Protecting gates against cyber warfare

Bryan Leyland, MSc, DistFEngNZ, FIMechE,
Leyland Consultants Ltd
17 Bangor Street,
Point Chevalier,
Auckland, New Zealand

1. Introduction

In several countries power systems have been subjected to cyber attacks that have caused blackouts and damage to generators and transformers. There is strong evidence that some of the major powers have hacked into power system control systems in other countries and planted malware that, if triggered, could cause widespread blackouts and damage. Nuclear power stations have been identified as a prime target and are carefully protected against cyber warfare.[1]

Hackers blocking the opening of spillway gates during a flood event could cause a catastrophic dam failure worse than any conceivable nuclear accident in a modern power station. Hackers could also open all the gates when water levels are normal, causing a devastating downstream flood.

This paper argues that all new and existing spillway gates that could be mal-operated by hacking into remote controls or by operator errors need to be protected against this happening.

2. Protecting against hacking

Gates that open and close according to the upstream water level without any external power supply or external control signals are inherently proof against hacking. It follows that, wherever possible, water level operated gates that have a proven record of reliability should be used. These gates are discussed below.

Existing dams with power operated and/or remote-controlled gates or, in proposed gated dams, gate operation should be protected against hacking by a control system that cannot easily be hacked backed up with a secure local control system that will open the gates if the water level is dangerously high and will stop too many gates being opened when the water level is normal.

Locally controlled gates that rely on a local operator initiating opening or closing also need to have an equivalent system to guard against operator error.

2.1. Hacking resistant systems

Many IT systems secure networks with gateways with tight controls on the data passed, and good auditing of user activities. These are a good protection against internet protocol attacks such as denial of service that would paralyze the control system. This is not a complete solution for gate controls because, if a denial of service attack takes some time to neutralise, the control system will be paralysed in the interval.[2]

The risk of hackers penetrating the control system and issuing rogue commands can also be reduced by using two-factor authentication where, for example, the remote system sends a text message to the operator's mobile phone containing a one-time password that the operator then keys into the remote control system. The control instruction is authorised on receipt of the password by the remote system. Other methods are available.

There is a fundamental problem in any defence against hacking. The more effectively a system is protected against hacking the higher the probability that a legitimate control instruction will fail to get through. A gate control system must be proof against this possibility because failure to transmit a legitimate command to open spillway gates could be catastrophic.

Given that it is effectively impossible to guarantee that legitimate remote control signals always get through or that a local operator will always do the right thing, a highly reliable secondary system is attractive, or even imperative. One option is to interpose an independent and completely isolated control system between the remote control system and the spillway gates that will detect and then ignore any rogue instructions affecting the operation of the gates and, if necessary, operate the gates as needed.

This paper proposes the installation of a small PLC in the gate control room that is carefully isolated from the Internet and local control systems. This PLC monitors the position of the gates and the water level. If the water level is dangerously high the PLC will isolate the external system, open the gates under control to maintain a safe water level and send an alarm. If the water level is normal and a remote instruction to open enough gates to cause a dangerous flood downstream is received, the PLC will isolate the external system, block the gate opening signals and send an alarm.

The PLC would need to monitor triplicated water level sensors and the position of each spillway gate. The water level measuring and gate position systems would need to be vandal and tamperproof. It must be virtually impossible for an unauthorised person to change the PLC program. This proposed arrangement is shown in Figure 1.

The only connections between the PLC and the outside world would be hardwired using isolating relays.

The PLC would also monitor the gate power supply and start an emergency diesel if power was needed for gate operation.

If the PLC failed it would be configured to send an alarm to the remote control system while reverting to a situation where remote control of the gates was still possible.

The authors recommend that this (or an equivalent system) should be regarded as absolutely essential on any dam where mal-operation of the gates for any reason could put lives at risk.

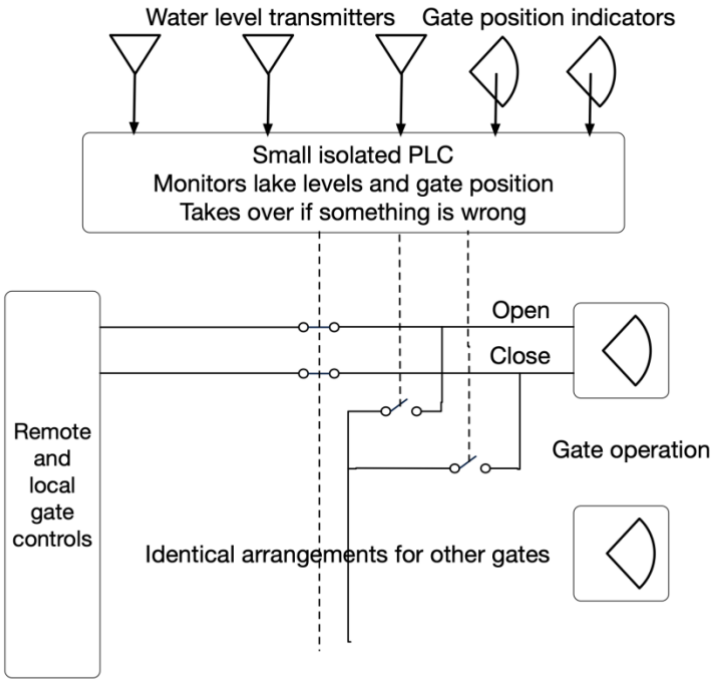

Fig. 1. Arrangement of safety PLC

3. Radial and vertical lift gates

Most radial gates and all vertical lift gates require a power supply to operate them. Most rely on remote control from the power station or local control centre or from a remote control centre. They are therefore at risk from mal-operation by the operator or from hacking into the remote control system.

Power operated gates are often the only option on large dams with high flood flows so it is essential to protect them against power failure, hacking or operator error.

It is common practice to provide a power supply for the lifting gear from the power station itself. That this is quite unsatisfactory was demonstrated at Sayano Shusenskaya in Russia where the catastrophic failure of a turbine flooded the power station and deprived the spillway gates 200 m above of a power supply. Fortunately, the dam was not full and so there was sufficient time to arrange an emergency supply. If the dam had been full and was over topped the dam may have eventually failed. This could have destroyed downstream dams and put many lives at risk.[3]

4. Flap gates

Figure 2 shows a typical flap gate supported by airbags.

Flap gates are more reliable than most other power operated gates because they can be relied upon to open without power in an emergency simply by arranging to have a water operated valve triggered by excess water level. This is not always a satisfactory solution because, once triggered, the gate is likely to open 100% even though only a relatively small opening was needed.

Flap gates need power to close so they still need protection against power failure, hacking or operator error.

It can be argued that flap gates have been largely superseded by the pivoting gate described below that does not require a power supply to open or close and is effectively invulnerable to hacking and operator error.

Figure 2 Flap gate supported by airbags.

5. Power supplies

Given that spillway gates must be able to operate during the worst weather conditions ever experienced, when power supplies are likely to be disrupted and operators may not be able get to the spillway. it is recommended that any gate systems requiring a power supply should have duplicate, independent power supplies – usually emergency generators with automatic starting – close to the gate. This arrangement is shown in Figure 3.

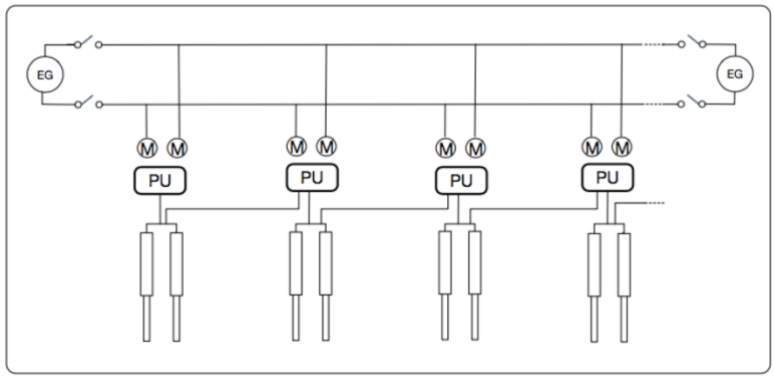

Figure 3 Gate power supplies

It must not be possible to disable the generators by hacking into the control system.

For additional security the generators should have hydraulic starting[4] rather than batteries, because this dramatically reduces the possibility of start failure, and, if possible, they should be air cooled because cooling system problems are a major cause of unreliability of emergency diesel generators.[5] They should also be arranged so that they can synchronise with the power system so that full load testing can be carried out easily and frequently.

6. Water operated gates

Any gate that opens and closes automatically without any external power supply or control signal is proof against hacking.

6.1. Float operated gates

There are many types of float operated gates but not all of them have been successful. One of the most successful is the buoyant weight operated gate. This gate is counterweighted to open and is held closed by another counterweight mounted in a well. The well has a water supply pipe with its intake at the level at which the gate should start to open and has an orifice controlled drain. When the flow into the pipe exceeds the capacity of the orifice the well commences to fill and steadily reduces the weight of the counterweight until it is no longer sufficient to hold the gate closed. As the gate opens it slowly raises the level of the intake of the water supply pipe to ensure stable operation.

Figure 4 below shows the principle of operation. The drawing is based on a gate Leyland Consultants Ltd designed in conjunction with Snowy Hydro
6
f Australia. The gate has been in service for more than 35 years on a spillway gate in New Zealand and, according to the owner, it and it has never failed to open when needed. It operates about 20 times each year, which corresponds to a failure rate better than 1:700. There was an initial problem with weed blocking the intake pipe. This was solved by changing the intake arrangement.

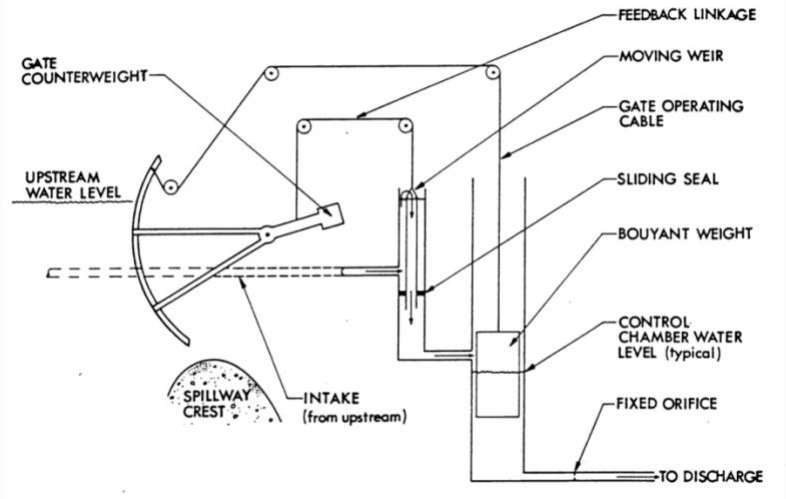

Fig 4 Buoyant weight operated gate

Snowy Hydro has used this system on radial gates 21 m wide and 11.5 m high and it could be used on even larger gates. These gates have been in service for about 50 years and there is no record of any serious problems or failure to operate when needed. They have had minor problems with seal friction which probably indicates that the counterweight was undersized.

If the gate sticks there is a limited amount of additional force available. Once the buoyant weight is submerged, the opening force is constant.

If the water intake is adequately screened and the counterweight is adequately sized the major remaining risk is failure of the rope attached to the counterweight. If the rope breaks, the gate will open and prompt action can be expected. This risk can be minimised by using modern plastic rope.

The gate can be arranged to open in response to a remote control system by simply adding a second lower level intake controlled by an electrically actuated valve or by providing a small winch that lifts the counterweight.

If the gate has remote controls there is always a possibility of someone hacking into the system and opening the gates. If it is properly designed hackers cannot stop it opening when needed.

6.2. TOPS pivoted gate

An excellent example of an extremely reliable water operated gate is the TOPS upstream pivoted gate recently developed in South Africa that is controlled by water ballast.[7]

Figure 5 shows one of these gate spilling water.

Fig 5 TOPS gate

The TOPS gate consists of a tank with a pivot above the lake level. Duplicate ducts connected to the lake keep the tank full of water at the level of the lake. When the lake level is in

the normal range, the tank has sufficient water in it to hold the gate in the closed position. As the lake level rises above the top of the gate, the tank is already full to capacity and the force on the gate soon exceeds the weight of the water in the tank, so the gate begins to open. As the gate opens it tilts and water drains out of the tank, which reduces its weight and allows it to open even more. In a major flood, all the water drains out of the tank and it floats on top of the nappe, providing only a very small restriction to the spillway flowt. This is illustrated in Figure 6.

When the flood abates, the tank descends and fills with more and more water, thus restricting the flow to maintain the upstream water level. As the flow continues to decrease, the tank continues to fill with water and finally the gate closes completely.

It is possible to open the gate at any time simply by opening a drain valve in the tank. This can be done locally or remotely.

It is difficult to envisage a situation where this gate would fail to open. If the friction in the pivot bearings increases, it will mean the lake level must be higher than normal to open the gate and this, in itself, should flag the problem. As the force on the gate will increase steadily as the head level rises above normal, it is hard to see how the increased bearing friction would be able to stop the gate opening most of the way. It is also difficult to imagine how problems with high friction seals would prevent the gate opening because the gate moves away from seals rather than sliding and there are very high forces available to overcome any initial seal sticking and allow the gate to open normally.

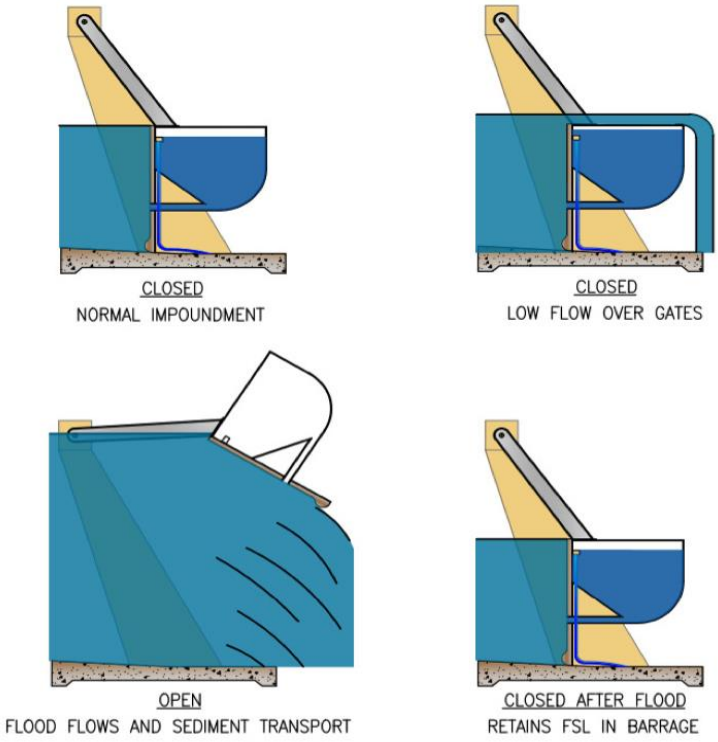

Fig 6 Operation of TOPS gate

A number of TOPS gates have been installed on dams in southern Africa with, as far as the authors know, no problems at all. The biggest gate so far is 12 m by 4 m, but Amanziflow has done design studies that show that gates up to 30 m long and up to 10 m high are feasible. Other studies indicate that it is about 30% lighter than an equivalent radial gate and, when the savings from eliminating the lifting gear and power supply are factored in, it should be considerably cheaper than a conventional gate.

As a 20 m by 10 m gate would pass about 1,000 m3/s of flow, it would seem that TOPS gates are a simple, reliable and economic way of passing flows as much as 5,000 m3/s or, in some circumstances, even more.

They are an ideal candidate for the replacement of obsolete and unreliable gates. If, for instance, they replace flash boards then it will also be possible to raise the normal operating the level of the lake which can have a considerable economic benefit.

In circumstances where large trees might be brought down by major floods, TOPS gates may not be suitable . They are also unsuitable for use in icing conditions.

7. Conclusions

Hacking presents a significant risk to any spillway gate that relies on remote control. Any dam where mal-operation of the spillway gates puts downstream populations at risk should be protected against the possibility of hacking.

On any dam where gates are needed, pivoted gates should be the first to be considered because they are highly reliable and proof against hacking.

Any new or existing gate that relies on remote control or local control by an operator, and could cause a disaster if mal-operated, should be protected against hacking or operator error. If either occur, a backup system should intervene to operate the gates as needed to keep the dam and downstream populations safe.

The Author

Bryan Leyland is a mechanical and electrical engineer with more than 50 years experience in hydropower. He has been involved in many hydropower projects in New Zealand and overseas and is currently working for the World Bank on a dam safety panel in Nigeria. He is a member of Committee V of ICOLD which deals with the safety of spillway gates. He believes that much more attention needs to be paid to the safety of large dams and spillway gates. He is the author of "Small Hydroelectric Engineering Practice"

1 **Larry Bell,** Cyberwarfare: Targeting America, Our Infrastructure and Our Future Amazon Kindle
2 The NZ Stock Exchange was paralysed by a denial of service attack for four days in late August 2020.
3 **B W Leyland,** Lessons from the accident at Sayano-Shusenskaya hydropower station. EEA Conference and Exhibition 2010 17-18 June 2010 Christchurch, NZ.
4 https://www.ipu.co.uk/products/hydraulic-engine-starting/
5 https://powerelectrics.com/blog/four-reasons-why-your-generator-fails-to-start
6 Snowy Mountains Hydro-electric Authority, now Snowy Hydro Limited.
7 https://amanziflow.com/products-2/tops-gate/