

A Restart Is Not Permission

When an Agent Gate Forgets “No”

Cenab Batu Bora
Georgia Tech



**You rejected the action.
Then the service restarted.**

It ran.

A recorded rejection no longer blocked
a retry of the same action.

Illustrative email scenario. The experiment uses a harmless tool and sends no email.

The gate controls access to the tool

Agent gate

The model proposes a tool call.
The gate decides whether it may run.

It records decisions in a log, then reads that log after restart to restore restrictions.

The gate constrains only calls that pass through it.

An unfinished line hides the rejection

01

First restart

The gate skips an unfinished log record but leaves its bytes in the file.

02

New rejection

It appends the new rejection directly to that fragment and confirms the save.

03

Next restart

It skips the combined invalid line. The saved rejection no longer blocks the action.

**The bytes survived.
The restriction didn't.**

Recovery must restore readable decisions
before the gate accepts new requests.

The gate repairs its log first

Recovery barrier

Validate complete records.

Repair the log ending.

Sync the file and restore decisions.

Then accept requests.

Acknowledged records stay intact. Later write or sync errors stop the service.

A test at every byte boundary

153

We cut three log records
at every byte position.

Rejection, cancellation, release.

test scenarios per policy

Three policies. 459 executions. These cases do not estimate a deployment failure rate.

Restrictions held. Work continued

Recovery policy	Prohibited executions	Startup refusals	Unrelated work ran
Original	143	4	149
Strict refusal	0	147	6
Recovery barrier	0	0	153

Each policy faced 153 test scenarios. Fresh work means an unrelated allowed action.

153 / 153

Restrictions held.
Unrelated work ran.

Recovery barrier, 153 test scenarios in the pinned SoundGate version.

Recovery can restart, too

30

forced exits during recovery

Across ten recovery tests,
the barrier restored restrictions
and ran unrelated allowed work.

**All ten boundary and error
checks passed.**

Process terminations and constructed storage states. No electrical power-loss test.

What the evidence supports

One implementation

SoundGate 0.1.3

Pinned source revision 6568403

Explicit storage assumptions

Intact acknowledged records.

A stable, protected log path.

Cooperating writers and successful sync.

The result does not establish exactly-once execution, power-loss safety, or real-world frequency.

The failure is reproducible. So is the repair.

```
python3 reproduce.py
```

Checks the saved evidence. Python 3.11 or newer.

github.com/cenab/a-restart-is-not-permission