is simulated and staff have to act in real time. A full scale emergency exercise should be undertaken at least once every three years, and should involve practising both communications with the administrative control centre and the independent action that could be necessary if such communication is lost.

CONCLUSIONS

The benefits of reliability assessment are both qualitative and quantitative. There are clear principles of design and operation which will lead to improved reliability in practice. As a broad generalisation for systems intended to provide some type of standby function, where the appropriate reliability measure is probability of failure on demand, a well designed and operated system should be able to achieve a reliability of $\sim 10^{-3}$, a high integrity system intended for a safety critical function should aim to achieve a standard of $\sim 10^{-4}$, and only an exceptionally carefully engineered, designed and operated system is likely to achieve a reliability of $\sim 10^{-5}$.

Spillway gate installations are safety critical structures. A number of gate systems assessed by the authors have not achieved a reliability standard of 10^{-3}. Sometimes they have been an order of magnitude or more worse. This might be expected from installations that were designed and constructed 30–50 years ago, but the same trend has been found in gates commissioned in the last 15 years. While certain design and operation principles may appear self-evident, many of the installations visited by the authors have fallen far short of the recommendations laid out in this paper.