From Design Points to Machine-Checked Parameter Regions: Reusable Certificate Templates for Engineering Models

Dr. Tamás Nagy

tnagyphd@gmail.com

Working Paper • 2026-05-06

Build-std v2.0+a8ba48a394 | 2026-07-20 07:32 | 4f6ea192

Overview

Engineering models often produce a result at one selected parameter point. This paper asks a different question: **which conclusions follow throughout a region once the model, inequalities, and perturbation bounds have been declared?**

The paper compares four recurring algebraic patterns for combining positive margins, comparing certificate requirements, propagating stated monotonicity, and bounding margin changes across materials, energy, biotechnology, and multi-parameter examples. A fifth deterministic uncertainty-penalty rule is checked separately as a generic conditional template.

Stored proof manifests record **323 named conditional checks**. This is an inventory of formal implications, not 323 independent discoveries: some entries directly restate supplied conditions, while others derive arithmetic or algebraic consequences.

The central limitation is equally important. The formal layer does not establish that a physical model is accurate, that the illustrative named values are measured, or that a machine-checked margin is a real-world safety guarantee. Those questions still require model validation, simulation, experiment, and domain review.

Abstract

We present a reusable algebra for machine-checked certificates in declared engineering models, where supplied equations, inequalities, monotonicity directions, and perturbation bounds imply an encoded safety, lifetime, stability, or performance predicate. Four recurring rules describe meet, dominance, monotonicity, and margin perturbation across thirteen model domains and eight certificate geometries; a fifth deterministic uncertainty-penalty rule is implemented once as a generic conditional suite and is not instantiated in the thirteen domain suites. Stored manifests record 323 named conditional claims—189 in fourteen abstract suites and 134 in thirteen illustrative named-scenario suites—with zero sorry placeholders; the count includes direct condition restatements as well as derived arithmetic and algebraic consequences. Reported robustness quantities are slack budgets in margin units, not parameter-space radii without an additional sensitivity bound. The named values and comparisons are illustrative inputs, not empirical findings about the named products or systems. The proof tooling supports Lean 4 export, but none of the retained suites has a current-source Lean seal and this paper does not claim Lean-validated theorem equivalence. Formal

checking establishes consequences of the declared assumptions; it does not validate the assumptions or the physical models.

Keywords: formal verification, safety certificates, battery thermal safety, electromigration, battery degradation, catalyst design, phase stability, binding stability, screening bounds, uncertainty-penalized certificates, proof assistants, industrial design

1. Introduction

1.1 The Problem

Engineering design decisions in batteries, semiconductors, and materials science commonly combine simulation, physical testing, safety factors, and uncertainty-aware optimization. A simulation or test at one operating point does not by itself certify a neighboring region unless a validated model and an explicit sensitivity, invariance, or robustness argument connect the points.

This matters because:

- **Experimentation is costly and time-consuming.** Battery abuse testing and semiconductor reliability qualification require specialized facilities, equipment, and repeated measurements.
- **Design spaces are high-dimensional.** A battery cell has dozens of design parameters (chemistry, geometry, cooling, operating limits). Exhaustive testing is impossible.
- **Small improvements can have material value.** Higher yield and wider operating windows can improve manufacturing economics and reduce qualification risk.
- **Safety margins are not uniformly formalized.** Engineering practice uses several notions of safety factor, buffer, excess, tolerance, and uncertainty margin, whose meanings and propagation rules are not always explicit.

1.2 Prior Art and Novelty Boundary

Region-level safety certification is established prior art. Barrier certificates separate reachable trajectories from unsafe regions without explicit reachability computation (Prajna and Jadbabaie, 2004), and modern tools synthesize Lyapunov-like and barrier certificates for dynamical models with solver-checked soundness (Edwards, Peruffo, and Abate, 2024). Formal assurance frameworks also integrate machine-checked and informal evidence with explicit provenance rather than treating an entire engineering argument as formal (Nemouchi et al., 2019). In engineering design, margins are an established but heterogeneous concept (Eckert, Isaksson, and Earl, 2019), while risk-based design optimization supplies stronger uncertainty semantics and optimization guarantees than deterministic slack alone (Chaudhuri et al., 2022).

Accordingly, this paper does **not** claim to invent safety certificates, barrier methods, margin-based design, robust optimization, formal verification, or assurance cases. Its narrower contribution is a comparative, proof-kernel-checked artifact: four recurring elementary implication patterns are encoded across thirteen declared engineering models and eight certificate geometries, while a fifth uncertainty-penalty template is supplied as a separate generic suite. The named-scenario suites apply domain-specific arithmetic predicates to illustrative inputs; they are neither data-driven validation nor evidence that the inputs describe real products. A repository literature search (OpenAlex and Crossref, 20 July 2026) using queries for cross-domain algebraic design certificates, parametric safety regions, and machine-checked certificate algebras found substantial adjacent work in compositional verification, assurance cases, barrier-certificate synthesis, and risk-aware design, but no retrieved publication with this exact comparative package and uniform theorem-level inventory. This negative search result supports only the scoped comparative-artifact claim; it is not a priority claim over unindexed literature.

1.3 Our Approach: Machine-Checked Conditional Certificates

We study **machine-checked design certificates in declared models**: formal implications that propagate stated model equations, inequalities, and perturbation assumptions across a defined parameter region. They complement point evaluations but do not establish that the declared model fits a physical system.

A certificate has the form:

> Given a physical model $\mathcal{M}$ and design parameters $\theta \in \Theta$, if the certificate condition $C(\theta)$ holds, then the safety/lifetime/performance property $P(\theta)$ is certified within the declared model. A positive margin supplies a quantitative slack budget against perturbations whose effect on that margin is bounded.

The key insight is that the **certificate algebra** — the mathematical structure governing how certificates compose, dominate each other, transfer under design improvements, and tolerate perturbations — can be expressed in a domain-agnostic way once model equations, monotonicity directions, and perturbation bounds are declared. Whether the model is Arrhenius-exponential (thermal safety, electromigration), power-law (battery degradation), interval-bounded (catalyst), multi-competitor (phase stability), binding thermodynamic, or classifier-statistical (screening), analogous algebraic properties hold under the stated assumptions:

1. **Meet (CA1):** The intersection of two valid certificates is a valid certificate.
2. **Dominance (CA2):** For certificates ordered by their declared margins or regions, the stronger certificate implies the weaker one.
3. **Monotonicity (CA3):** For margin-defined certificates, a parameter change proved to increase the margin preserves certification.
4. **Robustness (CA4):** A positive margin remains positive when the induced margin change is smaller than the available slack.
5. **Uncertainty penalty (CA5):** If the induced margin error is bounded in magnitude by $k\sigma$, then $m - k\sigma > 0$ preserves the certificate. Probabilistic coverage requires separate distributional assumptions.

1.4 Contributions

1. Proof-kernel implementations of recurring meet, dominance, monotonicity, and robustness implications (CA1–CA4) across thirteen declared models, plus one generic deterministic uncertainty-penalty suite (CA5), all with explicit trust boundaries (§2).

2. Five materials and energy suites (§3–7): battery thermal runaway, semiconductor electromigration, battery degradation, catalyst stability, and material phase stability (70 named kernel-checked claims).

3. Three biotech screening suites (§8–10): protein-ligand binding stability, screening error bounds, and gene regulatory network stability (42 named kernel-checked claims).

4. A coupled thermal-degradation suite (§11), in which a declared temperature perturbation affects two margins (14 named claims).
5. A 3-gene Routh-Hurwitz suite (§12) using the $p_1 p_2 > p_3$ cross-condition (12 named claims).
6. A triple coupled-margin suite (§13) for declared thermal, phase, and degradation interactions (14 named claims).
7. A linear half-space suite (§14) for polyhedral safe regions (11 named claims).
8. A quadratic suite (§15) for curved boundaries and declared cross-parameter interaction (12 named claims).
9. A deterministic uncertainty-penalty suite (§17) using a supplied $k\sigma$ margin-error budget (14 named claims).
10. Illustrative named-scenario checks (§16) for cell formats, technology nodes, chemistries, catalysts, alloys, battery packs, drug candidates, diagnostic tests, circuits, process windows, and multi-physics envelopes (134 named claims), including seven negative-margin checks under the declared values.
11. A theorem-level comparative inventory showing which conditional implications are actually encoded across thirteen declared models and eight certificate geometries (§18), without claiming uniform instantiation, completeness, or priority over other certificate formalisms.
12. Discussion of potential applications and limitations spanning two tracks plus cross-domain geometries (§19).

2. Framework: Certificate Algebra

2.1 Physical Model Abstraction

We formalize a physical model as a tuple (Θ, f, P) where:

- $\Theta \subseteq \mathbb{R}^d$ is the design parameter space
- $f : \Theta \to \mathbb{R}$ is the performance function (e.g., safety margin, lifetime)
- $P = \{f(\theta) > 0\}$ is the safe region

A **certificate** is a condition $C(\theta)$ such that $C(\theta) \implies P(\theta)$ is a theorem. For the margin certificates used below, $C(\theta)$ is the positivity condition $m(\theta) = f(\theta) > 0$. The value $m(\theta)$ is a slack budget in margin units: if a perturbation changes the margin by less than this budget, positivity survives. Converting it to a radius in parameter space requires a bound relating parameter perturbations to margin changes.

2.2 Certificate Algebra Templates

For the encoded margin predicates, the suites instantiate the following algebraic rules under their stated ordering, monotonicity, and perturbation assumptions:

CA1 (Meet). If C_A and C_B are certificates with margins $m_A, m_B > 0$, then $C_A \wedge C_B$ is a certificate with margin $\min(m_A, m_B) > 0$.

CA2 (Dominance). Within a declared certificate ordering, if certification of A supplies a margin satisfying $m_A \geq m_B > 0$, then the weaker positive-margin requirement $m_B > 0$ also holds.

CA3 (Monotonicity). A declared design improvement preserves certification whenever it does not decrease the encoded margin:

$$f(\theta_1) \le f(\theta_2), \qquad C(\theta_1) \implies C(\theta_2), \qquad C(\theta) := [f(\theta) > 0].$$

CA4 (Robustness). If $m(\theta) > \varepsilon > 0$ and $|m(\theta') - m(\theta)| \le \varepsilon$, then $m(\theta') > 0$.

CA5 (Uncertainty penalty). Let $\sigma > 0$ be an uncertainty scale and $k > 0$ a chosen multiplier. If the induced margin error is bounded by $k\sigma$ and $m(\theta) > k\sigma$, then the penalized margin $m_{\text{pen}}(\theta) = m(\theta) - k\sigma$ is positive. See §17 for the formal development.

2.3 Implementation in a formal proof kernel

All suites are implemented in a formal proof kernel with Lean 4 export support. Physical parameters are declared as design variables, while model equations, empirical inputs, positivity conditions, and certificate premises are declared as conditions. The proof layer checks consequences of those conditions. The reported count of 323 is therefore an inventory of named kernel-checked claims: it includes arithmetic consequences, structural assemblies, and direct restatements of declared conditions. It is not a count of 323 independent substantive theorems, and it does not validate the conditions empirically.

The machine-readable claim map identifies every retained theorem by source path, exact theorem ID, evidence layer, and conservative semantic grade. None of these retained suites has a current-source Lean seal: Lean export is a tooling capability, not evidence asserted by this paper. The formal status claimed here is therefore proof-kernel replay plus manifest validation only.

3. Domain 1: Battery Thermal Runaway Safety

3.1 Physical Model

Semenov thermal explosion theory. Heat generation follows the Arrhenius law:

$$q_{\text{gen}} = Q \cdot A \cdot \exp\left(-\frac{E_a}{R \cdot T}\right)$$

Heat removal is Newtonian:

$$q_{\text{rem}} = h \cdot S \cdot (T - T_{\text{amb}})$$

The Frank-Kamenetskii parameter δ determines stability: if $\delta < \delta_{\text{crit}}$, the cell is thermally stable.

3.2 Certificate

Safety margin: $m = q_{\text{rem}} - q_{\text{gen}} > 0$

Headline conditional claim (T13): Under the declared bridge assumption $\delta < \delta_{\text{crit}} \Rightarrow m > 0$, subcriticality implies $m > 0 \wedge q_{\text{gen}} < q_{\text{rem}}$.

3.3 Results

14 named conditional claims checked, 0 sorry. The suite verifies the algebra of meet, dominance, monotonicity, and margin perturbation under its declared conditions.

4. Domain 2: Semiconductor Electromigration Lifetime

4.1 Physical Model

Black's equation (1969):

$$\mathrm{MTTF} = A \cdot j^{-n} \cdot \exp\left(\frac{E_a}{k_B \cdot T}\right)$$

Same Arrhenius structure as battery thermal, different physical mechanism (electron-wind metal atom transport vs. thermal explosion).

4.2 Certificate

Lifetime margin: $m = \mathrm{MTTF} - \mathrm{MTTF}_{\mathrm{req}} > 0$

Headline conditional claim (T14): Given the declared MTTF model and perturbation bound, $\mathrm{MTTF} > \mathrm{MTTF}_{\mathrm{req}}$ and the lifetime margin remains positive.

4.3 Additional Results

- **Worst-case corner analysis (T10):** If the certificate holds at the worst-case corner $(j_{\mathrm{max}}, T_{\mathrm{max}})$, it holds at all operating points.
- **Technology scaling (T11):** If scaling reduces MTTF by factor α, the certificate remains valid iff $\mathrm{MTTF}_{\mathrm{req}} < \alpha \cdot \mathrm{MTTF}$.

14 named conditional claims checked, 0 sorry.

5. Domain 3: Battery Degradation Warranty

5.1 Physical Model

Dual-mechanism capacity fade (NOT Arrhenius):

$$Q(t, N) = Q_0 - k_{\mathrm{cal}} \cdot \sqrt{t} - k_{\mathrm{cyc}} \cdot N^{\alpha}$$

Calendar aging: SEI layer growth, diffusion-limited ($\sqrt{t}$). Cycle aging: mechanical fatigue, power-law (N^{α}, $\alpha \approx 0.5$–0.8).

5.2 Certificate

Warranty margin: $m = Q(t_w, N_w) - Q_{\mathrm{EOL}} > 0$

Headline conditional claim (T14): Given the declared degradation model and perturbation bound, capacity remains above the EOL threshold.

5.3 Key Difference

This domain uses power-law and square-root model equations, not Arrhenius-exponential equations. The same algebraic margin implications apply once the domain-specific equations and monotonicity assumptions are declared.

- **Warranty extension (T12):** If current margin is M and extended usage adds modeled degradation Δ, the extended-warranty inequality remains positive when $\Delta < M$.

14 named conditional claims checked, 0 sorry.

6. Domain 4: Catalyst Stability Design Rules

6.1 Physical Model

Sabatier principle and volcano plot. An optimal heterogeneous catalyst has adsorption energy E_{ads} within a bounded stability window:

$$E_{\min} \leq E_{\text{ads}} \leq E_{\max} \implies \text{activity} \geq \text{threshold}$$

If $E_{\text{ads}} > E_{\max}$, the surface is poisoned (adsorbate too strongly bound). If $E_{\text{ads}} < E_{\min}$, there is no adsorption (binding too weak). This model underlies catalyst screening for hydrogen evolution (HER), oxygen reduction (ORR), CO_2 reduction, and ammonia synthesis.

6.2 Certificate

Window certificate: $E_{\text{ads}} \in [E_{\min}, E_{\max}] \implies \text{activity} > A_{\text{threshold}}$

This is structurally different from the margin certificates of §3–5. The safe region is a bounded interval, not a half-space. The certificate algebra adapts: **meet** becomes interval intersection, **dominance** becomes interval containment, **robustness** becomes distance to the nearest window boundary.

6.3 Key Results

- **T05–T08 (Certificate algebra):** In the encoded endpoint case $E_{\min,2} \leq E_{\min}$ and $E_{\max,2} \leq E_{\max}$, and under the declared strict-overlap conditions, the intersection is a nonempty window contained in both parents. Its encoded width is no greater than the width of window 1; strict narrowing and a second width comparison are not claimed.
- **T09–T10 (Design monotonicity):** Better cooling widens the upper bound; higher purity lowers the lower bound. Both strictly widen the stability window.
- **T11–T14 (Perturbation robustness):** If both margins (distance to $E_{\min}$ and distance to $E_{\max}$) exceed the perturbation magnitude δ, the perturbed E_{ads} stays in the window.

6.4 Significance

This is the first **interval certificate** in the framework. The previous three domains use predicates of the form margin > 0; the catalyst suite uses the predicate value $\in [a, b]$. The same algebraic pattern can therefore be expressed for both half-spaces and bounded intervals.

14 named conditional claims checked, 0 sorry.

7. Domain 5: Material Phase Stability

7.1 Physical Model

Gibbs free energy competition. Let α denote the target phase and let β and γ denote the two competitors encoded in this finite model. The suite checks whether α has lower Gibbs free energy than both modeled competitors:

$$G_\alpha(T, x) < G_\beta(T, x), \qquad G_\alpha(T, x) < G_\gamma(T, x).$$

The stability margin against competitor β is $\Delta G_\beta = G_\beta - G_\alpha > 0$. Temperature dependence follows the Clausius-Clapeyron linearization: $\Delta G(T + \delta T) \approx \Delta G(T) - \Delta S \cdot \delta T$.

7.2 Certificate

Two-competitor margin: $\min(\Delta G_\beta, \Delta G_\gamma) > 0$

This introduces a finite multi-competitor geometry: the safe region requires simultaneous positivity of the two encoded margins. No quantified claim over unmodeled phases is made.

7.3 Key Results

- **T03 (Modeled-competitor stability):** If $\Delta G_\beta > 0$ and $\Delta G_\gamma > 0$, phase α is stable against the two encoded competitors.
- **T06–T07 (Certificate algebra):** Meet of two stability certificates is a valid certificate with margin $\leq$ each component.
- **T08 (Design monotonicity):** Alloying that reduces G_α strictly increases the stability margin.
- **T09 (Honest risk):** Annealing that reduces a competitor's G_β strictly decreases the stability margin — the certificate quantifies the risk.
- **T11–T12 (Temperature robustness):** Under the declared linearized relation, $\Delta S > 0$, $\delta T > 0$, and $\Delta G > \Delta S\, \delta T$, the encoded margin remains positive. The zero-margin boundary of that linearized model is $\delta T_{\text{linear}} = \Delta G / \Delta S$; it is not a validated physical maximum outside the range where constant ΔS and the linearization are justified.

7.4 Significance

This is the first finite **multi-competitor margin certificate** in the framework. Battery thermal and EM have single margins. The encoded phase model requires simultaneous margins against exactly two competitors. The result does not establish stability against an exhaustive physical phase set.

14 named conditional claims checked, 0 sorry.

8. Domain 6: Protein-Ligand Binding Stability

8.1 Physical Model

Thermodynamic binding equilibrium. A drug or ligand candidate binds to a target protein with free energy ΔG_{bind}. We work with binding strength $s = -\Delta G_{\text{bind}}$ (positive = favorable). At fixed temperature and standard state, using the monotone relation $\Delta G^\circ = RT \ln(K_d/c^\circ)$, a threshold on s can equivalently be written as an inverse threshold on K_d; no cross-temperature equivalence is claimed.

Three perturbation sources destabilize binding: mutation ($\Delta\Delta G_{\text{mut}}$), solvent/pH effects ($\Delta\Delta G_{\text{solv}}$), and temperature shifts ($\Delta\Delta G_{\text{temp}}$). The perturbed strength is $s' = s - (\Delta\Delta G_{\text{mut}} + \Delta\Delta G_{\text{solv}} + \Delta\Delta G_{\text{temp}})$.

8.2 Certificate

Binding margin: $m = s - s_{\text{threshold}} > 0$

Robustness: If $m >$ total perturbation, binding survives all three perturbation sources simultaneously.

Selectivity: On-target strength exceeds threshold while off-target strength falls below it.

8.3 Key Results

- **T01–T04 (Binding foundations):** Margin positive, candidate binds, perturbation is positive and weakens binding.
- **T05–T07 (Robustness):** If margin exceeds total perturbation, perturbed binding still exceeds threshold. Full robustness = binding survives AND perturbed margin remains positive.
- **T08–T09 (Selectivity):** Selectivity margin positive; on-target binds while off-target falls below threshold.
- **T10–T11 (Certificate algebra):** Meet of binding and selectivity margins; dominance (stronger binder has larger margin).
- **T12–T14 (Design monotonicity):** Affinity maturation increases margin; reducing off-target binding improves selectivity. Full headline certificate: robust binding + selectivity.

8.4 Significance

This is the first **biotech domain** in the framework. The certificate structure transfers directly from materials: margin certificates with perturbation robustness. The addition of selectivity (on-target vs off-target discrimination) is domain-specific and represents a new dimension not present in the materials track.

14 named conditional claims checked, 0 sorry.

9. Domain 7: Screening Error Bounds

9.1 Physical Model

Binary classifier with known sensitivity and specificity. A screening assay (drug screen, diagnostic test, genetic variant prioritization) has:

- Sensitivity = $P(\text{positive}|\text{true positive})$, with false negative rate $\text{FNR} = 1 - \text{sensitivity}$
- Specificity = $P(\text{negative}|\text{true negative})$, with false positive rate $\text{FPR} = 1 - \text{specificity}$

The regulatory requirement is that both error rates remain below thresholds: $\text{FNR} < \text{FNR}_{\text{max}}$ and $\text{FPR} < \text{FPR}_{\text{max}}$.

9.2 Certificate

Dual margin certificate: $m_{\mathrm{FNR}} = \mathrm{FNR}_{\max} - \mathrm{FNR} > 0$ and $m_{\mathrm{FPR}} = \mathrm{FPR}_{\max} - \mathrm{FPR} > 0$

Assay degradation increases error rates. If margins exceed the degradation, the certificate survives.

9.3 Key Results

- **T01–T04 (Error rate foundations):** Both FNR and FPR are positive (imperfect test), both margins are positive.
- **T05–T07 (Robustness):** If FNR margin exceeds degradation, perturbed FNR still acceptable. Same for FPR. Full robustness = both survive.
- **T08–T09 (Certificate algebra):** Meet of FNR and FPR margins is positive; meet dominance.
- **T10–T11 (Design monotonicity):** Better sensitivity → lower FNR → larger margin. Direction-preserving.
- **T12–T14 (PPV):** True positive rate positive, PPV denominator positive (well-defined PPV). Headline: full screening certificate.

9.4 Significance

This is the second biotech domain and introduces **dual margin certificates** where two independent error rates must simultaneously be controlled. The certificate algebra (meet, dominance, monotonicity) applies to each margin independently and to their conjunction. The suite also checks positivity of the declared PPV denominator under its stated conditions.

14 named conditional claims checked, 0 sorry.

10. Domain 8: Gene Regulatory Network Stability

10.1 Physical Model

Linearized ODE network stability. A gene regulatory network with n genes has dynamics $dx/dt = f(x)$. At a steady state x^*, the Jacobian $J = Df(x^*)$ determines local stability. For a 2-gene network:

$$J = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

where a, d are self-regulation terms (negative = decay) and b, c are cross-regulation terms. The Routh-Hurwitz stability conditions for 2D are:

$$\mathrm{trace}(J) = a + d < 0 \quad \text{and} \quad \det(J) = ad - bc > 0$$

These are necessary and sufficient for local asymptotic stability.

10.2 Certificate

Dual margin certificate: $m_{\text{trace}} = -\text{trace}(J) > 0$ and $m_{\text{det}} = \det(J) > 0$

Perturbations to self-regulation (changing a) affect the trace; perturbations to cross-regulation (changing bc) affect the determinant. The certificate survives if both margins exceed their respective perturbations.

10.3 Key Results

- **T01–T04 (Stability foundations):** Trace negative, both margins positive, full Routh-Hurwitz stability certificate.
- **T05–T07 (Robustness):** If trace margin exceeds self-regulation perturbation AND det margin exceeds cross-regulation perturbation, stability survives. Full robustness = both survive.
- **T08–T09 (Certificate algebra):** Meet of trace and det margins is positive; more negative trace implies larger trace margin (dominance).
- **T10–T11 (Design monotonicity):** Under the declared orderings, a more negative diagonal term decreases the trace. Separately, decreasing the **signed** product bc increases $\det(J) = ad - bc$. This is not an absolute-cross-talk claim: reducing $|bc|$ can decrease the determinant when $bc < 0$.
- **T12–T14 (Headline):** Dual margin positivity, individual gene decay, and full GRN stability certificate combining Routh-Hurwitz with individual decay.

10.4 Significance

This is the third biotech domain. It uses linearized ODE stability rather than thermodynamic equilibrium or classifier statistics. The dual-margin structure parallels screening bounds because two conditions must hold simultaneously; for a real 2×2 linearization, trace and determinant jointly determine local asymptotic stability. The encoded monotonicity claims state how the supplied stability margins change under declared parameter orderings.

14 named conditional claims checked, 0 sorry.

11. Domain 9: Joint Thermal-Degradation (Coupled Physics)

11.1 Physical Model

Coupled battery system where temperature affects degradation rate through Arrhenius-type kinetics. In the linearized regime, the degradation margin decreases linearly with temperature excess above a reference point:

$$m_{Q,\text{coupled}} = m_{Q,\text{base}} - \alpha \cdot (T_{\text{cell}} - T_{\text{ref}})$$

where $\alpha > 0$ is the thermal sensitivity of degradation (units: capacity-% per °C). A joint certificate requires BOTH margins to be positive simultaneously:

$$\text{joint safe} \iff m_T > 0 \ \wedge \ m_{Q,\text{coupled}} > 0$$

11.2 Certificate

Product certificate: Two coupled margins where a single perturbation propagates through physical coupling. Temperature increase δT reduces thermal margin directly ($m_T \to m_T - \delta T$) AND reduces degradation margin through coupling ($m_Q \to m_Q - \alpha \cdot \delta T$). This "double hit" is what individual certificates miss.

11.3 Key Results

- **T01–T03 (Individual margins + joint safety):** Both margins positive; joint safety as conjunction.
- **T04–T05 (Coupling effects):** Coupled margin is strictly less than base margin when temperature exceeds reference. Stronger coupling (larger α) $\to$ smaller coupled margin.
- **T06–T08 (Joint robustness):** Thermal survives if margin exceeds δT; degradation survives if margin exceeds $\alpha \cdot \delta T$; full joint robustness requires both.
- **T09–T10 (Certificate algebra):** Joint margin (min of both) is positive; joint dominance (both margins larger $\to$ dominant).
- **T11–T13 (Joint design monotonicity):** Under the declared coupling model, increasing cooling improves the thermal margin directly and the degradation margin through the supplied coupling relation.
- **T14 (Headline):** Full joint certificate combining safety, coupling conservatism.

11.4 Significance

This is the first coupled-margin domain in the paper. In the encoded model, individual inequalities do not imply the joint predicate because the supplied coupling term can erode one margin. The product structure is the fifth certificate geometry used here.

14 named conditional claims checked, 0 sorry.

12. Domain 10: 3-Gene Regulatory Network Stability

12.1 Physical Model

For a 3-gene network, the characteristic polynomial of the Jacobian is $\lambda^3 + p_1\lambda^2 + p_2\lambda + p_3 = 0$ where $p_1 = -\text{trace}(J)$, $p_2 = \sum(2\times 2 \text{ principal minors})$, $p_3 = -\det(J)$. The Routh-Hurwitz conditions for 3D stability are:

$$(RH1)\ p_1 > 0, \quad (RH2)\ p_3 > 0, \quad (RH3)\ p_1 \cdot p_2 > p_3$$

All three are necessary and sufficient. The third condition ($p_1 \cdot p_2 > p_3$) is the critical cross-condition that has no 2D analogue — it is what makes 3D stability fundamentally harder than 2D.

12.2 Certificate

Triple margin certificate: $m_{p_1} = p_1 > 0$, $m_{p_3} = p_3 > 0$, $m_H = p_1 \cdot p_2 - p_3 > 0$. This is the sixth certificate geometry, distinct from margin, interval, multi-competitor, dual margin, and product certificates.

12.3 Key Results

- **T01–T04 (Routh-Hurwitz stability):** All three conditions individually and as conjunction.
- **T05–T06 (Robustness):** p survives perturbation; Hurwitz cross-condition survives if margin exceeds combined perturbation $\delta p_1 \cdot p_2 + \delta p_3$.
- **T07–T08 (Certificate algebra):** Meet of three margins positive; dominance on first coefficient.
- **T09–T10 (Design monotonicity):** More decay (larger p_1) $\rightarrow$ larger Hurwitz margin. Smaller p_3 $\rightarrow$ larger Hurwitz margin. Both are constructive engineering principles.
- **T11 (2D vs 3D):** Hurwitz margin is strictly less than $p_1 \cdot p_2$ (showing the cost of the determinant term).
- **T12 (Headline):** Full 3-gene stability certificate.

12.4 Significance

The 3-gene suite illustrates the additional cubic Hurwitz cross-condition $p_1 p_2 > p_3$. Positivity of p_1 and p_3 alone does not imply cubic stability. In the declared linearized model, the Hurwitz-margin sign separates the supplied stable and unstable scenarios.

12 named conditional claims checked, 0 sorry.

13. Domain 11: Triple Joint Certificate (Thermal + Phase + Degradation)

13.1 Physical Model

Three coupled battery failure modes driven by a common temperature excess. Temperature affects phase stability through Clausius-Clapeyron-type coupling (coefficient β) and degradation through Arrhenius coupling (coefficient α):

$$m_{P,\text{coupled}} = m_{P,\text{base}} - \beta \cdot T_{\text{excess}}, \quad m_{Q,\text{coupled}} = m_{Q,\text{base}} - \alpha \cdot T_{\text{excess}}$$

13.2 Certificate

Triple product certificate: Three coupled margins must all be positive simultaneously. A single temperature perturbation δT reduces thermal margin directly, phase margin by $\beta \cdot \delta T$, and degradation margin by $\alpha \cdot \delta T$. This "triple hit" from a single perturbation is the key structural novelty over the 2-domain product certificate (§11).

13.3 Key Results

- **T01–T02 (Triple safety):** All three margins and the triple margin (min of three) are positive.
- **T03–T05 (Coupling effects):** Both couplings are conservative (coupled < base).
- **T06–T09 (Triple hit robustness):** Thermal, phase, and degradation each survive individually; full triple robustness as conjunction.

- **T10–T13 (Triple monotonicity):** Cooling improves ALL THREE margins simultaneously — a single design action (better thermal management) improves thermal safety, structural stability, and cycle life.
- **T14 (Headline):** Full triple joint certificate.

13.4 Significance

This suite extends the encoded product structure from pairs to triples. Under the declared coupling equations, individual and pairwise inequalities need not imply the triple predicate when combined coupling exhausts one margin.

14 named conditional claims checked, 0 sorry.

14. Domain 12: Linear Half-Space Certificates (Polyhedral Safe Regions)

14.1 Physical Model

Generalization of interval certificates to n dimensions. The safe region is defined by k linear constraints (half-spaces):

$$c_i \cdot x \leq d_i \quad \text{for } i = 1, \dots, k$$

Their intersection is a convex polyhedron, which is a polytope only when bounded. A design point x satisfies the strict encoded certificate exactly when it lies in the strict interior, $c_i \cdot x < d_i$ for every i. Closed-region membership permits zero margin on the boundary and is therefore weaker. The margin for constraint i is $m_i = d_i - c_i \cdot x > 0$, and the aggregate margin is the supplied lower bound represented by poly_margin.

14.2 Certificate

Polyhedral strict-interior certificate: All k constraint margins are positive simultaneously. This linear-inequality geometry subsumes one-sided margin certificates and finite conjunctions of linear inequalities; bounded interval and polytope cases require the corresponding bounding constraints.

14.3 Key Results

- **T01–T03 (Strict membership):** All three encoded margins are positive; the supplied aggregate margin is positive and no larger than each component margin. The source conditions supply these order relations but do not prove exact equality to the mathematical minimum.
- **T04–T07 (Robustness):** If perturbation δ is smaller than the supplied aggregate margin, each encoded strict inequality survives.
- **T08 (Meet):** If a point is in the strict interiors of regions A and B, it satisfies their combined constraints.
- **T09 (Dominance):** All margins larger → safer (componentwise dominance).
- **T10 (Supplied improved aggregate):** Positivity is extracted from the separately declared positive improved aggregate margin. This theorem does not derive monotonicity from a component-margin change.

- **T11 (Headline):** Strict component-margin positivity plus positive supplied aggregate margin.

14.4 Significance

The linear half-space suite encodes a convex polyhedron and checks strict-interior membership with a supplied quantitative boundary budget. Boundedness is not proved. Interpreting a constraint slack as Euclidean distance to a face requires normalized constraints, and identifying the aggregate scalar with the exact minimum requires an exact minimum definition rather than the lower-bound conditions used in this source.

11 named conditional claims checked, 0 sorry.

15. Domain 13: Nonlinear Certificates (Quadratic and Coupled Safe Regions)

15.1 Physical Model

Generalization from linear constraints (polytope) to quadratic constraints. The safe region is defined by a single nonlinear inequality:

$$C - a \cdot x^2 - b \cdot y^2 - d \cdot x \cdot y > 0$$

Three specializations:

- **Disk** ($a = b$, $d = 0$): isotropic circular safe region, $R^2 - x^2 - y^2 > 0$
- **Ellipsoidal** ($a \neq b$, $d = 0$): anisotropic in the convex/ellipsoidal (positive-definite) case; otherwise a general quadratic-inequality region
- **Coupled penalty case** ($d > 0$, $x > 0$, $y > 0$): positive cross-parameter term dxy

15.2 Certificate

Quadratic certificate: A single curved constraint defines the encoded region. Unlike independent axis-aligned linear bounds, it can represent curved boundaries and a supplied cross-parameter term. The margin is position-dependent.

15.3 Key Results

- **T01–T04 (Disk):** Membership, distance-radius bound, position-dependent robustness (closer to center means more margin), perturbation robustness.
- **T05–T06 (Ellipsoidal):** Anisotropic membership; heavier weight axis uses more margin budget for the same deviation.
- **T07–T09 (Coupling):** Cross-product positivity ($x > 0, y > 0 \Rightarrow x \cdot y > 0$), coupling penalty positivity, coupling reduces margin ($m_{\text{coupled}} < m_{\text{uncoupled}}$).
- **T10–T11 (Dominance):** Larger radius increases the modeled margin; removing a positive coupling penalty increases the margin, so retaining the penalty is the conservative treatment.
- **T12 (Headline):** Full nonlinear certificate.

15.4 Significance

The quadratic certificate is the eighth geometry in the framework. A positive-definite quadratic form gives an ellipsoidal region, while the term dxy represents a declared cross-parameter interaction. Two coordinates can satisfy separate bounds while the supplied cross term makes the joint quadratic margin negative. This is the parameter-level analogue of the coupling terms in §§11 and 13.

12 named conditional claims checked, 0 sorry.

16. Named Design Point Certificates

The abstract suites of §§3–15 check implications over regions defined by their assumptions. This section illustrates the resulting arithmetic at named scenarios inspired by products, technology nodes, drug candidates, and diagnostic assays. The values are supplied examples, not measurements established by this paper.

16.1 Battery Thermal Safety: Cell Formats

Illustrative, uncalibrated table. The stored scenario manifest checks arithmetic claims for three supplied cell-format parameter sets:

Design Point	q_{rem} (W)	q_{gen} (W)	Margin (W)	Checked margin bound
NP1: Cylindrical 18650 (forced air, $h = 25$ W/m²K)	3.0	1.2	1.8	> 1 W
NP2: Pouch cell (passive, $h = 10$ W/m²K)	1.2	0.5	0.7	> 0 W
NP3: Large prismatic (liquid, $h = 100$ W/m²K)	120	35	85	> 80 W

Conditional safety-margin ordering: pouch < 18650 < prismatic; the supplied liquid-cooling scenario has the largest margin. 13 named arithmetic claims checked.

16.2 Semiconductor Electromigration: Technology Nodes

Illustrative, uncalibrated table. The stored scenario manifest checks arithmetic claims for three supplied technology-node parameter sets:

Design Point	MTTF (years)	Warranty (years)	Margin (years)
NP1: Cu 7nm FinFET (leading edge)	15	10	5

Design Point	MTTF (years)	Warranty (years)	Margin (years)
NP2: Cu 14nm FinFET (mainstream server)	50	7	43
NP3: Al 180nm legacy (automotive)	200	15	185

Conditional lifetime-margin ordering: 7nm < 14nm < 180nm under the supplied values. 12 named arithmetic claims checked.

16.3 Battery Degradation: Cell Chemistries

Illustrative, uncalibrated table. The stored scenario manifest checks arithmetic claims for three supplied chemistry parameter sets:

Design Point	Q_{now} (%)	Q_{EOL} (%)	Margin (%)	Application
NP1: NMC 622 (10yr, 2000 cycles)	80	70	10	EV
NP2: LFP (20yr, 5000 cycles)	86	60	26	Grid storage
NP3: NCA (8yr, 1500 cycles)	73	70	3	Consumer

Conditional capacity-margin ordering: NCA < NMC < LFP under the supplied values. 11 named arithmetic claims checked.

16.4 Catalyst Stability: Reaction Systems

Illustrative, uncalibrated table. The stored scenario manifest checks arithmetic claims for three supplied catalyst parameter sets:

Design Point	Reaction	Window Width	Low Margin	Centered?
NP1: Pt	HER	4 (narrow)	2	Yes
NP2: Pd	ORR	20 (wide)	10	Yes
NP3: Fe	NH_3 synthesis	8 (moderate)	4	Yes

Conditional margin ordering: Pt < Fe < Pd under the supplied values; Pd has the largest modeled slack. 12 named arithmetic claims checked.

16.5 Material Phase Stability: Alloy Systems

Illustrative, uncalibrated table. The stored scenario manifest records arithmetic claims for three supplied material parameter sets:

Design Point	Target Phase	Competitors	Min Margin (scaled units; 10 units = 1 kJ/mol)	Closest Competitor
NP1: NiAl (turbine blade)	B2	L1 , BCC	35	L1
NP2: Fe-Cr steel (structural)	FCC austenite	BCC ferrite, -phase	5	BCC (**tight**)
NP3: NMC 811 (cathode)	Layered	Spinel, Rock-salt	15	Spinel

Conditional margin ordering: Fe-Cr (5) < NMC (15) < NiAl (35) under the illustrative inputs. 11 named arithmetic claims checked.

16.6 Binding Stability: Drug Candidates

Illustrative, uncalibrated table. The stored scenario manifest records arithmetic claims for three supplied protein-ligand parameter sets:

Design Point	Binding Strength (scaled units; 10 units = 1 kcal/mol)	Threshold	Margin	Off-Target	Selective?
NP1: Imatinib → BCR-ABL (kinase inhibitor)	123	90	33	75	Yes
NP2: Trastuzumab → HER2 (antibody)	115	90	25	60	Yes
NP3: Biotin → Streptavidin (biosensor)	180	90	90	—	—

Scenario strength ordering: Trastuzumab < Imatinib < Biotin. Under the declared illustrative values, Biotin-Streptavidin has the largest margin (90 units = 9.0 kcal/mol). This is a conditional comparison of the scenario inputs, not an empirical ranking derived by the proof. 12 conditional certificate lemmas are checked.

16.7 Screening Bounds: Diagnostic Tests

Illustrative, uncalibrated table. The stored scenario manifest records arithmetic claims for three supplied diagnostic/screening parameter sets (rates per 1000; for example, 20 means 2%):

Design Point	FNR	FPR	FNR Threshold	FPR Threshold	Passes?
NP1: PCR COVID-19 (gold standard)	20	5	100	50	**Yes**
NP2: Rapid Antigen (point-of-care)	150	10	100	50	**No** (FNR fails)
NP3: HTS Drug Screen (pharma)	80	30	100	50	**Yes**

Under the illustrative values, the rapid-antigen scenario fails the supplied FNR threshold. **Conditional FNR ordering:** PCR $<$ HTS $<$ rapid antigen. 11 named arithmetic claims checked.

16.8 Gene Regulatory Networks: Synthetic Circuits

Illustrative, uncalibrated table. The stored scenario manifest checks arithmetic claims for three supplied linearized circuit models:

Design Point	Circuit Type	Trace	Det	Stable?
NP1: Toggle Switch (Gardner 2000)	Mutual repression	-4	3	**Yes**
NP2: Negative Autoreg (Alon 2007)	Self-repression + activation	-4	3	**Yes**
NP3: Positive Feedback	Mutual activation	-2	-3	**No** (saddle)

Under the declared linearization, the positive-feedback scenario has $\det(J) < 0$ and is locally unstable. The toggle-switch and negative-autoregulation scenarios have equal supplied trace margins. 10 named arithmetic claims checked.

16.9 Joint Thermal-Degradation: Battery Packs

Illustrative, uncalibrated table. The stored scenario manifest checks arithmetic claims for three supplied coupled thermal-degradation parameter sets:

Design Point	Chemistry	margin_T	margin_Q_base		T_excess	Coupling	margin_Q_coupled	Joint?
NP1: LFP Prismatic	LFP	25	12	0.3	10	3	**9**	**Safe**
NP2: NMC Pouch	NMC	15	8	0.4	15	6	**2**	**Safe (tight)**
NP3: NMC Fast-Charge	NMC	7	5	0.3	23	6.9	**−1.9**	**FAILS**

The illustrative NMC fast-charge scenario passes its individual thermal inequality but fails the supplied joint inequality because the coupling term exceeds the base degradation margin. Under the supplied values, LFP has larger margins on both coordinates. 10 named arithmetic claims checked.

16.10 3-Gene GRN: Circuit Architectures

Illustrative, uncalibrated table. The stored scenario manifest checks arithmetic claims for three supplied cubic characteristic polynomials:

Design Point	Architecture	p	p	p	p · p	Hurwitz margin	Stable?
NP1: Stable Cascade	Feedforward	9	26	24	234	**210**	**Yes**
NP2: Repressilator (Elowitz 2000)	Cyclic repression	6	9	16	54	**38**	**Yes**
NP3: Strong Repressilator	Cyclic (strong)	3	0	28	0	**−28**	**No** (oscillates)

The illustrative strong-repressilator scenario satisfies $p_1 > 0$ and $p_3 > 0$ but fails the cubic cross-condition $p_1 p_2 > p_3$. In the declared linearized polynomial model, this is a Hurwitz-margin-negative scenario. The supplied cascade margin is 5.5 times the supplied damped-repressilator margin. 9 named arithmetic claims checked.

16.11 Triple Joint: Battery Pack Certification

Illustrative, uncalibrated table. The stored scenario manifest checks arithmetic claims for three supplied triple coupled-margin parameter sets:

Design Point	Chemistry	margin_T	P_coupled	Q_coupled	Triple?
NP1: LFP Prismatic	LFP	25	13	9	**Safe**
NP2: NMC Pouch	NMC	15	3.5	2	**Safe (tight)**
NP3: High-Perf NMC	NMC	10	−1	1	**FAILS**

The illustrative high-performance NMC scenario satisfies its individual thermal and degradation inequalities but fails the supplied phase-margin inequality. Under the supplied values, LFP has larger thermal and phase margins. 8 named arithmetic claims checked.

16.12 Polyhedral Constraints: Multi-Parameter Envelopes

Illustrative, uncalibrated table. The stored scenario manifest checks arithmetic claims for three supplied linear-constraint parameter sets:

Design Point	Application	Constraints	Margins	Aggregate margin	Strictly inside?
NP1: Semiconductor	Process window (T, P)	T [180,220], T+100P 370	20, 20, 70	20	**Yes**
NP2: Battery	Operating envelope (V, I)	V [2.5,4.2], V−0.1I 2.4	12, 10, 11	10	**Yes**
NP3: Alloy	Composition (Cr, Ni)	Cr 12, Ni 25, Cr+Ni 35	2, 2, −2	—	**FAILS**

The illustrative alloy composition satisfies its first two supplied constraints but fails the third because $Cr + Ni = 37 > 35$. The supplied semiconductor-process margin is twice the supplied battery-envelope margin. 7 named arithmetic claims checked.

16.13 Nonlinear: Multi-Physics Envelopes

Illustrative, uncalibrated table. The stored scenario manifest checks arithmetic claims for three supplied quadratic parameter sets:

Design Point	Application	Type	Margin	Safe?
NP1: Semiconductor CVD	Process window (ΔT, ΔP)	Disk, R^2=400	300	**Yes**
NP2: Chemical Reactor	Ellipsoidal (ΔT, ΔP)	Weighted, a=1 b=4	39	**Yes**
NP3: Turbine Blade	Coupled (Δ , ΔT)	Coupled, d=2	−31	**FAILS**

The illustrative turbine-blade scenario passes the uncoupled quadratic inequality but fails the supplied coupled inequality because the cross term exceeds the uncoupled margin. The supplied CVD margin is approximately 7.7 times the supplied reactor margin. 8 named arithmetic claims checked.

16.14 Cross-Design Implications

The illustrative named-scenario checks serve three purposes:

1. **Arithmetic illustration.** Each scenario shows how supplied values determine a modeled margin.
2. **Conditional comparison.** The cross-scenario claims check rankings under the stated values; they are not empirical observations.
3. **Failure-path illustration.** Negative margins show how the encoded certificate predicates expose violations of supplied thresholds. They are not evidence that named real-world products fail.

17. Deterministic Uncertainty-Penalized Certificate Algebra (CA5)

17.1 Motivation

The certificates in §3–15 assume known parameters. In practice, model inputs are uncertain: binding energies have measurement error, degradation rates vary across manufactured units, and screening assay sensitivities vary across batches. This section studies a deterministic penalty once a bound on the induced margin error has been declared. It does not derive that bound from data.

17.2 Uncertainty-Penalized Margins

We extend the certificate algebra with a fifth rule:

CA5 (Uncertainty penalty). Given a deterministic margin $m > 0$, uncertainty scale $\sigma > 0$, multiplier $k > 0$, and a declared bound that the induced margin error has magnitude at most $k\sigma$, define:

$$m_{\text{pen}} = m - k \cdot \sigma$$

If $m > k \cdot \sigma$, then $m_{\text{pen}} > 0$: the certificate holds for perturbations covered by the declared $k\sigma$ margin-error bound. A standard deviation alone does not provide this deterministic bound, and a coverage probability requires a distributional model.

17.3 Key Results

- **T01–T04 (Foundations):** The penalty $k\sigma$ is positive. The penalized margin is positive if $m > k\sigma$, and it is strictly smaller than the unpenalized margin.
- **T05–T07 (Multiplier ordering):** Higher k gives a larger penalty and smaller penalized margin. If $m > k_{\text{high}}\sigma$, the margin remains positive even under the larger declared penalty.
- **T08–T09 (Meet):** The meet of two positive penalized margins inherits positivity. CA5 composes with CA1.
- **T10–T11 (Monotonicity):** Improving the design ($m \uparrow$) increases the penalized margin at fixed uncertainty scale. Reducing σ increases the penalized margin at fixed design. Both implications are strict under the stated inequalities.
- **T12–T14 (Cross-domain):** For two domains with positive penalized margins, the comparison depends on both the unpenalized margins and the declared uncertainty penalties.

17.4 Significance

CA5 adds a deterministic uncertainty-margin rule to the certificate algebra. The five rules (CA1: meet, CA2: dominance, CA3: monotonicity, CA4: robustness, CA5: uncertainty penalty) provide a unified algebraic toolkit for reasoning about design certificates under declared perturbation bounds. CA5 does not derive an error bound or supply probabilistic coverage. It can be instantiated for each margin certificate in §3–15 once a domain-specific margin-error bound is supplied.

14 named conditional claims checked, 0 sorry.

18. Cross-Domain Transfer Analysis

18.1 What Transfers

Property	Batt.Th	Semi.EM	Batt.Deg	Catalyst	Phase	Binding	Screen	GRN-2D	Joint	GRN-3D	Triple	Polytope	**Nonlinear**
Track	Mat	Mat	Mat	Mat	Mat	Bio	Bio	Bio	Mat	Bio	Mat	Cross	**Cross**
Physics	Arrhen	Arrhen	Pow-law	Sabatier	Gibbs	ΔG	Sens/Sp	Jacob	Coupled	RH-3D	3-coupled	k-linear	**Quadratic**
Geometry	Margin	Margin	Margin	Interval	Two-comp	Margin	Dual-m	Dual-m	Product	Triple-m	Tri-prod	Polyhedral	**Quadratic**
Domain-specific CA1–CA4 subset	impl.	impl.	impl.	impl.	impl.	impl.	impl.	impl.	impl.	impl.	impl.	impl.	**impl.**

Property	Batt.Th	Semi.EM	Batt.Deg	Catalyst	Phase	Binding	Screen	GRN-2D	Joint	GRN-3D	Triple	Polytope	**Nonlinear**
Domain-specific CA5 error bound	—	—	—	—	—	—	—	—	—	—	—	—	—
Abstract	14	14	14	14	14	14	14	14	14	12	14	11	12
Named	13	12	11	12	11	12	11	10	10	9	8	7	8

Each domain suite implements a domain-specific subset or analogue of CA1–CA4; the table does not assert a uniform theorem schema. CA5 is a separate generic suite and has no domain-specific instantiation in the retained corpus. It becomes applicable only after a domain-specific induced-margin-error bound is declared. Total reported corpus: 189 abstract-suite claims + 134 named-scenario claims = 323 named kernel-checked claims. This inventory includes direct condition restatements as well as derived arithmetic and algebraic consequences.

The 189-claim abstract inventory follows each field's declared proof surface. In particular, the phase, binding, and screening counts use explore_phase_certificate.py, explore_binding_certificate.py, and explore_screening_certificate.py, respectively; the other eleven abstract counts use their field-level *_proof.py suite. The 134 named-scenario claims come from the thirteen explore_named_design_points.py suites. For every selected manifest, the counting algorithm retains all theorem entries except the infrastructure entry named Not; naïvely summing each manifest's total_theorems would therefore give 350 rather than 323. Additional same-domain proof files are not included.

The theorem-level claim map assigns a conservative semantic source grade to every retained row: **A: 0** substantive model theorems, **B: 243** residual arithmetic or algebraic derivations, **C: 62** structural assemblies or other kernel-checked implications, and **D: 18** direct premise restatements or conjunct extractions. The classifier resolves target aliases and compares each target with referenced conditions and their conjunction components before considering the closing tactic, so linarith or nlinarith cannot by itself promote a direct extraction to B. These grades describe theorem content within the declared formal model, not scientific importance; grade B does not validate a model equation or supplied number.

18.2 What Does NOT Transfer

- Physical parameter names and units
- The specific functional form of the performance function f
- Numerical values of critical thresholds
- The certificate geometry (half-space vs interval vs multi-competitor vs dual margin — but the algebra adapts)
- Domain-specific certificate dimensions (selectivity is binding-only; Jacobian trace/det is GRN-only; Arrhenius coupling is joint-only; Hurwitz cross-condition is 3D-only; polyhedral constraint geometry is application-specific; quadratic coupling coefficients are physics-specific)

18.3 The Template

The certificate algebra is a **reusable proof template.** For a new domain, one needs to:

1. Define the physical model parameters and safe region (margin, interval, multi-competitor, or dual margin)
2. Prove that design improvements preserve or enlarge the safe region
3. Instantiate only the applicable CA1–CA4 implications; add CA5 only after supplying a domain-specific induced-margin-error bound.
4. Optionally instantiate illustrative scenarios with supplied numeric values.

The repeated proof structure in the current suites provides implementation evidence that the template is reusable. No controlled timing or engineering-effort study was performed.

18.4 Eight Certificate Geometries

The framework covers eight distinct certificate geometries:

- **Margin certificates** (battery thermal, EM, degradation, binding): the encoded predicate is margin > 0. The region is a half-space, meet takes the minimum margin, and the margin magnitude is the available slack.
- **Interval certificates** (catalyst stability): the encoded predicate is value $\in [a, b]$. The region is a bounded interval, and the slack is the smaller distance to its endpoints.
- **Finite multi-competitor margin certificates** (phase stability): the encoded predicate is $\min(\Delta G_\beta, \Delta G_\gamma) > 0$ for the two modeled competitors.
- **Dual margin certificates** (screening bounds, GRN 2D stability): two margins must be positive simultaneously. Meet applies to each margin and to their conjunction.
- **Product certificates** (joint thermal-degradation, triple joint): multiple declared coupled margins must be positive simultaneously.
- **Triple margin certificates** (3-gene GRN): the three cubic Routh-Hurwitz conditions are $p_1 > 0$, $p_3 > 0$, and $p_1 p_2 > p_3$.
- **Polyhedral strict-interior certificates** (multi-parameter envelopes): the point must satisfy k strict linear constraints. Boundedness is not proved; Euclidean distance to a face requires normalized constraints.
- **Quadratic certificates** (nonlinear envelopes): the encoded predicate is $C - ax^2 - by^2 - dxy > 0$, allowing curved boundaries and a supplied cross-parameter term.

Across the eight encoded geometries, the sources reuse positive-margin conjunction, ordering, and perturbation patterns where their declared assumptions support them. This is shared algebraic structure, not a claim that every rule is instantiated in every domain.

19. Potential Applications and Limitations

19.1 Value Proposition

The formal layer can complement, but not replace, the established validation practices below.

Application	Current Practice	Potential role of conditional model certificates
Battery safety qualification	Physical tests + simulation	Check consequences of a declared operating-envelope model
Semiconductor reliability	Empirical Black's equation fits	Conditional worst-corner lifetime implication in the declared model
Battery warranty	Accelerated aging tests	Check a supplied degradation-model inequality
Catalyst screening	DFT + trial synthesis	Check consequences of a supplied interval model
Alloy/material design	Phase diagram lookup + trial	Check a supplied phase-margin model
Drug candidate screening	Binding assays + ADMET cascade	Check a supplied binding/selectivity model
Diagnostic test validation	Clinical trials + statistics	Check supplied error-rate inequalities
Parameter uncertainty	Safety factors (1.5×, 2×)	Declared uncertainty penalty (CA5, $k\sigma$)
Design optimization	Trial-and-error with safety factors	Use declared monotonicity assumptions to organize search
Synthetic biology design	Simulation + wet-lab iteration	Check local-stability implications in a declared linearization
Technical documentation	Engineering judgment	Record machine-checked implications and explicit assumptions

19.2 Three Certificate Domains

The framework now spans two distinct industrial tracks:

Track 1: Materials and energy models. Seven domains (§3–7, §11, §13) cover batteries, semiconductors, catalysts, materials, coupled thermal-degradation, and a triple coupled-margin model. The inventory contains 98 abstract-suite claims and 77 named-scenario checks. The examples range from single-parameter Arrhenius equations to supplied triple-coupled inequalities.

Track 2: Bio/genomic screening models. Four domains (§8–10, §12) cover binding, diagnostic screening, and 2D and 3D gene-network local stability. The inventory contains 54 abstract-suite claims and 42 named-scenario checks.

Cross-domain multi-parameter envelopes. Two domains (§14–15) encode polyhedral and quadratic geometries. The inventory contains 23 abstract-suite claims and 15 named-scenario checks.

19.3 Limitations

1. **Model fidelity.** The certificates are conditional on the physical model. A wrong model produces a formally correct but physically meaningless certificate.

2. **Parameter uncertainty.** CA5 propagates a supplied margin-error bound; it does not derive that bound from data or a probability model. Applications requiring coverage probabilities or posterior distributions need additional statistical assumptions and validation.

3. **Coupled effects beyond triples.** The current framework addresses pairwise (§11) and triple (§13) multi-physics coupling. Extending to 4+ coupled domains or continuous coupling networks remains future work.

4. **Named scenarios are illustrative.** The numeric values in §16 are supplied examples; this paper does not document their provenance as measurements of the named products or technologies.

19.4 Future Directions

- **Higher-order nonlinear** (extend quadratic certificates to cubic and beyond)
- **4+ gene networks** (Routh-Hurwitz for higher dimensions, Lyapunov-based approaches)
- **Automated certificate generation** (given a physics model, auto-derive the certificate suite)
- **Time-varying certificates** (margins that evolve with operating time, not just static snapshots)
- **Stochastic certificates** (combining uncertainty penalties with an explicit probabilistic model and time-varying dynamics)

20. Conclusion

The stored proof manifests show that the kernel checked a reusable family of conditional certificate implications across declared models from materials science, biotechnology, and multi-parameter operating-envelope design. Domain-specific subsets of the meet, dominance, monotonicity, and robustness patterns recur in thirteen suites. The uncertainty-penalty rule is implemented only in a separate generic suite; it is not domain-instantiated here. The reported inventory contains 323 named claims: 189 in fourteen abstract suites and 134 in thirteen named-scenario suites, with zero sorry placeholders. Some claims directly restate declared conditions; others are structural, arithmetic, or algebraic consequences. These artifacts complement, but do not validate or replace, simulation and experiment.

Seven findings stand out:

1. **Shared conditional algebra (template level).** Positive-margin conjunction, ordering, and perturbation implications recur across Arrhenius-exponential, power-law, interval, two-competitor, binding, classifier, Jacobian, coupled-margin, cubic Routh-Hurwitz, linear-constraint, and quadratic suites once each model's own equations and orderings are declared. No transfer of physical validity or parameter values is claimed.

2. **Eight certificate geometries.** The comparative artifact groups the suites as margin, interval, finite multi-competitor, dual margin, product, triple margin, polyhedral, and quadratic certificates. This taxonomy is descriptive, not proved complete or canonical.

3. **Cross-track reuse.** The same proof structure is instantiated for battery, binding, screening, and gene-network models, showing code-level reuse across the encoded suites.
4. **Coupled physics and higher dimensions.** Joint certificates (§11, §13) demonstrate that single-domain analysis is insufficient when physical coupling exists — a battery can pass individual and pairwise certificates but fail the triple joint analysis. 3-gene Routh-Hurwitz certificates (§12) show that the framework scales to higher-dimensional dynamical systems.
5. **Polyhedral and quadratic certificates (§14–15).** The linear suite handles strict interiors of half-space intersections without asserting boundedness; the quadratic suite handles curved boundaries with a supplied cross-parameter term.
6. **Deterministic uncertainty penalties (CA5).** Penalized margins $m_{\text{pen}} = m - k\sigma > 0$ preserve certification when the induced margin error is bounded by $k\sigma$. The rule can be instantiated across the thirteen domains only after supplying the relevant domain-specific error bound.
7. **Seven negative-margin scenario checks.** Under the illustrative inputs, seven named scenarios violate an encoded inequality: rapid antigen FNR (§16.7), positive-feedback GRN determinant (§16.8), NMC fast-charge coupling (§16.9), strong-repressilator Hurwitz margin (§16.10), NMC phase margin (§16.11), alloy workability (§16.12), and turbine-blade coupled margin (§16.13).

A machine-checked conditional certificate is not a replacement for physical testing or clinical trials. It is a complement: within the declared model, it identifies regions satisfying or violating the encoded inequalities, so experimental resources can focus on model validation and boundary cases.

Declaration of Generative AI and AI-assisted technologies in the writing process

During the preparation of this work the author used Cursor and its integrated AI models (Claude and GPT families) in order to assist with manuscript drafting, structural editing, and language polishing. After using this tool/service, the author reviewed and edited the content as needed and takes full responsibility for the content of the publication.

References

- Semenov, N. N. (1928). Zur Theorie des Verbrennungsprozesses. *Zeitschrift für Physik*, 48(7–8), 571–582. DOI: 10.1007/BF01340021
- Frank-Kamenetskii, D. A. (1955). Diffusion and Heat Exchange in Chemical Kinetics. Princeton University Press. DOI: 10.1515/9781400877195
- Black, J. R. (1969). Electromigration—A Brief Survey and Some Recent Results. *IEEE Transactions on Electron Devices*, 16(4), 338–347. DOI: 10.1109/T-ED.1969.16754
- Bloom, I. et al. (2001). An Accelerated Calendar and Cycle Life Study of Li-Ion Cells. *Journal of Power Sources*, 101(2), 238–247. DOI: 10.1016/S0378-7753(01)00783-2

- Nørskov, J. K. et al. (2009). Towards the Computational Design of Solid Catalysts. *Nature Chemistry*, 1, 37–46. DOI: 10.1038/nchem.121
- Medford, A. J. et al. (2015). From the Sabatier Principle to a Predictive Theory of Transition-Metal Heterogeneous Catalysis. *Journal of Catalysis*, 328, 36–42. DOI: 10.1016/j.jcat.2014.12.033
- Kaufman, L. and Bernstein, H. (1970). Computer Calculation of Phase Diagrams with Special Reference to Refractory Metals. Academic Press. https://archive.org/details/computercalculat0004kauf
- Du, X. et al. (2016). Insights into Protein–Ligand Interactions: Mechanisms, Models, and Methods. *International Journal of Molecular Sciences*, 17(2), 144. DOI: 10.3390/ijms17020144
- Bissantz, C. et al. (2010). A Medicinal Chemist's Guide to Molecular Interactions. *Journal of Medicinal Chemistry*, 53(14), 5061–5084. DOI: 10.1021/jm100112j
- Pepe, M. S. (2003). The Statistical Evaluation of Medical Tests for Classification and Prediction. Oxford University Press.
- Obuchowski, N. A. (2003). Receiver Operating Characteristic Curves and Their Use in Radiology. *Radiology*, 229(1), 3–8. DOI: 10.1148/radiol.2291010898
- Gardner, T. S. et al. (2000). Construction of a Genetic Toggle Switch in Escherichia coli. *Nature*, 403, 339–342. DOI: 10.1038/35002131
- Alon, U. (2007). Network Motifs: Theory and Experimental Approaches. *Nature Reviews Genetics*, 8, 450–461. DOI: 10.1038/nrg2102
- Murray, J. D. (2002). Mathematical Biology I: An Introduction. Springer. DOI: 10.1007/b98868
- Elowitz, M. B. and Leibler, S. (2000). A Synthetic Oscillatory Network of Transcriptional Regulators. *Nature*, 403, 335–338. DOI: 10.1038/35002125
- Gantmacher, F. R. (1959). The Theory of Matrices, Volume II. Chelsea Publishing Company. https://old.maa.org/press/maa-reviews/the-theory-of-matrices-volume-2
- Prajna, S. and Jadbabaie, A. (2004). Safety Verification of Hybrid Systems Using Barrier Certificates. *Hybrid Systems: Computation and Control*. DOI: 10.1007/978-3-540-24743-2_32
- Edwards, A., Peruffo, A., and Abate, A. (2024). Fossil 2.0: Formal Certificate Synthesis for the Verification and Control of Dynamical Models. *Proceedings of the 27th ACM International Conference on Hybrid Systems: Computation and Control*. DOI: 10.1145/3641513.3651398
- Nemouchi, Y. et al. (2019). Isabelle/SACM: Computer-Assisted Assurance Cases with Integrated Formal Methods. *Formal Methods and Software Engineering*. DOI: 10.1007/978-3-030-34968-4_21
- Chaudhuri, A. et al. (2022). Certifiable Risk-Based Engineering Design Optimization. *AIAA Journal*, 60(2), 551–565. DOI: 10.2514/1.J060539
- Eckert, C., Isaksson, O., and Earl, C. (2019). Design Margins: A Hidden Issue in Industry. *Design Science*, 5, e9. DOI: 10.1017/dsj.2019.7