SALAR
TECHNOLOGIES LLC
ENGINEERING THE FUTURE
AMERICAN GRIT. ADVANCED SYSTEMS.
salartechnologies.com

Defense Electronics Reliability and Supply-Chain Resilience

Internal strategic briefing book built from the public-safe five-lane SALAR framework: design reliability analysis, predictive failure analytics, semiconductor supply-chain risk intelligence, closed-loop manufacturing stability, and limited public positioning for AI-certified lithography control.

Prepared for internal planning, outreach alignment, and white-paper development.

Vikrant Salar
Founder & CEO

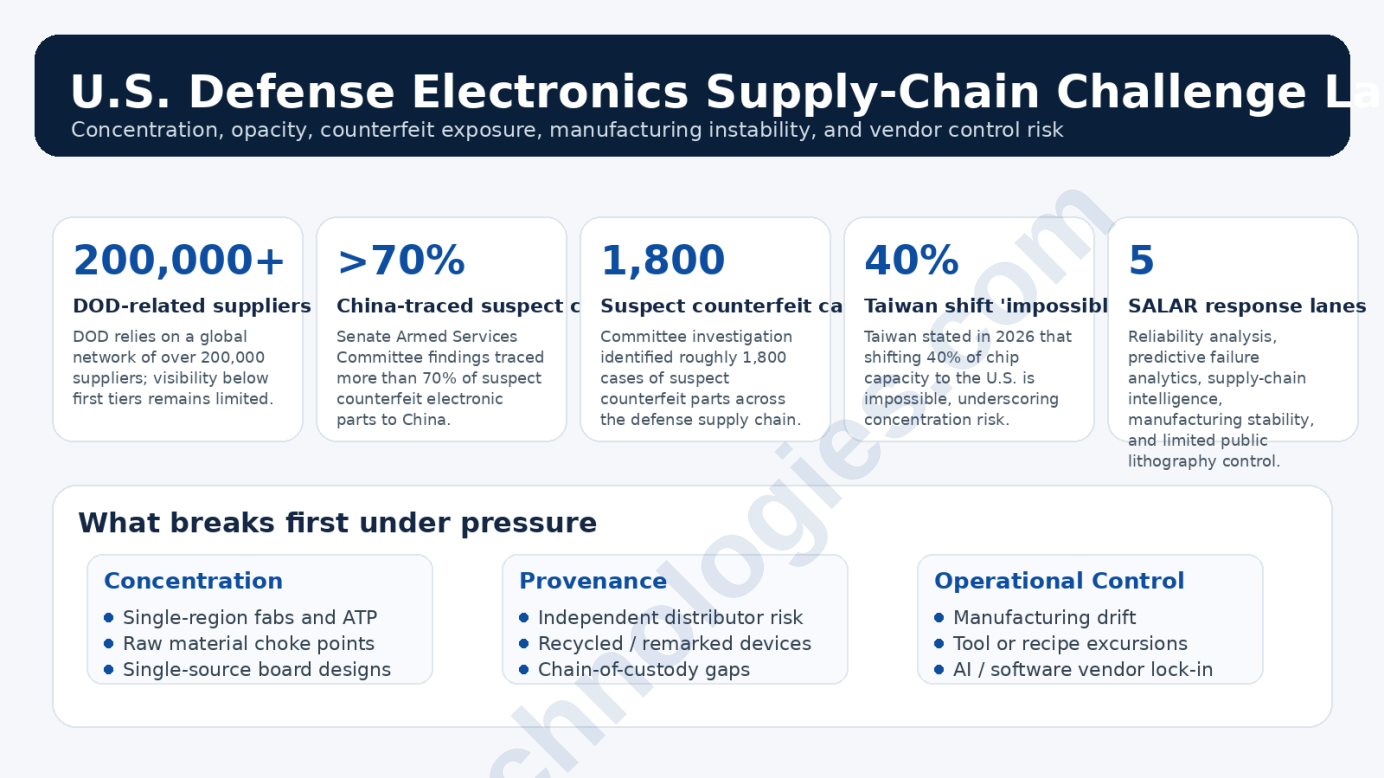
SALAR Technologies LLC
Registered in the State of Oregon
Oregon Registry No. 254232599

contact@salartechnologies.com
vikrant@salartechnologies.com
salartechnologies.com

Refocused thesis: SALAR is not just an AI company and not just a stack of patents. It is a resilience architecture for mission-critical electronics - reducing design fragility, counterfeit exposure, supplier concentration risk, manufacturing instability, and regional single-point failure.

1. Why this matters now

From a U.S. defense perspective, the core problem is not one single company or one single AI label. The core problem is concentration, opacity, and fragility across the electronics and semiconductor chain.



Key implication: supply-chain resilience must address hardware concentration, counterfeit/provenance exposure, manufacturing instability, and software/AI vendor dependency as one integrated system.

2. U.S. defense challenge landscape

• Foreign supplier dependence: DOD relies on a global network of over 200,000 suppliers and still has limited coordinated visibility into lower tiers and country-of-origin exposure.

• Semiconductor concentration: advanced manufacturing remains concentrated in a small number of geographies, creating choke-point risk under export controls, disaster, or conflict.

• Counterfeit and provenance exposure: suspect, remarked, recycled, or poorly handled parts can enter the chain and create latent mission failures.

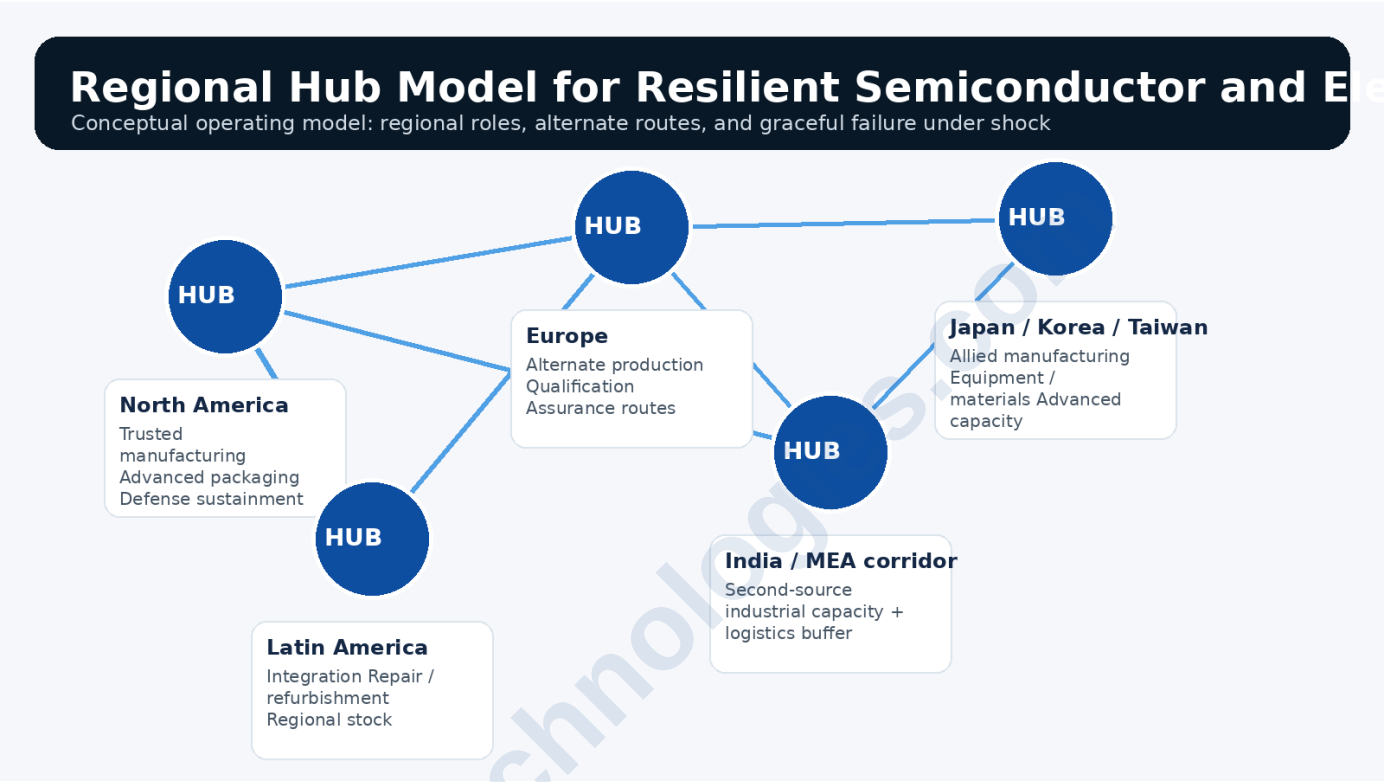
• Manufacturing instability: process drift and quality excursions can reduce throughput and downstream trust when demand is already stressed.

• Software / AI vendor control risk: loss of access to a critical AI or software provider can disrupt defense workflows even when the vendor is U.S.-based.

The Anthropic designation should be read less as a one-off corporate dispute and more as a signal that digital dependencies can now function like hardware choke points in defense operations.

3. Regional hub model

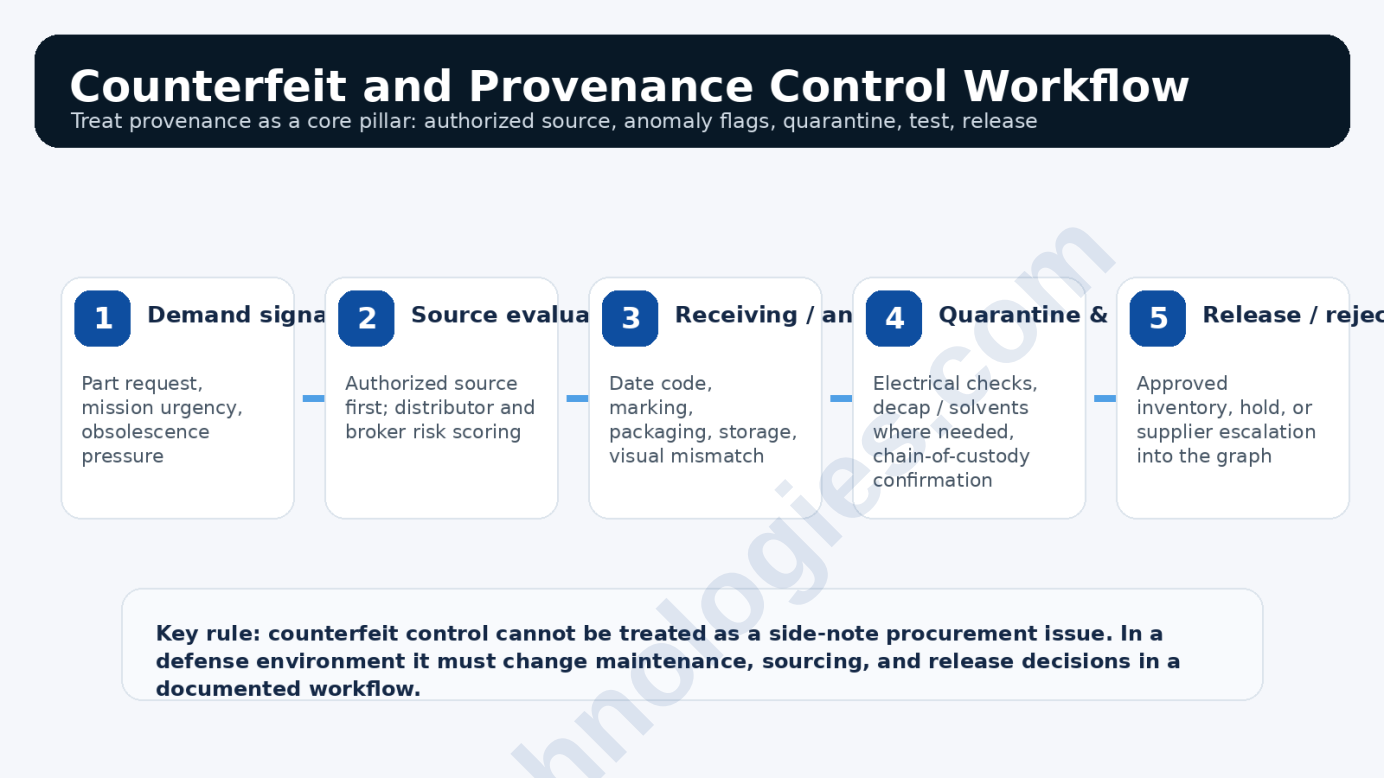
The strongest answer is not “move everything tomorrow.” The better answer is a differentiated regional network that can fail gracefully like the internet: if one node degrades, another carries load.



Region	Role
North America	Trusted manufacturing, advanced packaging, secure sustainment
Europe	Alternate production, qualification, assurance routes
India / MEA corridor	Second-source industrial capacity and logistics buffering
Japan / Korea / Taiwan	Allied manufacturing coordination and advanced capacity
Latin America	Integration, repair/refurbishment, regional stock positioning

4. Counterfeit and provenance must be a pillar

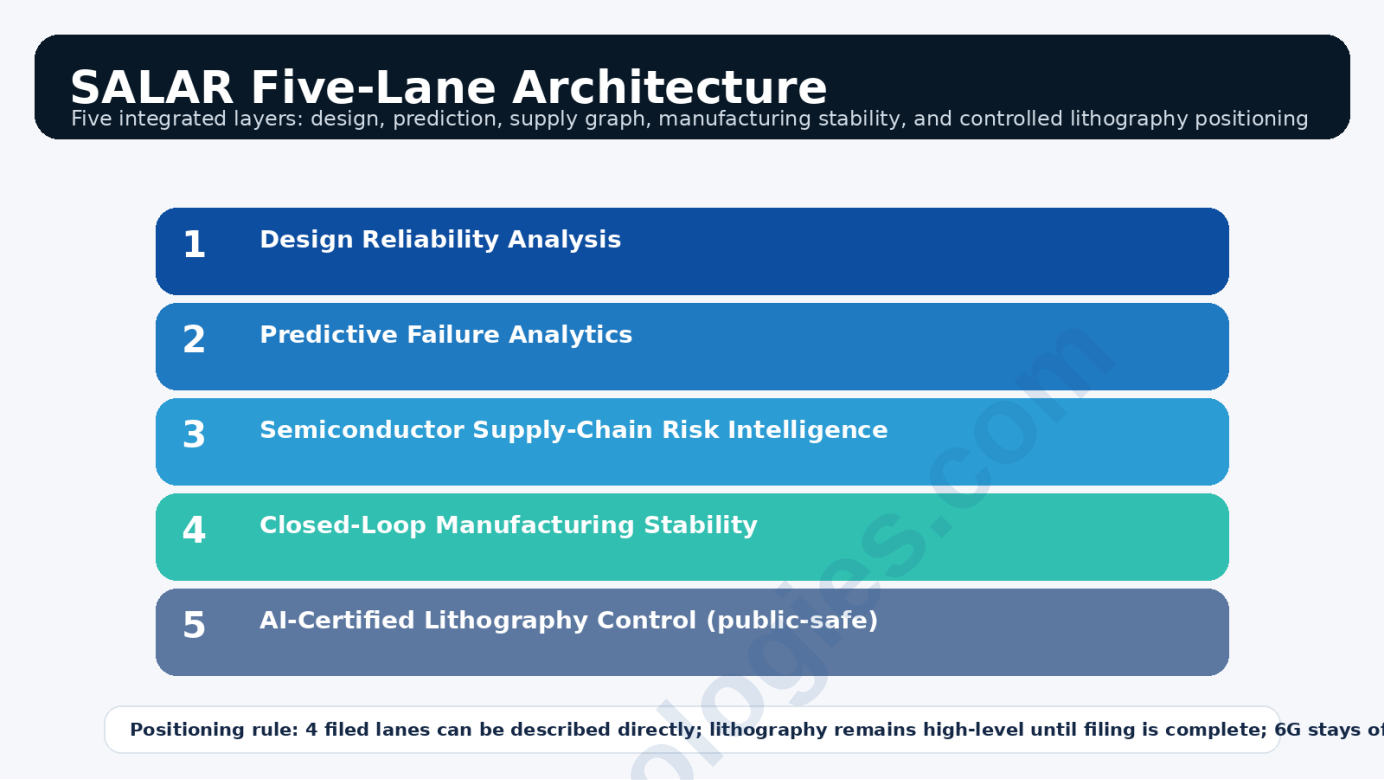
Counterfeit control should not sit in a small procurement appendix. In a defense environment, provenance should change maintenance, sourcing, and release decisions.



Operating model components:

- authorized-source preference
- chain-of-custody logic
- receiving anomaly flags
- quarantine / test / release workflow
- storage and handling history
- traceability back into the supply graph

5. The SALAR five-lane architecture



Lane 1 - Design Reliability Analysis: design for resilience at the board level so the platform is less fragile under part changes, thermal stress, and manufacturability constraints.

Lane 2 - Predictive Failure Analytics: use structured analytics to identify likely risk and maintenance priority before failure becomes a mission event.

Lane 3 - Semiconductor Supply-Chain Risk Intelligence: graph the supplier structure and identify concentration, provenance, dependency, and disruption exposure.

Lane 4 - Closed-Loop Manufacturing Stability: detect excursions early and preserve throughput and trust under stress.

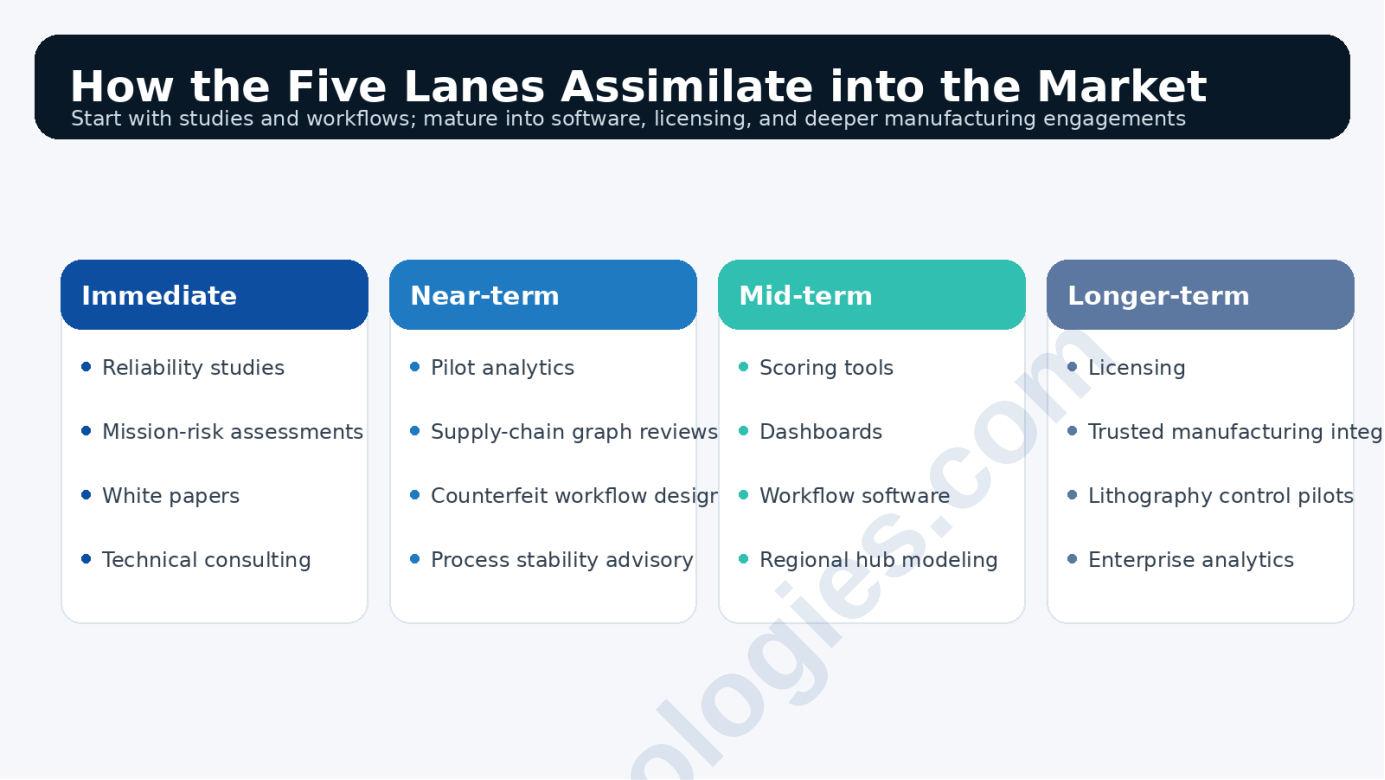
Lane 5 - AI-Certified Lithography Control: keep public positioning high-level and non-enabling until filing is complete.

6. Filed portfolio and disclosure discipline

Lane	Status	Public treatment
Board Design Reliability Analysis Checklist Guidelines (18/311,244)	Filed	Describe directly
Profile-Based Ethernet Connectivity for Multi-Lane SoC Devices (19/433,278)	Filed	Describe directly
Graph-Based Multi-Tier Semiconductor Supply-Chain Risk Scoring and Closed-Loop Mitigation (19/535,459)	Filed	Describe directly
Closed-Loop Manufacturing Stability Systems and Methods for Multi-Domain Control Production (19/534,285)	Filed	Describe directly
AI-Certified Lithography Control	Pre-filing	High-level public-safe only

6G is intentionally excluded from the current defense / supply-chain packet. Predictive failure analytics and counterfeit/provenance control should be emphasized as solution capabilities even where they are not being represented as separately verified filed applications in the current public packet.

7. How the five lanes assimilate into the market



Immediate market entry should come through consulting, reliability studies, mission-risk assessments, white papers, and technical strategy engagements. Pilot analytics, supply-chain graph reviews, counterfeit workflow design, and process stability advisory work follow. Software-backed scoring, dashboards, workflow tools, and licensing come after evidence and customer pull.

8. Working government path

The strongest immediate route is a DLA / defense research path built around one integrated problem-solution story instead of disconnected patent claims.

Step	What to do
1	Finish SAM registration and obtain active entity status / UEI.
2	Use the one-page concept summary for outreach only.
3	Use the white paper as the real technical response document.
4	Generate support letters from technical stakeholders.
5	Submit to the Contracting Office email listed in the active announcement.

Current relevant vehicle: DLA DLIR / Supply Chain Management BAA-0002-21.
Routing rule: for BAAs posted on SAM.gov, send the white paper to the Contracting Office email listed in the active announcement. If the idea is not listed within a BAA, DLA says to use Logistics.Research@dla.mil.

Key contacts to keep on file: DLASBIR2@dla.mil, RANDD.DCSO@dla.mil, Logistics.Research@dla.mil

9. Source notes

• GAO-25-107283, Defense Industrial Base: Actions Needed to Address Risks Posed by Dependence on Foreign Suppliers. GAO reported DOD relies on a global network of over 200,000 suppliers and still has limited visibility into lower tiers.

• Senate Armed Services Committee release on counterfeit electronic parts in the defense supply chain: more than 70% of suspect parts traced to China and approximately 1,800 suspect counterfeit cases identified.

• Reuters, February 2026: Taiwan said shifting 40% of semiconductor capacity to the U.S. is impossible, underscoring concentration risk.

• Reuters and AP, March 2026: Pentagon designation of Anthropic as a supply-chain risk, showing software/AI vendor-control risk as a real operational category.

• DLA innovation / small business routing page: BAA-0002-21, submission routing guidance, and innovation contact points.