



WHITE PAPER

Unifying Video, Access Control and License Plate Recognition Without a Rip-and-Replace

How to consolidate video, access control and license plate recognition through assessment, coexistence, phased migration, open standards and careful cutover.

By IoT Hybrid Solutions

UNIFIED SECURITY

ACCESS CONTROL

VIDEO MANAGEMENT

LPR

MIGRATION



Executive summary

- Most enterprises run video, access control and license plate recognition (LPR) as separate systems that grew independently. Unifying them improves response, investigations and audit, but a full rip-and-replace is rarely necessary or affordable.

- Start with an assessment of what exists, what is near end of life and what each site actually needs. The assessment drives the phasing, not the other way around.
- Coexistence is a legitimate design state. Federation, gateways and open standards such as OSDP and ONVIF let new and legacy systems run together while hardware is replaced on its natural cycle.
- The identity and data model is the hardest part. Decide early where people, credentials, vehicles and devices are mastered.
- Plan each cutover as a controlled change with rollback, train operators before go-live, and measure success with operational outcomes rather than device counts.

Why consolidate

Separate systems create separate workflows. An operator sees a door forced alarm in one application, finds the camera in another and looks up a vehicle in a third. Investigations take longer, evidence is harder to assemble, and audits require exports from several databases that do not agree.

Common drivers

- **Operator efficiency:** one alarm queue with linked video, maps and cardholder or vehicle context
- **Faster investigations:** search across access events, video and plate reads from one timeline
- **Consistent policy:** one place to define schedules, access levels and vehicle lists across sites
- **Lifecycle pressure:** controllers, recorders or servers approaching end of support
- **Cybersecurity:** retiring unsupported operating systems, legacy protocols and unencrypted reader wiring
- **Mergers and growth:** acquired sites arriving with their own platforms
- **Audit and compliance:** simpler evidence for access reviews and retention policies

Why not rip and replace

Replacing everything at once concentrates cost, risk and disruption. Field hardware such as readers, locks, cameras and cabling often has years of useful life left. A phased approach replaces the platform layer first where it adds value, and replaces field devices as they age or as each site is renovated.

Assessment

A structured assessment gives the program a fact base and keeps the platform decision honest. Remain platform-agnostic until the assessment is complete.

What to inventory

- Video: cameras, recorders, storage, retention settings, analytics, software versions
- Access control: controllers, panels, readers, credential technologies, lock hardware, door count per site
- LPR: cameras, recognition engines, hotlists, integration with gates and parking systems
- Servers, operating systems, databases and licensing
- Network: segmentation, addressing, switching, PoE budget, remote site connectivity
- Integrations: HR and identity systems, visitor management, intercom, alarm panels, mass notification
- Operations: who monitors what, from where, with which procedures

Questions to answer

- Which components are out of support or will be within the planning horizon?
- Which reader and controller hardware can be reused under a new platform, and which is proprietary?
- What credential technology is in use, and is it secure enough to keep?
- Where does cardholder data come from today, and how many sources are there?
- What do operators actually need on screen during an alarm?

Capture the results in an asset register with lifecycle dates. That register becomes the basis for phasing and budgeting.

Coexistence and phased migration

A phased migration lets the program show value early while spreading cost and risk.

Coexistence options

- **Federation:** a unified platform connects to existing video or access systems and presents their events and streams to operators, without migrating them immediately.

- **Gateways and drivers:** manufacturer drivers or middleware let a new platform communicate with legacy controllers or recorders for a transition period.
- **Hardware reuse:** many controllers and readers can be re-hosted on a new platform where the manufacturer supports open or published interfaces.
- **Parallel run:** the old and new systems run side by side for a defined period, with the old one as the fallback.

A typical phasing pattern

1. **Foundation:** stand up the target platform, directory integration, roles and permissions, and federate existing systems.
2. **Operations first:** move alarm monitoring and investigations to the unified console so operators feel the benefit early.
3. **Site by site:** migrate access control and video at each site, prioritizing end-of-life equipment and higher-risk locations.
4. **LPR and specialty integrations:** add plate recognition, gates, intercom and other subsystems once the core is stable.
5. **Decommission:** retire legacy servers and licenses only after data retention obligations are met.

Each phase should have entry criteria, exit criteria and a named owner.

Data and identity model

Unification fails most often on data, not devices. Decide where each record is mastered and how it flows.

Records to model

- **People:** employees, contractors, visitors, mastered in HR or the identity provider
- **Credentials:** card numbers, mobile credentials, PINs, biometric references, mastered in the access platform
- **Access levels and schedules:** mastered in the access platform, ideally driven by role
- **Vehicles:** plates, owners, permits and hotlists, linked to people where policy allows
- **Devices and locations:** cameras, doors, readers and areas, with consistent naming across systems

Good practice

- Automate provisioning and deprovisioning from the authoritative identity source rather than entering cardholders by hand.
- Standardize naming conventions for sites, doors, cameras and areas before migration, then enforce them.
- Define retention for video, access events and plate reads by data type, and confirm it with privacy and legal teams. LPR data in particular can raise privacy considerations, so consult counsel on applicable rules.
- Clean the data before migrating it. Expired cardholders and orphaned access levels should not move to the new platform.

Integration patterns

Open standards and documented interfaces keep the unified system flexible and avoid replacing one lock-in with another.

Open standards

- **OSDP (Open Supervised Device Protocol):** a secure, supervised protocol between readers and controllers. Moving from legacy Wiegand wiring to OSDP with secure channel improves security and allows reader monitoring. Plan for reader and controller compatibility and for any re-termination of cabling.
- **ONVIF:** profiles that let compliant cameras and recorders interoperate across manufacturers. Confirm which profiles and features a device actually supports, since conformance varies by feature.

Platform interfaces

- **SDKs and APIs:** use documented manufacturer SDKs and REST or event APIs for deeper integration, such as linking access events to camera bookmarks or LPR reads to gate control.
- **Event and alarm mapping:** map every source event to a consistent alarm type, priority and response procedure in the unified platform.
- **Directory and single sign-on:** integrate operator authentication with the enterprise identity provider.

Integration checklist

- Documented interface for every subsystem, with version and support status

- Test environment that mirrors production versions
- Defined owner for each integration and for its upgrades
- Monitoring for integration health, not just device health

Cutover planning

Every site cutover is a change to a live security system. Treat it as a controlled change.

Before cutover

- Confirm the door, camera and LPR schedule for the site, including access levels and lock behavior on power loss
- Verify network readiness: VLANs, addressing, PoE and firewall rules. Network and IT configuration is typically the customer's IT team unless the integrator is contracted for it.
- Confirm who performs electrical and low-voltage work, such as lock power, reader re-termination or new cabling. These are typically the customer's trades unless included in the integrator's scope.
- Pre-stage and test controllers and servers off site where possible
- Communicate the schedule to site occupants, reception and the GSOC

During and after cutover

- Cut over in small groups of doors or cameras, verifying each before moving on
- Test every door for valid, invalid, forced and held events, and confirm linked video
- Keep a rollback path until the site passes acceptance
- Hold a post-cutover review and record open items with owners and dates

Operator training

A unified platform changes how operators work. Training should be role-based and scenario-driven.

- Train on real alarm scenarios from your own sites, not generic demos
- Provide quick-reference guides for the top alarm types and investigation tasks
- Train supervisors on reporting, audit exports and permission management
- Schedule training before each go-live and refresh it after major upgrades

- Collect operator feedback in the first weeks and adjust alarm priorities and layouts

Measuring success

Measure outcomes that matter to the security program, and baseline them before the first phase.

- Time from alarm to verified assessment
- Time to assemble evidence for a typical investigation
- Volume of nuisance alarms reaching operators
- Accuracy and timeliness of cardholder provisioning and removal
- Number of platforms, servers and licenses retired
- Audit effort for access reviews
- System health: devices offline, integration failures, time to restore

How IoT Hybrid Solutions can help

IoT Hybrid Solutions helps enterprise security teams assess existing systems, design a target architecture and migrate in phases. We are platform-agnostic and work with platforms such as Genetec Security Center and with hardware ecosystems such as Mercury-based controllers, as examples rather than prescriptions. Our **integration services** cover federation, OSDP and ONVIF integration and cutover, and our **design and engineering** team produces the assessment and migration plan. See also **access control**, **video** and **command and control**.

Next step

If you are weighing a platform change, start with an assessment rather than a replacement. **Contact us** to plan a phased path to a unified system.