RELEASED PASS 16 / 16

Application Validation Report

SmartLift_Duplex — version 2.4.1

Attestation

Application	SmartLift_Duplex **v2.4.1**
Validated	2026-08-09T20:39:57Z
Device MAC	53430263
Firmware (core)	1.5.8
Source commit	`75c1535` (clean)
Release tag	`lift-station/v2.4.1` (at this commit)
Device files (SHA-256)	`sha256:2ba9656feabe52cbeb1ab35e2724dd935c6bcec975eddc4aebe60d85559513d2`
Files validated	app.py, app_vars.py, config.json, makliftstation.py, makstation.py
Promotion	Promoted to RELEASED 2026-08-09T20:40:40Z — device-file fingerprint verified byte-identical to the release tag. Run executed on commit `f78d210` prior to tagging.

What this report certifies

This report records an automated, end-to-end validation of the **SmartLift_Duplex** application running on a physical SmartController Classic with real m.Smart Universal IO modules. Each test drives the controller's field inputs (levels, floats, faults, currents, power status) over the live Modbus/RS-485 and cloud command path exactly as in the field, then observes the controller's pump run and speed outputs, confirming the control logic and protective lockouts behave as specified. The exact software validated is pinned by the source commit and the SHA-256 fingerprint of the deployed files above.

Results summary

PASS 16 / 16 (16 of 16 scenarios passed).

#	Scenario	Result
1	Auto drain: lead starts, lag joins, all stop	PASS
2	Rotation: lead alternates each cycle	PASS
3	Low-level (dry-run) lockout with hysteresis	PASS

4	Fault promotion: faulted lead hands off	PASS
5	Hand ignores fault	PASS
6	High-amp lockout: disqualify a pump (30 s) then release after cycle + 10 min	PASS
7	Radar geometry: well level computed from Well Height - Radar Distance	PASS
8	Flume level from the second radar (optional; Flume Height gates it)	PASS
9	Sensor failover: radar error -> rod control (3 min latch)	PASS
10	Level-fail lockout when every sensor is gone	PASS
11	Float control mode (primary = floats)	PASS
12	Speed output tracks the speed setpoint	PASS
13	Fault contact NO: active input = fault, fails over	PASS
14	Fault contact NC (fail-safe): open/inactive input = fault	PASS
15	Run-feedback NO: fail-to-start locks out a pump with no feedback	PASS
16	Run-feedback NC: fail-to-start works with inverted wiring	PASS

Test detail

1. Auto drain: lead starts, lag joins, all stop PASS

Confirms the wet well drains correctly: the lead pump starts when the level reaches the Start setpoint, the lag pump joins at the higher Lag Start setpoint, and both stop once the level falls to the Stop setpoint.

Requirement: drain start/lag/stop on level

	Step	At
✓	Configure 18 setpoint/mode value(s)	
✓	drive Well Level = 15	0.0 s
✓	wait 10.0s	10.0 s
✓	expect running == {} within 15.0s	0.0 s
✓	Configure 2 setpoint/mode value(s)	
✓	drive Well Level = 75	0.0 s
✓	expect running == {Pump 1 Run Out} within 15.0s	2.6 s
✓	drive Well Level = 90	0.0 s
✓	expect running == {Pump 1 Run Out, Pump 2 Run Out} within 15.0s	1.8 s
✓	drive Well Level = 20	0.0 s
✓	expect running == {} within 15.0s	1.8 s

2. Rotation: lead alternates each cycle PASS

In Rotate mode the lead role alternates between pumps on each pumping cycle, so duty is shared evenly and wear is balanced across both pumps.

Requirement: lead rotation at cycle end

	Step	At
✓	Configure 18 setpoint/mode value(s)	
✓	drive Well Level = 15	0.0 s
✓	wait 10.0s	10.0 s
✓	expect running == {} within 15.0s	0.0 s
✓	Configure 3 setpoint/mode value(s)	
✓	drive Well Level = 75	0.0 s
✓	expect single lead within 15.0s	2.2 s
✓	drive Well Level = 20	0.0 s
✓	expect running == {} within 15.0s	1.6 s
✓	drive Well Level = 75	0.0 s
✓	expect rotated lead within 15.0s	2.2 s

3. Low-level (dry-run) lockout with hysteresis PASS

Protects the pumps from running dry: when the level is below the Low Level Cutout the pumps are held off even though the level is above Start, and they only resume once the level recovers past the cutout plus a hysteresis margin.

Requirement: low-level cutout + hysteresis

	Step	At
✓	Configure 18 setpoint/mode value(s)	
✓	drive Well Level = 15	0.0 s
✓	wait 10.0s	10.0 s
✓	expect running == {} within 15.0s	0.0 s
✓	Configure 6 setpoint/mode value(s)	
✓	drive Well Level = 8	0.0 s
✓	expect running == {} within 15.0s	2.4 s
✓	drive Well Level = 20	0.0 s
✓	expect running == {Pump 1 Run Out} within 15.0s	2.4 s

4. Fault promotion: faulted lead hands off PASS

If the running lead pump faults, the station promotes the healthy standby pump so the well keeps draining instead of stalling on the failed pump.

Requirement: fault promotion

	Step	At
✓	Configure 18 setpoint/mode value(s)	
✓	drive Well Level = 15	0.0 s
✓	wait 10.0s	10.0 s
✓	expect running == {} within 15.0s	0.0 s
✓	Configure 2 setpoint/mode value(s)	
✓	drive Well Level = 75	0.0 s
✓	expect running == {Pump 1 Run Out} within 15.0s	2.2 s
✓	inject fault P1 on	0.0 s
✓	expect running == {Pump 2 Run Out} within 15.0s	2.8 s
✓	inject fault P1 off	0.0 s

5. Hand ignores fault PASS

In Hand (manual) mode the operator's command overrides automatic protections: the pump keeps running even with a fault asserted, as expected for manual control.

Requirement: hand runs through fault

	Step	At
✓	Configure 18 setpoint/mode value(s)	
✓	drive Well Level = 15	0.0 s
✓	wait 10.0s	10.0 s
✓	expect running == {} within 15.0s	0.0 s
✓	Configure 1 setpoint/mode value(s)	
✓	inject fault P1 on	0.0 s
✓	expect running == {Pump 1 Run Out} within 15.0s	1.2 s
✓	inject fault P1 off	0.0 s

6. High-amp lockout: disqualify a pump (30 s) then release after cycle + 10 min PASS

Guards against a jammed/failing pump: sustained over-current for 30 s disqualifies that pump (the other carries the load), and it is only returned to service after the cycle ends and a 10-minute cool-down has elapsed.

Requirement: high-amp lockout set + reset

	Step	At
✓	Configure 18 setpoint/mode value(s)	
✓	drive Well Level = 15	0.0 s
✓	wait 10.0s	10.0 s
✓	expect running == {} within 15.0s	0.0 s
✓	Configure 2 setpoint/mode value(s)	
✓	drive Well Level = 90	0.0 s
✓	expect running == {Pump 1 Run Out, Pump 2 Run Out} within 15.0s	2.4 s
✓	inject high_amp P1 on	0.0 s
✓	expect running == {Pump 2 Run Out} within 40.0s	15.8 s
✓	inject high_amp P1 off	0.0 s
✓	drive Well Level = 20	0.0 s
✓	expect running == {} within 15.0s	2.2 s
✓	wait 630.0s	630.0 s
✓	drive Well Level = 90	0.0 s
✓	expect running == {Pump 1 Run Out, Pump 2 Run Out} within 15.0s	2.2 s

7. Radar geometry: well level computed from Well Height - Radar Distance PASS

The radar measures the distance down to the liquid surface and the app computes the well level from the configured Well Height (mount height above the well bottom). Changing Well Height rescales the computed level - verified by the same physical distance reading starting or stopping the pumps as the configured geometry changes.

Requirement: well level = (Well Height - Radar Distance) / Well Height

	Step	At
✓	Configure 18 setpoint/mode value(s)	
✓	drive Well Level = 15	0.0 s
✓	wait 10.0s	10.0 s
✓	expect running == {} within 15.0s	0.0 s
✓	Configure 2 setpoint/mode value(s)	
✓	drive Well Level = 75	0.0 s
✓	expect running == {Pump 1 Run Out} within 15.0s	2.4 s
✓	expect Radar Level >= 73 within 150.0s	0.0 s
✓	expect Radar Level <= 77 within 150.0s	0.0 s
✓	Configure 1 setpoint/mode value(s)	
✓	expect running == {} within 15.0s	0.8 s
✓	Configure 1 setpoint/mode value(s)	
✓	expect running == {Pump 1 Run Out} within 15.0s	2.0 s

8. Flume level from the second radar (optional; Flume Height gates it) PASS

The optional second radar over the flume reports its distance on Modbus slave 4; the app computes Flume Level = Flume Height - distance (monitoring only). With Flume Height at 0 (no flume radar installed) the Flume Level stays pinned at 0.

Requirement: flume level = Flume Height - Flume Distance; 0 disables

	Step	At
✓	Configure 18 setpoint/mode value(s)	
✓	drive Well Level = 15	0.0 s
✓	wait 10.0s	10.0 s
✓	expect running == {} within 15.0s	0.0 s
✓	drive Flume Level = 4	0.0 s
✓	expect Flume Level == 0 within 150.0s	0.0 s
✓	Configure 1 setpoint/mode value(s)	
✓	expect Flume Level >= 3.5 within 150.0s	11.4 s
✓	expect Flume Level <= 4.5 within 150.0s	0.0 s
✓	drive Flume Level = 10	0.0 s
✓	expect Flume Level >= 9.5 within 150.0s	31.0 s
✓	expect Flume Level <= 10.5 within 150.0s	0.0 s
✓	Configure 1 setpoint/mode value(s)	
✓	expect Flume Level == 0 within 150.0s	30.0 s

9. Sensor failover: radar error -> rod control (3 min latch) PASS

Level-sensor redundancy: when the primary radar reads out of range for the error delay, the controller latches a radar error and fails over to the analog rod sensor so level control continues uninterrupted.

Requirement: sensor failover radar->rod + error latch

	Step	At
✓	Configure 18 setpoint/mode value(s)	
✓	drive Well Level = 15	0.0 s
✓	wait 10.0s	10.0 s
✓	expect running == {} within 15.0s	0.0 s
✓	Configure 2 setpoint/mode value(s)	
✓	drive Well Level = 90	0.0 s
✓	inject radar_fault on	0.0 s
✓	expect Radar error == 1 within 210.0s	90.6 s
✓	expect running == {Pump 1 Run Out, Pump 2 Run Out} within 210.0s	0.6 s
✓	drive Well Level = 20	0.0 s
✓	expect running == {} within 15.0s	3.2 s
✓	inject radar_fault off	0.0 s

10. Level-fail lockout when every sensor is gone PASS

Fail-safe when level can no longer be trusted: with floats disabled and both the radar and rod faulted, the controller raises a level-fail lockout and stops the pumps rather than operate blind.

Requirement: level-fail lockout

	Step	At
✓	Configure 18 setpoint/mode value(s)	
✓	drive Well Level = 15	0.0 s
✓	wait 10.0s	10.0 s
✓	expect running == {} within 15.0s	0.0 s
✓	Configure 3 setpoint/mode value(s)	
✓	drive Well Level = 90	0.0 s
✓	inject radar_fault on	0.0 s
✓	inject rod_fault on	0.0 s
✓	expect Level lockout == 1 within 210.0s	90.6 s
✓	expect running == {} within 210.0s	0.0 s
✓	inject radar_fault off	0.0 s
✓	inject rod_fault off	0.0 s

11. Float control mode (primary = floats) PASS

With floats selected as the primary level method, the start float engages the lead pump and the stop float drops it - verifying control works on discrete floats alone.

Requirement: float start/stop control

	Step	At
✓	Configure 18 setpoint/mode value(s)	
✓	drive Well Level = 15	0.0 s
✓	wait 10.0s	10.0 s
✓	expect running == {} within 15.0s	0.0 s
✓	Configure 3 setpoint/mode value(s)	
✓	drive Well Level = 90	0.0 s
✓	expect running == {Pump 1 Run Out} within 15.0s	2.6 s
✓	drive Well Level = 20	0.0 s
✓	expect running == {} within 15.0s	2.6 s

12. Speed output tracks the speed setpoint PASS

The VFD speed command output follows the operator's speed setpoint, so a running pump is driven at the commanded speed.

Requirement: speed output = setpoint

	Step	At
✓	Configure 18 setpoint/mode value(s)	
✓	drive Well Level = 15	0.0 s
✓	wait 10.0s	10.0 s
✓	expect running == {} within 15.0s	0.0 s
✓	Configure 3 setpoint/mode value(s)	
✓	drive Well Level = 90	0.0 s
✓	expect Pump 1 Speed Out >= 58 within 15.0s	0.0 s
✓	expect Pump 1 Speed Out <= 62 within 15.0s	1.8 s

13. Fault contact NO: active input = fault, fails over PASS

With the fault contact configured Normally-Open (active input = fault), an asserted fault locks the pump out, the logical Faulted state reflects it, and the station fails over to the healthy pump.

Requirement: fault polarity NO -> logical fault + failover

	Step	At
✓	Configure 18 setpoint/mode value(s)	
✓	drive Well Level = 15	0.0 s
✓	wait 10.0s	10.0 s
✓	expect running == {} within 15.0s	0.0 s
✓	Configure 4 setpoint/mode value(s)	
✓	drive Well Level = 75	0.0 s
✓	expect running == {Pump 1 Run Out} within 15.0s	2.6 s
✓	inject fault P1 on	0.0 s
✓	expect Pump 1 Faulted == 1 within 15.0s	0.0 s
✓	expect running == {Pump 2 Run Out} within 15.0s	2.8 s
✓	inject fault P1 off	0.0 s
✓	expect Pump 1 Faulted == 0 within 15.0s	2.0 s

14. Fault contact NC (fail-safe): open/inactive input = fault PASS

With the fault contact configured Normally-Closed (fail-safe: active = OK, an open or cut contact = fault), losing the contact is read as a fault, locks the pump out, and fails over.

Requirement: fault polarity NC -> logical fault + failover

	Step	At
✓	Configure 18 setpoint/mode value(s)	
✓	drive Well Level = 15	0.0 s
✓	wait 10.0s	10.0 s
✓	expect running == {} within 15.0s	0.0 s
✓	Configure 4 setpoint/mode value(s)	
✓	drive Well Level = 75	0.0 s
✓	expect running == {Pump 1 Run Out} within 15.0s	2.4 s
✓	inject fault P1 on	0.0 s
✓	expect Pump 1 Faulted == 1 within 15.0s	1.8 s
✓	expect running == {Pump 2 Run Out} within 15.0s	2.0 s
✓	inject fault P1 off	0.0 s
✓	expect Pump 1 Faulted == 0 within 15.0s	2.2 s

15. Run-feedback NO: fail-to-start locks out a pump with no feedback PASS

When a pump is commanded to run but its run-feedback never confirms (Normally-Open wiring), the fail-to-start timer locks that pump out and the station fails over to the other pump.

Requirement: fail-to-start, run-feedback NO

	Step	At
✓	Configure 18 setpoint/mode value(s)	
✓	drive Well Level = 15	0.0 s
✓	wait 10.0s	10.0 s
✓	expect running == {} within 15.0s	0.0 s
✓	Configure 4 setpoint/mode value(s)	
✓	drive Well Level = 75	0.0 s
✓	withhold_feedback P1 on	0.0 s
✓	expect running == {Pump 2 Run Out} within 45.0s	10.8 s
✓	withhold_feedback P1 off	0.0 s

16. Run-feedback NC: fail-to-start works with inverted wiring PASS

The same fail-to-start protection with the run-feedback contact configured Normally-Closed: the logical run state is derived correctly from the inverted input, so a missing feedback still trips fail-to-start.

Requirement: fail-to-start, run-feedback NC

	Step	At
✓	Configure 18 setpoint/mode value(s)	
✓	drive Well Level = 15	0.0 s
✓	wait 10.0s	10.0 s
✓	expect running == {} within 15.0s	0.0 s
✓	Configure 4 setpoint/mode value(s)	
✓	drive Well Level = 75	0.0 s
✓	withhold_feedback P1 on	0.0 s
✓	expect running == {Pump 2 Run Out} within 45.0s	10.2 s
✓	withhold_feedback P1 off	0.0 s

Generated 2026-08-09 20:40 UTC. This document is uncontrolled when printed.