

Smart Building & Campus Integration Checklist

Scope a smart-building or campus surveillance build by its integration — which subsystems reach the operator, which standard carries each link, how the campus federates, and where the privacy line falls — before you buy hardware. Companion to the article; pair it with the surveillance cost model.

1 • The rule: the building is one system, the camera is one part

The value is not the cameras; it is whether they talk to the doors, the alarms, and the building. The test of integration: a forced-door event automatically calls up the right camera on one screen and offers a one-click lockdown — instead of an operator hunting through 400 cameras. Decide early between one unified platform (video + access + intrusion in one product) and separate best-of-breed systems joined through standards and SDKs; both can work, but the joins are the project.

2 • Specify the standard on every link

Link	Standard to specify	Note
Video	ONVIF Profile S / T / G	Deep features still need the vendor SDK
Access config	ONVIF Profile A	Credentials, schedules, access rules
Door events	ONVIF Profile C	Open / forced / held; door control
Reader link	OSDP + Secure Channel	IEC 60839-11-5; specify over Wiegand
Metadata	ONVIF Profile M	Analytics events; detection quality varies
Building	BACnet (ISO 16484-5)	HVAC / lighting / lifts / fire link

3 • Campus, multi-tenant & fleet — tick before go-live

- ☐ Federation set: each building records locally and runs analytics at the edge; stream across the network only on demand (do not centralise every stream).
- ☐ Multi-tenant partitions defined per tenant / department, enforced by role-based access control (RBAC) in the permission model and the audit log — not just hidden in the UI.
- ☐ Shared spaces (lobbies, car parks, perimeter) given an explicit owner and a central cross-partition role.
- ☐ Fleet management planned as a system: onboarding, firmware, certificate rotation, password management, and health monitoring for every device.
- ☐ Occupancy / space-utilisation analytics count anonymously (a count, not an identity); prefer non-camera sensors where only utilisation is needed.

4 • Cybersecurity & the privacy gate — tick before you ship

- ☐ Cameras, controllers, and building systems on isolated network segments (VLANs), separated from the corporate network and the internet.
- ☐ Default passwords changed, device certificates rotated, firmware current across the fleet; OSDP Secure Channel used instead of Wiegand.
- ☐ Supply-chain screen applied (US NDAA Section 889 / FAR 52.204-25 named-vendor check where federal funding, contracts, or grants apply).
- ☐ Workplace-monitoring basis documented (GDPR Art. 6(1)(f) + necessity / proportionality; Art. 88 employment rules; staff informed where required).
- ☐ Cameras out of private spaces; clear notice / signage; retention set to the minimum needed (GDPR Art. 5(1)(e)); DPIA where monitoring is systematic and large-scale (Art. 35).
- ☐ Face / fingerprint identification at a door or camera held behind a deliberate legal review — GDPR Art. 9 / Illinois BIPA, not a default toggle.

Engineering guidance, not legal advice. The privacy gate names GDPR Art. 6(1)(f) / 9 / 35 / 88 / 5(1)(e), the EDPB Guidelines 3/2019, and Illinois BIPA (740 ILCS 14) as the controlling frame; confirm specifics with qualified counsel before deploying any workplace or biometric analytic.

Companion to: 'Smart Building and Campus Surveillance'

www.forasoft.com/learn/video-surveillance/articles-vms/smart-building-and-campus-surveillance



GO DEEPER · THE 7-VOLUME HANDBOOK

Fora Soft Video Engineering Handbook

Seven volumes, 9,000+ pages: encoding, streaming, audio and AI for video products — from the pixel to production.

By Nikolay Sapunov, CEO at Fora Soft · Kindle & paperback on Amazon

[Browse the handbook on Amazon →](#)

This checklist scopes a smart-building or campus surveillance build: the integration map, the standard on each link, fleet and privacy gates. We wrote seven volumes on the video stack. Start with Volume 6 for computer vision on camera feeds, then Volume 7 for biometrics and compliance, and Volume 1 for encoding.

WHAT YOU WILL FIND INSIDE

- Computer vision on camera feeds
- Biometrics, GDPR and BIPA compliance
- Edge versus cloud deployment topologies
- Encoding and storage for camera fleets

THE FULL HANDBOOK · 7 VOLUMES · 9,000+ PAGES · ALL ON AMAZON

Vol. 1 · Video Encoding — pixels and color to H.264, HEVC, AV1, quality metrics and AI

Vol. 2 · Video Streaming I — network transport, contribution and ingest, HLS, MPEG-DASH, CMAF

Vol. 3 · Video Streaming II — ABR, CDNs, players, WebRTC, DRM and the economics of delivery

Vol. 4 · Audio for Video I — PCM, codecs, loudness, accessibility, real-time voice processing

Vol. 5 · Audio for Video II — jitter buffers, lip sync, Atmos, quality metrics, neural codecs

Vol. 6 · AI for Video I — models and inference, computer vision, speech, search, generative video

Vol. 7 · AI for Video II — real-time pipelines, agents, serving, cost, compliance, verticals

Integrating cameras, access control and building systems into one pane?

We will map every subsystem link, build the ONVIF, OSDP and BACnet integrations, and ship a single operator view with audit logging. 250+ video products shipped since 2005.

[Book a 30-min call →](#)

[WhatsApp →](#)

[Email us →](#)