DECEPTION CHECK

EPICS BASE / PATH AND DEPLOYMENT

Who can reach the control software?

Check who can connect, which software was deployed, and whether the fixed build is running. Use case aliases here; retain raw infrastructure details in your approved evidence store.

01 / Service, owner, and operational dependency

IOC or protocol-server alias; site and service owner; monitoring or control dependency; review time UTC.

02 / Actual network paths

Listeners, advertised/nondefault ports, gateways, and approved clients. Include remote access and management paths; reference existing rules and flow evidence.

03 / Build and component evidence

EPICS Base build; Channel Access server; classic pvAccess/pvDataCPP where present; supplier/backport statement; deployed binary/library and manifest reference.

DECEPTION CHECK

EPICS BASE / RUNNING FIX AND CLOSEOUT

Make the update verifiable.

04 / Maintenance and running fix

Supported update or backport; artifact/signature reference; build recipe; approved restart or replacement; evidence linking the service process to that build.

05 / Client and operational acceptance

Test older Channel Access clients, displays, scripts, gateways, and required operational sequences. Record results, owner, and rollback plan.

06 / Hunt, gaps, and next owner

Unexpected connections, parser errors, crashes, or restarts; network/host correlation; retention limits; remaining exposure and next review time.

Reference checks

CISA ICSA-26-300-01 / CVE-2026-114595 to 114598. Upstream update: EPICS Base 7.0.11. Use supported backport evidence for downstream builds. Access rules and segmentation remain useful, but do not replace the relevant fixes.

Primary guidance: epics.anl.gov/base/R7-0/11.php
Research and response notes: deceptioncheck.ai/research