



SMART SECURITY | SPECIAL REPORT

SPECIAL REPORT

# What Can an AI Security Camera Actually See?

*Smarter alerts, faster searches and the limitations buyers are seldom told about*

A practical guide for South African SMEs deciding whether intelligent video analytics will improve security—or simply add another feature to the quotation.

JULY 2026 • EDUCATIONAL BUSINESS TECHNOLOGY REPORT

## EXECUTIVE SUMMARY

# Executive Summary

An “AI camera” is not a camera that understands a business, recognises every threat or makes reliable security decisions on its own. In most commercial systems, AI means that software analyses video to classify objects, apply defined rules and create searchable event information.

**The central buying question:** Do not begin with “Which AI camera should we buy?” Begin with “Which event must the system detect, under what conditions, who will verify it, and what will happen next?”

1. **Useful functions** include distinguishing people from vehicles, detecting movement across a virtual line, alerting when someone remains in a restricted zone, searching recordings by event, and reading number plates where the camera and scene are designed for it.
2. AI can reduce nuisance alerts, but it can also miss genuine events. Camera position, lighting, weather, object speed, obstructions and configuration affect performance.
3. Remote viewing and alerts depend on more than the camera. The PoE switch, recorder, storage, router, fibre link and backup power all form part of the security system.
4. Important alerts still need a trained person to confirm what happened and decide on the response. Detection is not the same as understanding intent.
5. Footage that identifies people, vehicles or behaviour must be managed with a clear purpose, controlled access, appropriate retention and reasonable security safeguards.

The value of intelligent CCTV is therefore not the AI label. It is whether the system produces usable evidence and useful alerts at the customer’s actual site—during the day, at night, in poor weather and during realistic power or connectivity failures.

## MAIN ARTICLE

# What Can an AI Security Camera Actually See?

*The practical difference between detecting movement, classifying an object and understanding an incident*

Imagine that movement is detected at the back fence of a small warehouse at 02:17. A conventional motion rule may react to a person, a dog, a branch or a change in light. A well-configured analytics system can try to classify the object, apply an after-hours rule and send a short clip to the responsible person. That is useful. It is also much less dramatic than the phrase “AI-powered security” suggests.

The camera has not decided that a crime is taking place. It has identified patterns in an image, compared them with a trained model and applied a rule. A person must still check the scene, consider the context and decide whether to call a guard, contact a manager or dismiss the alert.

## 1 What “AI” usually means in a camera system

In this market, AI usually refers to computer-vision analytics. The analysis may run inside the camera, on the network video recorder, on a local server or in the cloud. When it runs inside the camera it is often called edge analytics. Edge processing can reduce the need to send every frame elsewhere and can produce fast local events, but it does not remove the need for power, recording, maintenance or a working route for remote alerts. [1]

The software is trained to recognise selected visual patterns. It may classify an object as a person or vehicle, determine whether it crossed a virtual boundary, measure how long it remained in a zone, or attach metadata that makes the recording easier to search. Different products support different combinations, and some features require specific cameras, recorders, licences or subscriptions.

## 2 What the system can usefully detect

The most useful functions are usually narrow and specific. They work best when the buyer defines the event before choosing the equipment.

| Capability               | What is analysed                                    | Practical use                                                                                  |
|--------------------------|-----------------------------------------------------|------------------------------------------------------------------------------------------------|
| Object classification    | Person, vehicle or selected vehicle type            | Filters ordinary motion events so the team can focus on the objects that matter.               |
| Rule-based alert         | Line crossing, entry into a zone or time in an area | Flags a defined event at a defined place and time; it does not determine criminal intent.      |
| Smart search             | Recorded events and object metadata                 | Reduces the time spent dragging through hours of footage. Search attributes vary by system.    |
| Number-plate recognition | A readable plate image converted into text          | Supports vehicle logs, gate rules and investigations when the capture conditions are suitable. |
| Image-health alert       | Blur, obstruction, redirection or underexposure     | Warns that a camera view may be degraded. This is available only on some platforms.            |

*Examples are based on current vendor documentation and are not a statement that every camera or recorder includes these functions. [1] [2] [4]*

For a small warehouse, the useful requirement may be: “Alert the duty manager if a person enters the fenced loading area between 20:00 and 05:00, and keep video from thirty seconds before and after the event.” That is testable. “Provide intelligent perimeter security” is not.

### 3 Detection is not understanding

A camera may detect that a person is running. It does not know whether the person is escaping from a robber, rushing to help a colleague or trying to catch a closing gate. A system may detect that someone remained near a storeroom door for three minutes. It does not know whether the person is loitering or waiting for authorised access.

This distinction matters because marketing language sometimes moves too quickly from “detects a person” to “detects suspicious behaviour.” The first claim can be tested against defined conditions. The second depends heavily on context and human judgement.

Even object classification is not infallible. A person may be partly hidden, carrying a large box, moving too quickly or appearing too small in the image. Vendor guidance acknowledges that analytics can generate false detections and can also miss alarms. It recommends evaluating performance at each site and keeping a person involved in important decisions. [1]

### 4 Why good analytics fail at real sites

The algorithm receives only the image the installation gives it. If the image is weak, the analysis will be weak.

**Camera position.** A wide view may look impressive on a monitor while leaving each person too small for reliable classification. A camera aimed too high may record the tops of heads but not useful identifying detail.

**Lighting.** Bright headlights, strong backlighting, darkness, reflections and dirty camera covers can reduce image usability. A colour image that looks acceptable to a person is not automatically suitable for analytics.

**Distance and speed.** The software needs enough usable frames to detect and classify an object. A fast vehicle or a person passing close to the camera may leave the field of view before the rule is triggered.

**Obstructions.** Trees, parked vehicles, shelving, walls, rain, spider webs and objects carried in front of the body can hide the features the model needs.

**Scene changes.** A delivery container, new fence, seasonal vegetation or relocated light can change the scene after commissioning. Analytics need physical inspection and periodic re-testing, not only remote viewing.

**Configuration.** Detection zones, minimum object size, schedules, sensitivity, pre-event recording and post-event recording all affect what the customer receives.

**Important trade-off:** Tighter filters may reduce nuisance alerts, but a system that records only AI-classified events may also fail to retain something important. For higher-risk areas, consider continuous or conventional motion recording alongside intelligent alert filtering. Current Axis guidance makes this same distinction. [2]

### 5 Number-plate recognition shows why the details matter

Number-plate recognition is often presented as a software feature. In practice, it is a chain with three separate jobs:

6. **Capture a clear plate.** The camera must produce an image with sufficient detail, appropriate exposure and limited motion blur.
7. **Read the characters.** Recognition software converts the visible plate into text.

8. **Use the result.** The plate may be stored, checked against an authorised list, linked to an access event or presented to a person for review.

If the plate is a small blur in the corner of a general overview image, better AI will not recreate the missing detail. Camera angle, lane width, capture distance, vehicle speed, night lighting and shutter settings all matter. Specialist guidance recommends keeping the view close to head-on and testing the complete route under real day and night conditions. [3]

This is why a dedicated plate-capture camera at the gate may outperform a higher-resolution general camera mounted to watch the entire driveway. More megapixels do not automatically mean more reliable recognition.

## 6 Power, fibre and storage are part of the camera system

A customer may see live video on a phone and assume the cameras are protected by the business fibre connection. The complete path is longer: camera, power source, PoE switch, local network, recorder or cloud service, storage, router, internet connection and viewing device.

| Failure                                      | What may continue                                                                | What the buyer must verify                                                                |
|----------------------------------------------|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| Fibre fails; local equipment remains powered | Local recording may continue if the design supports it.                          | Remote viewing, cloud processing or mobile alerts may stop unless failover is configured. |
| PoE switch loses power                       | The connected cameras normally stop, even if the recorder and fibre remain live. | Confirm which switches and cameras are on UPS, inverter or solar-backed power.            |
| Recorder or storage fails                    | Live viewing may continue while evidence is no longer retained.                  | Test storage-health alerts, overwrite rules and retrieval—not only the live picture.      |
| Router loses power                           | Some local recording can continue.                                               | Remote access and alerts fail although the fibre service itself is still available.       |

A failover connection is useful only if it has enough capacity for the required traffic and if the router switches automatically. It may be sensible to prioritise alarms and selected low-bandwidth streams during an outage rather than trying to carry every camera at full resolution.

## 7 The alert is only useful if somebody owns the response

An alert that arrives on five phones but belongs to nobody is not a security process. For each rule, decide who receives it, how quickly it should be checked, what evidence the person will see, when it must be escalated and what happens when the primary person is unavailable.

The operator should be able to view enough context before and after the event. A still image may show a person inside a zone but not the authorised employee who opened the gate moments earlier. Pre-event and post-event video can prevent an unnecessary response.

The system should also record whether the alert was received, reviewed, dismissed or escalated where the risk justifies that level of control. This makes it possible to improve the rules rather than simply assuming the technology is working.

## 8 Privacy, access and retention cannot be added afterwards

CCTV footage can contain identifiable employees, customers, visitors and vehicle registration information. POPIA requires personal information to be processed lawfully and reasonably, for a specific purpose, with appropriate transparency, retention and security safeguards. It also requires reasonable technical and organisational measures against loss, unauthorised access and unlawful processing. [5]

**Purpose.** Record why each camera and analytic rule exists. Security at an entrance does not automatically justify monitoring unrelated private or staff areas.

**Notice.** Use appropriate signage and notices so people understand that surveillance takes place and who is responsible for it.

**Access.** Limit live viewing, playback, downloading and sharing. Remove access when employees or service providers change roles.

**Retention.** Keep footage for a period linked to the purpose and legal needs, then delete or overwrite it securely. “Keep everything forever” is not a control.

**Supplier arrangements.** Where another company stores, monitors or processes footage, clarify responsibilities, safeguards, incident reporting and contract terms.

**Biometric functions.** Face detection is not the same as facial recognition. Matching a face against an identity database can involve biometric information and requires a much higher level of legal, ethical and security consideration.

The Information Regulator’s 2026 draft Code of Conduct on Gated Accesses is not a general final CCTV code, but it is a useful indication of the Regulator’s attention to CCTV, access systems and personal information at controlled entrances. [6]

## 9 Test the system before accepting it

A brochure demonstration proves that the feature exists. It does not prove that the customer’s site will produce a usable result. A practical acceptance test should include:

9. **Define the event.** Write the person, vehicle or activity to be detected; the exact area; the schedule; and the required response.
10. **Test day and night.** Include backlighting, headlights, shadows, rain where practical and the normal lighting conditions of the premises.
11. **Test realistic movement.** Use the expected walking direction, vehicle speed, clothing, carried objects and entry route—not only a slow walk directly in front of the camera.
12. **Test nuisance events.** Include animals, moving foliage, staff activity and ordinary deliveries so the alert volume can be assessed.
13. **Test evidence retrieval.** Confirm the date and time, pre-event and post-event footage, search process, export format and whether the clip remains usable outside the viewing application.
14. **Test outages.** Disconnect the primary internet link and simulate loss of grid power to the approved extent. Confirm recording, alerts, failover and recovery.
15. **Record the result.** Agree what counts as a pass, which limitations are accepted and who is responsible for adjustments, training and maintenance.

## PRACTICAL TOOL

# AI CCTV Buyer's Decision Record

*Complete this before accepting an intelligent camera or analytics proposal*

Use one decision record for each important camera area or analytic rule. A single system may have different requirements at the gate, loading bay, reception and stockroom.

| Decision area           | Required answer or evidence                                                                                                                  | Status           |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| Business problem        | What specific loss, delay, safety concern or investigation problem must improve? Avoid a general answer such as "better security."           | Pass / Gap / N/A |
| Required event          | State exactly what must be detected: person, vehicle, line crossing, time in zone, plate or another supported event.                         | Pass / Gap / N/A |
| Area and schedule       | Mark the detection area and exclusion zones. Record the days and times when the rule must operate.                                           | Pass / Gap / N/A |
| Camera suitability      | Confirm lens, position, angle, object size, lighting, weather exposure and expected movement speed.                                          | Pass / Gap / N/A |
| Analytics location      | Record whether analysis runs in the camera, recorder, local server or cloud—and what happens if that component is unavailable.               | Pass / Gap / N/A |
| Recording method        | State whether recording is continuous, motion-based, AI-event based or combined. Record resolution, frame rate and pre/post-event duration.  | Pass / Gap / N/A |
| Storage and retention   | Confirm usable storage days at the agreed settings, overwrite behaviour, health alerts and the reason for the retention period.              | Pass / Gap / N/A |
| Alert owner             | Name the primary and backup recipients, expected review time, escalation path and action outside normal hours.                               | Pass / Gap / N/A |
| Power continuity        | List the cameras, PoE switches, recorder, storage and router that have backup power. Record the tested runtime.                              | Pass / Gap / N/A |
| Connectivity continuity | Confirm what remains local, what requires fibre or mobile data, how failover works and which traffic is prioritised.                         | Pass / Gap / N/A |
| Privacy controls        | Record purpose, signage or notice, authorised viewers, supplier access, download rights, retention and incident handling.                    | Pass / Gap / N/A |
| Commercial scope        | List included cameras, analytics channels, licences, subscriptions, monitoring, storage, installation, training, maintenance and exclusions. | Pass / Gap / N/A |
| Acceptance evidence     | Attach day/night and outage test results. Record accepted limitations, outstanding adjustments and the person who approved the result.       | Pass / Gap / N/A |

**Acceptance rule:** Do not accept an important analytic function only because it worked once in daylight. Acceptance should reflect the conditions in which the customer expects to rely on it.

## CLOSING PERSPECTIVE

# Choose evidence, not the AI label

A good security-camera system does not have to be the most intelligent system on the market. It must capture the right scene, preserve usable evidence, send manageable alerts and continue operating as designed when normal business conditions become difficult.

AI video analytics can make CCTV more useful. It can help a small team pay attention to the events that matter and find relevant footage more quickly. Its value is greatest when the task is specific, the image is suitable, the response is owned and the result has been tested.

The sensible decision is therefore not “AI or no AI.” It is whether the selected analytics solve a defined problem reliably enough to justify the additional equipment, configuration, licensing, training and governance.

Before signing, ask the supplier to show what the system can detect at your site, what it may miss, what continues during a power or fibre failure, and how a person will verify and act on the alert. Those answers are more valuable than the badge on the camera box.

---

*Important note: This report is educational. It does not constitute legal advice, a site-specific security assessment or a guarantee that any camera or analytics function will detect every event. Product capabilities and licensing vary.*