

Waterloo Road Pump Station

Control Philosophy

Document number	Title	Revision	Date	Status
WRPS-CTL-001	Control Philosophy	A	11 August 2026	Issued for demonstration

Rev	Date	Description	Prepared	Checked	Approved
A	11 Aug 2026	First issue - demonstration environment	C. Huang	-	-

1. Purpose

This document states how Waterloo Road Pump Station is to be controlled and why. It defines the control objectives, the priority order between them, the operating modes, the automation boundary and the alarm philosophy. It is the parent document for the Functional Design Specification (WRPS-CTL-002), which defines how these principles are implemented.

Where the Functional Design Specification and this document disagree, this document governs and the specification is to be corrected. A principle in this document may only be changed by revision, not by an implementation decision taken downstream.

2. Reference documents

Document number	Title
WRPS-PRO-001	Process Basis of Design and Process Description
WRPS-DRG-001	Piping and Instrumentation Diagram
WRPS-INS-001	Instrument Index and Equipment List
WRPS-CTL-002	Functional Design Specification
WRPS-CTL-003	OpenPLC Implementation Brief (demonstration environment)

3. Control objectives and their priority

The station has four control objectives. They are not of equal standing, and the order below is a requirement of the design, not a preference. Every control decision in the Functional Design Specification must be traceable to this ordering.

Priority	Objective	Character	Consequence of failure
1	Protect personnel and plant	Absolute. Never traded against anything.	Injury, or destruction of a pump or the switchboard.
2	Prevent an uncontrolled spill	Hard constraint. May not be traded for cost or asset life.	Environmental incident, licence breach, reportable event. Irreversible.
3	Minimise energy cost	Soft. May be pursued only within the margin defined in Section 6.	A larger electricity bill. Fully recoverable.
4	Maximise asset life	Soft. Influences which unit runs, never whether a unit runs.	Earlier overhaul. Recoverable, and statistical rather than immediate.

The asymmetry between objective 2 and objectives 3 and 4 is the single most important principle in this document. A spill cannot be undone. An energy cost or a shortened bearing life can be absorbed. Any logic that allows a cost or asset consideration to defer or prevent a start required to protect wet well headroom is non-compliant with this philosophy, however small the calculated risk.

4. Control hierarchy

Four layers, each able to function without the layer above it. This is a requirement, not a description: the station must remain safe as each upper layer is removed.

Layer	Implemented in	Function	Behaviour if the layer above fails
4 - Decision support	SCADA and higher level applications	Advises the operator on start timing and unit selection. Makes no automatic change to plant.	-
3 - Supervisory	CI Server SCADA	Operator monitoring, alarm presentation, setpoint entry, manual mode commands.	Layer 3 continues unaffected. No plant function depends on layer 4.
2 - Automatic control	PLC-001	Level based start and stop, duty selection, speed control, protective trips, alarms.	Station continues to operate automatically with the last accepted setpoints. Loss of SCADA does not stop the station.
1 - Hardwired protection	LSHH-102, LSLL-103, drive safety circuit	Dry run protection and high high level response, independent of the PLC.	Protection remains effective with the PLC stopped, in fault, or being reprogrammed.

Layer 1 does not read LIT-101 and does not execute PLC code. This independence is the reason two discrete level switches are installed alongside a perfectly adequate analogue transmitter, and it must not be removed to simplify the design.

Layer 4 is advisory in this revision. It may present a recommendation to the operator and it may explain its reasoning, but it holds no write access to any command register and cannot start, stop or defer a pump. The operator remains the sole means by which a layer 4 recommendation reaches the plant.

5. Operating modes

The station has three modes. Mode is selected from SCADA and is reported back so that the displayed mode is always the mode the PLC is acting on, never the mode last requested.

Mode	Selected from	Pump starting	Speed	Intended use
Auto	SCADA	PLC decides how many units and which units, from level.	PLC level controller.	Normal operation. The default and the mode the station reverts to.
SCADA manual	SCADA	Operator nominates the individual unit to run or stop.	Operator enters a speed reference, clamped to 38 - 50 Hz.	Testing, commissioning, troubleshooting, and deliberate operator intervention.
Off	SCADA	No automatic starting. All units stopped.	-	Station isolated for maintenance or investigation.

5.1 What manual mode does not suspend

Manual mode transfers the start, stop and speed decision to the operator. It transfers nothing else. The following remain fully active in manual mode and cannot be disabled from SCADA:

- Hardwired dry run protection on LSLL-103. A manual start command against a low low level is refused, not queued.
- Hardwired high high level response on LSHH-102. If LSHH asserts while in manual, the station reverts to automatic control and starts all available units. See Section 5.2.
- All motor protection: thermal, vibration high high, and the no-flow trip after start.
- Minimum run and minimum off timers. These protect the motor and are not an operating convenience.
- The speed clamp at 38 Hz. Below the static lift cutoff a pump absorbs power and delivers nothing, so an operator entry below the clamp is raised to the clamp and annunciated.
- All alarms. Manual mode is not a quiet mode.

An operator in manual mode may make the station perform poorly. They may not make it unsafe, and they may not make it spill without the station intervening. That is the boundary this section draws.

5.2 Reversion to automatic

The station reverts from manual to automatic without operator action in one circumstance only: assertion of LSHH-102. The reversion is annunciated as a priority 1 alarm and is latched, so that the operator must consciously re-select manual afterwards rather than silently regaining control.

Loss of communication with SCADA does not change the mode. If the station is left in manual and the link fails, it stays in manual with the last commanded units running, and raises a communication alarm. Automatic reversion on comms loss was considered and rejected: a link that fails intermittently would cycle the station between modes, which is more dangerous than either mode alone.

6. Headroom, and the limit on deferring a start

The governing operational quantity at this station is time to breach, defined in WRPS-PRO-001 Section 7.2 as remaining volume divided by net accumulation. Level alone is not a sufficient basis for a decision: the same level is comfortable under dry weather inflow and urgent under wet weather inflow.

Because objective 3 permits energy cost to be considered, and because considering it means deferring starts, a floor is required. The following reserve is a control system design parameter and is set by this document.

Component	Allowance	Basis
Pump start to delivered flow	1 minute	Permissives, drive ramp and time to reach duty flow.
Inflow forecast error	9 minutes	Wet weather catchment response is non-linear and a second rain band gives no warning. This is the dominant and least certain term.

Component	Allowance	Basis
One failed start and retry on another unit	5 minutes	Failure to start is a real probability. If the margin is spent, there is no second attempt.
Minimum headroom reserve	15 minutes	Sum of the above.

The rule. A start may be deferred for energy cost reasons only while the projected time to breach, evaluated at the end of the proposed deferral, remains greater than 15 minutes. Once projected time to breach falls to 15 minutes or less, cost ceases to be a consideration and the start proceeds immediately.

Two consequences follow, and both are intended. First, the reserve is evaluated against the projected condition at the end of the deferral, not the condition now, so a deferral that would consume the reserve is refused before it begins. Second, because the forecast error term dominates, the reserve is deliberately larger than the mechanical time required. The station is buying certainty, not reaction time.

In this revision no automatic function defers a start for cost. The reserve exists so that the layer 4 advisory function has a defined and auditable limit, and so that any future automatic implementation inherits that limit rather than reinventing it.

7. Pump starting and stopping

7.1 How many units

The number of units required is determined by wet well level against the ascending thresholds in WRPS-PRO-001 Section 6. Between thresholds the number is held, not recalculated: this hysteresis is what prevents the station cycling a unit on and off around a single level.

7.2 Which unit

Unit selection is a separate decision from the number of units, and is ranked as follows:

- Availability is absolute. An unavailable unit is excluded and cannot be selected by any subsequent rule.
- A unit not approaching its service interval is preferred to one that is.
- Within that grouping, the unit with the lowest accumulated run hours is preferred.
- Ties are broken by ascending unit number, so that selection is deterministic and repeatable.

Service interval is a preference, never a veto. If the only available unit is due for service, it runs. Rank 2 above must never be able to produce an empty selection while an available unit exists. Objective 4 does not outrank objective 2.

A running unit is not displaced. Once a unit is running and remains available, it keeps its position, even if another unit subsequently ranks better on run hours. Re-ranking applies only when a position becomes free. Without this rule the station swaps units every time accumulated hours cross over, which increases starts, which is what actually wears a pump.

7.3 Speed control

Running units share a common speed reference from a level controller, so that the station holds level near a setpoint rather than filling and emptying between fixed start and stop points. Proportional and integral action only. Derivative action is excluded: the measurement carries surface turbulence and derivative gain would amplify it into the drives.

The speed reference is clamped to 38 - 50 Hz. The lower clamp is set by the 22 m static lift, below which no flow is delivered, and is a physical limit rather than a tuning choice. Integral action is frozen whenever the output is clamped, and the controller is reset on stop so that a restart does not inherit stale integral action.

7.4 Staged starting

Where more than one unit is to start, starts are staggered so that the electrical inrush and the hydraulic transient in the rising main are not coincident. The stagger is suspended under the high high level response, where the cost of a transient is accepted against the cost of a spill.

8. Protection philosophy

Protective functions are distinguished from control functions by three properties: they act regardless of mode, they latch, and they require a deliberate operator action to reset. A function that clears itself when the condition clears is a control function, not a protection function.

Principle	Application at this station
Fail safe on loss of signal	LSLL-103 and LSHH-102 are wired normally closed, so a broken wire or lost supply presents as the protective state.
Trips latch	Motor thermal, high high vibration and no-flow trips latch the affected unit out and clear only on an operator reset command. They never clear on the condition clearing.
A trip removes one unit, not the station	A tripped unit is marked unavailable and the next ranked available unit is promoted immediately. The station continues.
Alarm and trip are different	A seal leak alarms and flags the unit for service. It does not remove availability. Water in the seal chamber is a maintenance finding, not an immediate hazard.
Detect the failure that hides	A frozen level transmitter reading a plausible value is more dangerous than one reading out of range, because a range check will not find it. Detection is required on both range and rate of change.

Principle	Application at this station
Degrade to the layer below	On loss of LIT-101 the station falls back to discrete switch control on LSHH-102 and LSLL-103 and continues to protect the wet well, with reduced performance and an alarm.

9. Alarm philosophy

An alarm requires an operator response. A condition that requires no response is an event or a status, and is logged rather than alarmed. Every alarm carries a priority, a consequence and a defined operator action, and any alarm for which those three cannot be written is to be removed rather than issued.

Priority	Meaning	Response time	Examples
1 - Urgent	Spill imminent or in progress, or the station cannot protect itself.	Immediate	High high level, spill active, dry run lockout, all units unavailable.
2 - High	Station capacity or protection is reduced. Action required this shift.	Within 30 minutes	Pump tripped, level signal fault, mains failure, high level.
3 - Low	Maintenance finding. No immediate operational consequence.	Next working day	Seal leak, high vibration, service interval reached, setpoint rejected.

9.1 Rules

- One condition raises one alarm. A pump trip does not also raise a separate stopped alarm and a separate availability alarm.
- An alarm on a consequence is suppressed while its cause is alarmed. Low discharge flow is not alarmed separately while the unit that would have produced it is tripped.
- Priority 1 alarms cannot be shelved from SCADA.
- The high level alarm at 5.20 m is set below the high high level at 5.50 m so that it is a warning rather than an annunciation of an event already under way.
- Alarms are annunciated on the same basis in every mode. Manual mode does not suppress alarms.

10. Interface with SCADA

The PLC holds all control functions. CI Server presents them and provides operator entry. The division is deliberate: the station must operate correctly with SCADA unavailable.

The PLC does	SCADA does
Decides how many units run and which units.	Displays the decision and the reason for it.
Executes all protection and interlocks.	Presents alarms and accepts acknowledgement.
Calculates time to breach and net accumulation.	Trends and displays them.
Accumulates run hours and service status.	Displays them and issues the service reset.
Validates and clamps every setpoint it receives.	Offers setpoint entry and displays the accepted value, not the entered one.
Continues unchanged if SCADA is lost.	Alarms on loss of the link.

Setpoint entry is validated at the PLC, not at SCADA. A start level above the spill weir is refused by the controller regardless of what the operator interface would have permitted, and the refusal is alarmed. Validation performed only in the display layer protects nothing, because it is bypassed by any other client on the network.

Commands from SCADA use an explicit handshake: the PLC executes on the transition, echoes the command it acted on, and takes no further action until the command is cleared. A command that is merely written and left in place is executed once, never repeatedly.

11. Design constraints carried into the implementation

Constraint	Origin	Consequence
Firm capacity of 240 L/s is below PWWF of 300 L/s	WRPS-PRO-001 Section 7.1	All three units are required to pass design wet weather flow. Availability of the third unit is an operational concern, not a redundancy nicety.

Constraint	Origin	Consequence
Downstream storage is unconstrained	WRPS-PRO-001 assumption A02	No downstream level feedback and no discharge restriction logic. If this assumption is closed differently, Sections 3, 6 and 7 require revision, because the risk model becomes two sided.
All three units are variable speed	WRPS-PRO-001 Section 4	Units are functionally interchangeable, so duty selection is a free choice and needs no unmatched-duty compensation.
Start frequency is not a constraint	WRPS-PRO-001 Section 7.4	Approximately seven starts per unit per day at ADWF. Level control may be tuned for stability rather than cycle minimisation.

12. Compliance

The Functional Design Specification is compliant with this philosophy if, for every function it defines, the following can be answered:

- Which control objective in Section 3 does this serve, and does it ever allow a lower priority objective to override a higher one?
- Which layer in Section 4 does it sit in, and does the layer below remain sufficient without it?
- Does it behave identically in auto and in manual, and if not, is the difference listed in Section 5.1?
- If it defers or prevents a start, does it respect the 15 minute reserve in Section 6?
- If it raises an alarm, does that alarm have a priority, a consequence and an operator action?

A function that cannot be placed against these five questions has not been designed. It has been written.