Vocabotics

A VOCABOTICS LAB NOTE

MEASURED · not asserted

THE LAB · A RESEARCH LANE

Certifiable by construction: a memory leak is now a compile error

qc2 --safety runs six static checkers against a NASA/JPL-style profile and refuses to compile a violation — issuing a certificate on clean code. The real arena bug it kills: 1.5 GB down to 3.4 MB, a 441× reduction. The rejection is the audit trail. What is designed-not-proven: the full SIL/DO-178C profile lattice and WCET certificates.

A measured research lane

Shipped — measured, gate-clean

COVER: A MEASURED OSCILLOSCOPE WAVEFORM ON A LAB GRATICULE

Vocabotics

A VOCABOTICS LAB NOTE

Certifiable by construction: a memory leak is now a compile error

qc2 --safety runs six static checkers against a NASA/JPL-style profile and refuses to compile a violation — issuing a certificate on clean code. The real arena bug it kills: 1.5 GB down to 3.4 MB, a 441× reduction. The rejection is the audit trail. What is designed-not-proven: the full SIL/DO-178C profile lattice and WCET certificates.

PREPARED

2 July 2026

VERIFIED BY

Jon Ross — Founder, Vocabotics — 15 years building safety-critical systems

HOW TO READ IT

Drafted with AI, verified by a named human. Sources at the back.

01 The claim, in brief

> *The leak doesn't get caught at runtime — it doesn't compile. The rejection is the audit trail.*
>
> The costly signal

The measured result

Every number carries its own honesty tier — the tiering is the credibility.

6 static safety checkers 🟢 SHIPPED	**441×** arena bug: 1.5 GB → 3.4 MB 🟢 SHIPPED
1 certificate emitted on clean code 🟢 SHIPPED	**5** profile lattice (SIL4…IEC62304) — designed 🔭 VISION

Fifteen years of safety-critical delivery across global rail and metro leaves you with one conviction: *runtime is too late.* An audit does not want to hear that you caught the memory leak in testing; it wants evidence the unsafe program could never have been built. So we built exactly that into the compiler.

02 The leak that will not compile

🟢 SHIPPED — MEASURED, GATE-CLEAN

As of 2026-07-02, `qc2 --safety nasa-p10.safety` **rejects violations** against a NASA/JPL "Power of Ten"-style profile and **issues a certificate on clean code**. 🟢 Six static checkers run at compile time:

- no heap allocation after initialisation
- bounded loops only

no recursion

a function-length ceiling

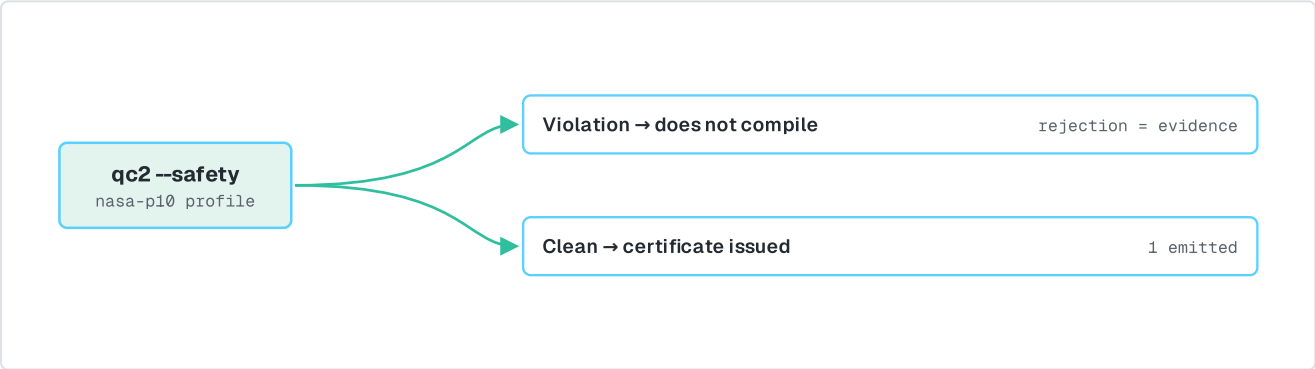
a minimum assertion density

all return values checked

A program that breaks one of these **does not compile**. The real arena bug this kills in practice: memory use from **1.5 GB down to 3.4 MB — a 441× reduction** — because the class of mistake that caused it is now rejected at the door. 🟢

> **The rejection is the audit trail.**
>
> When the compiler refuses an unsafe program, the refusal — with the rule it violated and the line it violated it on — *is* the evidence an assessor wants. You are not documenting that you tested for the fault; you are showing it was impossible to ship. That is a stronger claim, and a cheaper one to maintain.

The profile is general: a `.safety` parser reads a profile file, and the profiles form a lattice — `nasa-p10` sits under SIL4, which sits under DO-178C. Seven patents cover the mechanism.



Runtime is too late. qc2 --safety runs six static checkers at compile time: a violation does not compile; clean code gets a certificate. The rejection — with the rule and the line — is the audit trail.

1 **No heap after init**	2 **Bounded loops only**	3 **No recursion**
4 **Function-length ceiling**	5 **Minimum assertion density**	6 **All return values checked**

The six checkers, run at the door. Break one — a heap allocation after init, an unbounded loop, a recursion — and the program cannot be built.

The real arena bug this class-of-mistake now forbids: memory use fell 441×, because the mistake is rejected at the door rather than caught at runtime.

03 What is designed, not yet proven

VISION — DESIGNED, HONEST

We hold the line between "built" and "designed":

The full profile lattice — SIL4, DO-178C, EN50128, ISO 26262, IEC 62304 — is **designed, not yet proven**. `nasa-p10` is the one that compiles and certifies today.

A WCET (worst-case execution time) certificate is designed and is the next build. Bounding time, not just memory, is what a hard-real-time assessor ultimately needs.

The STABILITY gate for plastic/learning updates — a Lyapunov-bounded update, potentially a bigger moat than the static gate — is designed and **unproven**.

6	**IEC 62304** medical devices	DESIGNED
5	**ISO 26262** automotive	DESIGNED
4	**DO-178C** aviation	DESIGNED
3	**EN 50128** rail	DESIGNED
2	**SIL4** functional safety	DESIGNED
1	**NASA/JPL Power of Ten** the profile that certifies today	COMPILES TODAY

The profile lattice, honestly tiered: nasa-p10 compiles and certifies today; the higher assurance profiles are designed, not yet proven. We hold the line between 'built' and 'designed'.

04 The heritage underneath

This is not a bolt-on. It sits on roughly **15 years of real safety-critical delivery across global rail and metro** — environments where "wrong" is a safety risk and every claim is assessed. (We name no clients; the discipline is the point, not the logos.) When AI enters aviation, rail, medicine and infrastructure — and it will — "proven correct, proven bounded, proven honest, certifiable" stops being one option among many. It becomes the only one that passes.

05 Why it ladders back

AI safe enough for the things that keep people alive is trust at scale — and trust at scale is the precondition for letting capable systems actually help in the places that matter most.

What is still open — kept visible

The honest edges of this lane, shown next to the wins. None of these is a footnote; each is a claim we have not yet earned — and marking it is what earns the right to be believed on the rest.

- [ ] The full profile lattice (SIL4 / DO-178C / EN50128 / ISO26262 / IEC62304) is designed, not yet proven.
- [ ] A WCET (worst-case execution time) certificate is designed and is the next build.
- [ ] The STABILITY gate for plastic updates is designed, unproven.

06 Sources, glossary & the ledger

Where every claim comes from — and what the plain words mean.

Sources

01 **Vocabotics Dashboard — Cross-cutting: Safety (certifiable by construction), 2026-07-02** — Vocabotics internal record (as of July 2026)

02 **The Power of Ten — Rules for Developing Safety-Critical Code** — G. J. Holzmann, NASA/JPL (the P10 ruleset the profile implements) (as of 2006)

Vocabotics

THE HONESTY LEDGER

🟢 Shipped — measured, gate-clean.

🔬 Research — measured, partial; the gap is shown.

🔭 Vision — designed, honest; not yet built.

The bigger claim goes up a tier, never down. We show the eval beside the demo — the tiering is the credibility.

See the company that builds this way

Certifiable-by-construction is a discipline, not a feature. Read how one founder and a gated fleet run the same discipline as an operating model.

/research/agentic-operating-model

Nothing faked.

Measured, not asserted. Every claim carries its own honesty tier and the open edges are shown next to the wins — the tiering is the credibility.

Vocabotics · calm, clear, candid · no client names · global rail & metro heritage