

Waterloo Road Pump Station

Functional Design Specification

Document number	Title	Revision	Date	Status
WRPS-CTL-002	Functional Design Specification	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 and structure

This document defines the behaviour of the control system for Waterloo Road Pump Station in sufficient detail that it can be implemented, tested and accepted without further interpretation. It is subordinate to the Control Philosophy (WRPS-CTL-001); where the two disagree, the philosophy governs.

Requirements are numbered **F-nnn** and are testable statements. Each is referenced by the test schedule in Section 12. A statement that cannot be tested is not a requirement and appears here only as explanatory text.

This document is platform independent. It defines behaviour, not code. Implementation on OpenPLC for the demonstration environment, including the Modbus register map, is covered by WRPS-CTL-003.

2. Reference documents and conventions

Document number	Title
WRPS-CTL-001	Control Philosophy - governs this document
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-003	OpenPLC Implementation Brief - demonstration environment

Conventions

- All levels are metres above the wet well floor (local datum, floor = 0.00 m).
- **Shall** denotes a requirement. **Should** does not appear in this document.
- Pump n refers to PU-301, PU-302 or PU-303 for n = 1, 2, 3.
- Timer values are elapsed real time and are not scaled by any simulation function.

3. Control system overview

A single PLC (PLC-001) executes all control and protection. CI Server provides operator monitoring, alarm presentation, setpoint entry and manual mode commands. Hardwired protection on LSHH-102 and LSLL-103 acts on the variable speed drive safety circuit independently of the PLC.

Ref	Requirement
F-001	The control program shall execute cyclically at a scan interval not exceeding 100 ms.
F-002	All control functions shall reside in PLC-001. No control decision shall depend on communication with CI Server.
F-003	On loss of communication with CI Server the station shall continue to operate in its current mode with the last accepted setpoints, and shall raise a communication alarm.
F-004	Loss of communication with CI Server shall not change the operating mode.

Ref	Requirement
F-005	Hardwired protection on LSHH-102 and LSLL-103 shall remain effective while the PLC is stopped, in fault, or being reprogrammed.

4. Operating modes

Modes are as defined in WRPS-CTL-001 Section 5. Mode is selected from CI Server and reported back from the PLC.

Ref	Requirement
F-010	The station shall support three modes: Auto, SCADA Manual and Off.
F-011	The mode reported to CI Server shall be the mode the PLC is acting on, not the mode last requested.
F-012	In Auto the PLC shall determine the number of running units from wet well level per Section 5, and which units shall run per Section 6.
F-013	In SCADA Manual the operator shall nominate each unit to run or stop individually, and shall enter a speed reference applied to all running units.
F-014	In Off no unit shall start, and any running unit shall stop subject to its minimum run timer.
F-015	A mode change shall not stop a running unit other than as required by F-014.
F-016	Assertion of LSHH-102 while in SCADA Manual shall force the station to Auto, latch that reversion, and raise a priority 1 alarm.
F-017	A latched reversion per F-016 shall require the operator to re-select SCADA Manual explicitly. The station shall not return to manual automatically.

4.1 Functions active in every mode

The following are protection functions and are not suspended by mode selection. This table is the exhaustive list of what SCADA Manual does not transfer to the operator, per WRPS-CTL-001 Section 5.1.

Ref	Requirement
F-020	Dry run protection on LSLL-103 shall be active in every mode. A manual start command issued while LSLL-103 is asserted shall be refused and alarmed, and shall not be queued for later execution.
F-021	Motor thermal, high high vibration and no-flow protection shall be active in every mode.
F-022	Minimum run and minimum off timers shall be active in every mode, and shall not be bypassable from CI Server.
F-023	The speed reference clamp of 38.0 to 50.0 Hz shall be active in every mode. An operator entry below 38.0 Hz shall be raised to 38.0 Hz and annunciated; the entered value shall not be applied.
F-024	All alarms shall be annunciated identically in every mode.

5. Determining the number of running units

Applies in Auto mode. The number of units required is a function of level with hysteresis, then subject to three overrides.

Condition	Units required
Level rises to or above the start pump 3 level (5.00 m)	3
Level rises to or above the start pump 2 level (4.50 m)	2
Level rises to or above the start duty level (4.00 m)	1
Level falls to or below the stop all level (1.00 m)	0
Level between thresholds	Previous value is held
Ref	Requirement
F-030	The number of units required shall be determined from ascending level thresholds as tabulated above.
F-031	Between thresholds the number of units required shall be held at its previous value and shall not be recalculated. A falling level shall not reduce the number of running units until the stop all level is reached.
F-032	Override: while LSHH-102 is asserted, the number of units required shall be the number of available units, and minimum off timers shall be bypassed.

Ref	Requirement
F-033	Override: on assertion of LSSL-103 the number of units required shall be zero, a dry run lockout shall be latched, and no unit shall start until the lockout is reset by operator command.
F-034	A dry run lockout shall not clear on level recovery alone.
F-035	Override: in Off mode the number of units required shall be zero.
F-036	Where the number of units required increases by more than one, starts shall be staggered by 30 s per additional unit.
F-037	The stagger in F-036 shall be suspended while LSHH-102 is asserted.

6. Duty selection

Selection determines which units run. It is evaluated independently of Section 5 and shall not alter the number of units required.

6.1 Ranking

Rank rule	Statement
1	Unavailable units are excluded from selection entirely.
2	Units not due for service rank above units due for service.
3	Within each group, the unit with the lowest accumulated run hours ranks first.
4	Remaining ties are broken by ascending unit number.
Ref	Requirement
F-040	Units shall be ranked by the rules above and the highest ranked available units assigned, up to the number required.
F-041	A unit shall be considered available when it is not tripped, not locked out, and its motor thermal protection is healthy.
F-042	A seal leak shall not remove availability. It shall raise a priority 3 alarm and flag the unit for service.
F-043	Service interval is a preference, not a veto. Where the only available unit is due for service, that unit shall be selected. Ranking shall never produce an empty selection while an available unit exists and units are required.
F-044	A running unit shall not be displaced. A unit that is running and remains available shall retain its assignment even if another unit subsequently ranks higher. Re-ranking shall apply only when an assignment becomes free.
F-045	Where a running unit becomes unavailable, the next ranked available unit shall be assigned within one scan.
F-046	Accumulated run hours shall increment only while a unit is running, and shall be reset only by the service reset command in Section 10.
F-047	A unit shall be flagged due for service when its accumulated run hours reach the service interval setpoint.

7. Speed control

A single level controller generates one speed reference applied to all running units.

Ref	Requirement
F-050	In Auto, drive speed shall be generated by a PI controller acting on wet well level against the control setpoint (default 4.20 m).
F-051	Derivative action shall not be used.
F-052	The speed reference shall be clamped to 38.0 - 50.0 Hz.
F-053	Integral action shall be inhibited while the output is at either clamp.
F-054	The controller output and integral term shall be reset when no unit is running.
F-055	While LSHH-102 is asserted the speed reference shall be forced to 50.0 Hz, overriding the controller.
F-056	In SCADA Manual the speed reference shall be the operator entered value, subject to F-023 and F-055.
F-057	Initial tuning shall be proportional gain 12 Hz/m and integral time 120 s, to be confirmed during commissioning.

8. Headroom calculation

The station publishes time to breach as defined in WRPS-PRO-001 Section 7.2. This is a calculation only: it initiates no control action in this revision.

```

net accumulation = inflow - total discharge flow
volume to spill = (6.000 - level) x 120
time to spill = volume to spill x 1000 / net accumulation

```

Ref	Requirement
F-060	The station shall continuously calculate and publish net accumulation, volume remaining to the spill weir, time to the spill weir and time to LSHH-102.
F-061	Inflow shall be filtered through a first order lag of 30 s before use in the headroom calculation.
F-062	Where net accumulation is less than or equal to 0.5 L/s, published times shall indicate that the wet well is not filling. A negative time shall never be published.
F-063	Published times shall be clamped to a non-negative range.
F-064	At level 4.00 m, inflow 165 L/s and one unit running at 120 L/s, time to the spill weir shall be 5 333 s +/- 1 s and net accumulation shall be 45.0 L/s. This reproduces the reference condition in WRPS-PRO-001 Section 7.3.
F-065	No automatic function shall defer a pump start on the basis of energy cost in this revision. The 15 minute headroom reserve of WRPS-CTL-001 Section 6 is published for advisory use and is not consumed by any control action.

9. Protection functions

Ref	Requirement
F-070	Every protective trip shall latch and shall clear only on an operator reset command. No trip shall clear automatically on the initiating condition clearing.
F-071	A trip shall render the affected unit unavailable and shall not stop the station while another unit is available.
F-072	Motor thermal. Loss of the healthy signal from TE-31n shall trip unit n immediately.
F-073	Vibration. VE-31n above 7.1 mm/s shall raise a priority 3 alarm. Above 11.0 mm/s it shall trip unit n.
F-074	No flow on start. Where 20 s after a run command the discharge pressure at PIT-31n remains below 150 kPa, unit n shall be tripped and the next ranked available unit assigned.
F-075	Level signal fault. LIT-101 shall be declared faulty when its value is outside 0.000 - 7.000 m, or when it changes by less than 0.001 m over 10 minutes while a unit is running.
F-076	On a level signal fault the station shall continue under discrete switch control: start all available units on LSHH-102, stop all on LSL-103, and raise a priority 2 alarm.
F-077	Spill detection. Assertion of LSH-104 shall raise a priority 1 alarm and shall log the start and end time of the event.
F-078	A spill event shall not by itself alter pump control action, which is already at maximum output under F-032.

F-075 addresses the failure that a range check cannot find. A transmitter frozen at a plausible mid-range value satisfies every limit while the wet well fills beneath it. Rate of change detection is the only means by which the control system can identify it.

9.1 Cause and effect matrix

T trip affected unit, latched **S** stop all units **R** start all available units **A** alarm only **P** promote next available unit
L latched lockout, manual reset

Initiator	Tag	PU-301	PU-302	PU-303	Station	Alarm priority	Reset
High high level	LSHH-102	R	R	R	R	1	Auto on falling level
Low low level	LSLL-103	S	S	S	S, L	1	Manual
Spill active	LSH-104	-	-	-	A	1	Auto
High level	LIT-101	-	-	-	A	2	Auto
Level signal fault	LIT-101	-	-	-	A	2	Auto
Motor thermal, unit 1	TE-312	T	P	P	-	2	Manual
Motor thermal, unit 2	TE-322	P	T	P	-	2	Manual
Motor thermal, unit 3	TE-332	P	P	T	-	2	Manual
No flow on start, unit 1	PIT-311	T	P	P	-	2	Manual
No flow on start, unit 2	PIT-321	P	T	P	-	2	Manual
No flow on start, unit 3	PIT-331	P	P	T	-	2	Manual
Vibration high high, unit 1	VE-314	T	P	P	-	2	Manual
Vibration high high, unit 2	VE-324	P	T	P	-	2	Manual
Vibration high high, unit 3	VE-334	P	P	T	-	2	Manual
Vibration high, any unit	VE-31n	A	A	A	-	3	Auto
Seal leak, any unit	MSE-31n	A	A	A	-	3	Manual
Mains failure	XA-502	-	-	-	A	2	Auto
Service interval reached	-	A	A	A	-	3	On service reset

10. Operator commands

Commands are issued from CI Server and executed by the PLC using an explicit handshake.

Command	Parameter	Effect
Reset all trips	-	Clears every latched trip and the dry run lockout, subject to F-081.
Reset trip on unit n	Unit number	Clears the latched trip on the nominated unit.
Lock out unit n	Unit number	Marks the unit unavailable for maintenance.
Release lockout on unit n	Unit number	Returns the unit to service.
Service reset on unit n	Unit number	Resets accumulated run hours and clears the service due flag.
Acknowledge alarms	-	Acknowledges all unacknowledged alarms.
Start unit n	Unit number	SCADA Manual only. Requests the nominated unit to run.
Stop unit n	Unit number	SCADA Manual only. Requests the nominated unit to stop.
Ref	Requirement	
F-080	A command shall be executed once on its transition to a non-zero value. The PLC shall echo the executed command and shall take no further action until the command is cleared to zero.	
F-081	A reset command shall have no effect while its initiating condition remains present. A dry run lockout shall not clear while LSLL-103 is asserted.	
F-082	Start and stop commands shall be accepted only in SCADA Manual and shall be rejected and alarmed in Auto or Off.	
F-083	A start command shall be refused where the nominated unit is unavailable, its minimum off timer is running, or LSLL-103 is asserted. A refusal shall be alarmed and shall not be queued.	

11. Setpoints

Setpoint	Default	Permitted range	Validation
Level control setpoint	4.20 m	3.50 - 4.80 m	Between start duty and start pump 2
Start duty level	4.00 m	2.00 - 5.00 m	Above stop all, below start pump 2
Start pump 2 level	4.50 m	2.50 - 5.20 m	Above start duty, below start pump 3
Start pump 3 level	5.00 m	3.00 - 5.40 m	Above start pump 2, below LSHH
Stop all level	1.00 m	0.70 - 3.00 m	Above LSLL, below start duty
High level alarm	5.20 m	4.50 - 5.45 m	Below LSHH
Minimum drive speed	38.0 Hz	35.0 - 45.0 Hz	Below maximum speed
Service interval	4 000 h	500 - 20 000 h	-
Minimum run time	5 min	1 - 30 min	-
Minimum off time	5 min	1 - 30 min	-
Ref	Requirement		
F-090	Every setpoint shall be validated at the PLC on receipt against the range and the ordering constraints tabulated above.		
F-091	A setpoint failing validation shall be rejected, the previous accepted value retained, and a priority 3 alarm raised. The rejected value shall not be applied even transiently.		
F-092	No start level shall be accepted at or above the spill weir level of 6.000 m under any circumstance.		
F-093	The value reported to CI Server shall be the accepted value in use, not the value last written.		

Validation resides in the PLC because validation performed only in the display layer is bypassed by any other client on the network.

12. Test schedule

Each test below is to be witnessed and signed. A test is passed only where the observed values are recorded, not merely marked satisfactory.

Test	Requirement	Method	Expected result
T-01	F-030, F-031	Raise level to 4.1 m, then lower to 3.9 m, then to 0.9 m	One unit starts at 4.1 m, continues at 3.9 m, stops at 0.9 m
T-02	F-030, F-036	Raise level to 4.6 m then 5.1 m	Two then three units running, each additional start staggered by 30 s
T-03	F-040, F-044	Set run hours 500 / 100 / 100, trigger a duty start	PU-302 selected. With PU-302 running, raise its hours above PU-303: PU-302 continues
T-04	F-043	Set PU-302 due for service, make PU-301 and PU-303 unavailable, trigger a start	PU-302 starts
T-05	F-045, F-074	Start a unit and hold its PIT below 150 kPa	Unit trips at 20 s, next ranked unit assigned, priority 2 alarm
T-06	F-070, F-072	Drop TE-312, then restore it	PU-301 trips and stays tripped after restoration. Clears only on reset command
T-07	F-032, F-037	Assert LSHH-102 with a minimum off timer running	All available units start at 50.0 Hz with no stagger and no timer delay
T-08	F-033, F-034, F-081	Assert LSLL-103, then restore level, then issue reset	All stop and lock out. No restart on level recovery. Restart only after reset
T-09	F-016, F-017	In SCADA Manual with one unit running, assert LSHH-102	Station reverts to Auto, all available units start, priority 1 alarm, reversion latched
T-10	F-020, F-083	In SCADA Manual with LSLL-103 asserted, command a start	Command refused and alarmed. No start occurs when LSLL clears
T-11	F-023	In SCADA Manual enter a speed reference of 30 Hz	Applied speed is 38.0 Hz, annunciated. 30 Hz is not applied at any point
T-12	F-075, F-076	Hold LIT-101 constant for 10 minutes with a unit running	Level signal fault alarm, station continues on discrete switches
T-13	F-090, F-091, F-092	Write a start duty level of 6.5 m	Rejected, previous value retained and reported, priority 3 alarm
T-14	F-064	Level 4.00 m, inflow 165 L/s, one unit at 120 L/s	Time to spill 5 333 s +/- 1 s, net accumulation 45.0 L/s
T-15	F-003, F-004	Disconnect CI Server with a unit running in SCADA Manual	Unit continues, mode unchanged, communication alarm on restoration of the link
T-16	F-005	Stop the PLC with the wet well at low level	Hardwired LSLL-103 prevents any drive from running

T-14 is the acceptance test for the process model itself. If it does not reproduce the figure in WRPS-PRO-001 Section 7.3, the Basis of Design and the running system disagree and one of them is wrong. T-16 is the only test that proves layer 1 independence, and cannot be substituted by any test performed with the PLC running.

13. Open items

ID	Item	Impact	Owner
O-01	PI tuning constants in F-057 are initial values only	Level control stability. Requires confirmation against the commissioned station	Commissioning
O-02	Whether all three units may run on standby generation	May restrict capacity during mains failure. F-032 assumes no restriction	Electrical

ID	Item	Impact	Owner
O-03	Alarm rationalisation not yet performed	Priorities in Section 9.1 are proposed, not agreed with operations	Operations
O-04	Assumption A02, unconstrained downstream storage	If closed differently, Sections 5, 8 and 9 require revision to include downstream feedback	Process