creating a better place
for people and wildlife

Environment Agency

Horncastle Reservoir
Low-Level Outlet Sluice Gate

Asset Performance Review
Feb 2024

Document Owner:
Chief Engineer / Director of Asset Management & Engineering

Document Originator:
Engineering and Technical Assurance, Asset Management & Engineering

Environment Agency
Chief Engineer
Seacole, 2 Marsham Street, London, SW1P 4DF

Glossary of Terms

AEP – Annual Exceedance Probability – the likelihood of a given size flood in any one year.
AIR – Area Incident Room – the area commend centre from where duty staff manage an incident
AME – Asset Management & Engineering Directorate
CE – Catchment Engineer – a Chartered Engineer who provides engineering leadership to an Area.
DCE – Deputy Catchment Engineer – An Incorporated Engineer who supports the Catchment Engineer.
FCRM – Flood and Coastal Risk Management – A function within the Environment Agency
FGS – Flood Guidance Statement – 5-day Flooding outlook issued by the Flood Forecasting Centre
FIDO – Flood Incident Duty Officer
FMEA – Failure Modes and Effects Analysis
FODO – Flood Operations Duty Officer
HAZOP – Hazard and Operability Study
HMI – Human Machine Interface – essentially a small touch screen used by operators to interact with the control system.
MEICA – Mechanical, Electrical, Instrumentation, Control and Automation
M&E – Mechanical and Electrical
O/I Card – Output input card for a PLC or telemetry outstation – takes and sends out signals
PLC – Programmable Logic Controller
RAC – Reservoirs Act Coordinator – Environment Agency member of staff with responsibility for ensuring compliance with the Reservoirs Act 1975 for an Area.
SupE – Supervising Engineer – A member of a relevant reservoir panel who is appointed to supervise the reservoir under Section 12 of the Reservoirs Act 1975.
SWANTEL – South West and Anglian Telemetry System
AME – Asset Management & Engineering Directorate

Horncastle Reservoir Asset Performance Review

Scope of Review

On the 23rd October 2023, the Environment Agency Chief Executive commissioned his Chief Engineer to review the delayed closure of the sluice gate at Horncastle Reservoir during Storm Babet. The key requirements of the review are to determine:

1. What happened, did the asset operate as expected, in particular, it has been alleged that the office was contacted about non-operation of the asset – what is the timing around these circumstances?
2. The history of the asset, inspections, testing.
3. What was the impact on flood levels in normal operation and in this incident.

The Chief Engineer appointed his National Engineering Manager, a chartered civil engineer, in the FCRM, Asset Management and Engineering Team (part of the EA's Technical Authority service), to lead this review.

In establishing answers to the above questions, the review considers, as far as possible, the root causes of the issues, and makes recommendations to reduce the likelihood of a similar failure happening again.

Infrastructure Failure – the Swiss Cheese Model

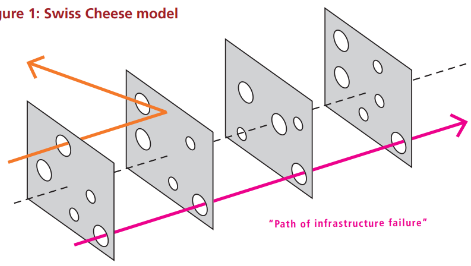
Approach/Methodology: In response to the Grenfell Tower fire, concerns were raised that failings may be found to be systemic and not site specific. This led to a review by the Institution of Civil Engineers; In Plain Sight: assuring the whole-life safety of infrastructure (October 2018) which considered the potential vulnerabilities that can lead to serious asset failures, and to look at how that risk can be reduced. Potential vulnerabilities were identified at all levels in the design, build and operation of infrastructure. Individual blind-spots or vulnerabilities will seldom lead to catastrophic failure on their own, but when vulnerabilities from a range of sources line up, in combination, then failure can occur. Vulnerabilities can include design flaws, the operation of control systems, the application of maintenance regimes, issues of governance, organisational culture, knowledge management and training.

The 'In Plain Sight' review Panel used the well-established Swiss Cheese model of risk analysis to help it consider the systemic nature of risk to infrastructure. In this model, lines of defence against an incident occurring are conceptualised as slices of Swiss Cheese, with vulnerabilities presented as holes in the cheese (see Figure 1).

The review team studied a wealth of academic work about the causes of failure, and they determined that the following reoccurring themes could be seen:

- Failure to identify all risks within the system.
- Operations not in accordance with design intent.
- Weak or non-existent procedures for approving.
- Incomplete or inadequate information available to decision makers.
- Increased demands on assets.
- Lack of access to engineering input.
- Disabling of safety controls for 'operational reasons'.
- Poor quality supervision and assurance, including over-reliance on visual inspection.
- Failure to share lessons from earlier incidents.

Figure 1: Swiss Cheese model



This review into the failure of the asset at Horncastle considers the vulnerabilities of the asset from a range of sources and recommends improvements to the lines of defence against failure re-occurring.

Background to the Reservoir

Horncastle Reservoir is an earth-fill embankment dam, approximately 750m long, situated approximately 6km North of Horncastle on the River Bain. The reservoir became operable in December 2016 and has a capacity of 1,517,000m^3. It protects the town of Horncastle from a 1% annual exceedance probability (AEP) flood event. Floods exceeding the design event, discharge along a 300m long grasscrete spillway.

A control structure situated within the dam uses a passive, automatic Hydroslide flow regulator to limit the downstream pass- forward flow to 7.1m^3/s into the River Bain. The Hydroslide operates without intervention, using a float to control the position of the gate to limit the pass-forward flow. A separate outlet is in place to drain the lowest part of the reservoir, discharging through a 1.5m diameter culvert, via a sluice gate, downstream of the mill weir, below the main outlet of the dam. The sluice gate is designed to close automatically by electrically actuated mechanical means, before the reservoir starts to fill, to ensure that the Hydroslide controls the downstream flow to a maximum of 7.1m^3/s. The trigger level for sluice gate closure is set so that it occurs several hours before the flow in the River Bain reaches the 7.1m^3/s design flow. This early closure allows time for the sluice gate to be closed manually if required. A schematic of the flow control can be found in Appendix A.

The low-level culvert also acts as a ‘scour valve’ to enable the reservoir to be drawn down in an emergency, or to discharge water when there is an issue with the Hydroslide. Upstream of the sluice gate and Hydroslide there is a coarse bar screen with an automated screen rake.

The operation of the sluice gate during Storm Babet on the 20th October 2023 was the thirty-third time that the River Bain had reached the trigger level to close the sluice gate, with the most recent event prior to Storm Babet being in April 2023.

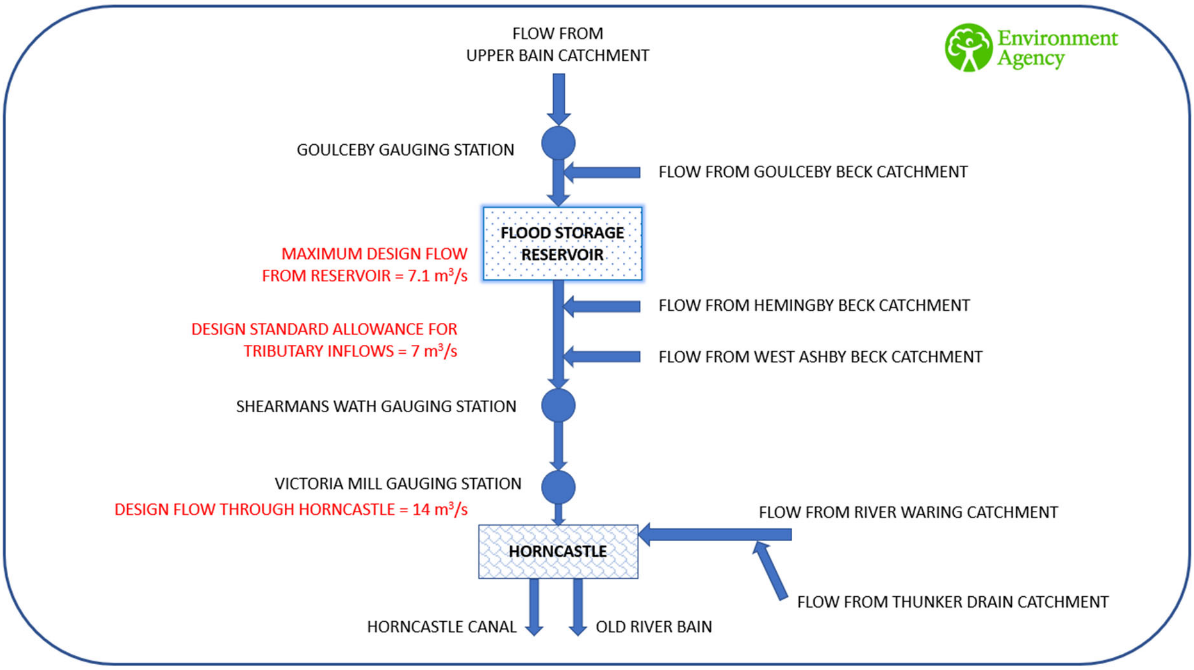


Figure 2 – River Bain Schematic

The onset of property flooding in Horncastle occurs when the flow rate in the river channel exceeds 14m^3/s. With flow from the reservoir limited to 7.1m^3/s, this flow is joined by two further tributaries before it reaches Horncastle. The uncontrolled flood flow from these two tributaries during the 1% AEP design event is estimated to be 7m^3/s, which results in the peak flow in the town of 14m^3/s for the design event when the dam is operating effectively.

History of the Asset

The dam and associated structures were constructed between 2015 and 2017 to restrict the pass-forward flow on the River Bain, and thereby provide flood protection to the town, up to the 1% AEP flood level. The requirement for the low-level outlet, and associated sluice gate, is a result of the design requirements where the main outlet and river channel does not sit at the lowest point in the basin, but is artificially 'perched' on the valley side. This is a legacy of a river diversion, pre-1840s to supply water to a mill, at a higher level, to operate a water-wheel, with the river flowing over a weir adjacent to the mill. Figure 3 shows old maps of the area – note the dotted line which represents a parish boundary and is likely to be the original course of the river. This is unusual in that normally a mill would be served by a mill-race which is an offtake from the river to supply water to the mill at a higher level, rather than by diverting the whole river.

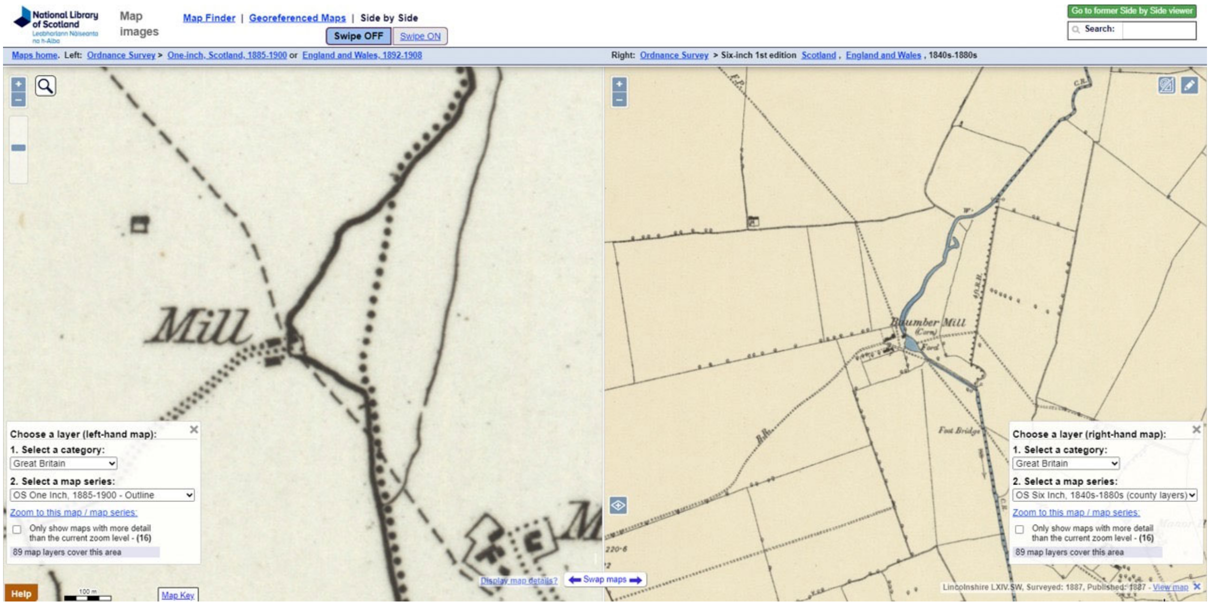


Figure 3 – Maps of the site from the 1800s

During development of the scheme, the optimum solution would have been to restore the river's original course, passing the main flow through the dam at the lowest point at its restricted pass forward flowrate. This would have enabled passive control of the river at the lowest point, eliminating the need for the additional automated sluice gate to be closed to fill the reservoir. However, to accommodate the mill rights of the landowner, the higher-level watercourse was maintained to allow for the potential use of the mill in the future, particularly for hydropower generation. An automated sluice gate at the lowest point of the reservoir does serve a useful safety feature of a dam, to enable the draw-down of the reservoir in an emergency.

Storm Babet

Storm Babet brought exceptional rainfall to parts of the country, with eastern Scotland seeing 150 to 200mm falling in the wettest areas, by far the wettest day on record in a series running from 1891. Heavy, persistent, and widespread rainfall also affected much of England, Wales and Northern Ireland from 18th to 20th October, with 100mm falling fairly widely. This was the third-wettest independent 3-day period for England and Wales, while the Midlands provisionally recorded its wettest 3-day period on record. This rain came on top of very wet weather earlier in October, with parts of Lincolnshire recording over 225% of the average monthly October rainfall in the first three weeks of the month.

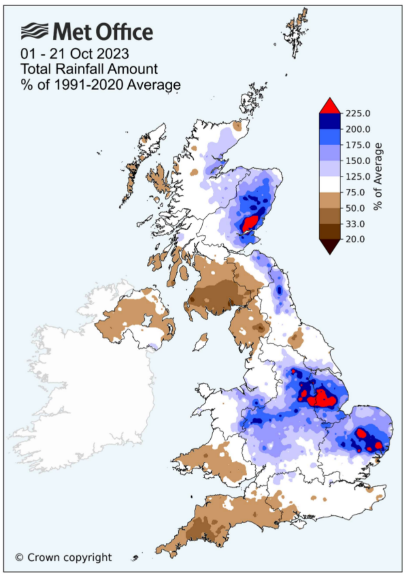


Figure 4 – Rainfall during the first 3 weeks of Oct compared to average

Atlantic storm systems affecting the UK in the autumn and winter months normally track west to east, driven by the jet stream, clearing eastwards quickly. In contrast, this storm was on an unusual track from south to north, enabling it to pick up additional moisture as it crossed the Bay of Biscay. Babet was also unable to clear eastward into the North Sea due to a blocking area of high pressure across Scandinavia. The rain-bearing fronts remained stationary across eastern Scotland for a prolonged period, before moving back across England and Wales.

Figure 5 shows the rainfall distribution for the storm, with Lincolnshire seeing up to 100mm of rainfall quite widely over the four days from the 18th to the 21st October. More significantly, due to lower monthly average rainfall totals in Lincolnshire, the county saw some of the most extreme rainfall compared to long-term averages, with around 150% of the normal rainfall for October experienced during Storm Babet.

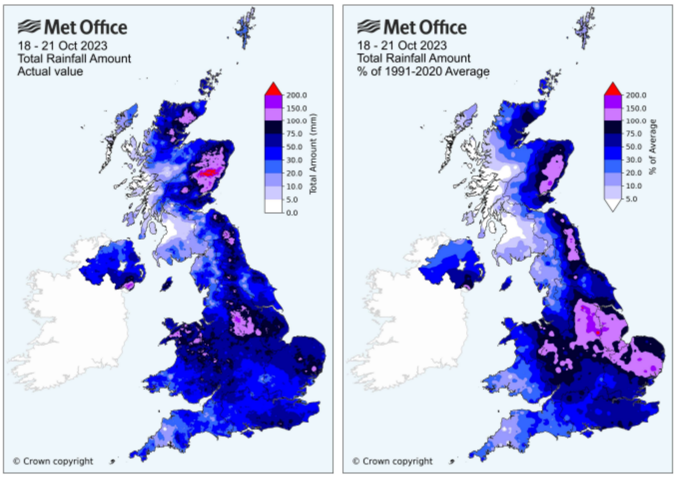


Figure 5 – Rainfall totals and percentage of LTA during Babet

The antecedent conditions were wet, and Storm Babet brought significant additional rainfall.

On the 19th October 2023, the Flood Forecasting Centre, issued the Flood Guidance Statement (FGS) for the coming days. This highlighted the likelihood of significant inland flooding impacts in the North. Lincolnshire was shown on the FGS coloured yellow for the 20th and 21st October, with the associated yellow weather warning giving a low likelihood of significant impacts from rivers and surface water.

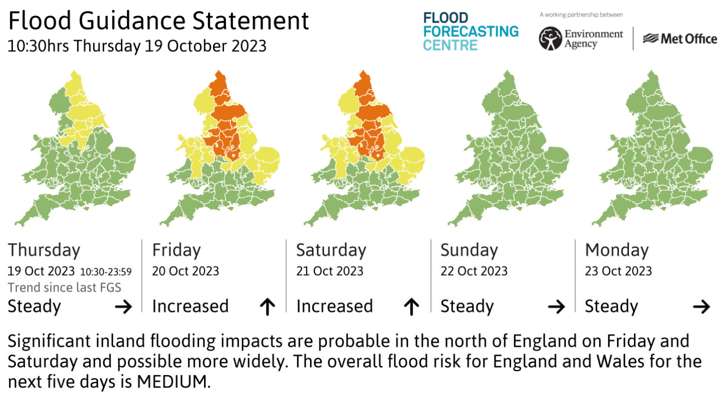


Figure 6 – Flood Guidance Statement for the 19th October 2023

Asset Incident

In the early hours of the 20th October 2023, after prolonged heavy rainfall, the river level on the River Bain began to rise. When a level of 42.3mAOD was reached, at 03:23 BST, the sluice gate on the low-level outlet should have closed automatically to ensure that the Hydroslide limited the pass-forward flow to 7.1m^3/s. The sluice gate did not close automatically. The sluice gate has pre-set alarms to provide notice that the reservoir is ready to fill, and separately a warning if the automatic operation of the gate has failed, which should prompt an operational response from flood duty staff.

The automatic alarm that informs duty staff that the reservoir is ready to fill (i.e. has reached the tigger point for sluice gate closure) was activated at 03:23 BST. The automatic gate-failure alarm was not activated. Duty staff were not aware that the sluice gate had failed to close until advised by the Area Catchment Engineer, initially by email at 7:17am, and then by telephone at 9:27am. Prompted by a phone call from the landowner at 12:41, the Catchment Engineer again contacted the Area Incident Room and the FODO instructed a field team to divert to Horncastle. The sluice gate was closed at around 14:15 on the 20th October 2023, some 10 hours 45 minutes after the closure level was reached.

With the sluice gate open, water passed through the reservoir via the low-level outlet, as well as through the main outlet. This prevented the reservoir from impounding as designed, and resulted in a lack of control of the pass-forward flow. It takes several hours for the flow to increase to 7.1m^3/s, reaching the rate at which the Hydroslide would begin to control the out-flow, allowing time for a manual closure of the sluice gate if required. The flow through the reservoir reached 7.1m^3/s at around 11:45 meaning, in combination with flow through the sluice gate, the total pass-forward flow below the dam was greater than the design amount for around 2.5 hours. The flow through the dam reached a maximum of 9.4m^3/s before the sluice gate was closed, resulting in around 7,800m^3 of additional flow passing downstream of the dam. Further details can be found in the *Horncastle Asset Operation Failure Impact Assessment* report.

It should be noted that no additional flow passed through the dam than would have occurred naturally if the scheme was not in place (i.e. at no stage did the reservoir release additional water into the downstream catchment). The timeline from the trigger level for sluice gate closure being met, and the manual closure of the sluice gate is shown below [All times in British Summer Time]:

<u>20th October 2023</u>

03:23 – Trigger level for sluice gate closure reached. Alarm E3463 issued: *[INFO - FSR Sluice gate Closure]*

06:40 – Catchment Engineer noticed sluice gate reading at 100% (fully open)

07:17 – Catchment Engineer emailed the FIDO to ask whether sluice gate was closed

09:27 – Catchment Engineer contacted the FIDO by telephone to ask whether they had checked the sluice gate

09:44 – Catchment Engineer checked the webcam and reported it open to the FIDO and requested Field Team be sent to close the sluice gate

12:41 – Landowner who was on site phoned Catchment Engineer to inform him that reservoir was draining through the low-level outlet (sluice gate open)

12:46 – Catchment Engineer alerted the FODO who diverted Field Team staff to go to Horncastle FSR

14:15 – The Sluice gate was closed on site by the Field Team

Further detail is provided in the sections below.

Response to the Incident

The timeline above indicates a period of 10 hrs 45 minutes between the threshold for the sluice gate closure being reached, and the time the sluice gate was closed. The gate was not closed manually at the earliest opportunity.

The two most relevant SWANTEL alarms for the asset are as follows:

1) ***B3478 Horncastle FSR Sluice gate Failed. If triggered and the reservoir is in use or will be imminently – send field team to investigate.***

This alarm description does not match those within the Functional Design Specification, so it is unclear exactly which alarm this message is associated with. This alarm is only triggered if there has been a power failure, or the actuator has failed in over-torque (generally meaning the gate is jammed or blocked). The 'failure to move' alarm is generated on the PLC, but this is not connected to telemetry. If the site is in 'manual', or tripped (ie circuit break activated), the actuator will not be called upon to operate the gate and therefore this alarm will not be raised. This alarm was NOT triggered on 20th October 2023, most likely because the actuator was not called upon to operate the gate.

2) ***E3463 INFO – FSR Sluice gate Closure @ 42.3 m aod.***

This alarm was activated and issued by SWANTEL to the FIDO at 03:23. The FIDO accepted the alarm on the SWANTEL system immediately. This alarm states that it is for "information" and alerts the FIDO to the fact that the reservoir is ready to fill because the threshold for sluice gate closure has been met. The FIDO prepared an email to the Supervising Engineer (SupE), Reservoirs Act Coordinator (RAC), Catchment Engineer (CE) and Deputy Catchment Engineer (DCE) informing them that the reservoir was filling. The wording of the alarm could be taken to indicate that that sluice gate has closed as it contains the phrase "FSR Sluice gate Closure"

The alarm B3478 only activates if there is a demand to close, and the gate can't close, and is a clear warning that something has gone wrong. When activated this includes an action to send a field team to investigate. It follows that had this alarm activated, the FIDO would have accepted and then actioned this alarm and field team response.

However, alarm E3463 is labelled 'for information' and the alarm message does not contain any actions. It appears that the FIDO did believe, from the alarm received, that the sluice gate had been closed because in his email to the SupE he uses the phrase "Sluice gate closed threshold at 03:23hrs". It is reasonable at a time when levels are rising, and many alarms are being received, for the FIDO to focus on the alarms that require action and pay less attention to alarms that are for information.

While alarm E3463 states that it is for information, the thresholds and warnings page available on the Area Incident Room, National Telemetry system monitor, for Horncastle FSR, includes the following information:

FSR ready to fill.

FSR Bypass sluice gate closes as the FSR starts to fill. If the sluice gate is faulty, arrange for M&E to attend site to close manually.

Check the Trend View sluice gate position = 0% (fully closed). If not, contact M&E to attend site immediately.

The need for action included in the detail of the warning is somewhat hidden by the "information" status of the alarm title. However, if the FIDO had read the detail of the alarm it is assumed that this would have triggered the actions required. The trend plot shown below, does include the action to check that the sluice gate is closed, with an indication on the trend that the sluice gate is not closed.

However, the ‘for information’ status of the alarm would naturally curtail the duty officer’s desire to interrogate the further detail when an incident is busy and multiple alarms are being received.

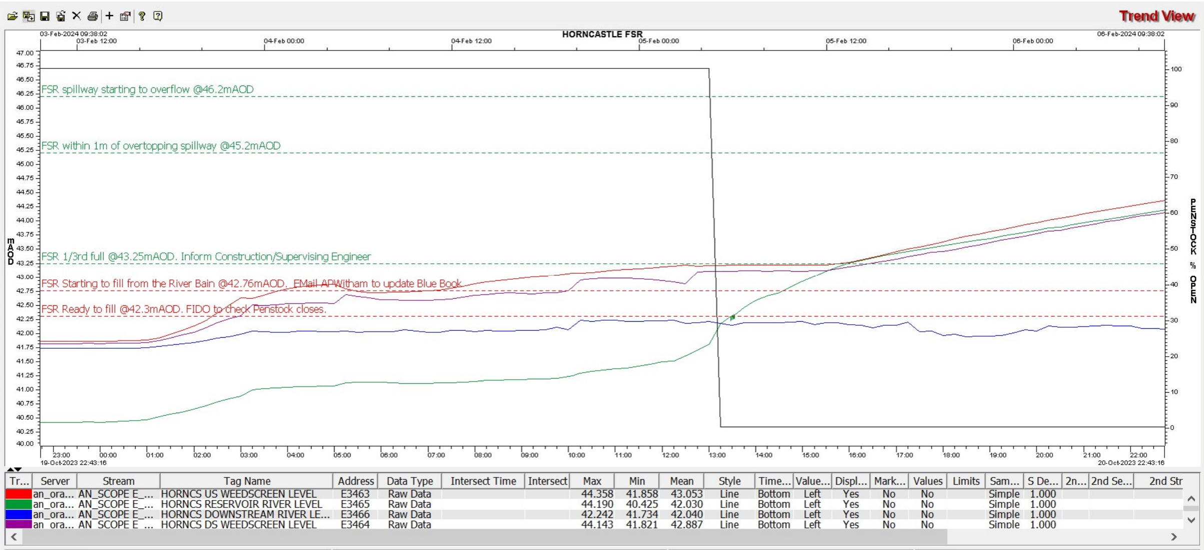


Figure 7 – Trend plot from SWANTEL showing the action levels for Horncastle FSR.
Note: This trend also shows the gate closure (black line) and filling of the reservoir (green line)

At 07:17, the Catchment Engineer, on reviewing the trend, noticed that the sluice gate was showing as open and he emailed the FIDO to check that the gate had closed. At 09:27 the Catchment Engineer called the FIDO to see if they had checked on the sluice gate. A different FIDO was now on duty who confirmed that they had not actioned anything on Horncastle during their shift. As the FIDO was about to go into a meeting, the Catchment Engineer checked the webcam which confirmed that the sluice gate had not been closed. He emailed the FIDO at 09:44 to request that the field team close the sluice gate. There is no evidence that these messgaes were actioned.

At 12:41, a landowner at the site phoned the Catchment Engineer to inform him that the sluice gate was open and water was flowing through the dam. The Catchment Engineer phoned the FODO who immediately diverted field team members on their way from Boston to Kirby-on-Bain, to go to Horncastle reservoir. It took some time to get to the reservoir site due to traffic and poor weather conditions, and the sluice gate was closed at 14:15 via the control panel in the kiosk.

Past Performance of the Asset

The reservoir was commissioned and became operational in December 2016, with the scheme formally opened in June 2017. In that time the sluice gate has been required to operate in flood conditions on thirty-three occasions, and it has been tested regularly, particularly during Reservoir Act Section 12 statutory Inspections. There is evidence of the asset not operating effectively in flood operations, and in test operations.

Flood Operations

Performance of the sluice gate system spanning all thirty-three flood events can be summarised into performance bands as follows [in chronological order]:

- **10th Mar 2018 to 27th Nov 2019 – 15 Operations – Performance Good**
  On all the occasions in this period, the sluice gate operated automatically on demand, with closure recorded within 15 minutes of the threshold being exceeded.

The performance on the final event of this period on the 27th November 2019, while successful in closing the sluice gate to make the reservoir operational, gives the first indication of a performance issue with the sluice gate. The FIDO Logbook states: *"Horncastle FSR Sluice gate failure, gate position 0% therefore in the closed position as required".* This is referring to the gate having closed but then a failure alarm has been activated. It is understood that the gate failed in the closed position due to over-torque and it had to be reset.

- **12th Dec 2019 to 23rd Dec 2020 – 9 Operations – Performance Poor**
  On all occasions during this period the sluice gate did not operate automatically when the activation threshold was met. Either the automation had failed, or the sluice gate was set to manual mode. During this period it appears there was established knowledge of the lack of automation with regular entries in the duty logs relating to the automation not working and the need for manual operation. The quickest manual closure during this period was 45 minutes, but the average was around 2 hours.

  There are three events during this period where the sluice gate was not closed manually while the river level was above the threshold for closure. There is some evidence that these could be conscious decisions based on river level forecasts. In two of these three events the river level did not reach the threshold for reservoir filling. In one of these events the FIDO logbook records "*Horncastle FSR level dropped. Now at 42.286m. Penstock still open. No action*". However, in one of these events, it appears that the FIDO believed the sluice gate to be closed, with the logbook stating "sluice gate shut".

  In the event of 23rd December 2020 the gate did not close automatically and the river level exceeded the level for reservoir filling, but with the sluice gate in the open position. The telemetry confirms that that the sluice gate was open, but the logbook suggests that the Field Team checked the sluice gate: "*Field Team checked closure but not reading correctly on SWANTEL*". The trend clearly shows that the sluice gate was open so there appears to be a lack of understanding from the Field Team as to the operating position of the gate.

  The weekly handover report the 23rd December 2020 notes that the "*Penstock automation is now repaired*"

- **14th Jan 2021 to 6th Feb 2021 – 6 Operations – Performance Medium**

  For these six operations, in a three-week period, the performance of the sluice gate was varied with four automatic closures and two manual closures.

On the 20th December 2021 it was discovered that the watchdog relay control on the PLC was set too frequently and wore out the O/I card. The control was changed and a new O/I card installed by Solar Software Solutions.

On the 17th May 2022 a simulation test on the operation of the sluice gate took place. This included the MEICA Field Team, Supra Area MEICA Team and Catchment Engineer. The simulation test was deemed a success. The test did identify confusing labels above the level instruments which were then changed.

- **17th Nov 2022 to 15th Apr 2023 – 2 Operations – Performance Very Poor**
  In both of these events, the automation of the gate failed and the incident response did not trigger a manual closing of the gate.

  In both of these events, the two events prior to Storm Babet, the automation of the gate failed and the incident response did not trigger a manual closing of the gate. The gate therefore remained open for both events. For the event in November, the river level exceeded the threshold for closure of the sluice gate for 19.5 hours. In one event, the logbook suggests that MEICA were requested to attend site, but there is no such record in the other event. It is not clear whether the decision not to close was intentional based on forecast river levels.

- **20th Dec 2023 (Storm Babet) – 1 Operation – Performance Poor**
  In Storm Babet the gate did not operate automatically, and no failure alarms were issued. The gate was closed manually after 10hrs 45 mins.

Test Operations

The sluice gate receives 6 monthly mechanical and electrical checks, along with test closures at least every 12 months as part of the statutory Section 12 Inspections required under the Reservoirs Act 1975. Some of the Section 12 test closures have experienced issues with the performance of the gate. The Section 12 Statement of February 2020 contains the following statement by the designated Supervising Engineer:

> *The actuated sluice gate was in good condition and operated over its range via the control kiosk during the examination. It was noisy and moving side to side but otherwise operated effectively with no issues.*

The Interim Section 12 Statement of August 2020 contains the following statement by the designated Supervising Engineer:

> *The sluice gate actuator has failed (appears to be a plc issue), but the sluice gate can still be operated by using the manual override and this was done during this examination. The sluice gate was in good condition and operated over its range. It was noisy and rocked side to side (this is part of the VBA defects list) but otherwise operated effectively, it needs to be greased.*

Both of these statements during separate test operations of the gate show that the gate wasn't moving smoothly, and in the case of August 2020, the sluice gate failed to operate on demand. The VBA defects list does not, in fact, contain a defect regarding the sluice gate.

It should be noted that the issues experienced with the sluice gate is not a reservoir safety issue as the failure cannot result in an uncontrolled release of stored water. Failure for the gate to close makes the dam safer as it is not able to store water. Therefore, while noted by the Supervising Engineer, they would not necessarily require action to be taken from a reservoir safety perspective.

Performance Analysis

The previous operations of the sluice gate indicate significant issues with the automation of the gate, with 40% of occasions where the sluice gate failed to operate automatically at the required threshold during flood events (13 of 33 events). In some of these cases the lack of automation was not expected, and the manual contingency was implemented. However, in other cases it seems that the gate had been set to manual due to a lack of confidence in the automation.

In most cases there appears to be good awareness of the need to operate the gate manually, but there are five events prior to Storm Babet where the gate was not closed manually after the automation failure. In three of these events the river level did not exceed the threshold for reservoir filling and there is some evidence that decisions have been made to not close the gate based on river level forecasts. However, there are two events, on the 23rd December 2020 and the 17th November 2022, where the river level exceeded the threshold for reservoir filling and the sluice gate was not closed. Of the five occasions when the sluice gate was not closed, there are two occasions when the gate is believed to have been closed (according to duty logs) when it is not.

Whether set to "auto", or switched to manual, there are clearly periods of time where the gate is operating in manual mode. There is no way of knowing for certain which mode the asset was operating in as, unusually for EA assets, there is no clear indication or telemetry of the asset status.

Looking specifically at the most recent flood operations of the sluice gate, which give the best indication of the likely performance of the asset in Storm Babet, the following has been identified:

- **15th April 2023** – Trigger level met. Trigger level exceeded for 5 hours. Gate failed to close automatically. No manual intervention deployed as FIDO noted the level returned to normal.
- **17th November 2022** – Trigger level met. Trigger level exceeded for 19 hours. Gate failed to close. FIDO notified FODO who contacted MEICA Team. MEICA team attended and notified FODO that sluice gate was operating normally (but was open) and that operation of sluice gate was different to that in the FIDO procedures. It is not yet clear what this meant but there appeared, on this occasion, to be a different understanding of how the sluice gate operates between the FIDO manuals and the MEICA Field Teams

On both occasions prior to the Storm Babet, the sluice gate failed to close on demand, and it was left open for the duration of the storm.

Past Investigations into Performance

Some investigations into the performance of the asset have taken place, with the investigations into the watchdog relay control in December 2021 resulting in the control being changed and a new O/I card installed. This led to a significant improvement in the performance of the asset – moving from a performance of 'poor' to a performance of 'medium'. After a five-month period of relatively successful operations, a simulation test of the sluice gate took place in May 2022. The test was successful. However, the general performance of the asset dropped after this test from a performance of 'medium' before the test, to a performance of 'very poor' after the test. The following three flood operations after the simulation test, including for Storm Babet, all resulted in a failure of the automation, with the two events immediately after the simulation test also not triggering a manual closure of the sluice gate. Detail for some example operations can be found in Appendix B.

Technical Review of the Sluice gate Design and Function

On Thursday 2nd November 2023 members of the Anglian Supra-area MEICA team and the Field MEICA team attended site to investigate the issues that had occurred during storm Babet, and to conduct a test to identify whether the equipment was operating correctly. A subsequent site visit by AME national MEICA engineers took place on Tuesday 7th November 2023.

During the 2nd November 2023 test, the control panel was found to be in manual mode, but that was to be expected after the most recent manual operation. However, on switching the panel into auto mode it was discovered that there was an additional electronic switch within the HMI (Human Machine Interface) screen. This is where the panel selector is switched to "auto", but manual mode is selected on the HMI screen (termed "manual (HMI)") mode. So while appearing as being in "auto" on the panel selector, the sluice gate is actually in manual. This arrangement is unusual for Environment Agency assets, and somewhat confusing, and seems likely to result in issues around the awareness of the operating mode of the sluice gate. When both the manual and electronic switch were switched correctly into "auto" mode the system operated correctly. It was also identified that operation could be locked out, such as when a short-duration power outage can trip the system, without an alarm being raised. Once the system has tripped, an operator is required to attend site to reset the panel but without any warning having been given to alert duty staff that the panel needs to be reset.

The on-site technical review concluded that the panel was in “manual (HMI)” mode for Storm Babet, and that mode prevented automatic operation of the sluice gate or the issuing of any failure alarms. It is also likely that the asset was in “manual (HMI)” mode in the events preceding Storm Babet, where the sluice gate also failed to close, and probably other events where automatic operation did not occur. It is clear that the ‘manual (HMI)’ mode was not understood, and this seems to be the likely cause of most, if not all, of the failures to close automatically when the panel selector is set to “auto”.

Staff were not aware that when the main panel selector switch was set to “auto”, the PLC could still be in manual mode, and so automatic operation wasn’t possible, and no failure alarms would be activated. The control system alarms only react to a failure of a demanded action.

If the previous failures of automation had been fully investigated, then the PLC being in manual mode while the main switch was set to “auto” could have been identified.

The site visit and technical review by AME national MEICA engineers also identified a number of issues with the design of the system. These issues are summarised below:

- Debris-screen blinding was not fully considered during the design, and so the sluice gate modulates frequently in response to river levels changing rapidly as the screen blinds and then is cleared.
- Confusing wording on the HMI Screen, the inclusion of a manual mode when “auto” is selected (as described above), issues with trips and alarms, and no clear indication of panel status.
- Lack of input from Supra-Area MEICA team in the scheme design.
- No site-acceptance test.
- Unclear handover on completion.
- No Automation Risk Assessment carried out prior to construction (a mandatory requirement) which identifies the underlying requirements that need to be considered during design, for example in respect to redundancy of instruments, alarms etc.
- The “Functional Design Specification” not appearing to match the as-built version.
- No hardcopy of the software logic or a backup copy of the software (requirement of our MEICA specifications).
- No Failure Mode Effects Analysis (FMEA) in accordance with MEICA specifications which may have addressed many of the issues.
- No evidence of a Declaration of Conformity or any CE marking in respect of the Supply of Machinery (Safety) Regulations.
- The system relies on external checks by duty staff to ensure that the system is operating correctly which is undesirable.

It is likely that a robust design in line with BS EN 13849: *Safety of Machinery* and BS EN 61508: *Functional safety of electrical/electronic programmable electronic safety-related systems,* and compliance with the MEICA Specifications, would have included better indication and alarms, including indication that the panel was ready to operate in auto mode. Common practice is also to provide a telemetry signal to indicate whether the site is in auto mode so that duty staff can be aware that the site is not going to operate without intervention.

Some issues with the control system have since been addressed or mitigated by making changes to operating procedures or site settings. Any changes should be controlled with management of change measures and, ideally, tested using tools such as Bowtie, Hazop or FMEA, and well documented. Changes and site activities should, at least, be recorded in a site log book.

There is a need to fully understand and review the site operation against the functional requirements and appropriate standards, to review the alarms and alarm handling process, ensure backups are held and ensure there is a mechanism for the control of change and documenting events on site.

Flood Impacts of the Sluice gate Failure

The *Horncastle Asset Operation Failure Impact Assessment* report has undertaken hydrological and hydraulic modelling of the catchment during Storm Babet. This modelling has looked at the response and impact in the catchment with the sluice gate operating normally, and with the delay to the sluice gate closure allowing additional flow downstream. *Figure 8* below shows the outputs from the model runs for Victoria Mill (Horncastle). The open sluice gate appears to have allowed river levels to rise sooner in Horncastle but did not cause a greater peak flow in the town, and therefore did not contribute to the flooding of properties. The flooding in Horncastle is due to the very significant flood event occurring on the uncontrolled tributaries downstream of the dam, which caused a flood peak some 4 hours after the sluice gate at the dam was closed.

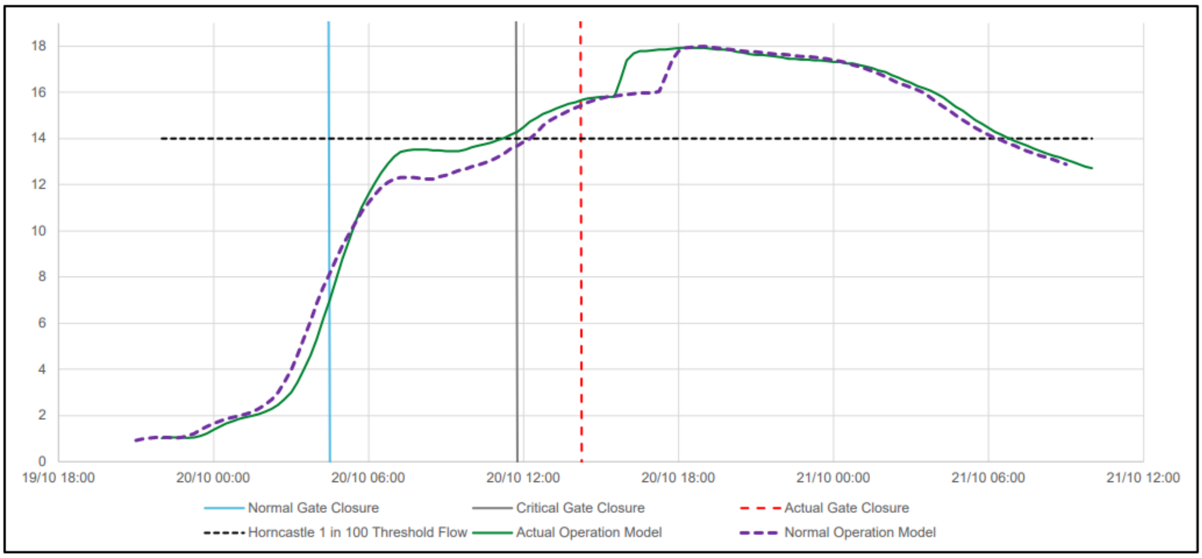


Figure 8 – Modelled River Level trends in Horncastle with and without sluice gate closure.

The full detail of the impacts downstream from the sluice gate failure can be found in the *Horncastle Asset Operation Failure Impact Assessment* report.

Findings and Recommendations

As discussed at the outset of this report, an asset failure is rarely caused by a single vulnerability presenting itself. In most cases the failure is a result of weaknesses in the design, the operation of control systems, the application of maintenance regimes, issues of governance, organisational culture, knowledge management and training. If the vulnerabilities within the overall system are too great, symbolised by the holes in the layers of Swiss Cheese in the "Swiss Cheese Model", then there is a greater likelihood that the holes within the layers can line up and a failure will occur. To reduce the likelihood of asset failure, the potential vulnerabilities can be reduced (reduce the size and frequency of the holes in the layers of Swiss Cheese), and/or additional layers of assurance can be added (increase the number of layers of Swiss Cheese in the system).

The asset failure at Horncastle is no exception and is a good example of several vulnerabilities in different parts of the system, that have lined up to cause the failure of the asset. Many of the themes that lead to failure identified by the 'In Plain Sight' Panel can be identified with the sluice gate at the Horncastle FSR. Vulnerabilities have been created because:

1) The design of the scheme is non-standard with the passive structure at a higher level than the active structure.
2) The operational sluice gate design is not in accordance with EA or industry standards.
3) The sluice gate operational modes are non-standard and confusing.
4) The alarm handling is sub-optimal and relies on manual intervention.
5) The issues with past poor performance haven't been fully investigated and addressed.
6) There is a lack of clarity on when the sluice gate is in manual mode.
7) There was a reliance on ad-hoc operational procedures.

These eight vulnerabilities have been considered separately, with recommendations for improvement against each.

1) Non-Standard Scheme Design

The scheme was built with a low-level outlet due to the need to maintain river flow over a weir downstream. The low-level outlet is open in normal conditions and is required to close for the passive Hydroslide to control pass-forward flow. A failure of the sluice gate to close results in the uncontrolled pass-forward flow through the dam. This provides an inherent major vulnerability with the structure. While this arrangement cannot be modified without a significant re-build, the set-up can be modified to reduce this vulnerability significantly. If the sluice gate was set to a significantly lower pass-forward flow, say 10% open, as its normal operating position, then a failure to close the sluice gate would only result in a small increase in flows downstream.

This operational setup could be further enhanced, and made fully passive, if the Hydroslide could be lowered to reflect the flow passing through the 'slightly open' sluice gate. If this could be achieved, then the sluice gate could be left in the 'slightly open' position while limiting the downstream flow to 7.1m3/s. This would mean that no operation of the sluice gate would be required, other than for testing or if it was necessary to speed up the final drainage of the lower part of the basin.

RECOMMENDATION 1: Investigate the potential to modify the sluice gate's 'normal' position to limit downstream flow if the sluice gate fails to close. Furthermore, consider whether the Hydroslide can be modified to pass forward a lower flow so that the sluice gate can remain 'slightly open' at all times, and therefore make the structure completely passive.

2) Design not in Accordance with EA or Industry standards

It does not appear that the design is in line with BS EN 13849: *Safety of Machinery* and BS EN 61508: *Functional safety of electrical/electronic programmable electronic safety-related systems*, and it does not comply with EA MEICA Specifications. Common practice is also to provide a telemetry signal to indicate whether the site is in auto mode so that duty staff can be aware that the site is not going to operate without intervention. There has been a lack of input from Supra-Area MEICA team in the scheme design and it appears that no site-acceptance test took place. No Failure Mode Effects Analysis (FMEA) has been undertaken in accordance with MEICA specifications and there is no evidence of a Declaration of Conformity or any CE marking in respect of the Supply of Machinery (Safety) Regulations.

RECOMMENDATION 2: Review the design of the system, with support from Supra-Area MEICA, against industry standards and EA specifications, with a back-to-basics approach to look at the design from first principles. Undertake an FMEA analysis and secure a CE marking for the machinery. Make any changes required as a result of the design review.

3) Sluice gate Operation is Non-Standard and Confusing

The Sluice gate can be in manual mode while it appears to be in “auto” mode. In addition, the system can be locked out without alarming, leaving the asset inoperable without a reset. The wording on the HMI Screen is confusing with no clear indication of the panel status. There was no Automation Risk Assessment carried out prior to construction and the “Functional Design Specification” does not appear to match the as-built version. Changes do not appear to be well controlled with management of change measures, or tested with industry tools. Changes on site are not recorded and no hardcopy of the software logic or a backup copy of the software is available.

RECOMMENDATION 3: Undertake a detailed review of the site operation against the functional requirements and appropriate standards, ensure backups are held and ensure that there is a mechanism for the control of change and for documenting events on site.

4) The Alarm Handling is Sub-Optimal and Relies on Manual Intervention

There are a number of issues with the alarm handling that need to be reviewed and addressed. Notwithstanding the fact that the sluice gate failure alarm won’t be issued if the sluice gate is in manual mode, and it can easily be mistakenly left in manual mode as described above. There are other alarms that are sub-optimal and rely too much on duty staff intervention. The main alarm that is triggered when the river reaches 42.3mAoD is “*E3463 INFO – FSR Sluice gate Closure @ 42.3 mAOD”* This alarm is signalled as being for information but contains the action to check that the sluice gate has closed. The “For Info” title is confusing, when action is required, but the alarm requires duty staff to perform a manual check that the sluice gate is operating correctly on every operation. This is sub-optimal when duty staff are busy and receiving multiple alarms during the rising limb of a flood event. E3463 could be designed as a truly “For Info” alarm to give duty officers awareness that the reservoir is coming into operation, but an extra alarm should be set up to provide warning that something is not working as expected. An alarm that is issued if the river level reaches 42.5mAoD (halfway between the sluice gate closure level and reservoir filling level) in combination with the sluice gate being open, would alert duty officers to the fact the gate was open after a point it should have closed. This could be a FOR ACTION alarm to require the manual operation of the sluice gate. In that way, FOR ACTION alarms are only issued when something has gone wrong, not every time the trigger level is met.

RECOMMENDATION 4: Review the alarm handling to consider the wording and importance of existing alarms, and consider modifying or creating a new alarm to only require action when something has failed, rather than requiring an action for all operations.

5) Poor performance has not been Fully Investigated and Addressed

There has been a history of poor performance of the sluice gate, which is evidenced by the low number of automatic operations – 20 out of 33 flood closures required. There is also strong evidence of the sluice gate not working effectively in test closures, with failures occurring and reports of the gate movement being noisy and rocking from side to side. Some changes have been implemented such as changing the watchdog relay control and replacing the O/I card in December 2021. There was also a simulation test that involved MEICA in May 2022. While this test was a success, there were some changes made to confusing levels above the level instruments. However, the success of the test does not appear representative of the general performance of the asset, and therefore the test did not result in any investigations into the past poor performance, or make any significant improvement recommendations. In fact, it is likely that, due to the ability for sluice gate to still be in manual while in "auto" mode, it is probable that the sluice gate was unintentionally left in manual after this test, leading to the subsequent automation failures. All of the following flood closures resulted in the sluice gate not operating automatically and there is no evidence of failure alarms being issued. In addition, the technical review after Storm Babet found the panel was in "manual (HMI)" mode for the event. The incident duty logs suggest that manual operation was not an expectation during this time.

RECOMMENDATION 5: There are no recommendations here in relation to Horncastle that will not be addressed by other recommendations. However, more generally, where an asset has suffered from poor performance, it is important that issues are fully investigated. If a simulation test is successful then further investigation is required to understand the causes of the asset issues as it should be assumed that the test is not accurately representing the actual operating scenario.

6) Lack of Clarity on when the Sluice gate is in Manual Mode

The system setup is confusing and unconventional, with an additional manual mode within the "auto" mode. It is clear that this is sub-optimal and was not well understood, if at all, by duty staff and MEICA staff. The onsite investigation and test on the 2nd November is described as "discovering" this additional manual mode. The reasons for this 'hidden' manual mode, and recommendations to address it at Horncastle, and on future schemes, are already covered earlier in this section regarding the issues with the design of the system. The lack of knowledge of this single issue is considered to be the biggest individual vulnerability of the asset and is therefore included here specifically in its own section. The records of past events and test closures show an expectation of automatic operation when the asset was in "auto" mode, and confusion when the asset hasn't operated effectively in "auto". This lack of confidence has led to the automation being switched off which removes a layer of defence to asset failure because the sluice gate then requires manual intervention.

RECOMMENDATION 6: Recommendations regarding the design of the system have already covered above. However, it is recommended that the "auto" status is clearly and accurately displayed on the telemetry and clearly indicated on the control panel by means of "auto available" indication.

7) Reliance on Ad-Hoc Operational Procedures

The initial delay to enact the manual response to close the sluice gate during Storm Babet can be explained by the confusing asset status, and the sub-optimal alarm handling process. It could be reasonably expected that the duty officer was not initially aware that the sluice gate had not closed automatically – in fact the wording, and the lack of a failure alarm, could be taken to suggest the gate was closed. Between 03:23 and 07:17 the duty staff could reasonably assume that there were no issues with the sluice gate. From 07:17, however, awareness of the sluice gate failure could be reasonably expected as there were indications made to the FIDO that the sluice gate had not closed – firstly with an email from the Catchment Engineer at 07:17am, then at 09:44am when the Catchment Engineer again contacted the FIDO, then at 12:41 when the Landowner contacted the Catchment Engineer, who then instigated the closure himself, via the FODO. There is no clear explanation as to why the two initial alerts to the FIDO at 07:17 and 09:44 did not trigger a manual intervention. In mitigation for this delay, the other system failures that had occurred had left the manual intervention as the last line of defence, and at this point the team were operating outside of normal procedures.

The Catchment Engineer noticing and alerting the FIDO was on an ad-hoc basis, and based on good diligence, rather than any operational procedure at that stage – the operational procedures had already failed. So the FIDO was receiving failure 'alerts' via a non-standard method at what was clearly a very busy time. The rainfall was very intense on the morning of the 20th October and in no way should duty officers be relied upon to act on ad-hoc processes because defined processes have failed. It is accepted that there were opportunities for the FIDO to act earlier, but in the circumstances, the FIDO had been let down by all of the prescribed systems, and therefore failure to act immediately can be understood. The FIDO should not be in a position where they are responding to non-standard alerts due to system failings. While it is possible that they may be able to act to 'save the day', as a business we cannot, and should not, expect this approach to be successful, and so no blame is attached to the FIDO for their response. The Catchment Engineer should be commended for their identification of the issues and ultimately their role in ensuring the sluice gate was closed.

RECOMMENDATION 8: Ad-hoc operational procedures should never be relied upon in an incident and it is important that assets perform as expected, and the pre-prescribed procedures deal effectively with failures that do occur. However, ad-hoc processes do provide a last line of defence in the Swiss-Cheese model and therefore some improvements would be beneficial to ensure that where issues are flagged they are understood and prioritised appropriately. Duty Staff training and awareness of the key asset operational requirements during an incident is important to ensure that the correct priorities can be placed on operational response activities. It is recommended that duty staff training on operational requirements is increased, including site visits to key assets within the Area for duty staff, which are vital for asset operational awareness.

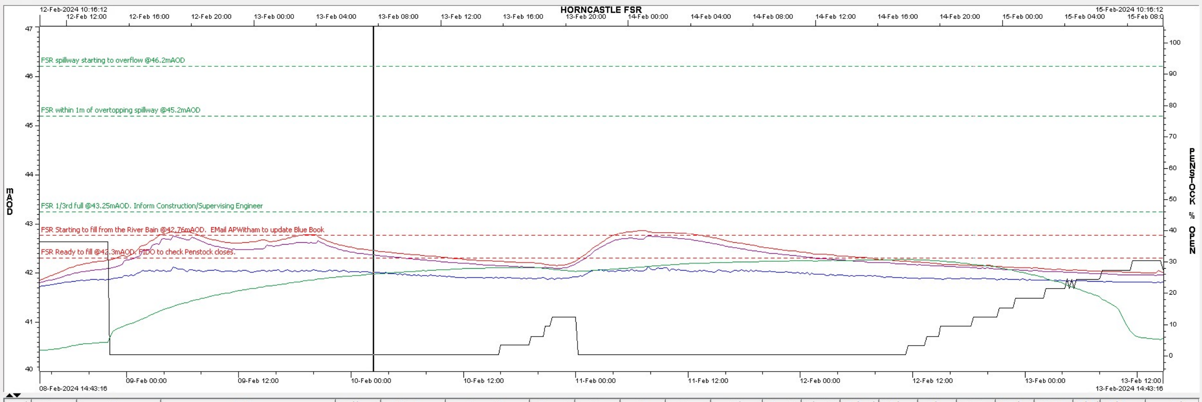
Recent Improvements to FSR Systems and Operations

There have been several improvements implemented to the systems and operation of the Horncastle FSR, as this review has been undertaken. While there is a more to do, the Area team are progressing actions from this report, and from their own learning from the incident.

Several vulnerabilities have been identified in this report which need to be addressed, but the main vulnerability in the *operation* of the sluice gate was the electronic 'manual (HMI)' mode within the system. This left the sluice gate in manual mode when staff believed it to be in 'auto' mode, based on the physical switch position. This has been identified as a key weakness and this has been addressed quickly. This, along with other improvements already completed are listed below:

1. The electronic 'manual' switch has now been removed and the gate can only be set to auto or manual using the panel selector switch. This switch is set to auto and can only be changed to manual using a key, available only to trained and competent MEICA field team.
2. The alarm messages have been made clearer that they are for 'action' rather than for 'information'. The action required is now part of the alarm text. Previously, the FIDO would need to look up in the action in separate procedures.
3. The sluice gate is now held in a partially closed position to limit the impact should there be any future issues with the automation or manual response.
4. The procedures used by duty teams on the operation of the sluice gate have been updated.
5. The latching of alarms has now been removed. Previously, for example, a short power failure would raise a power failure alarm which would require a site visit to reset the control system. Now the system will reset automatically when the power returns.
6. The time-period between gate movements has been extended from 5 mins to 15 minutes resulting in considerably less modulation of the sluice gate.

Since these improvements have been implemented, the performance of the penstock has been much improved. For the period 18th November 2023 to 15th February 2024, the penstock has closed automatically on all eight occasions that it was required to do so. The Swantel trend view for the event on 8th February 2024 is shown in Figure 9 below.



Trend	Server	Stream	Tag Name	Address	Data Type	Intersect Time	Intersect	Max	Min	Mean	Style	Time Axis	Value Axis	Displayed	Markers	Values	Limits	Sampling	S Deviation	2nd Col	2nd Server	2nd Strea
	an_oracle	AN_SCOPE E_VALUE	HORNCS US WEEDSCREEN LEVEL	E3463	Raw Data	10-Feb-2024 02:19:12	42.456	42.872	41.861	42.391	Line	Bottom	Left	Yes	No	No		Simple	1.000			
	an_oracle	AN_SCOPE E_VALUE	HORNCS RESERVOIR RIVER LEVEL	E3465	Raw Data	10-Feb-2024 02:19:12	41.978	42.281	40.441	41.820	Line	Bottom	Left	Yes	No	No		Simple	1.000			
	an_oracle	AN_SCOPE E_VALUE	HORNCS DOWNSTREAM RIVER LEVEL	E3466	Raw Data	10-Feb-2024 02:19:12	42.010	42.137	41.729	41.954	Line	Bottom	Left	Yes	No	No		Simple	1.000			
	an_oracle	AN_SCOPE E_VALUE	HORNCS DS WEEDSCREEN LEVEL	E3464	Raw Data	10-Feb-2024 02:19:12	42.368	42.753	41.807	42.300	Line	Bottom	Left	Yes	No	No		Simple	1.000			
	an_oracle	AN_SCOPE E_VALUE	HORNCS PENSTOCK POSITION	E3467	Raw Data	10-Feb-2024 02:19:12	0.466	36.378	0.442	7.281	Line	Bottom	Right	Yes	No	No		Simple	1.000			

Figure 9 – Trend view of a recent flood event at Horncastle FSR

The trend view in Figure 9 shows the sluice gate (black line) held at around 35% open, and then closing automatically when the closure threshold of the river (red line) is met. The reservoir level (green line) then increases until the river level falls below the threshold and the gate starts to open and the reservoir level starts to fall. The gate closes again as the river level increases, increasing the levels in the reservoir, until the river level drops and the sluice gate returns to its partly open position.

Further improvements will be delivered as the Area team review the findings from this report.

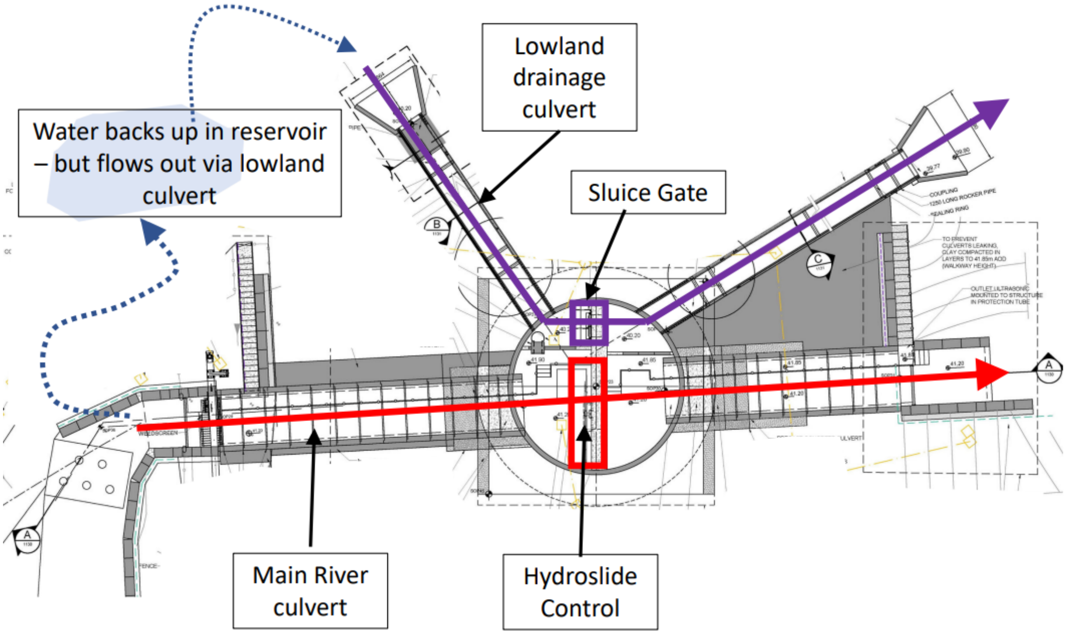
Author:
National Engineering Manager
Asset Management and Engineering

Approved:
Chief Engineer
Director Asset Management and Engineering

Date: February 2024

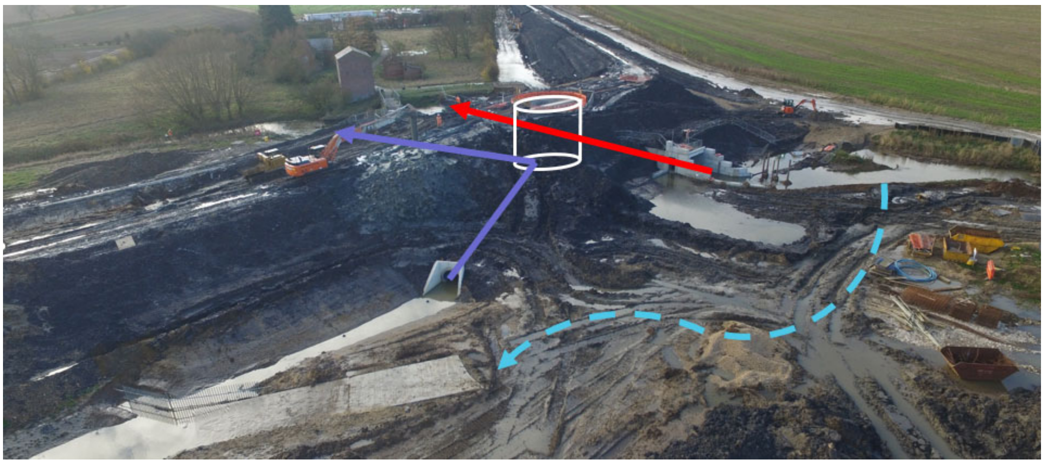
Appendix A – Schematic of the Flow Control

Schematic showing the Flow Control on the Horncastle FSA. The dam runs 'north to south' over the structures shown below. Flow moves from upstream on the left to downstream on the right.



Key Features:

1) The normal river flow passing under the dam is shown by the red line.
2) In the central chamber the Hydroslide (red rectangle) remains open for normal flow.
3) The normal river is perched higher than the storage basin (see photo below).
4) The low-level outlet sits at the base of the reservoir and is shown by the purple line.
5) The low-level outlet passes through the central chamber where the low-level sluice gate (purple square) is housed.
6) When levels in the river increase, the low-level sluice gate should close automatically.
7) As river levels continue to rise, floodwater (blue dotted line) spills into the basin and is retained.
8) If the sluice gate is open, then floodwater spilling into the basin will flow out of the reservoir through the low-level culvert.
9) When flow reaches 7.1m^3/s, the Hydroslide comes into operation to limit flows, and the reservoir impounds all flow above 7.1m^3/s.
10) During Storm Babet, the low-level sluice gate was open, and flood flow passed through the low-level culvert instead of being retained.

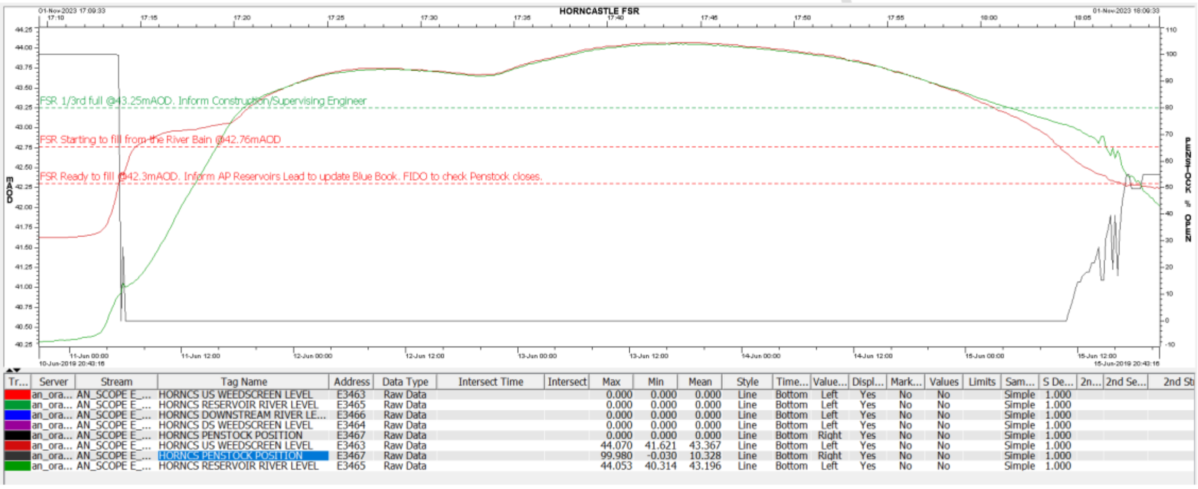


Appendix B – Performance Examples

The information below provides three example operations of the sluice gate which includes a successful closure, a closure with some issues, and a failed closure.

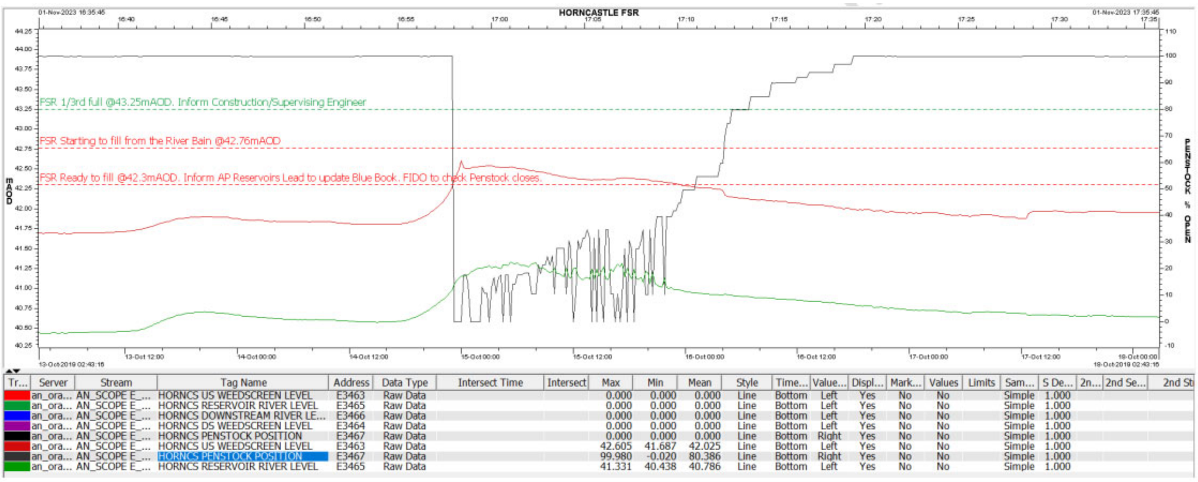
1) 11th June 2019 – Successful Closure

The River Level (red line) at the Weedscreen passes the threshold for gate closure. The gate opening trend (black line) quickly moves from 100% (fully open) to 0% (fully closed). The reservoir (green line) starts to fill immediately. Reservoir levels increase rapidly to meet and drown-out the perched river level. As river levels return to the threshold, the gate (black line) starts to open. This was a significant storage event. Note the gate closure trend intersecting the river level trend at the point the river level reaches the gate closure trigger.



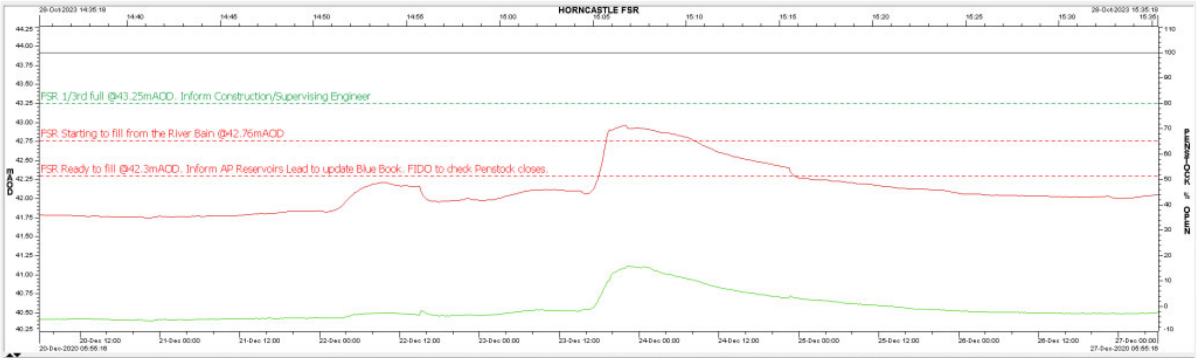
2) 15th October 2019 – Successful Closure but significant modulation

The River Level (red line) at the Weed-screen passes the threshold for gate closure. The gate opening trend (black line) quickly moves from 100% (fully open) to 0% (fully closed). The reservoir (green line) starts to fill. Not long after closure, with river levels still above the threshold, the sluice gate starts to modulate with frequent openings up to 20% and then 30% open. This results in the reservoir not filling effectively as the retained water is constantly released with the gate openings. The modulation of the gate was a regular feature up to November 2019 when the gate automation stopped working, or was turned off, and the subsequent closures occurred manually.



3) 23rd December 2020 – No Closure

The River Level (red line) at the Weedscreen passes the threshold for gate closure. The gate opening trend (black line) stays horizontal at 100% (fully open) – i.e. the sluice gate does not close. The river level passes through the threshold for reservoir filling for a significant period of time, but the reservoir level (green line) shows minimal response to the 'filling' because the sluice gate is in the open position. The river is above the sluice gate closure level for 29.5 hours while the reservoir was above the 'filling' level for 15 hours.



Tr...	Server	Stream	Tag Name	Address	Data Type	Intersect Time	Intersect	Max	Min	Mean	Style	Time...	Value...	Displ...	Mark...	Values	Limits	Sam...	S De...	2n...	2nd Se...	2nd Strea
	an_ora...	AN_SCOPE E_...	HORNCS US WEEDSCREEN LEVEL	E3463	Raw Data			0.000	0.000	0.000	Line	Bottom	Left	Yes	No	No		Simple	1.000			
	an_ora...	AN_SCOPE E_...	HORNCS RESERVOIR RIVER LEVEL	E3465	Raw Data			0.000	0.000	0.000	Line	Bottom	Left	Yes	No	No		Simple	1.000			
	an_ora...	AN_SCOPE E_...	HORNCS DOWNSTREAM RIVER LE...	E3466	Raw Data			42.242	41.830	41.956	Line	Bottom	Left	No	No	No		Simple	1.000			
	an_ora...	AN_SCOPE E_...	HORNCS DS WEEDSCREEN LEVEL	E3464	Raw Data			43.733	42.020	42.339	Line	Bottom	Left	No	No	No		Simple	1.000			
	an_ora...	AN_SCOPE E_...	HORNCS PENSTOCK POSITION	E3467	Raw Data			0.000	0.000	0.000	Line	Bottom	Right	Yes	No	No		Simple	1.000			
	an_ora...	AN_SCOPE E_...	HORNCS US WEEDSCREEN LEVEL	E3463	Raw Data			42.965	41.742	42.111	Line	Bottom	Left	Yes	No	No		Simple	1.000			
	an_ora...	AN_SCOPE E_...	HORNCS PENSTOCK POSITION	E3467	Raw Data			100.100	100.060	100.082	Line	Bottom	Right	Yes	No	No		Simple	1.000			
	an_ora...	AN_SCOPE E_...	HORNCS RESERVOIR RIVER LEVEL	E3465	Raw Data			41.117	40.391	40.561	Line	Bottom	Left	Yes	No	No		Simple	1.000			