

VisualGuard

OpenCV 5 on AWS / Technical report

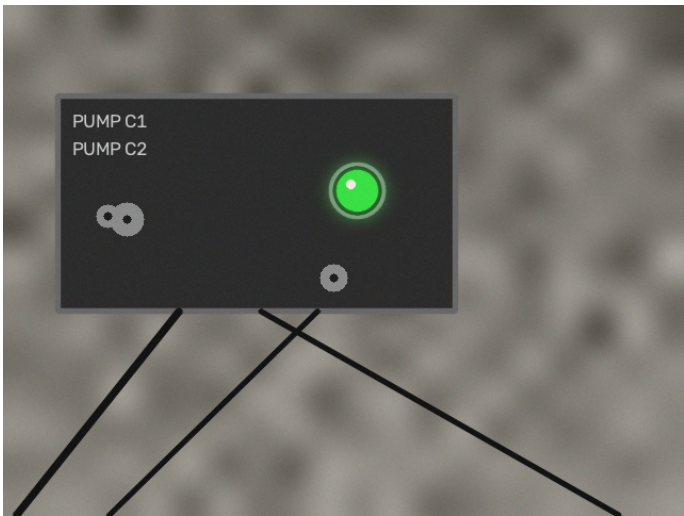
YOUNG-FU | Single-person entry | 27 October 2026

Private AWS execution is verified for synthetic inputs. The 2:20 owner-review film is public; it is not byte-bound to CHECK146 or independently reviewed. This Devpost entry remains a draft.

Problem and users

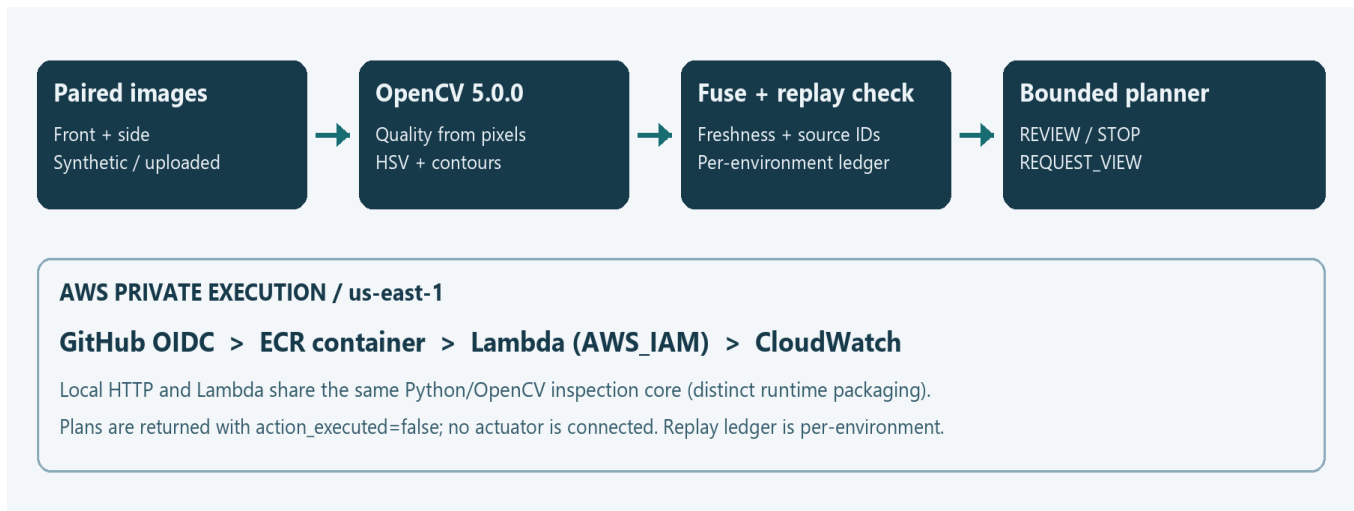
Equipment-panel inspection should distinguish a visible alarm from an unusable view. VisualGuard is a prototype for inspection operators and reviewers: it examines front and side images and returns a bounded next step. No equipment control, safety certification or field accuracy is claimed.

Decision	Planned follow-up	Meaning
REVIEW	QUEUE_HUMAN_REVIEW	Usable views, no detected alarm; a person confirms
STOP	HOLD_AUTOMATION	Alarm or integrity failure; a hold is proposed
REQUEST_VIEW	REQUEST_NEW_CAPTURE	Unusable or incomplete visual evidence



Example: procedural synthetic panel, not a photograph.

Architecture and implementation



Substantive OpenCV 5 processing

For each 640 x 480 BGR image: grayscale conversion, Gaussian blur, directional Sobel sharpness and Laplacian variance; histogram exposure checks; low-texture dark-cell occlusion; HSV red-band masks, morphology, contours, circular fill, area and aspect tests. View fusion and provenance checks feed a deterministic planner. Configuration SHA-256 is bound to capture evidence.

Freshness, view skew, source IDs, capture IDs and a SQLite replay ledger constrain reuse. The ledger is per process or Lambda execution environment, not a global distributed replay service. The planner emits perceive / decide / plan traces and never calls an actuator.

AWS component	Actual configuration
Lambda	visualguard-inspector; us-east-1; x86_64; 1024 MB; timeout 30 s
ECR / deployment	One container image; GitHub OIDC; deployed source 832b1b4
Function URL	AWS_IAM; anonymous access denied
CloudWatch	Saved Lambda REPORT lines plus supplemental Console log
Concurrency / budget	Reserved concurrency 2 rejected by account quota; budget alert is not a hard cap

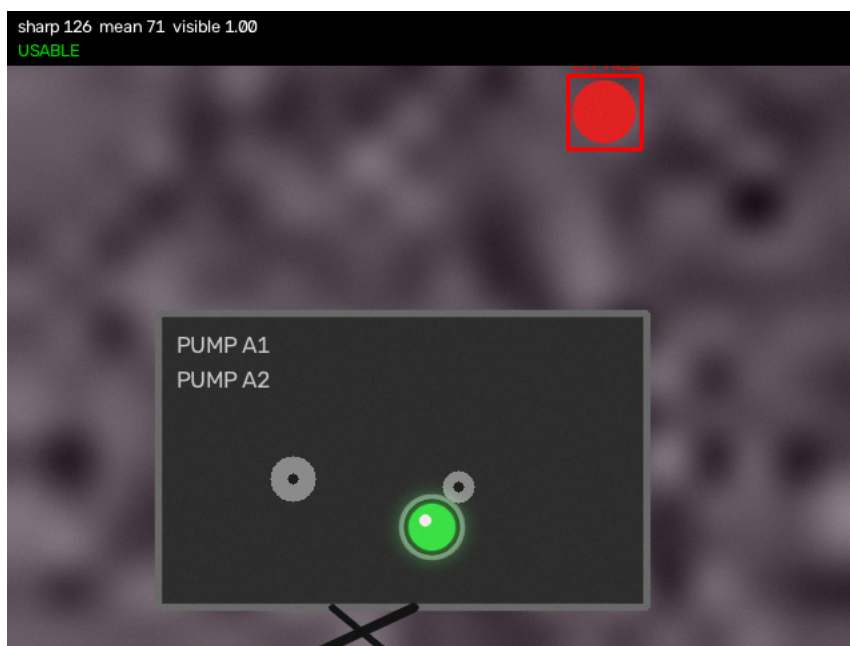
Synthetic evaluation and failures

Thresholds were chosen on 180 development pairs. The held-out split contains 540 pairs across 18 scenario families with disjoint seeds and wider rendering ranges. Ground truth is defined by generator parameters. Generator and detector share an author; these measurements establish performance on this generator only.

Method	Exact	Alarm -> REVIEW misses	False stops
Full pipeline	94.26%	0 / 210	30 / 330
Without quality gates	55.56%	60 / 210	30 / 330
Naive red count	50.00%	60 / 210	61 / 330
Legacy brightness	31.85%	76 / 210	244 / 330

Known failures remain visible

All 30 bright round red non-emissive stickers falsely return STOP. One motion-blur test case returns REVIEW rather than REQUEST_VIEW. No threshold was retuned on the held-out set for this submission package. Geometry of a lamp housing and temporal evidence are future experiments, not completed fixes.



Synthetic sticker failure: the red disc is detected as an alarm.

Real AWS execution evidence

The approved private deployment completed from application source 832b1b476ce88e3fa95e83ac5749f64af0f4bd63. Evidence-only commit 3442e3aa0e8d6003c538ecd2045cd65b2e697710 did not change application code. The later local Windows fixture/documentation changes are review candidates and have not been redeployed or validated in remote CI.

Recorded invoke	Observed result	Saved detail
Health	HTTP 200; OpenCV 5.0.0 / package 5.0.0.93	Workflow summary
Side-only alarm	STOP / ALARM / HOLD_AUTOMATION	Workflow summary
Clear pair	REVIEW / HUMAN_REVIEW / QUEUE_HUMAN_REVIEW	Workflow summary
Empty views	REQUEST_VIEW / INCOMPLETE_COVERAGE / REQUEST_NEW_CAPTURE	Full Console event, response and log

The three deployment REPORT lines show durations 11.16, 395.52 and 173.29 ms. The first includes 3464.37 ms initialization and 3476 ms billed duration. Saved summaries do not directly bind each of these request IDs to a per-case full response. The fourth call has Lambda request ID 5e91ad05-2270-4828-b1dc-619fc4ebdd62: 3.75 ms duration, 4 ms billed duration. Four calls are not a latency benchmark.

Traceability

Image digest: sha256:78d00e60f73ec608d65c054b220cd1bfaa8293ad752849dff6352aabd9324ddd

Deployment: [GitHub Actions run 40223113044](#). Evidence-commit CI: [run 40224824470](#). Both test and container jobs succeeded for the evidence commit.

The companion viewer replays saved records and makes zero AWS requests. It is not a live judge endpoint. Three complete raw request/response pairs were not archived; they must not be reconstructed and presented as originals.

Reproduction and Windows verification

Pinned runtime: numpy==2.5.3 and opencv-python-headless==5.0.0.93. Lambda adapter: awslambdarc==3.1.1. Install the vision requirements and pytest==9.0.2, then run the repository tests. Build and deployment commands are documented in the included AWS deployment runbook.

Baseline b85ebb0: remote CI and CHECK146

GitHub Actions run 40249719964 at b85ebb0873cf030ab95fd32c1d886df59bf74c86 reports 268 passed and 116 subtests passed in 13.62 seconds; test and container jobs succeeded. The judge evidence index independently passed: 6 bound artifacts, 4 recorded AWS cases and 8 local negative controls. It verifies saved consistency, not origin authentication or completed human review.

Windows candidate: 266 passed, 2 skipped, 116 subtests passed.

Executed on the b85ebb0-based review candidate with Python 3.12.10 and SQLite 3.49.1. Two POSIX directory-fsync probes are unsupported on Windows. JSON artifact-path keys now use forward slashes on all platforms; no digest or assertion was weakened. Windows changes remain local and were not remotely CI-verified. This is not a claim of 100% Windows coverage.

Root causes and corrections

The restricted default TEMP directory blocked SQLite. A normal local process and a writable project TEMP directory restored HTTP/SQLite tests. Further tests exposed SQLite context managers that committed transactions without closing connections; the fixture wrapper now preserves transaction behavior and closes handles. Git checkout newline conversion changed evidence hashes; evidence JSON now preserves exact Git bytes. Image-analysis and decision logic were unchanged.

Windows: ops/run_windows.ps1 -Action Test -Python python

Serve: ops/run_windows.ps1 -Action Serve -Python python -Port 8766

Recorded evidence: python ops/verify_aws_recording.py

Byte integrity is separate from origin authentication

The committed evidence file has one extra trailing newline relative to the original local export. Parsed JSON objects are identical. The earlier byte-equality claim is corrected. The verifier pins the committed copy; it does not verify an AWS digital signature.

Git copy SHA-256: 6f4d06d997b67be292e1cc9ad9febe6e59dddde7e661010e02da459e75d362b0

Original export SHA-256: a86e06f6324b9cbc611bba85ca39201eba1812ee95e01c6631f7c9dce954612b

Responsible use and submission status

All reported image evaluations and AWS image calls used synthetic scenes. A real-camera check using owner-provided footage has not been run. Synthetic results do not establish factory performance. No camera-origin authentication or safety certification is claimed.

After **REQUEST_VIEW**, an operator can provide another pair and run inspection again. In the recorded local demonstration, human resubmission takes an occluded case to **REVIEW**. The system does not control a camera, dispatch a webhook, complete a work order, or actuate equipment; **action_executed** remains false.

Images are processed in memory; only digests enter the replay ledger. The repository is public. The AWS inference endpoint remains private behind **AWS_IAM**; there is no public inference endpoint, and a judge screen-share has not been arranged.

Submission item	Current state
Team	Single-person author YOUNG-FU
Video	Public 2:20 owner-review film; not CHECK146-bound or independently reviewed
Code	Public repository; Devpost code link points to claude/practical-ride-st6n28
Report / architecture	Included for review
AWS access	Private IAM endpoint; judge access or screen-share not arranged
Real-camera / physical action	NOT_RUN / NONE
Final entry	Devpost draft; not submitted; no receipt

Repository: [public review branch](#) | **Public video:** [VisualGuard | Two Views. One Next Step. \(2:20\)](#)

The technical evidence remains limited to the stated synthetic evaluation and private AWS records.

Official requirements and conservative deadline

The official page header gives 27 October 2026, 14:45 Asia/Taipei (26 October, 23:45 PDT); its overview text gives 23:59 PDT. This package uses the earlier time. The listed materials include a technical report, judge-accessible code, reproduction instructions, architecture, a working endpoint or arranged screen-share, a judge-accessible video of at most five minutes, and evaluation evidence.

[Official competition page](#) | [Rules and submission-material license](#)