

[OPEN](#)

SEN-98-003

Sentinel Grid: Design Rationale

DATED	July 15, 1998	TYPE	Research brief
ORIGIN	Directorate I	SITE	--
PAGES	12	CUSTODY	MERIDIAN

Why the institution built its own fabric rather than buying one, and the single assumption the whole design rests on: that any site can be gone at any time, without warning, for an unbounded period.

THE ASSUMPTION

Sentinel Grid is built on one assumption, and every property of the system follows from it:

Any site may be unreachable at any time, without warning, for an unbounded period, and the institution must continue to function while it is.

This is not a disaster-recovery posture. It is the normal operating condition. Station LOWFIELD is staffed eleven weeks at a time and is intermittently reachable by design. Treating that as an exception would have meant building a system that spends most of the year in its exception path.

CONSEQUENCES OF THE ASSUMPTION

No implicit intra-network authority

Being inside the fabric confers nothing. Every request is authenticated and authorised on its own merits regardless of origin, because "inside" is not a meaningful category when a third of the estate is regularly outside.

This was an unfashionable position in 1998. It has since acquired the name zero trust, which we adopted because arguing about vocabulary is a poor use of anyone's time.

Content addressing

Records are addressed by the hash of their contents rather than by location.

A record does not live at a site; it exists, and some number of sites happen to hold it. This makes "is this the same record?" answerable without contacting the origin, which matters when the origin is a hut in the Arctic in February.

Custody in three places, provable

Every record has custody at no fewer than three sites, and each site can demonstrate what it holds without reference to the others. Integrity audit is independent per site and runs continuously. A site that has quietly lost or altered a record reports it rather than waiting to be asked.

Reconstructible from any two

Full institutional state can be rebuilt from any two surviving sites. This has been rehearsed annually since 2001 and has failed twice -- in 2006 and 2014 -- both times revealing a dependency that had crept in unnoticed. Both were corrected. The rehearsals continue because they keep finding things.

WHY NOT BUY ONE

The brief records the 1997 evaluation honestly: commercial fabrics of the period were substantially better engineered than what we could build, and we did not build our own because we thought we were smarter.

We built our own because every option evaluated failed the custody test that later became formalised in SEN-23-041. Each required a third party -- a vendor, a hosted control plane, a licence server -- that could prevent us from withdrawing the system.

For an institution whose founding condition is the ability to stop, that was disqualifying, regardless of engineering quality.

WHAT IT DOES NOT DO

Sentinel Grid is not fast. It is not a general-purpose platform, it is not offered to anyone outside the institution, and several of its design choices would be actively wrong in a setting with reliable connectivity and no custody constraint.

It is a system built for a specific and unusual set of assumptions, published here because the reasoning may be useful to others, not because the artefact is.

End of record SEN-98-003. Reproduced from the Archive of record at MERIDIAN. Handling markings are internal publication conventions of Sentinel Research Group and correspond to no external scheme.