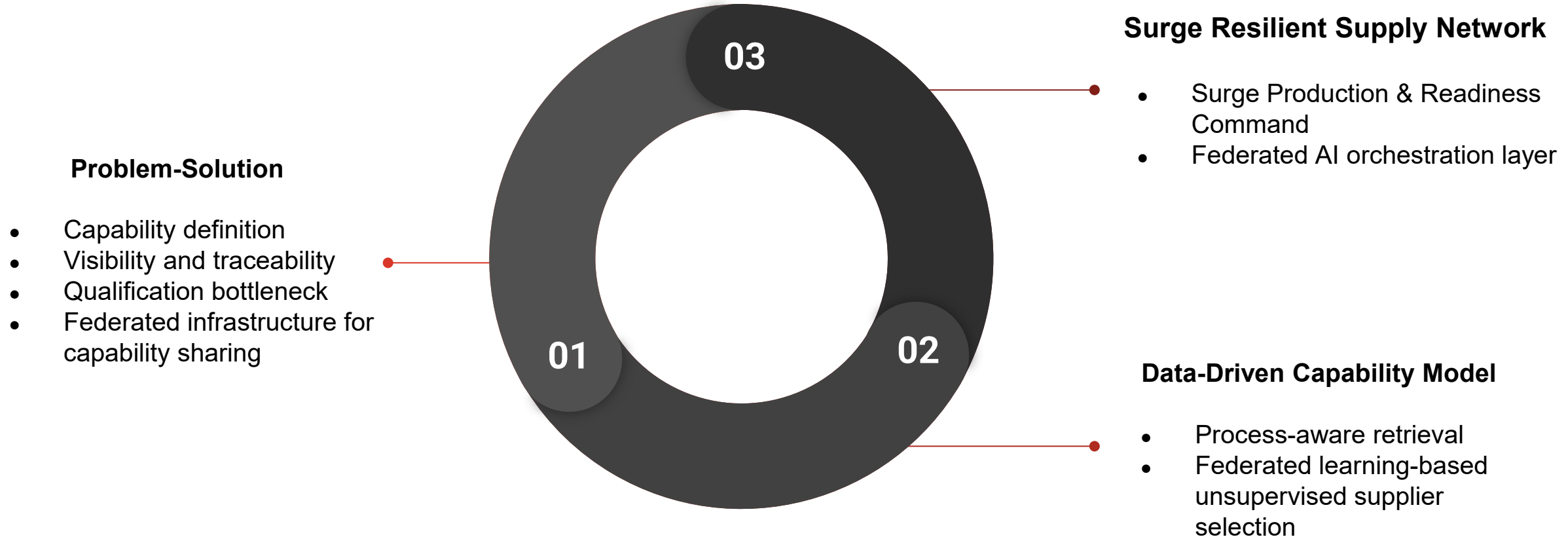
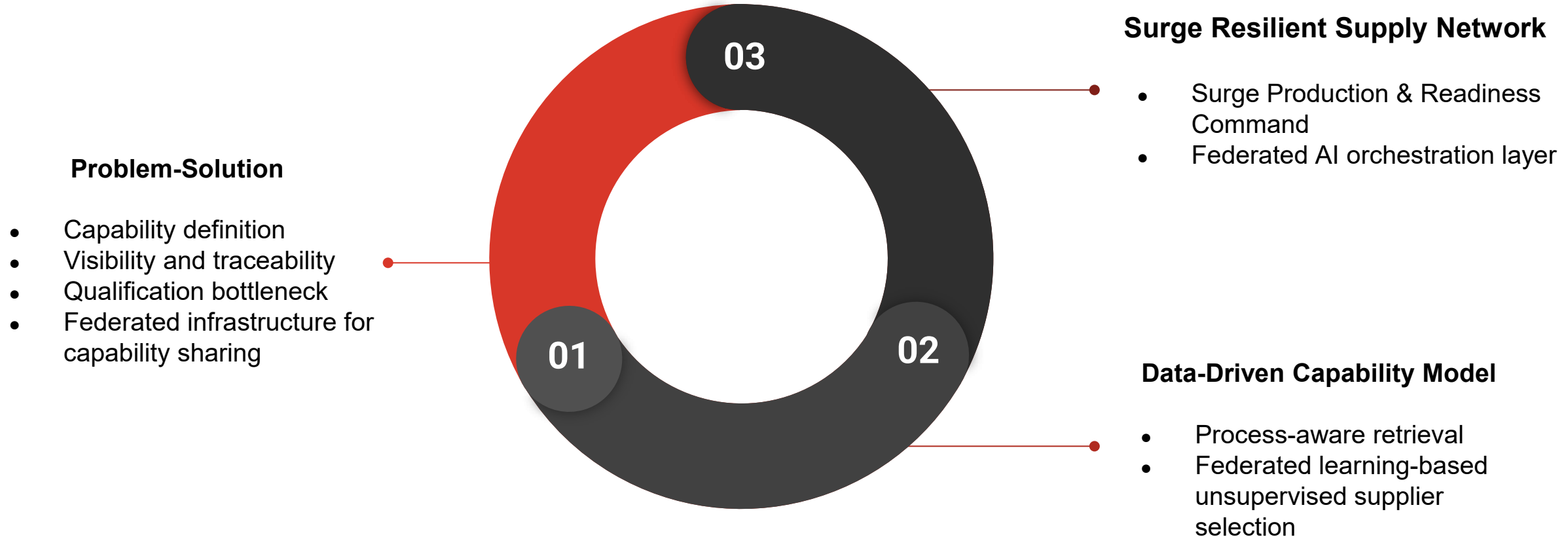


Federated Learning for Secure Cyber Manufacturing Capability Matching in Defense Supply Chains

Xiaoliang (Mike) Yan, PhD
Co-founder & CEO
OpenWerks, Inc.
mike.yan@openwerks.org

Shreyes Melkote, PhD
Professor, Mechanical Engineering
Georgia Institute of Technology
shreyes.melkote@me.gatech.edu





Problem: Lack of visibility and traceability into actual capabilities of the industrial base

“Small and mid-size manufacturers make up over half of US manufacturing value and are essential to defense industrial base, but **we have no real visibility into what they can actually make or when they can make it.** This blind spot means we can't respond to **surge demand**, can't find backup suppliers when things go wrong, and we are essentially flying blind on our own industrial capacity—which is a massive national security risk. **We have to find a solution before the next crisis.**”

– *Program*

Manager @ Defense Logistics Agency

Problem: Capability as defined today

Contact Supplier

Request Information

Visit Website

View Phone Number

Profile ▼

Full Catalog

Certifications

More Information ▼

Contact

Capabilities

Computer Numerical Control (CNC) Turning, Milling, and Drilling Services

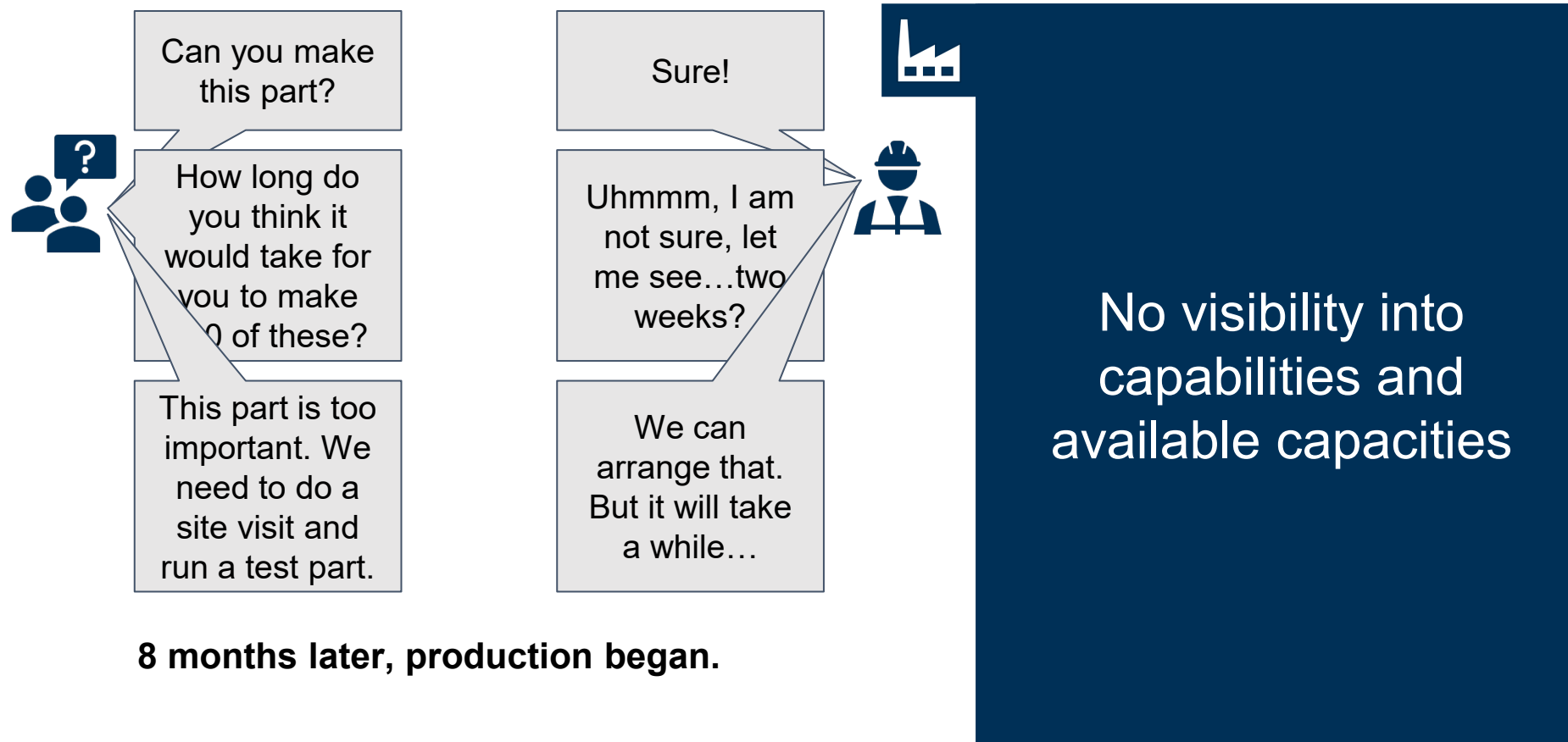


At , we have extensive capabilities in the areas of CNC turning, milling, and drilling. We have more than 38 years of experience as a CNC machining shop and a great deal of expertise for efficiently combining turning, millin...

[More +](#)

[View Details](#)

Problem: “Concurrent engineering” in its current state

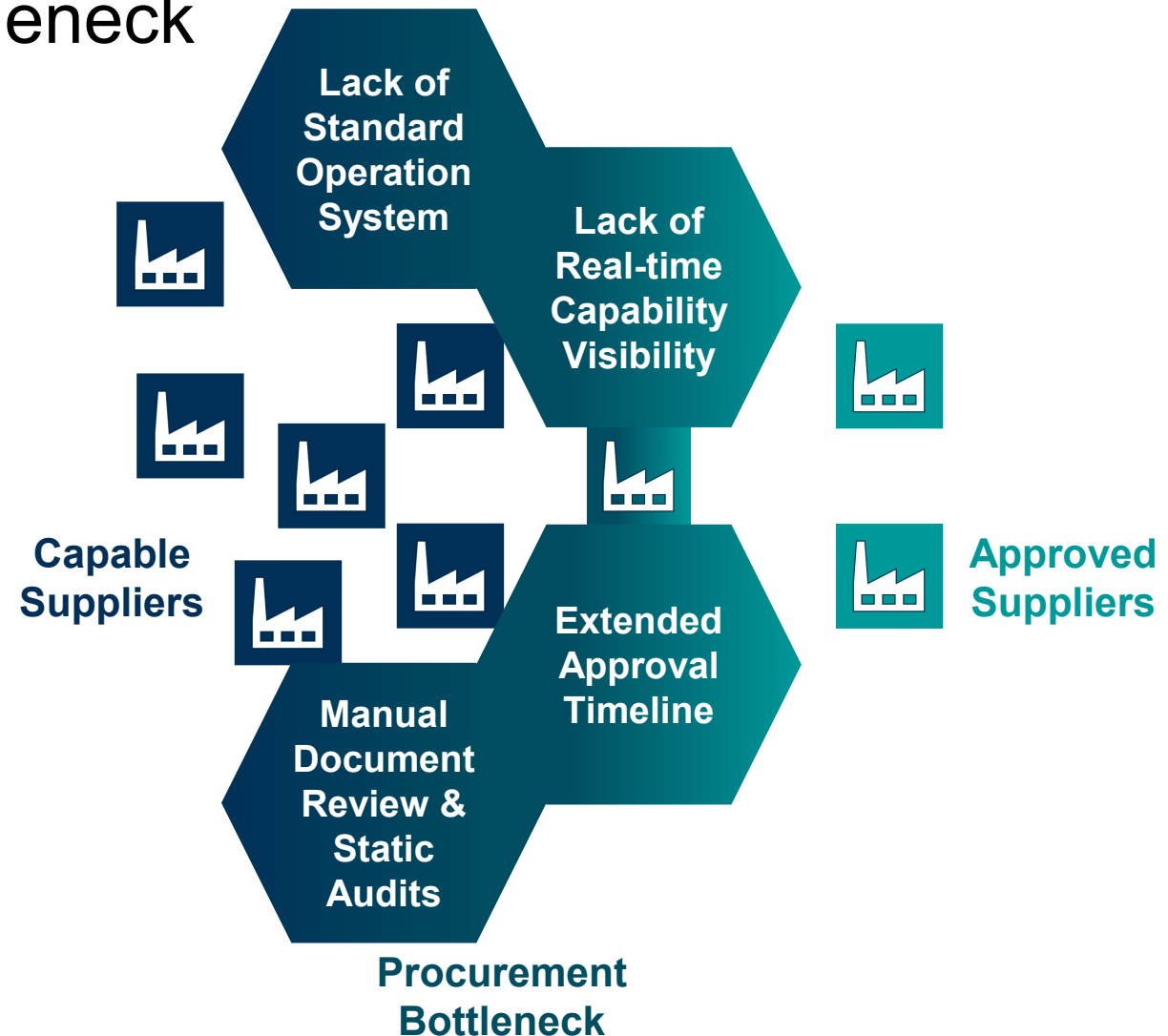


Problem: Qualification bottleneck

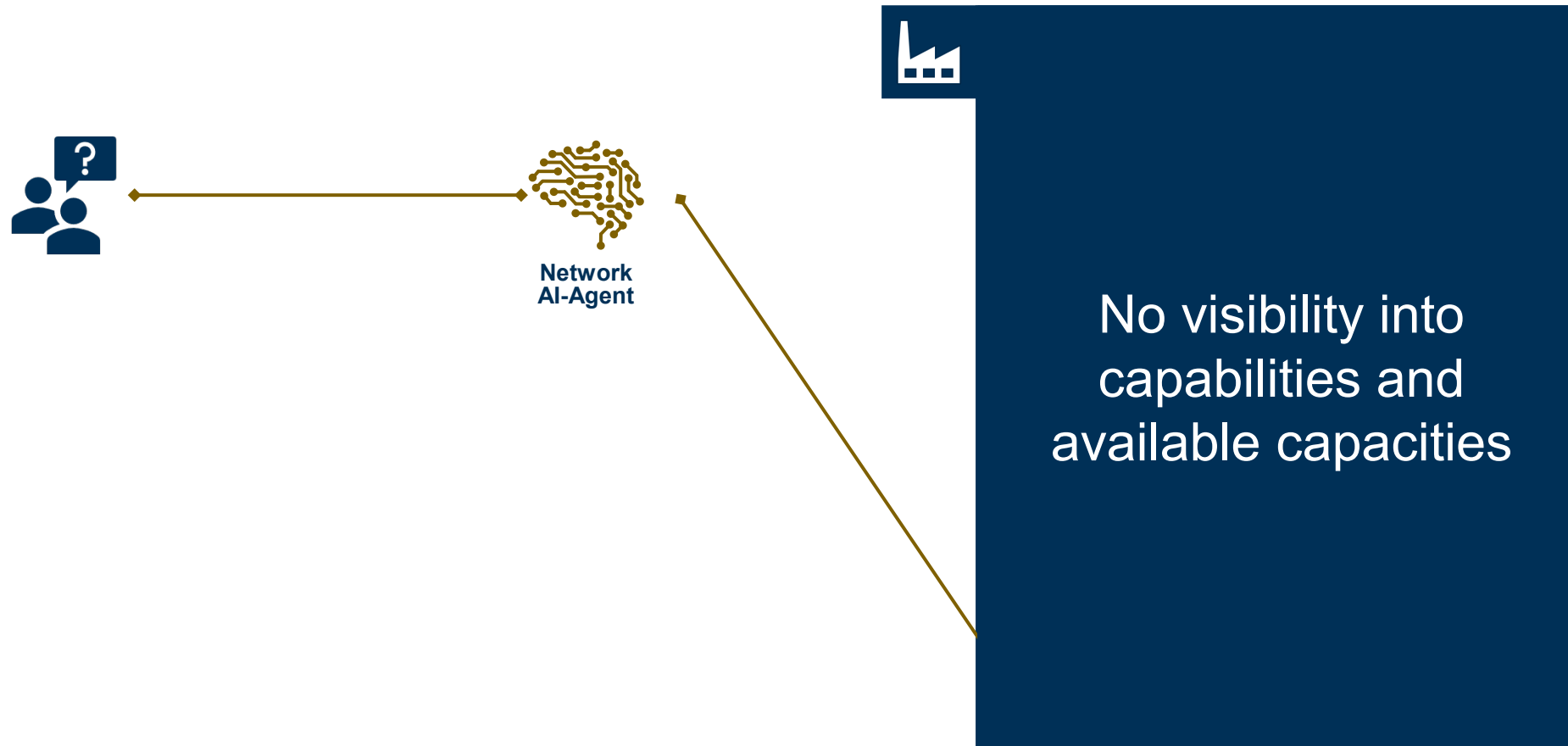


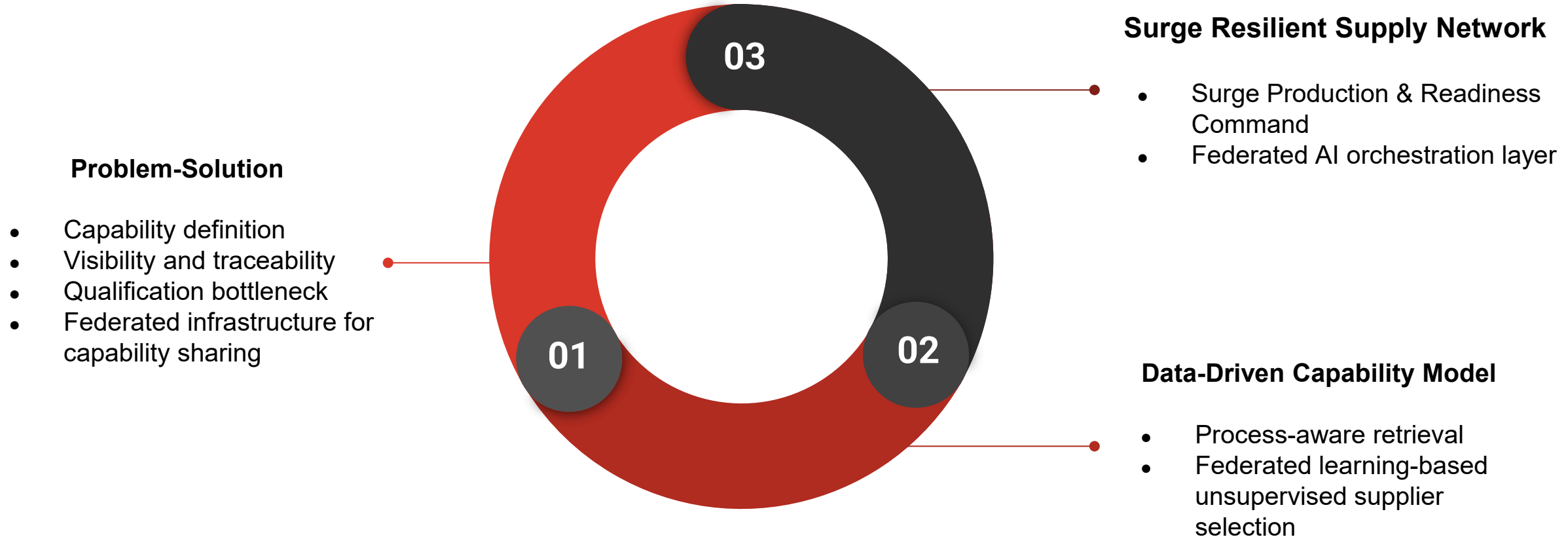
Traditional procurement process takes months with supplier site visits and test part runs

Even if suppliers are pre-approved, there is no guarantee that they have the available capability and capacity at the right time



Problem - Solution: Federated infrastructure for capability sharing





Background: Levels of capabilities

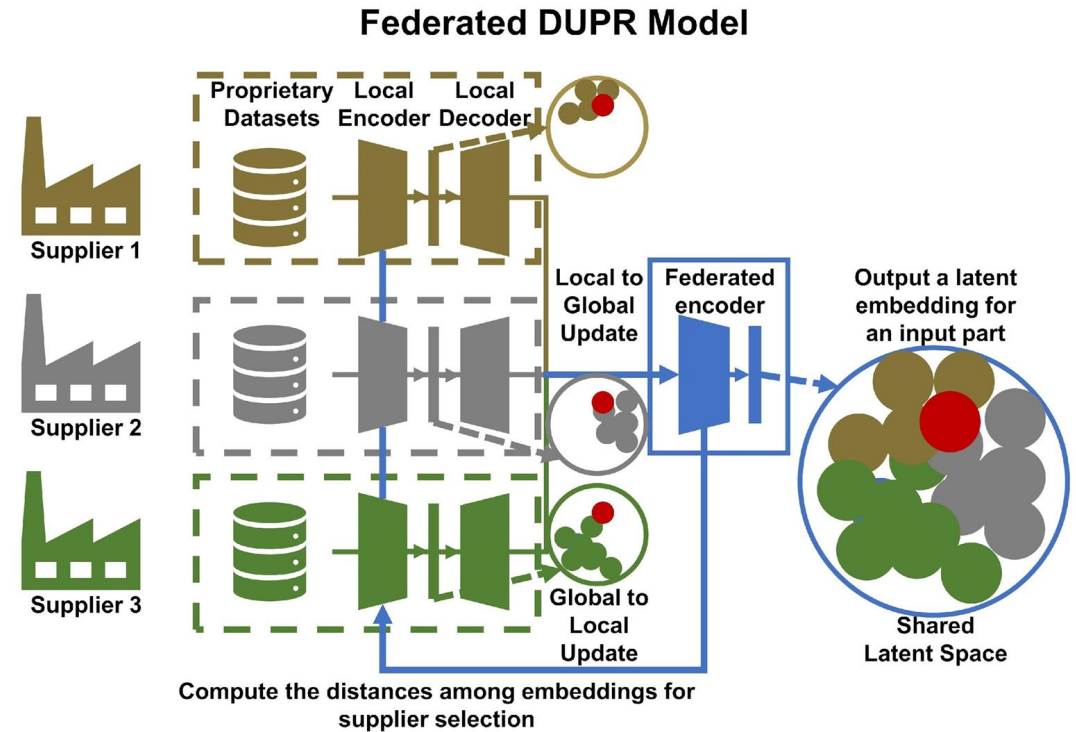
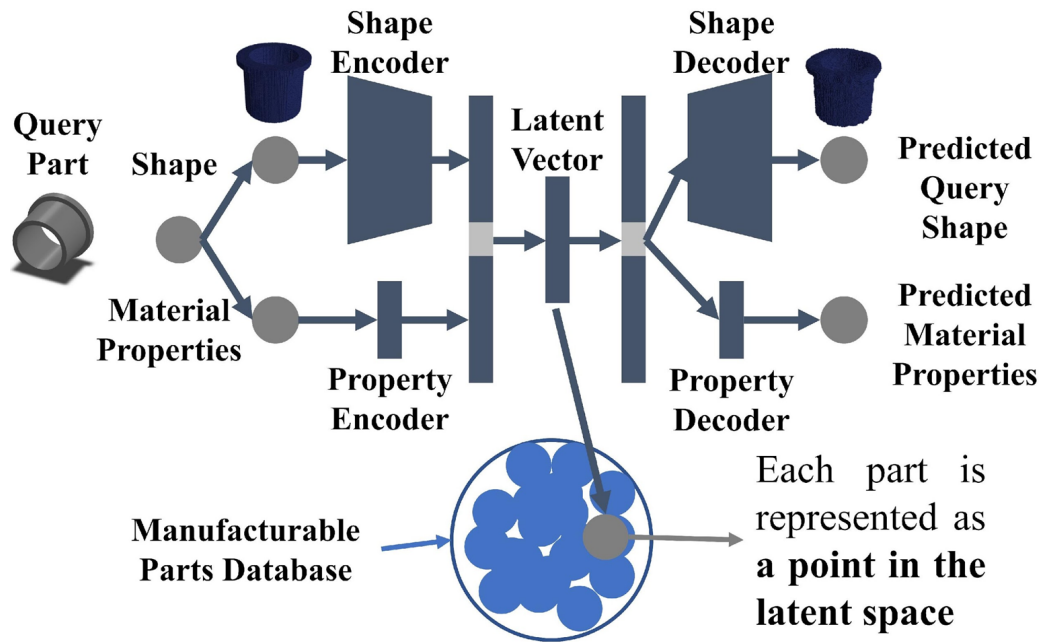
1. Theoretical Machine Capability Assessment

2. Historical Performance and Operation Verification

Cannot resolve with first-principles
→ data-driven models required

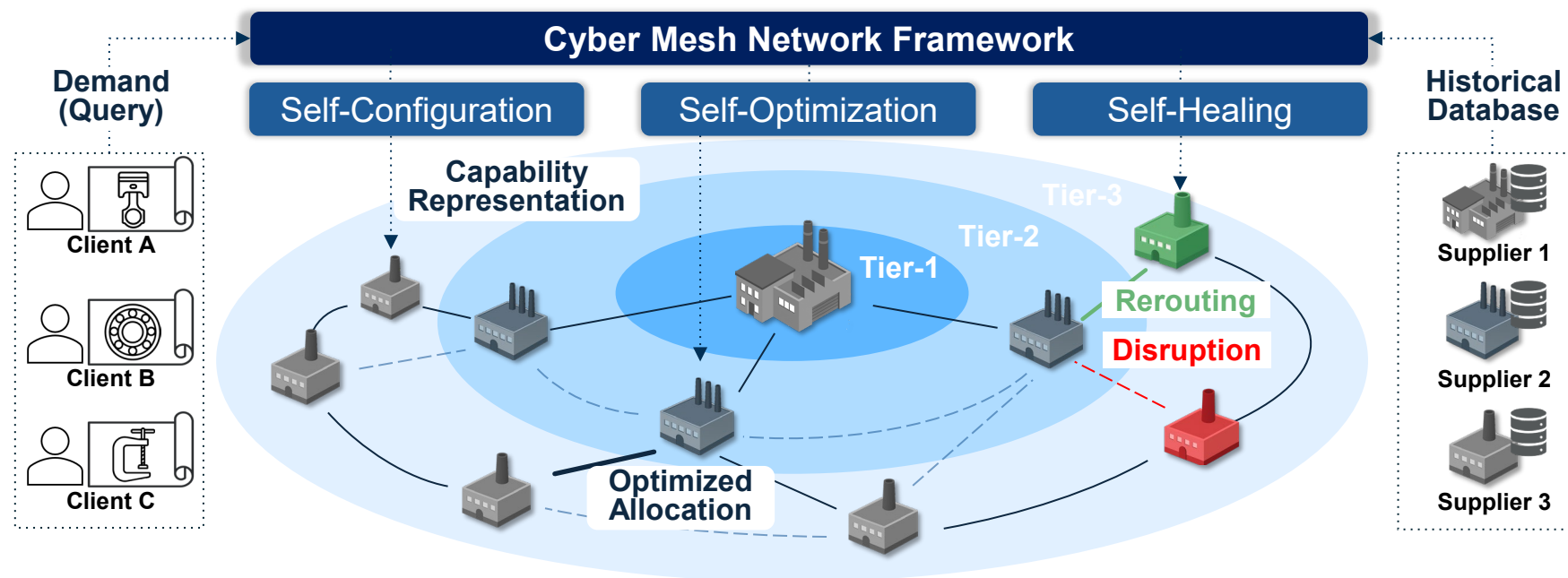
1. Physical Accessibility and Material Handling Logistics

Capability: Data-driven Capability Models



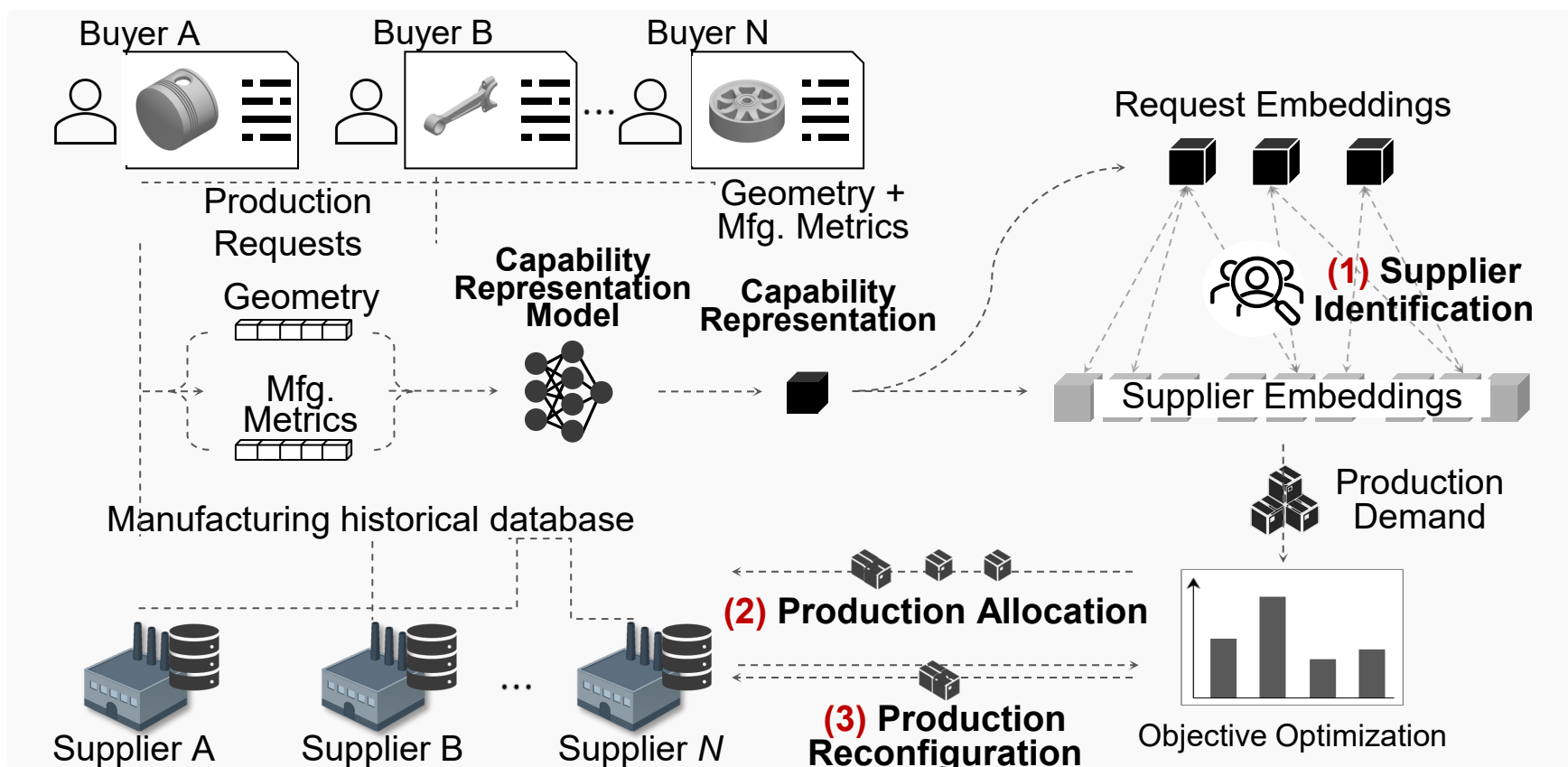
Capability: Resilient Cyber Manufacturing Mesh Network

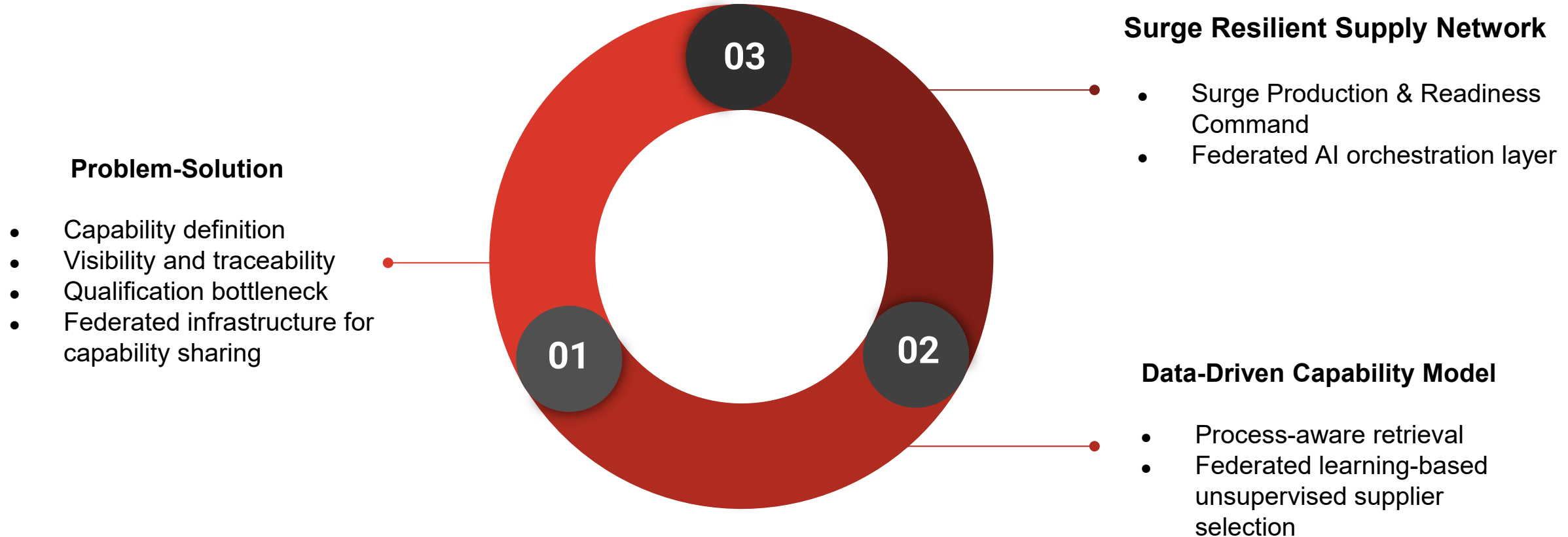
- **Self-Configuration:** Identify feasible suppliers from the historical database using capability-aware representations
- **Self-Optimization:** Optimize production allocation under demand, capacity, cost, and time constraints
- **Self-Healing:** Reroute and reallocate production when disruption occurs to maintain supply continuity



Capability: Resilient Cyber Manufacturing Mesh Network

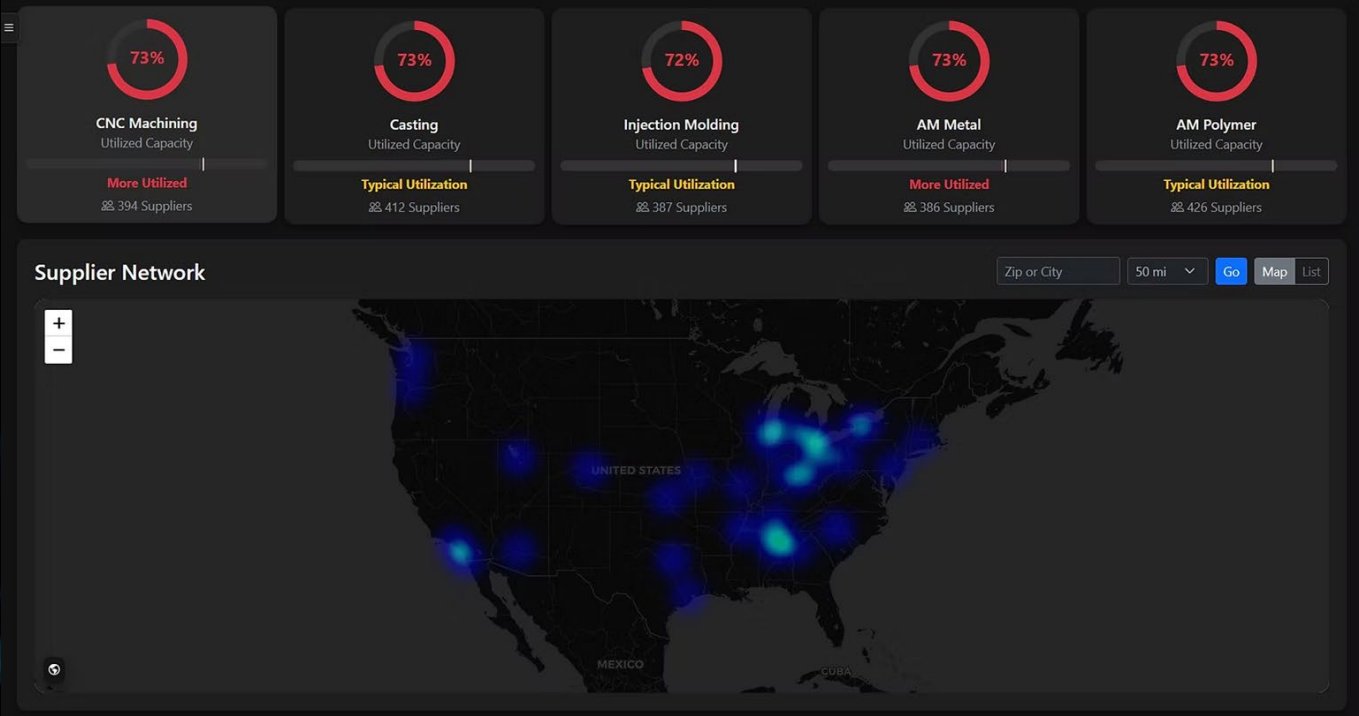
- Production requests are encoded into capability-aware request representations.
- Feasible suppliers are identified by matching request and supplier embeddings.
- The identified supplier pool is used for production allocation and reconfiguration.





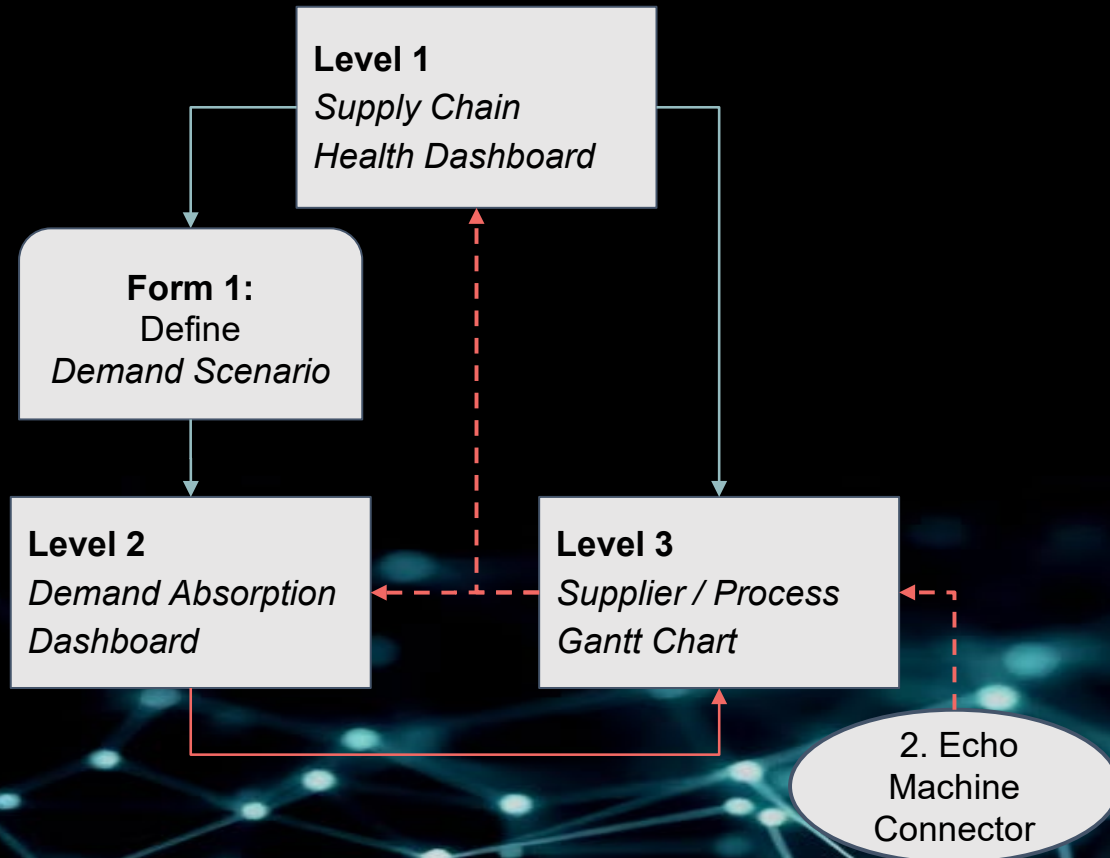
SURGE-RESILIENT SUPPLY NETWORK

Phase 2 - Resilient Production Ready Pilot
Surge Production & Readiness Command (SPARC)



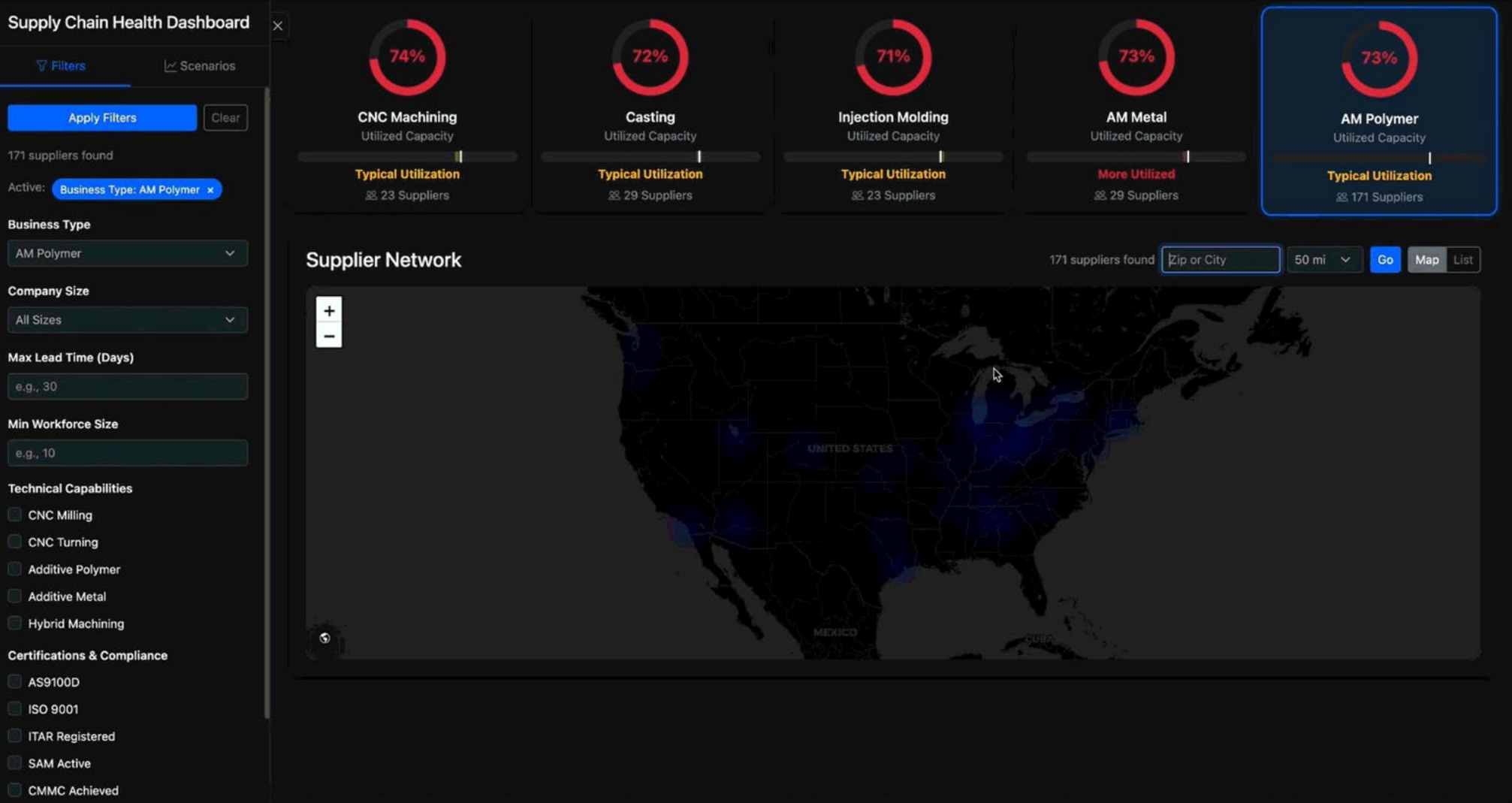
Phase 1 Foundation Delivered

SPARC

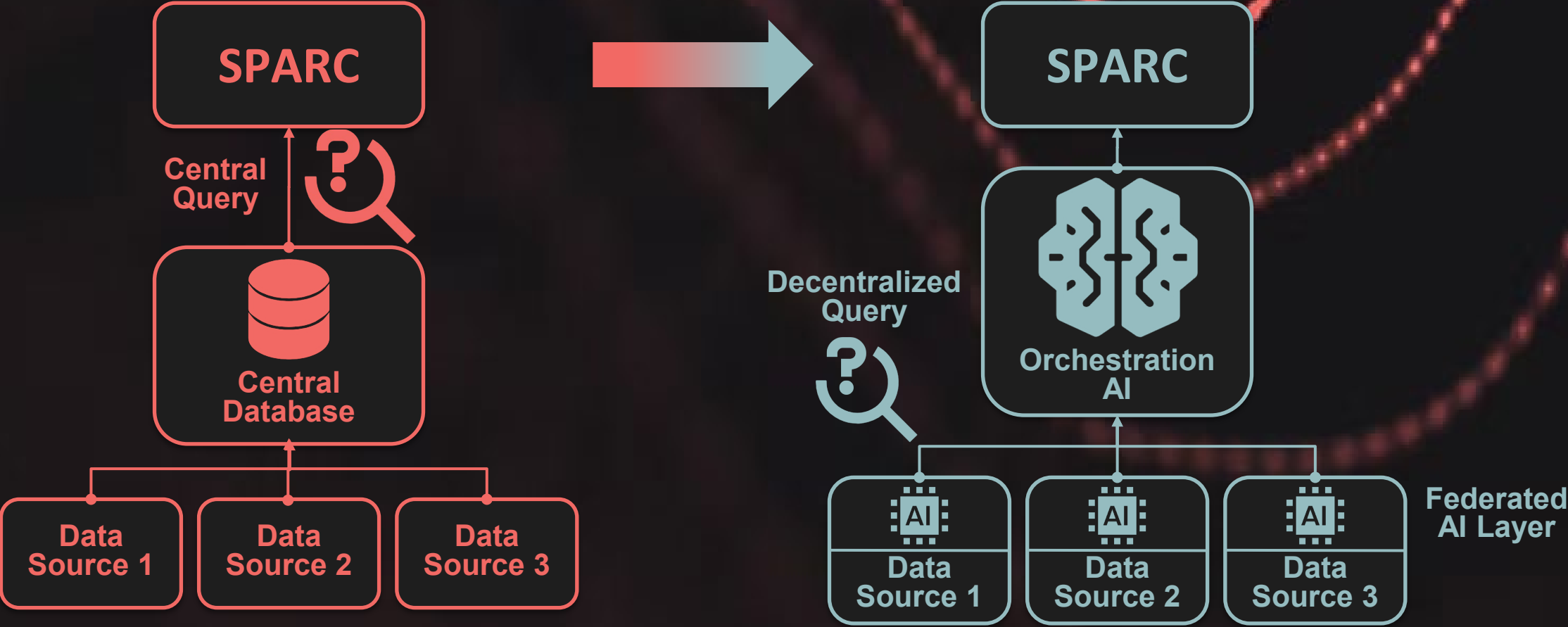


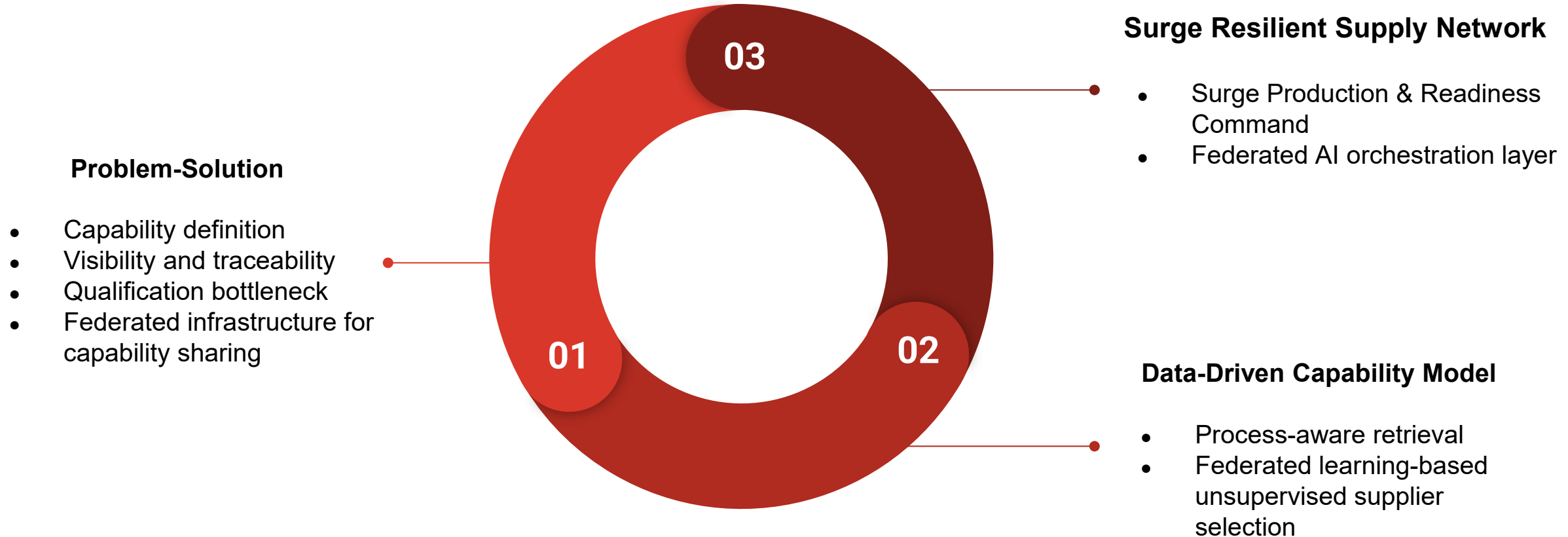
- **System Design Delivered:** GCC-High security/infrastructure package completed
- **Initial Demonstrator Built:** Supplier network with capability search and availability logic
- **Integration Path Defined:** Architecture ready to pull live capacity data
- **Market Validation:** OIB and private suppliers requesting data integration post-press release

Phase 1 Foundation Delivered



Phase 2: Decentralized Resilient Architecture





Conclusion & Next Steps

1. Data-driven capability modeling provides insights into actual capabilities of suppliers, facilities, and machines that cannot be otherwise “hard-coded” through model-based definition
2. Such capability model when combined with federated learning, enables privacy-preserved querying of the capabilities without exposing raw data
3. A secure data exchange and capability visibility platform is feasible as demonstrated at a relevant facility, but federated querying remains the immediate next step

Key Questions for Discussion

1. **What is the minimum necessary information required to assess machine capability?**
 - a. How do we standardize reporting of "as-maintained" versus nameplate machine specifications?
 - b. Machine performance degrades over time. What standards should require suppliers/machines to report actual, verified capabilities rather than original specifications?
2. **What is the minimum necessary information necessary to assess the manufacturing capability of a supplier?**
 - a. What constitutes sufficient capability history for qualification, and how do we share this data without compromising IP?
 - b. How might industry define "similar enough" historically produced jobs and enable capability verification while protecting proprietary processes?
2. **Should digital facility models become standard for supplier qualification?**
 - c. Material handling constraints can disqualify capable suppliers. Should we formalize physical layout modeling (e.g., via OpenUSD) to test virtual feasibility?

| Appendix