

CONTROLLED

SEN-93-112

Incident Report: Loss of Reference at ARGENT

DATED	February 8, 1993	TYPE	Incident report
ORIGIN	Directorate I	SITE	ARGENT
PAGES	8	CUSTODY	MERIDIAN

A nineteen-hour period during which the primary site believed it knew the time and did not. No data was lost; eleven months of prior data became unusable, which was worse.

REDACTION: Two personnel names and the specific failure signature of a third-party reference unit are withheld. The manufacturer was notified in 1993 and the fault was corrected in a subsequent revision.

SUMMARY

On 6 February 1993 the primary reference at Site ARGENT entered a fault state in which it continued to output a valid-looking signal derived from a failed internal source.

It did not flag the fault. It did not fall back. It asserted, for nineteen hours, that it knew the time.

Downstream systems believed it, because they had been designed to believe it.

SEQUENCE

Time (UTC) Event
06 Feb 04:12 Internal source fails. Unit continues to output; no alarm raised.
06 Feb 04:12 ? 23:31 Nineteen hours of timestamped acquisition against a drifting reference.
06 Feb 23:31 Operator notices a disagreement with a secondary unit during routine comparison.
07 Feb 00:04 Acquisition halted.
07 Feb 06:20 Fault confirmed as internal to the reference unit.
08 Feb Scope of affected data assessed.

CONSEQUENCE

No data was lost. Every byte written during the nineteen hours is still held.

The damage was to everything before it. The site had been operating with a single reference and a secondary used only for periodic comparison. When the primary was found to have failed silently, the institution could no longer demonstrate when the failure had begun -- only when it had been noticed.

The last comparison that could be trusted was eleven months earlier.

Eleven months of acquisition therefore became unusable, not because it was wrong, but because we could no longer prove it was right. Most of it probably was. That is not a standard this institution accepts.

ROOT CAUSE

The proximate cause was a component failure in a third-party reference unit, in a mode the manufacturer had not anticipated and which is withheld here.

The actual cause was ours: a design in which a single instrument could assert correctness with no independent means of contradiction, and a comparison schedule sparse enough that a silent failure could hide in it for the better part of a year.

The unit did exactly what it was built to do. We had built a system in which that was sufficient to destroy eleven months of work.

CHANGES

- 1. No single reference may be authoritative. Three-way comparison, with disagreement surfaced rather than voted away.
- 2. Comparison cadence raised from quarterly to continuous, with the comparison itself logged as a first-class observation.
- 3. Disagreement is an alarm state, not a diagnostic to be reviewed later. A system that cannot say what time it is must say so.
- 4. Provenance attached at acquisition, so that any future loss of confidence has a bounded blast radius instead of extending back to the last good check.

Item 4 is the direct ancestor of the signed time attestations now carried by Project Polaris, and item 3 is why Polaris is built to report disagreement rather than to resolve it.

STANDING LESSON

This incident is taught to every incoming member of Directorates I and III. The lesson is not that instruments fail. It is that ****an instrument that fails loudly costs you an afternoon, and an instrument that fails quietly costs you a year**** -- and that the difference is a design choice made long before the failure.

End of record SEN-93-112. Reproduced from the Archive of record at MERIDIAN. Handling markings are internal publication conventions of Sentinel Research Group and correspond to no external scheme.