

# Design, Analytical Dimensioning and Field Evaluation of a Low-Cost IP-Camera and DVR Security Monitoring System for a University Computer Engineering Laboratory

Owigho Benedicta, Edward O. Odesa, Omolegho A. Ibok, Jones U. Ekwemuka

Department of Computer Engineering, Faculty of Engineering, Southern Delta University, Ozoro, Delta State, Nigeria

**Abstract-** University computer-engineering laboratories contain high-value technology, but in resource-constrained settings, they are typically protected solely by locks, attendance registers, and manual supervision, none of which provide a continuous record of events. The design, analytical dimensioning, and field testing of an Electronic Laboratory Security Monitoring System (ELSMS) built from commercially available parts consisting of three 2-megapixel IP cameras, a Gigabit Ethernet switch, an 8-channel DVR with a 1 TB surveillance drive, Cat6 cabling, a regulated supply, and a 650 VA UPS are presented in this paper. The system is dimensioned using closed-form models for camera coverage, pixel-density-based identification range, storage retention, network load, and dependability. With the specified 1920-pixel sensors, identification-grade pixel density (250 px/m) is only achievable within 2.2-3.8 m of a camera (120°-90° field of vision); three cameras load less than 2% of a gigabit link; and 1 TB offers roughly 7.7 days of continuous recording at 4 Mbit/s per camera (15.4 days at 2 Mbit/s). 83 of the 86 structured tests were successful (96.5%; 95% Wilson CI 90.2-98.8%). Nine out of ten controlled occurrences were found, the recording and network tests each reported one failure in thirty tries, and the camera-coverage, video-quality, and playback tests all passed. The lag between display and recording was roughly two seconds. The findings demonstrate that evidence-grade picture detail, recording retention, and power autonomy rather than network capacity are the binding design limitations and validate the architecture's appropriateness for low-cost deployment. The models are reusable by other institutions.

**Keywords:** : laboratory security; IP camera; digital video recorder; storage dimensioning; pixel density; structured cabling; video surveillance; Nigeria

## I. INTRODUCTION

Computer engineering laboratories combine computers, servers, networking hardware, embedded-system kits, and test instruments in a single space that is heavily used by students, technicians, and visiting faculty. This equipment's worth and portability make it a prime target for theft and damage, and the open-access working pattern of a teaching laboratory makes unauthorized use difficult to identify and attribute. Conventional controls such as locks, guards, and handwritten registers record who was supposed to be present rather than what actually happened. Continuous video surveillance is the apparent solution, but human monitoring alone is insufficient. Kim et al. [1], citing previous research, state that when one person monitors multiple CCTV

feeds, approximately 45% of incidents are missed after 10 minutes and almost 95% after 22 minutes.

Recorded video is thus less useful as a live-viewing assistance than as an evidence record that can be searched after an incident. For this job, the practical questions are concrete: can the cameras resolve a face or an item well enough to be helpful, how many days of footage will the recorder store, will the network and power arrangements keep the system going, and how reliable is the entire chain? In the majority of new installations, IP-based surveillance has taken the place of analog CCTV, as reviewed in a number of recent studies [2], [3], and [4]. The change offers flexibility and remote access, but it also creates a much larger attack surface than analog systems [5]. Botnets like Mirai, which at one point had about 600,000 infected, mostly Internet-

of-things and embedded devices, have frequently targeted networked surveillance equipment [6]. A significant portion of current research focuses on cloud architectures, deep learning, and video analytics [2, 3, 4].

Comparatively little guidance addresses the engineering arithmetic a small institution needs when it specifies a single-laboratory system on a limited budget and an unreliable electricity supply: how wide-angle lenses trade coverage against image detail, how much disk is needed, and how much network headroom exists. Outage data for Nigerian distribution feeders illustrate the power problem; a recent analysis of medium-voltage feeders in one Nigerian city reported load-shedding and forced outages typically lasting about six hours [7]. The design and assessment of an ELSMS for a University in Nigeria, is described in this study. The contributions consist of:

- a bill of materials and reference architecture for an extendable, three-camera, eight-channel laboratory surveillance system constructed from commodity parts;
- an analytical dimensioning framework that connects bitrate and disk capacity to recording retention, network load, and reliability, and the camera specification to coverage width, pixel density, and identification range; the framework produces design conclusions that are not obvious from the datasheet alone;
- a field evaluation of 86 structured tests, reported with small-sample confidence intervals rather than plain percentages; and
- A critical analysis of the constraints that dictate the direction of future engineering efforts..

## II. BACKGROUND AND RELATED WORK

### 1. Surveillance system architecture

Tsakanikas and Dagiuklas [2] outline the evolution from basic capture-and-display systems to distributed, edge- and cloud-assisted analytics, characterizing a contemporary video surveillance system as a chain of acquisition devices, processing and analysis modules, and storage units. Elharrouss et al. [3] examine architectures, components, and

analysis tasks and contrast the features, benefits, and challenges of current systems. A comprehensive survey of intelligent video surveillance research spanning methods, frameworks, and datasets is given by Shidik et al. [4]

### 2. Video compression and storage

The bitrate generated by the encoder controls recording retention. H.264/AVC [8] is the long-established coding standard for surveillance recorders, while High Efficiency Video Coding (HEVC, H.265) was meant to deliver much enhanced compression, in the region of 50% bitrate reduction for equivalent perceived quality relative to prior standards [9]. HEVC encoders obtained comparable subjective quality to H.264/AVC at an average bitrate of roughly 50%, according to subjective testing published by Ohm et al. [10]. Since the encoder and content determine actual savings on surveillance scenes, bitrate is treated as a parameter rather than a constant in the storage models.

### 3. Security and dependability of IP surveillance

Kalbo et al. [5] review the attack surface of IP-based surveillance systems, identifying threat agents, attack goals, attack vectors and consequences, and discuss countermeasures and best practice. Their conclusion that IP systems are far more complex than analogue ones, and hence more exposed, motivates the network-isolation and hardening choices.

### 4. Evaluation practice

Venetianer and Deng [11] present a case study and best-practice guidance for evaluating intelligent video surveillance systems. Kim et al. [1] report detection rates for an embedded surveillance system (88.51% for intruder detection, 92.63% for fire detection, 80% for loitering detection and 93.54% for fall detection) using dedicated datasets and real-time trials. Field evaluations of small installations, however, often report success percentages from a few trials without any indication of statistical uncertainty. With trial counts as small as those in this study, the Wilson score interval is preferable to the normal-approximation interval [12], and it is used throughout.

## 5. Gap addressed

Within the sources reviewed, we did not find a worked treatment that combines (i) the coverage and pixel-density geometry of the installed lenses, (ii) storage and network dimensioning, and (iii) a counted field evaluation for a single teaching laboratory operating under unstable power. This paper provides one.

## III. SYSTEM DESIGN

### 1. Requirements and constraints

The design used a systems-design method encompassing requirement analysis, modeling, hardware selection, integration and testing. The functional requirements were continuous video surveillance, real-time monitoring, centralised recording and playback of footage for incident investigation, and coverage of entry and exit points, equipment storage zones and general workspaces. The non-functional requirements were reliability, cost-effectiveness, ease of installation and low maintenance. Two constraints shaped the design: a

limited budget and modest technical infrastructure, and the need to keep operating, at least in recording mode, when the electricity supply or the campus network is unstable.



Figure 1. Architecture of the ELSMS. Three IP cameras (1–3) connect through a Gigabit Ethernet/PoE-capable switch to an 8-channel DVR with a 1 TB surveillance drive; channels 4–8 are reserved for expansion. The power path (dashed lines) runs through a regulated 12 V supply and a 650 VA UPS

Table 1 lists the components and their key specifications. Components were chosen for reliability, compatibility, affordability and local availability

| Component                     | Key specification                                                                                                            | Role                                                                  |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| IP camera (×3)                | 2 MP, 1920 × 1080; CMOS; 90°–120° view; IR night vision up to 20 m; RJ45; 12 V DC; H.264/H.265                               | Image acquisition at entrance, workstation area and rear/storage area |
| 8-channel DVR                 | 8 channels; H.264/H.265; HDMI/VGA output; up to 6 TB HDD; continuous, scheduled and motion recording; multi-channel playback | Central encoding, recording, playback                                 |
| Surveillance HDD              | 1 TB; SATA III; 5400-7200 rpm; rated for continuous recording                                                                | Video storage                                                         |
| Ethernet switch               | 8-port, 10/100/1000 Mbit/s; plug-and-play; PoE-capable unit used in the rack                                                 | Interconnects cameras, DVR and PC                                     |
| Cat6 UTP cable                | 250 MHz; up to 1 Gbit/s; 100 m maximum channel; RJ45-terminated                                                              | Physical transmission medium                                          |
| Power                         | Regulated 12 V DC supply; 650 VA UPS                                                                                         | Stable supply; ride-through of short outages                          |
| Monitor and PC                | 19-22 in LED monitor; PC with Intel Core i3/i5 and at least 4 GB RAM                                                         | Live view; configuration and maintenance                              |
| Mounting and cable management | Adjustable brackets; PVC trunking and cable clips                                                                            | Camera aiming; cable protection                                       |

## 2. Architecture

Figure 1 shows the system architecture. Three IP cameras connect over Cat6 cabling to an 8-port Gigabit Ethernet switch, which carries the video streams to an 8-channel DVR. Each camera is assigned to one DVR channel, and the DVR encodes (H.264/H.265), records to an internal 1 TB surveillance hard disk drive, and drives a local monitor for live view.

A management PC on the same local network is used for configuration, remote viewing and maintenance. The five unused channels allow expansion without changing the recorder. A regulated 12 V DC supply and a 650 VA UPS power the equipment. The DVR used here accepts IP camera inputs (a hybrid recorder).

## 4. Camera placement and installation

IP Camera 1 (a dome camera) covers the entrance; IP Camera 2 (a bullet camera) covers the workstation and equipment area; and IP camera 3 covers the rear and storage area (Figure 2). Placement was driven by entry and exit points, equipment arrangement and the areas needing high-level monitoring.

Cables were run in PVC trunking and secured with cable clips to protect them from the frequent movement of students and equipment; the switch was mounted in a rack with structured patching, and the UPS was placed beside the rack (Figure 3).



Figure 2. Installed cameras: (a) entrance camera; (b) camera covering the workstation and equipment area; (c) camera covering the rear/storage area.



Figure 3. Installed hardware: (a) 8-channel DVR with live-view monitor; (b) rack-mounted network switch with Cat6 patching; (c) cable trunking; (d) UPS beside the equipment rack.

## IV. ANALYTICAL DIMENSIONING

The models used are derived to size the system. The parameters are those of Table 1. The 90°–120° view range is treated as the horizontal field of view; if the datasheet value is diagonal, the horizontal field of view is smaller and all range figures below shrink accordingly.

### 1. Coverage geometry

For a camera at distance  $D$  from a fronto-parallel scene plane, the pinhole model [13] gives the width of the scene covered:

$$W = 2 \cdot D \cdot \tan(\theta/2) \quad (1)$$

Where,  $\theta$  is the horizontal field of view. The covered floor area is approximately

$$A = W \times L \quad (2)$$

Where,  $L$  is the depth of the region of interest. Wider lenses cover more floor but spread the same 1920 pixels over a larger width, reducing pixel density  $\rho = N_h / W$ , where  $N_h = 1920$  is the horizontal pixel count. Table 2 illustrates the trade-off.

## 2. Pixel density and identification range

Coverage is not the same as usefulness. IEC 62676-4 [14] defines operational requirements in terms of pixel density on the subject: about 25 px/m to detect, 63 px/m to observe, 125 px/m to recognise and 250 px/m to identify an individual (values as tabulated in a manufacturer white paper based on the 2014 edition [15]; the standard was revised in 2025 with updated terminology, so the thresholds

should be re-checked against the edition that applies when the system is certified). These thresholds apply to images interpreted by human operators. Setting  $\rho$  equal to the required density and solving Eq. (1) gives the maximum distance at which a requirement is met

$$D_{\max} = N_h / (2 \cdot \rho_{\text{req}} \cdot \tan(\theta/2))$$

Table 2. Coverage width  $W$  (Eq. 1) and horizontal pixel density  $\rho$  for a 1920-pixel sensor

| Distance $D$ (m) | $W$ at $90^\circ$ (m) | $\rho$ at $90^\circ$ (px/m) | $W$ at $120^\circ$ (m) | $\rho$ at $120^\circ$ (px/m) |
|------------------|-----------------------|-----------------------------|------------------------|------------------------------|
| 3                | 6.0                   | 320                         | 10.4                   | 185                          |
| 5                | 10.0                  | 192                         | 17.3                   | 111                          |
| 8                | 16.0                  | 120                         | 27.7                   | 69                           |
| 10               | 20.0                  | 96                          | 34.6                   | 55                           |

Table 3. Maximum distance at which each operational requirement is met by a 1920-pixel camera (Eq. 3).

| Requirement | Required density (px/m) | $D_{\max}$ at $90^\circ$ (m) | $D_{\max}$ at $120^\circ$ (m) |
|-------------|-------------------------|------------------------------|-------------------------------|
| Detect      | 25                      | 38.4                         | 22.2                          |
| Observe     | 63                      | 15.2                         | 8.8                           |
| Recognise   | 125                     | 7.7                          | 4.4                           |
| Identify    | 250                     | 3.8                          | 2.2                           |

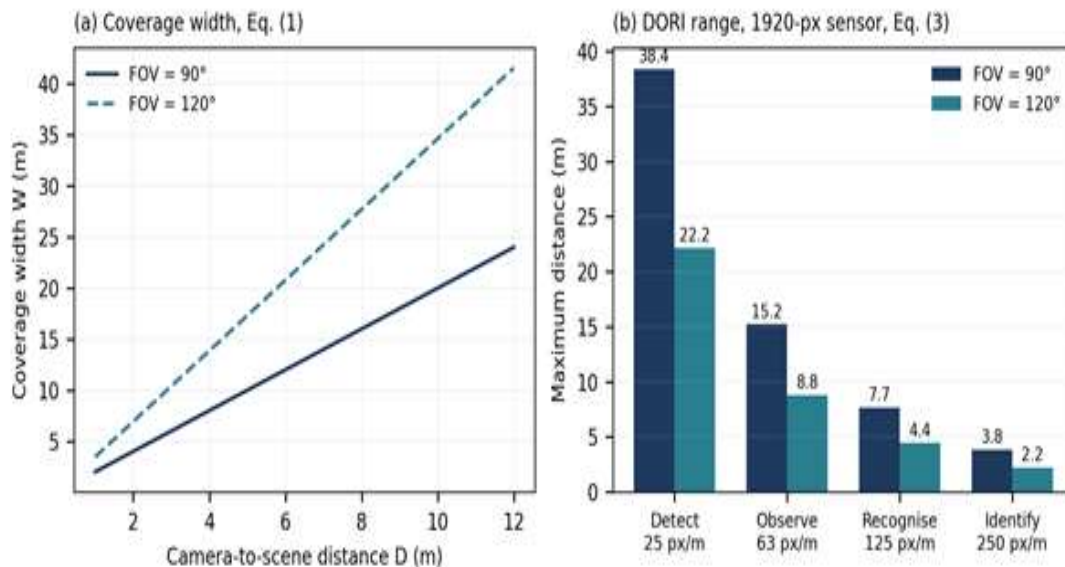


Figure 5. (a) Coverage width against distance for  $90^\circ$  and  $120^\circ$  lenses (Eq. 1). (b) Maximum distance for each IEC 62676-4 operational requirement for a 1920-pixel sensor (Eq. 3).

The consequence is significant for a laboratory. A 2 MP camera with a wide lens supports identification of a person only within about 2.2 m ( $120^\circ$ ) to 3.8 m ( $90^\circ$ ) of the camera, and recognition within about

4.4–7.7 m. The entrance camera should therefore be mounted close to the door frame and aimed along the line of entry, as in Figure 2a; a camera covering a whole workstation row from across the room will

detect and observe activity but will not, on its own, supply identification-grade evidence. Narrower lenses, higher-resolution sensors (4 MP or above) or a dedicated identification camera at the entrance are the options when evidential identification of every entrant is required.

### 3.Storage and retention

For  $N$  cameras each producing a constant bitrate  $B$  (bit/s), the storage consumed over time  $T$  (s) is

$$S = B \cdot T \cdot N / 8 \text{ (bytes)}$$

and the continuous-recording retention for a disk of capacity  $C$  (bytes) is

$$T_{\text{ret}} = 8 \cdot C / (N \cdot B \cdot 86400) \text{ (days)}$$

Capacities are expressed in decimal bytes: a nominal 1 TB drive holds 1012 bytes, which is 931 GiB, so dividing by 10243 as a conversion to “GB” would understate the mismatch between nominal and usable capacity. Table 4 gives retention for typical 1080p H.264 bitrates.

Table 4. Daily data volume and continuous-recording retention (Eq. 5).

| Cameras $N$ | Bitrate $B$ (Mbit/s) | Data per day (GB) | Retention, 1 TB (days) | Retention, 6 TB (days) |
|-------------|----------------------|-------------------|------------------------|------------------------|
| 3           | 2                    | 64.8              | 15.4                   | 92.6                   |
| 3           | 4                    | 129.6             | 7.7                    | 46.3                   |
| 3           | 6                    | 194.4             | 5.1                    | 30.9                   |
| 8           | 2                    | 172.8             | 5.8                    | 34.7                   |
| 8           | 4                    | 345.6             | 2.9                    | 17.4                   |
| 8           | 6                    | 518.4             | 1.9                    | 11.6                   |

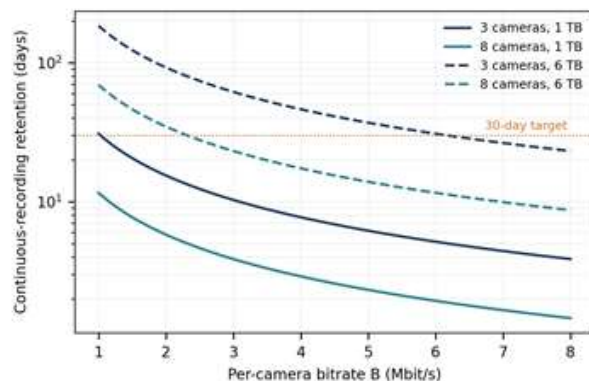


Figure 6. Continuous-recording retention against per-camera bitrate for 3 and 8 cameras on 1 TB and 6 TB disks (Eq. 5). The dotted line marks a 30-day target.

Three findings follow. First, the 1 TB drive provides about one week of continuous recording at 4 Mbit/s per camera; this is the tightest design margin. Second, because HEVC can deliver comparable quality at roughly half the bitrate [9], [10], enabling H.265 on the recorder approximately doubles retention. Third, motion-triggered recording with duty cycle  $\delta$  (fraction of time recording) multiplies retention by  $1/\delta$ ; for three

cameras at 4 Mbit/s,  $\delta = 0.25$  gives about 31 days on 1 TB. Full expansion to eight cameras at the same bitrate would cut 1 TB retention to under three days, so storage must grow with the camera count up to the recorder’s 6 TB limit. Retention is also a data-protection decision (Section 7.4), not only a storage one.

### 4. Network load

The aggregate stream load is

$$BW = N \cdot B$$

For three cameras at 4 Mbit/s this is 12 Mbit/s, about 1.2% of a 1 Gbit/s link; for eight cameras at 6 Mbit/s it is 48 Mbit/s (4.8%). The switch backplane and the Cat6 cabling (rated to 1 Gbit/s over 100 m) therefore have ample headroom, and the network is not a capacity bottleneck at this scale

### 5. Reliability and power

Taking a constant failure rate  $\lambda$ , the probability that a component operates without failure for time  $t$  is

$$R(t) = e^{-\lambda t}, \text{ MTBF} = 1/\lambda$$

[17]. For components that must all work, reliabilities multiply, so failure rates add:  $R_{\text{sys}}(t) = \exp(-\Sigma \lambda_i t)$ . In

the ELSMS the DVR, the hard disk drive, the switch and the power chain are single points of failure, whereas the loss of one camera degrades coverage but not recording. To achieve  $R \geq 0.99$  over 30 days (720 h), the combined failure rate must satisfy  $\lambda \leq 1.4 \times 10^{-5} \text{ h}^{-1}$ , that is, a system MTBF of at least about 71,600 h.

Power is the most likely cause of loss of recording. A UPS bridges an outage for a time

$$t_{\text{run}} = E_b \cdot \text{DoD} \cdot \eta / P_L$$

Where,  $E_b$  is the usable battery energy, DoD the permitted depth of discharge,  $\eta$  the inverter efficiency and  $P_L$  the load. Outages of around six hours [7] far exceed what a small 650 VA unit is designed to bridge, so the UPS here provides ride-through and orderly operation rather than autonomy. Extended battery banks or an inverter-battery system would be needed for multi-hour autonomy.

## 6. Evaluation metrics

Two metrics are used in the field evaluation. Surveillance efficiency is the monitored fraction of the laboratory area,  $E = (A_m/A_t) \times 100\%$ , and detection probability is  $P_d = N_d/N_t$ , the fraction of controlled events that were detected.

# V. FIELD EVALUATION METHOD

## 1.Test families

The installed system was evaluated through six families of tests comprising 86 tests in total (Table

5). The coverage test checked whether each of the three cameras monitored its assigned area (3 tests, one per camera), and the video-quality test assessed the clarity of each camera's image (3 tests). The recording test (30 trials) and playback test (10 trials) checked that the DVR stored footage and could retrieve it. The network test (30 trials) checked transmission of video between cameras and recorder. The incident-detection test (10 trials) used controlled movement and access activities within the monitored areas.

In addition, unit tests of each component, integration tests of the combined hardware, functional tests of required operations and a ten-indicator performance assessment were carried out, together with acceptance testing by administrators in a simulated laboratory setting. Response time was taken as the time from an activity entering a camera's field of view to its appearance on the monitor and in the recording.

## 2.Statistical treatment

For a test family with  $k$  successes in  $n$  trials, the success rate is  $\hat{p} = k/n$ , and a 95% Wilson score interval [12] is reported because  $n$  is small and some rates are at or near 100%. The pooled rate over all 86 tests is given for completeness but is descriptive only, since the families differ in difficulty and in their numbers of trials

# VI. RESULTS

Table 5. Field-test results with 95% Wilson intervals

| Evaluation criterion  | Successes / tests | Success rate (%) | 95% interval (%) |
|-----------------------|-------------------|------------------|------------------|
| Camera coverage       | 3/3               | 100.00           | 43.9-100.0       |
| Video quality         | 3/3               | 100.00           | 43.9-100.0       |
| DVR recording         | 29/30             | 96.67            | 83.3-99.4        |
| Video playback        | 10/10             | 100.00           | 72.2-100.0       |
| Network communication | 29/30             | 96.67            | 83.3-99.4        |
| Incident detection    | 9/10              | 90.00            | 59.6-98.2        |
| Total (pooled)        | 83/86             | 96.51            | 90.2-98.8        |

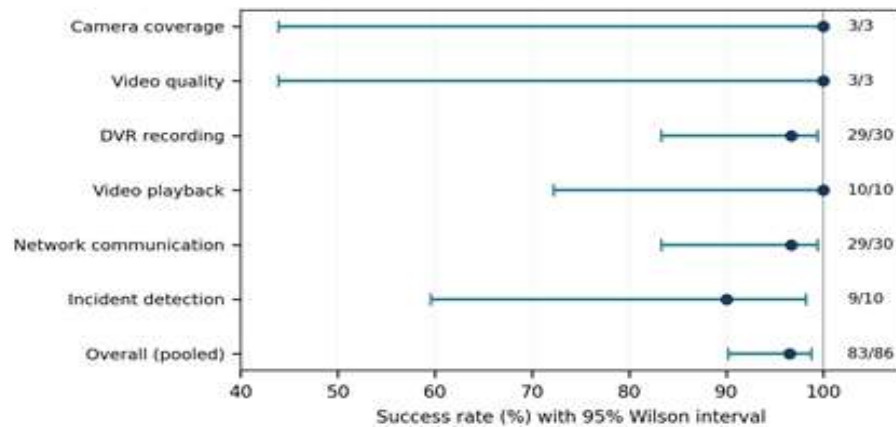


Figure 7. Success rate per test family with 95% Wilson intervals (points: observed rate; bars: interval). Labels give successes/tests

Of 86 tests, 83 succeeded (96.51%; 95% interval 90.2–98.8%). All coverage, video-quality and playback tests passed. One of 30 recording trials and one of 30 network trials failed (each 96.67%; interval 83.3–99.4%), and one of ten controlled incidents was not detected (90%; interval 59.6–98.2%), giving a detection probability  $P_d = 0.90$ . The intervals make the evidential weight of the small families explicit: 3/3 successes is consistent with true success rates as low as 44%, and even 10/10 playback successes is consistent with rates down to 72%. The causes of the three failures were not diagnosed in the trials; the missed incident may

relate to camera position or lighting, but this was not tested.

All eight integration tests and all five functional tests passed (Table 6), and all ten performance indicators, covering real-time transmission, video quality, recording, storage, retrieval, responsiveness, power stability, network stability and overall reliability, were assessed as satisfactory. Mean display-and-record latency was about 2 s, consistent with near-real-time operation. The UPS kept the system operating through power fluctuations and interruptions in the tests, although the outage durations were not recorded

Table 6. Integration and functional tests (all passed)

| Integration tests (8/8)         | Functional tests (5/5)                     |
|---------------------------------|--------------------------------------------|
| IP camera–DVR connection        | Unauthorised-access monitoring (simulated) |
| Live video display              | Motion detection                           |
| Multi-camera video processing   | Continuous monitoring                      |
| Video recording                 | Live monitoring through the web dashboard  |
| Software video-stream access    | Video playback and retrieval               |
| Motion detection                | -                                          |
| Database storage                | -                                          |
| Hardware–software communication | -                                          |

## VII. DISCUSSION

### 1. What the dimensioning shows

The field tests indicate that the chain from camera to recorder to playback works reliably at this scale. The dimensioning models explain where the design is nevertheless thin. Identification-grade pixel

density is achievable only within a few metres of a camera (Table 3), so the footage will usually suffice to establish that an event occurred, where and roughly by whom, but not to identify a person who is more than a few metres away.

One week of continuous retention at plausible bitrates (Table 4) is short for an institution that may

notice a loss only after a vacation. Network capacity is not a concern. These findings are design-level and follow from the specifications, independently of the test results; they are the main practical lesson for other laboratories.

## 2. Improving retention and power

Three low-cost measures would extend retention: enabling H.265 [9], [10], using motion- or schedule-based recording, and adding disk capacity up to the DVR's 6 TB limit. For power, the long outages reported for Nigerian feeders [7] mean that a 650 VA UPS cannot be relied on beyond short interruptions; sizing the battery with Eq. (8) from a measured load is the first step, and an inverter-battery system the next.

## 3. Network security

Because IP cameras and recorders are attractive botnet targets [5], [6], the camera network should be isolated from the general campus network, default credentials changed, unused services disabled, firmware kept current and the recorder not exposed directly to the Internet. These measures are consistent with the countermeasures and best-practice discussion in [5]. Remote viewing, where needed, should be provided through a VPN or another authenticated gateway.

## 4. Limitations

Single site and small trial counts: several test families have 3-10 trials, giving wide intervals (Table 5).

- No false-alarm measurement and no diagnosis of the three failed tests.
- Latency is summarised by an approximate mean; its spread and the measurement protocol are not reported.
- No longitudinal failure-rate data, so the reliability model sets a target rather than an estimate; UPS autonomy and night-time (infrared) image quality were not quantified.
- Dimensioning uses scenario bitrates and assumes that the 90°-120° specification is the horizontal field of view.
- The system is scoped to a single laboratory and excludes facial recognition, cloud storage and mobile application development.

# VIII. CONCLUSION

A three-camera, 8-channel IP-camera and DVR security monitoring system was designed, installed and evaluated for a university computer-engineering laboratory. In 86 structured tests, 83 succeeded (96.5%; 95% interval 90.2-98.8%), and 9 of 10 controlled incidents were detected. The analytical models show that the system's real constraints are identification range (2.2-3.8 m at 250 px/m), recording retention (about 7.7 days on 1 TB at 4 Mbit/s per camera) and power autonomy, not network capacity. Future work should repeat the evaluation with more trials across lighting conditions, report false-alarm rates and latency distributions, measure UPS runtime and failure rates over a long period, and test the retention and identification improvements identified here.

# REFERENCES

1. J. S. Kim, M.-G. Kim, and S. B. Pan, "A study on implementation of real-time intelligent video surveillance system based on embedded module," *EURASIP J. Image Video Process.*, vol. 2021, Art. no. 35, 2021, doi: 10.1186/s13640-021-00576-0.
2. V. Tsakanikas and T. Dagiuklas, "Video surveillance systems—current status and future trends," *Comput. Electr. Eng.*, vol. 70, pp. 736–753, 2018, doi: 10.1016/j.compeleceng.2017.11.011.
3. O. Elharrouss, N. Almaadeed, and S. Al-Maadeed, "A review of video surveillance systems," *J. Vis. Commun. Image Represent.*, vol. 77, Art. no. 103116, 2021, doi: 10.1016/j.jvcir.2021.103116.
4. G. F. Shidik, E. Noersasongko, A. Nugraha, P. N. Andono, J. Jumanto, and E. J. Kusuma, "A systematic review of intelligence video surveillance: Trends, techniques, frameworks, and datasets," *IEEE Access*, vol. 7, pp. 170457–170473, 2019, doi: 10.1109/ACCESS.2019.2955387.
5. N. Kalbo, Y. Mirsky, A. Shabtai, and Y. Elovici, "The security of IP-based video surveillance

- systems," *Sensors*, vol. 20, no. 17, Art. no. 4806, 2020, doi: 10.3390/s20174806.
6. M. Antonakakis et al., "Understanding the Mirai botnet," in *Proc. 26th USENIX Security Symp.*, Vancouver, BC, Canada, 2017, pp. 1093–1110.
7. G. Akinsipe, "160 days in the dark: Understanding electricity unreliability in Nigeria," *Energy for Growth Hub*, Memo, Feb. 2025. [Online]. Available: <https://energyforgrowth.org/article/160-days-in-the-dark-understanding-electricity-unreliability-in-nigeria/>
8. T. Wiegand, G. J. Sullivan, G. Bjøntegaard, and A. Luthra, "Overview of the H.264/AVC video coding standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 7, pp. 560–576, Jul. 2003, doi: 10.1109/TCSVT.2003.815165.
9. G. J. Sullivan, J.-R. Ohm, W.-J. Han, and T. Wiegand, "Overview of the High Efficiency Video Coding (HEVC) standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 12, pp. 1649–1668, Dec. 2012, doi: 10.1109/TCSVT.2012.2221191.
10. J.-R. Ohm, G. J. Sullivan, H. Schwarz, T. K. Tan, and T. Wiegand, "Comparison of the coding efficiency of video coding standards—Including High Efficiency Video Coding (HEVC)," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 12, pp. 1669–1684, Dec. 2012.
11. P. L. Venetianer and H. Deng, "Performance evaluation of an intelligent video surveillance system—A case study," *Comput. Vis. Image Underst.*, vol. 114, no. 11, pp. 1292–1302, 2010, doi: 10.1016/j.cviu.2010.07.010.
12. L. D. Brown, T. T. Cai, and A. DasGupta, "Interval estimation for a binomial proportion," *Stat. Sci.*, vol. 16, no. 2, pp. 101–133, 2001, doi: 10.1214/ss/1009213286.
13. R. Hartley and A. Zisserman, *Multiple View Geometry in Computer Vision*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2004.
14. *Video Surveillance Systems for Use in Security Applications—Part 4: Application Guidelines*, IEC 62676-4:2014, International Electrotechnical Commission, Geneva, Switzerland, 2014. (A revised edition, IEC 62676-4:2025, has since been published with updated terminology.)
15. Axis Communications, "Pixel density based on IEC 62676-4:2014: Meeting operational requirements in network video," White paper, Oct. 2025. [Online]. Available: <https://whitepapers.axis.com>
16. *IEEE Standard for Information Technology—Local and Metropolitan Area Networks—Specific Requirements—Part 3: CSMA/CD Access Method and Physical Layer Specifications—Amendment 3: Data Terminal Equipment (DTE) Power via the Media Dependent Interface (MDI) Enhancements*, IEEE Std 802.3at-2009, Oct. 2009.
17. A. Birolini, *Reliability Engineering: Theory and Practice*, 8th ed. Berlin, Germany: Springer, 2017.