

BEYOND RAG STATUSES

The Governance Illusion: Why Defence and Engineering Portfolios Fail Despite Rigorous Assurance

A Practitioner's Perspective on Portfolio Prioritisation and Decision Dynamics in Regulated Engineering Environments

Giovanni Leonardi

May 2020



The Governance Illusion: Why Defence and Engineering Portfolios Fail Despite Rigorous Assurance

Portfolio · No. 95

Originally written May 2020 | Re-edited and re-rendered for the WhereBeyond Edition, 2025

“Traditional portfolio assurance does not mitigate risk in complex engineering environments; it merely standardises the vocabulary used to explain failure after it occurs.”

1. The Problem Nobody Wants to Name: Compliance as a Substitute for Control

The uncomfortable truth confronting executive leadership across defence, aerospace, and advanced engineering sectors is that portfolio governance mechanisms are fundamentally failing to deliver predictability. Millions are invested annually in assurance frameworks, risk registers, and elaborate stage-gate architectures, yet multi-million-pound programmes consistently experience schedule slip, budget overshoot, and capability compromises.

The standard response from senior leadership to these systemic failures is depressingly predictable: enforce tighter controls, demand more granular reporting, and add additional governance gates. This approach rests on a flawed premise—the belief that delivery failure is caused by a lack of oversight.

In reality, traditional portfolio assurance does not mitigate risk in complex engineering environments; it merely standardises the vocabulary used to explain failure after it occurs. The primary function of contemporary portfolio management has quietly shifted from dynamic resource allocation and active intervention to administrative risk absorption and narrative management.

Across highly regulated, capital-intensive engineering portfolios, an inverse relationship frequently exists between the volume of governance reporting and actual delivery control. The more complex the reporting machinery, the greater the insulation between executive decision-makers and the engineering ground truth. Until portfolio leadership confronts the reality that process compliance is not operational control, large-scale capital programmes will continue to drift under the guise of rigorous oversight.

“Traditional portfolio assurance does not mitigate risk in complex engineering environments; it merely standardises the vocabulary used to explain failure after it occurs.”

2. Why It Happens: Three Structural Reasons

The persistence of this governance breakdown is rarely attributable to incompetence or lack of effort. Rather, it is driven by three entrenched structural failure modes inherent to complex engineering environments.

2.1.1. The Myth of Static Plan Execution in Dynamic Systems

Portfolio governance in engineering sectors is overwhelmingly built upon deterministic assumptions: a baseline plan is established, milestone dates are locked, and delivery teams are monitored on variance against this plan. This model operates effectively in low-complexity, linear environments. However, in major defence and engineering programmes characterised by concurrent technology development, evolving regulatory standards, and volatile supply chains, determinism is a dangerous illusion.

When a portfolio mechanism treats baseline plans as absolute, it penalises early variance detection rather than encouraging adaptive response. Programme managers quickly learn that highlighting emerging technical friction triggers immediate governance scrutiny and administrative overhead. Consequently, issues are suppressed, buffered, or rephrased as "manageable issues" until technical dependencies collapse, causing non-linear, catastrophic schedule slips.

2.2.2. Governance as Narrative Management

In matrixed organisations, portfolio dashboards serve a political function as much as an operational one. Red-Amber-Green (RAG) status reporting incentivises a culture of permanent optimism, often referred to as the "watermelon effect"—green on the outside, red on the inside.

Because governance bodies disproportionately reward visible progress over structural risk reduction, senior leaders receive sanitized data. Key performance indicators report activities completed (e.g., gates passed, design reviews conducted) rather than true system maturity or integrated risk reduction. The assurance process becomes an exercise in validating paper milestones while structural technical debt quietly accumulates across parallel workstreams.

2.3.3. Resource Phantomization and Capacity Delusions

Portfolio management assumes that human and technical resources are fungible assets that can be allocated, reallocated, and smoothed across programmes via spreadsheets. In advanced engineering, this assumption breaks down entirely.

Critical path capabilities—such as systems architecture, specialized safety engineering, or nuclear test cell access—cannot be arbitrarily divided into percentage allocations across six competing programmes. Yet, portfolio dashboards routinely mask critical resource over-commitment by reporting high-level headcounts rather than skill-specific constraint metrics. The result is "resource phantomization": resources appear fully assigned and balanced on paper, but in reality, key technical authorities are catastrophically over-allocated, creating hidden single points of failure that paralyse multiple programmes simultaneously.

Resource phantomization occurs when portfolio reporting shows engineering resources as balanced based on FTE headcounts, while masking the reality that critical technical specialists are assigned to multiple high-priority critical paths concurrently.

3. What Good Looks Like: The Three-Level Fix

To break the cycle of governance illusion, organisations must transition from static portfolio administration to dynamic constraint-based execution. This requires an opinionated restructuring across three distinct operational layers.

Domain	Traditional Governance Approach	Constraint-Based Portfolio Execution
Governance & Structure	Baseline variance tracking & fixed gates	Dynamic resource reallocation & capacity limits
Data & Insight	Activity-based milestones & subjective RAGs	Technical maturity vectors & constraint metrics
People & Culture	Narrative protection & variance penalty	Radical transparency & early-friction reward

3.11. Governance / Structural Level: Capacity-Indexed Portfolio Architecture

Organisations must abandon the practice of funding every approved strategic requirement and instead cap portfolio commitments to absolute, verified engineering capacity. Governance boards must cease acting as passive progress reviewers and operate as dynamic capacity allocators.

- **Implement Work-In-Progress (WIP) Limits at Portfolio Scale:** Establish strict caps on the number of major technical workstreams active concurrently across the enterprise. If a new high-priority defence mandate enters the portfolio, an existing programme must be paused, de-scoped, or explicitly de-prioritised.
- **Decouple Strategic Assurance from Line Management:** Independent technical assurance teams must report directly to executive portfolio boards, empowered to audit deep technical readiness rather than process compliance.
- **Dynamic Re-baselining Triggers:** Establish automated, non-punitive re-baselining events whenever strategic constraints (e.g., supply chain disruption, engineering

authority availability) cross predefined tolerance thresholds.

3.2.2. Data / Insight Level: Constraint-Based Delivery Reporting

Portfolio reporting must shift away from qualitative, self-reported RAG indicators toward objective metrics grounded in technical maturity and systemic flow.

- **Track Technical Maturity Vectors:** Replace milestone tracking with empirical measures of risk burn-down, such as physical integration progress, qualification test completion rates, and regulatory compliance closure rates.
- **Measure Resource Velocity & Contention Indexing:** Monitor real-time resource utilization at the critical specialist level rather than the general FTE level. Flag multi-programme contention points automatically before they manifest as schedule delays.
- **Leading Flow Indicators:** Focus governance oversight on leading flow metrics, such as lead time for technical change notes, open engineering query counts, and cross-workstream dependency lag.

3.3.3. People / Stakeholder / Culture Level: Psychological Safety for High-Friction Truths

No governance framework can succeed if reporting bad news carries personal or professional penalties for program directors. The human element of portfolio management requires deliberate cultural engineering.

- **Reward Early Friction Identification:** Restructure performance management to explicitly reward leadership teams that surface systemic cross-programme dependencies and technical risks early.
- **Standardise Deprioritisation Routines:** Normalise the stopping or de-scoping of projects. Executives must demonstrate that deprioritising non-viable workstreams is a mark of strong operational leadership, not project failure.
- **Build Shared Accountability Across Matrix Lines:** Align performance incentives between operational engineering leads, commercial procurement teams, and portfolio governance managers, eliminating regional or functional silos.

4. The Sector-Specific Complication: Regulatory Rigidity and Technical Interdependence

In sectors such as defence, nuclear, and aerospace, transitioning to modern, adaptive portfolio management faces an explicit obstacle: the strict regulatory and safety frameworks that govern physical engineering delivery.

Unlike software environments where features can be continuously deployed and rolled back, major defence assets operate within uncompromising regulatory regimes. Design baselines must be frozen, safety cases verified, and commercial contracts structured around rigid progress milestones. This creates an inherent tension between portfolio-level agility and system-level compliance.

Too often, organisations conflate regulatory compliance with rigid internal governance. While safety verification and regulatory sign-offs must remain non-negotiable and rigorous, the operational processes used to allocate resources, manage dependencies, and sequence engineering work across the enterprise do not need to be bureaucratic.

The strategic error made by many prime contractors and public sector bodies is projecting regulatory rigidity back into internal management structures. Governance frameworks must insulate engineering teams from administrative friction while maintaining strict alignment with regulatory authorities, ensuring that safety-critical path activities receive prioritised enterprise support.

5. What This Means in Practice: Decisive Interventions

Executing this transformation requires specific, practical interventions across the portfolio operational model:

1. **Audit the Assurance Burden:** Conduct an immediate assessment of all reporting routines across the portfolio. Eliminate any governance reporting that does not directly inform strategic resource allocation, risk mitigation, or prioritization decisions.
2. **Establish a Central Constraint Register:** Identify the top 5% of critical engineering capabilities and infrastructure assets across the organization. Map all active projects against these specific constraints to expose hidden single points of failure.
3. **Shift to Capacity-Based Prioritisation:** Conduct quarterly portfolio reviews focused on matching active delivery commitments against verified, skilled capacity, rather than theoretical project budgets.
4. **Implement Integrated Dependency Mapping:** Deploy dynamic, data-driven dependency mapping tools across all major workstreams to replace static manual updates, making cross-programme friction visible in real time.

6. Conclusion: The Uncomfortable Question

Portfolio management in complex defence and engineering environments stands at a critical juncture. Organizations can continue to expand administrative governance frameworks, generating endless progress reports while major capital assets suffer persistent cost and schedule inflation. Or they can confront the fundamental truth: governance without dynamic resource control is merely an expensive ritual.

Achieving true delivery maturity requires executive courage. It demands a willingness to strip away redundant process layers, establish strict capacity limits, and enforce realistic strategic prioritization across enterprise capabilities.

For executive leaders, portfolio directors, and programme heads across the sector, the fundamental question is no longer whether your governance framework is sufficiently comprehensive. The question you must ask yourself is this:

Does your current portfolio governance framework provide actionable control over critical engineering dependencies—or does it merely provide institutional cover while systemic risk accumulates across your enterprise?