FLUX

FLUX-TWP-001 · Revision 1.0
October 2026 · Public

Technical White Paper

Any tower. Already installed. Run remotely.

How FLUX connects existing mechanical parking towers of any make to remote monitoring, remote error handling and remote updates, without replacing the machine.

Written for engineering, maintenance and product teams at parking-system manufacturers, maintenance operators and distributors.



Contents

1	Summary	3
2	The engineering problem	4
3	System architecture	5
4	Integration with an installed tower	6
5	Any tower: two integration paths	7
6	Remote operation	9
7	Safety concept	12
8	Security	12
9	Platform and data	13
10	Specifications	13
11	Deployment and responsibilities	14
12	Status and roadmap	14

Technical White Paper

Document	FLUX-TWP-001 · Revision 1.0 · October 2026
Classification	Public
Issued by	Gigto Co., Ltd.

Public document. Implementation details are provided under NDA in the FLUX Integration Specification (FLUX-IS-001).

Available **In validation** **Roadmap** **Project**

Available: implemented and covered by automated tests. In validation: built, field validation in progress. Roadmap: planned for a future release.

1 Summary

FLUX is a retrofit layer for mechanical parking towers that are already in service. A compact gateway is fitted inside the existing control cabinet and connects to the tower's controller. From then on the tower can be monitored, diagnosed, corrected and updated from anywhere.

1

Built for towers that already exist

The gateway is installed inline on the existing panel-to-controller link. Motors, sensors, interlocks and the safety circuit are not modified. If the gateway fails or loses power, the original link is restored automatically.

2

Any tower, through one of two paths

Path A analyses the existing controller's communication and builds a site profile that is applied remotely, without a firmware change. Path B replaces the operator panel, and where necessary the controller, with supported equipment when analysis is not possible.

3

Remote updates, error handling and deployment

Firmware and configuration are updated over the air with automatic rollback. Faults are classified as they occur, and approved commands are executed with full acknowledgement. New sites are provisioned and rolled out in stages from the cloud.

At a glance

Item	Value
Installation	Inside the existing control cabinet, one site visit
Controller link	RS-232 / RS-485 serial, inline with fail-safe bypass
Cloud link	MQTT over TLS 1.2+, X.509 identity per device
Heartbeat / telemetry	60 s heartbeat, 5 s telemetry (configurable 1–60 s)
Offline detection	3 minutes without heartbeat, or broker last-will message
Firmware update	A/B partitions, integrity check, health gate, automatic rollback
Site profile update	Applied remotely and hot-reloaded without reboot
Local buffering	Up to 10,000 telemetry records while offline

Pilot programme reported in FLUX IR 2026: 3 sites, 153 units, 3 weeks, Seoul and Busan. 99.4% system uptime, 22 min average fault detection, 55.6% of incidents resolved remotely (30 of 54). Results at individual sites will vary.

2 The engineering problem

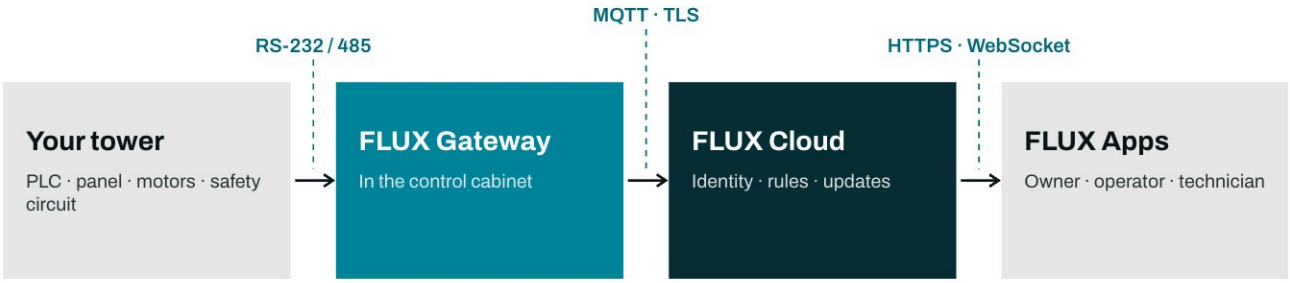
Mechanical parking towers are long-lived machines. A typical installed base mixes manufacturers, controller generations and operator panels, and most units were never designed to be connected. Their controllers already know what is happening, through machine states, positions and alarm codes. That information stays inside the cabinet.

As a result, maintenance is reactive. A fault is reported by phone, a two-person crew is dispatched, and many visits end with a reset that could have been performed safely from a distance if the right information and controls had been available.

Design constraints FLUX was built around

Constraint	What it means for the design
The machine cannot be redesigned	No changes to motors, sensors, interlocks or safety wiring. FLUX attaches to the existing communication link.
Controllers are heterogeneous and often closed	Support must come from configuration and analysis, not from a new firmware build per site.
Safety must never depend on FLUX	Emergency stops and interlocks stay hard-wired in the original controller. FLUX failures must leave the tower as it was.
Sites are remote and unattended	Everything after installation, including updates and diagnosis, must work over the network with safe fallbacks.
Connectivity is imperfect	Data must survive network loss, and the tower must keep running normally while FLUX is offline.

Where FLUX sits



3 System architecture

FLUX consists of four layers. Each layer can fail without affecting the safe operation of the tower.

Layer	Component	Responsibility	Status
Machine	Existing controller (PLC), panel, motors, safety circuit	Unchanged. Remains the authority for motion and safety.	
Edge	FLUX Gateway	Relays the panel-to-controller link, decodes machine data, buffers it, executes approved commands, updates itself.	In validation
Cloud	FLUX Cloud	Device identity, messaging, alarm rules, history, update distribution, site profiles, APIs.	Available
People	Owner App, Operator Console, technician app	Live status, alarms, approvals, work orders and reports for each role.	Available

Data flow

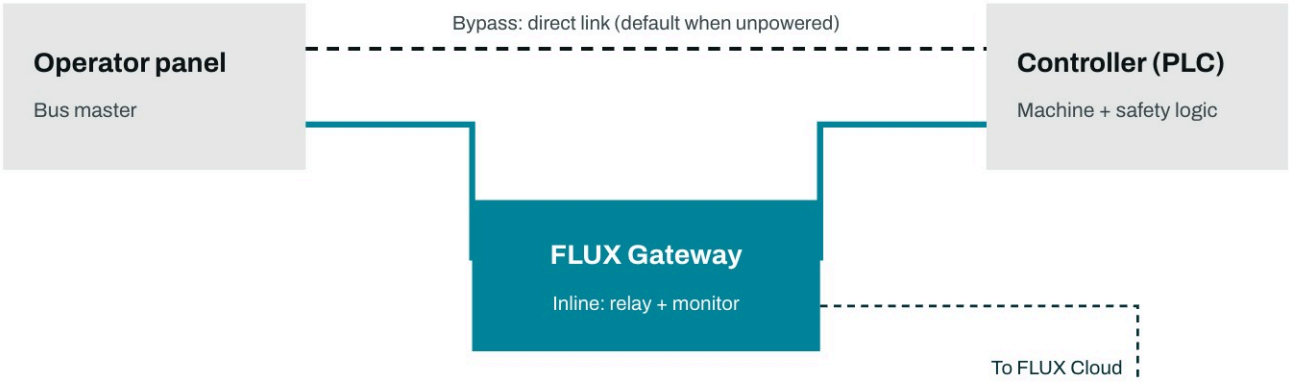
1	**Observe**	The gateway relays every frame between panel and controller without altering normal operation and decodes the values defined in the site profile.
2	**Report**	States, positions, counters and alarm codes are published as telemetry. Events such as alarms are sent immediately.
3	**Decide**	Cloud rules classify alarms by severity, open tickets and notify the right people. Operators see the live state and history.
4	**Act**	Approved commands travel back to the gateway, are checked again on the device and executed through the controller's own interface.

Optional modules

Module	Purpose	Status
FLUX Vision	Live camera view of the platform for visual verification before remote commands, with before/after capture.	In validation
FLUX Touch Panel	Android-based operator panel replacing ageing HMIs. Also the hardware basis for integration Path B.	In validation

4 Integration with an installed tower

The gateway is placed inline on the serial link between the operator panel (bus master) and the controller. In normal operation it relays traffic transparently. Physically, a bypass path connects panel and controller directly whenever the gateway is not fully healthy.



Link states

Situation	Link state	Effect on the tower
Gateway unpowered	Bypass	Panel and controller connected directly. Tower operates as before installation.
Gateway booting or updating	Bypass	Unchanged operation until all health checks pass.
Gateway healthy	Inline	Transparent relay with monitoring and approved command injection.
Software hang or watchdog trip	Bypass	Hardware supervision restores the direct link, then restarts the gateway.
Power loss	Bypass	Stored energy allows an orderly shutdown; the direct link is restored by default.

What is and is not touched

Not modified

- Controller program and safety logic
- Emergency stop and interlock wiring
- Motors, drives, sensors and limit switches
- Operator panel behaviour for drivers

Added

- FLUX Gateway in the control cabinet
- Serial connection on the panel-to-controller link
- Power from the cabinet supply (DC 9–36 V)
- Network connection over site Ethernet or Wi-Fi

Electrical and environmental design

Aspect	Design
Serial interfaces	RS-232 and RS-485. Galvanically isolated interfaces recommended (2.5–5 kV class).
Bypass path	Normally closed to the direct link. Surge protection on the line side.
Power input	DC 9–36 V, compatible with 12 V and 24 V cabinet supplies. AC sites use an external DC supply.
Power-loss hold-up	Supercapacitor bank sized at 2.2× the energy needed for an orderly shutdown.
File system	Read-only system partition with a separate data partition, so power cuts cannot corrupt the software.
Supervision	Independent hardware watchdog that restarts the gateway if the software stops responding.
Operating temperature	–10 to +55 °C (design target, validation in progress).
Enclosure	Aluminium, approx. 130 × 110 × 72 mm, DIN rail or wall bracket.

Timing

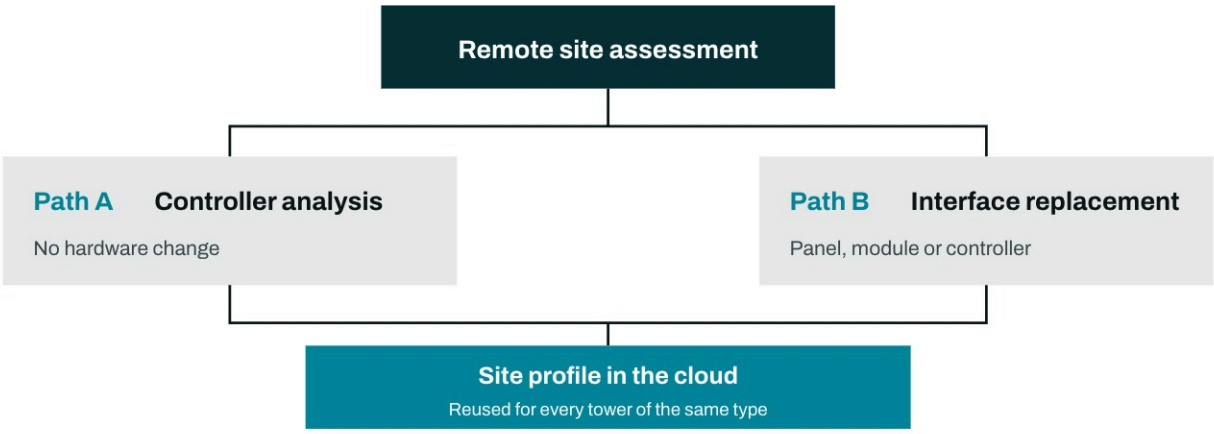
Inline relaying must stay inside the controller's own communication timeouts. Added latency is qualified per site against the 99.9th percentile with a 2× margin before the link is switched inline. Where a site needs tighter timing, the gateway supports an on-board transceiver option and a real-time tuned operating system profile.

Safety principle

FLUX is a non-safety device. The controller and its hard-wired safety circuit remain the only authority over motion. FLUX cannot bypass an emergency stop or an interlock, and every command it sends is a command the panel could already send.

5 Any tower: two integration paths

Mechanical parking towers use many controller families and private protocols. FLUX does not depend on any single one. Each site is supported through one of two paths, chosen after a remote assessment.



Path A: controller analysis (no hardware change)

1	**Capture**	The gateway is installed in monitoring mode and records the traffic between panel and controller during normal operation.
2	**Identify**	The protocol family and line settings are identified automatically from the traffic, with a confidence score reported to the cloud.
3	**Profile**	Values are classified and correlated with real operator actions and machine events to build a draft site profile: which values mean state, position, counter or alarm, and which commands exist.
4	**Verify**	The profile is reviewed by FLUX engineers and tested against a simulator of the site before any command is enabled.
5	**Apply**	The verified profile is pushed to the gateway and hot-reloaded without a reboot. Supporting a new site is a configuration change, not a firmware change.

Path B: controller interface replacement

When the existing equipment cannot be analysed reliably, for example because the controller is closed, obsolete or undocumented, FLUX replaces the interface instead.

Option	What changes	Typical case	Status
Panel replacement	The operator panel is replaced by FLUX Touch Panel, connected to the controller over an open interface.	Ageing HMI, controller readable over Ethernet or serial	In validation
Communication module	An open communication module is added to the existing controller.	Closed loader port, controller otherwise sound	In validation
Controller replacement	The controller is replaced by a supported model and the machine sequence is re-implemented, keeping motors, sensors and safety wiring.	Obsolete or unsupported controller	Project

Path B changes the control equipment, so it follows the local inspection regime for mechanical parking. The machine sequence and safety logic remain in the controller, emergency stops stay hard-wired, and the previous configuration is kept for rollback.

Current controller coverage

Interface	Equipment	Coverage	Status
LS Master-K (serial)	FLUX Gateway	Read path verified on a 37,000-frame capture from a working tower, 100% checksum-valid	In validation
Modbus RTU (serial)	FLUX Gateway	Codec and simulator tests	Available
Automatic protocol / baud identification	FLUX Gateway	Verified on recorded and synthetic traffic	In validation
LS XGT over Ethernet, Modbus TCP	FLUX Touch Panel	Verified against controller simulators	In validation
LS XGT serial	FLUX Touch Panel	Implemented, hardware validation pending	In validation
Other controller families	Either	Through Path A analysis or Path B replacement, assessed per project	Project

Remote site assessment

Before any visit, partners send the following. FLUX confirms the path, the scope and the equipment list.

Information	Why it is needed
Tower manufacturer, model, year, number of bays	Selects reference profiles and estimates scope
Controller make and model, photo of the nameplate	Identifies the protocol family and available ports
Operator panel make and model	Determines whether the inline link or Path B applies
Photos of the control cabinet and the panel-to-controller cable	Confirms mounting space, connector type and power supply
Cabinet supply voltage	Confirms the DC 9–36 V input or the need for an external supply
Network availability at the cabinet	Ethernet, Wi-Fi or a separate router
Fault history for the last 12 months, if available	Prioritises alarms and remote-resolution rules

What partners receive

- A site profile maintained by FLUX for every controller type you deploy
- A digital-twin simulation of the site used for testing commands before they are enabled
- Remote support from FLUX engineers during capture, profiling and the first weeks of operation

6 Remote operation

Once a site is connected, everything that follows happens over the network: monitoring, diagnosis, approved corrective commands, configuration changes and software updates.

6.1 Monitoring and connectivity

Function	Behaviour	Status
Heartbeat	Every 60 s	Available
Device status	Every 5 min and immediately on network change	Available
Telemetry	Every 5 s, configurable from 1 to 60 s	Available
Events and alarms	Sent immediately when they occur	Available
Offline detection	No heartbeat for 3 min, or the broker's last-will message. A critical ticket is opened automatically.	Available
Reconnection	Automatic with back-off from 1 to 30 s; keep-alive every 30 s	Available
Offline buffering	Up to 10,000 telemetry records stored locally and delivered on reconnection; raw controller frames kept on the device	Available

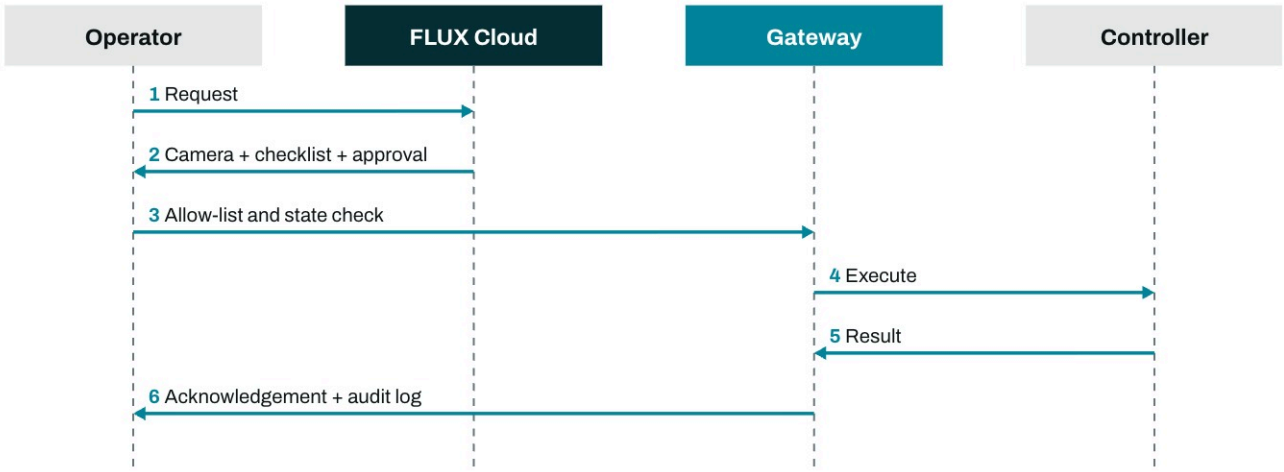
6.2 Alarm handling

Alarm rules are defined in the cloud per site or per fleet. Each rule combines a value, a condition, a threshold and how long the condition must persist. When a rule fires, FLUX assigns a severity, can open a service ticket automatically and notifies the responsible users in real time.

Property	Value
Severities	Critical, high, medium, low
Repeat suppression	Cool-down period, 10 min by default
Lifecycle	Active, acknowledged, resolved, with full history
Escalation	Automatic ticket creation and technician dispatch from the Operator Console

6.3 Remote error handling

Every remote command follows the same controlled sequence. Commands that are not on the device's allow-list are refused.

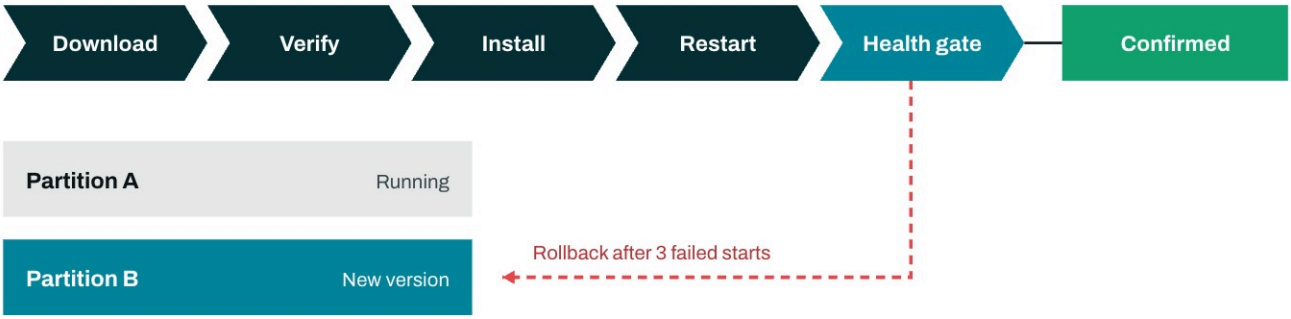


Fault class	Remote action	Status
Non-critical, resettable	Remote reset after the operator has checked the camera view and the safety checklist and approved the command	In validation
Mechanical or sensor faults	Remote reset refused. A field-repair ticket is created with the full alarm history.	In validation
Emergency stop active	Motion commands rejected on the device until the stop is cleared on site	Available
Power-off or safety-relevant actions	Never available remotely	Available

Command handling	Behaviour
Acknowledgement	Every command returns success, failure or rejected, linked to its request
Long-running commands	Interim acknowledgement after 5 s, final result when complete
Delivery	Acknowledgements retried 3 times and kept across reconnections
Cloud timeout	Command marked as timed out if no acknowledgement arrives within 60 s
Remote diagnostics	System information, logs, configuration and the last 100 commands can be retrieved remotely

6.4 Remote software and configuration updates

Gateways update themselves over the air using two system partitions. The running system is never overwritten, so a failed update cannot leave a tower without a working gateway.



Stage	Behaviour	Status
Download and verify	Image downloaded and checked against its SHA-256 digest; errors reported as download, integrity or write failure	Available
Install	Written to the inactive partition while the tower keeps running	Available
Health gate	New version must confirm it is healthy within 120 s of starting	Available
Automatic rollback	After 3 unconfirmed starts the previous version is restored	Available
Device-side rollout control	Version checks, maintenance windows and per-device canary selection	Available
Fleet strategies	Immediate, scheduled, canary (e.g. 10% first, automatic halt above 10% failures) and staged waves	In validation
Signed update packages	Cryptographic signature verification of every image	Roadmap

Configuration follows the same path. Site profiles, polling settings and alarm parameters are pushed from the cloud and applied without a reboot. The Touch Panel receives screens, languages and content the same way.

6.5 Remote deployment

1	**Prepare**	Gateways are flashed and registered at the factory. Each receives a single-use enrolment token valid for 24 hours.
2	**Install**	The technician mounts the gateway, connects the serial link, power and network. No configuration is entered on site.
3	**Enrol**	At first start the gateway exchanges the token for its own X.509 certificate. The token is then deleted.
4	**Self-check**	The gateway runs its self-test and an acceptance checklist and reports the result to the cloud.
5	**Activate**	The site profile is applied remotely. Monitoring starts immediately; commands are enabled after verification.
6	**Scale**	Further sites with the same controller type reuse the verified profile and are rolled out in stages.

7 Safety concept

Layer	Principle
1. Machine authority	Emergency stops and interlocks stay hard-wired in the original controller. FLUX is designed so it cannot override them.
2. Fault classification	Alarms are classified as they arrive. Safety-relevant faults can never be reset remotely.
3. Human verification	An operator checks the live situation and a safety checklist and approves each remote command. Control sessions are locked to one operator at a time.
4. Hardware fallback	If anything in the FLUX chain fails, watchdog and bypass return the tower to its original configuration.

8 Security

Area	Control	Status
Device identity	Individual X.509 certificate per gateway, issued at enrolment from a single-use token	■ Available
Transport	MQTT over TLS to a managed cloud broker; anonymous access blocked	■ Available
Update integrity	SHA-256 verification, health gate and automatic rollback	■ Available
Command control	Device-side allow-list, emergency-stop interlock, acknowledgement and audit log of issuer and ticket	■ Available
Platform access	Tenant-isolated data, role-based access, multi-factor authentication for operators	■ Available
Data protection	Encryption of sensitive fields at rest, encrypted backups, append-only audit log	■ Available
Development	Automated dependency, code and secret scanning in the build pipeline	■ Available
Hardware key storage	Secure element on the gateway board for key protection	☐ Roadmap
Signed updates and secure boot	Code signing of update images and verified boot chain	☐ Roadmap
Governance	Controls aligned to ISO/IEC 27001 Annex A; external penetration testing	☐ Roadmap

9 Platform and data

Item	Description
Messaging	Managed MQTT broker on AWS IoT Core, TLS on port 8883
Storage	Relational database with time-series extension for telemetry
Retention	Telemetry kept 90 days by default, compressed after 7 days; alarms, commands and update history kept for audit
Interfaces	REST and WebSocket APIs for provisioning, control, telemetry, alarms, updates and fleet statistics
Applications	Owner portal, Operator Console for maintenance companies, administration console
Integration	Partner integrations through the API on request

10 Specifications

FLUX Gateway

Item	Specification
Compute	Quad-core ARM Cortex-A76, industrial carrier board
Controller interface	RS-232 / RS-485, inline with fail-safe bypass
Protocols	LS Master-K, Modbus RTU, automatic identification; others through site profiles
Network	Ethernet, Wi-Fi
Cloud protocol	MQTT over TLS, X.509
Power	DC 9–36 V, supercapacitor hold-up
Operating temperature	–10 to +55 °C (target)
Enclosure	Aluminium, approx. 130 × 110 × 72 mm, DIN rail or wall
Updates	A/B over-the-air with health gate and automatic rollback
Software quality	83 automated tests in the gateway firmware test suite

Preliminary specification. Subject to change. Certification (KC, CE) in preparation; no certification marks are claimed in this document.

11 Deployment and responsibilities

Activity	FLUX	Partner	Owner
Remote site assessment	Lead	Provides data	Grants access
Gateway supply and enrolment	Lead	Receives	
Installation in the cabinet	Trains, supports	Lead	Grants access
Capture and site profile (Path A)	Lead	Supports	
Panel or controller replacement (Path B)	Engineering	Lead on site	Inspection
Remote monitoring and first-line response	Second line	Lead	Informed
Software and profile updates	Lead	Informed	Informed

12 Status and roadmap

FLUX reports the status of each capability openly. The status of every row in this document follows the legend below.

■ Available ■ In validation □ Roadmap ■ Project

Available: implemented and covered by automated tests. In validation: built, field validation in progress. Roadmap: planned for a future release.

Next releases	Target
Field validation of the gateway hardware reference design	2026
Signed update packages and verified boot	Next major release
Secure-element key storage	Next major release
Two-person approval for selected remote commands	Roadmap
AI-assisted site profiling to shorten Path A	Roadmap
Vehicle detection and licence-plate recognition on FLUX Vision	Roadmap

Not disclosed in this document

To protect FLUX's intellectual property and the security of installed sites, this paper does not include protocol grammars, controller address maps, identification and profiling methods, fault-code decision tables, circuit design or internal system addresses. Qualified partners receive the FLUX Integration Specification (FLUX-IS-001) under a non-disclosure agreement.

Contact

FLUX · Gigto Co., Ltd.
contact@fluxmobi.kr · +82 2 6956 5002 · fluxmobi.kr
Headquarters: 5F, 518-4 Bongcheon-ro, Gwanak-gu, Seoul, Republic of Korea
R&D Center: Room 505, 25 Seonyu-ro 13-gil, Yeongdeungpo-gu, Seoul, Republic of Korea