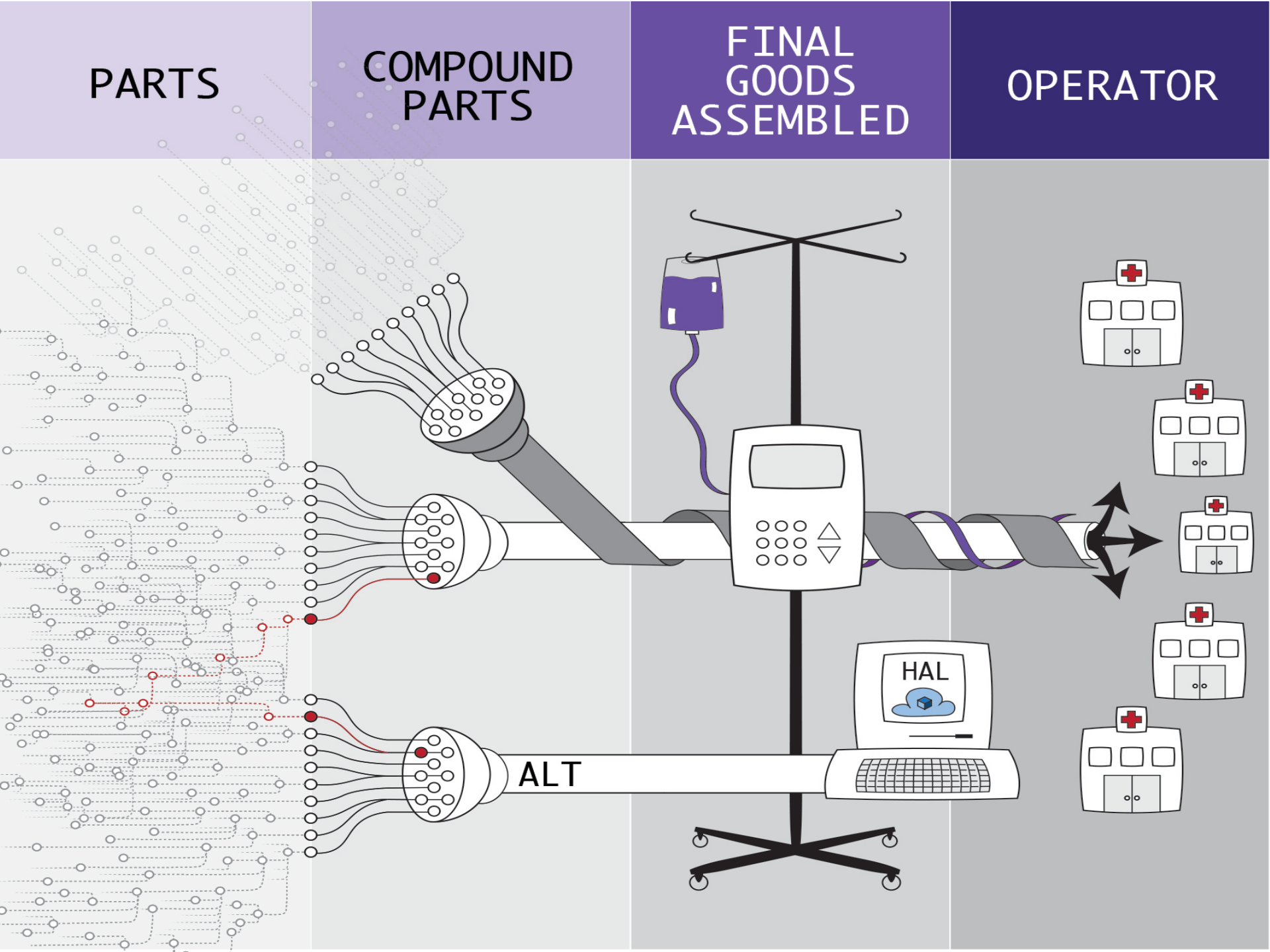
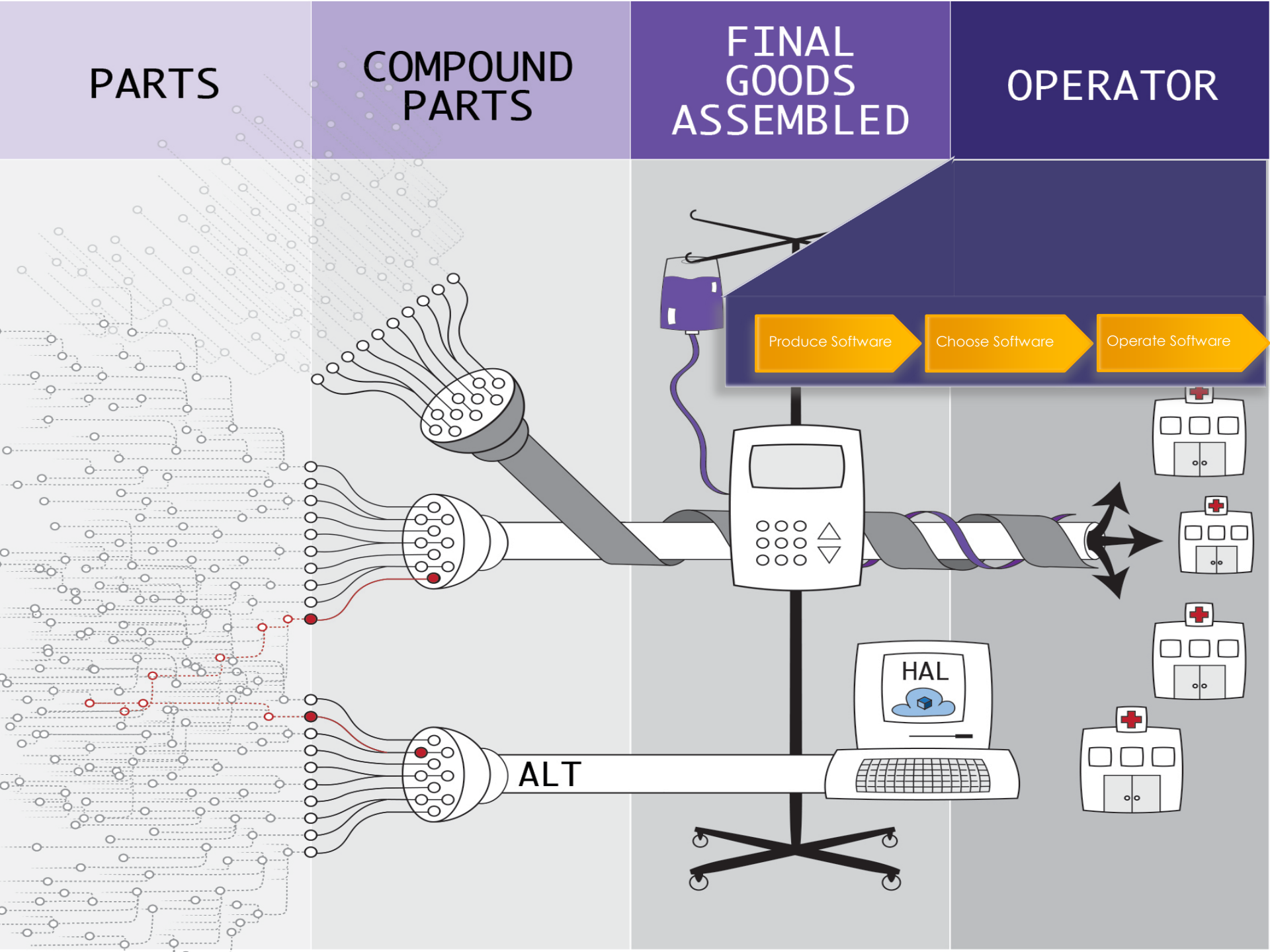
Software Bill of Materials

Practices & Use Cases Working Group

NTIA Software Transparency
Joshua Corman, Charlie Hart, Ben Ransford

June 27, 2019


PARTS
COMPOUND PARTS
FINAL GOODS ASSEMBLED
OPERATOR
HAL
ALT


PARTS
COMPOUND PARTS
FINAL GOODS ASSEMBLED
OPERATOR
Produce Software
Choose Software
Operate Software
HAL
ALT

Software Supply Chain Roles / SBOM Benefits

Produce Software

- Less unplanned maintenance work
- Reduce code bloat / streamline component choice
- Understand component and code dependencies
- Know and comply with licensing
- Monitoring/reviewing for vulnerability
- Awareness of component EOL, orphan, etc.
- Streamlined code review
- Streamline release/ production
- Enable black- and whitelists
- SBOM and transparency for customers

Choose Software

- Identify vulnerable components
- Targeted security analysis
- Verify sourcing
- Compliance with policies
- Awareness of component EOL, orphan, etc.
- Integrate with asset, compliance, ERT systems
- Audit and verify supplier claims
- Show best practices by supplier

Operate Software

- Easily ID vulnerabilities
- Drive independent mitigations
- Better risk analysis - "Roadmap for the defender"
- Awareness of component EOL, orphan, etc.
- Streamline administration

Interviews: What's the State of Practice?

Live interviews to find out **how people use** SBOM, what **works,** & what are **stumbling blocks**

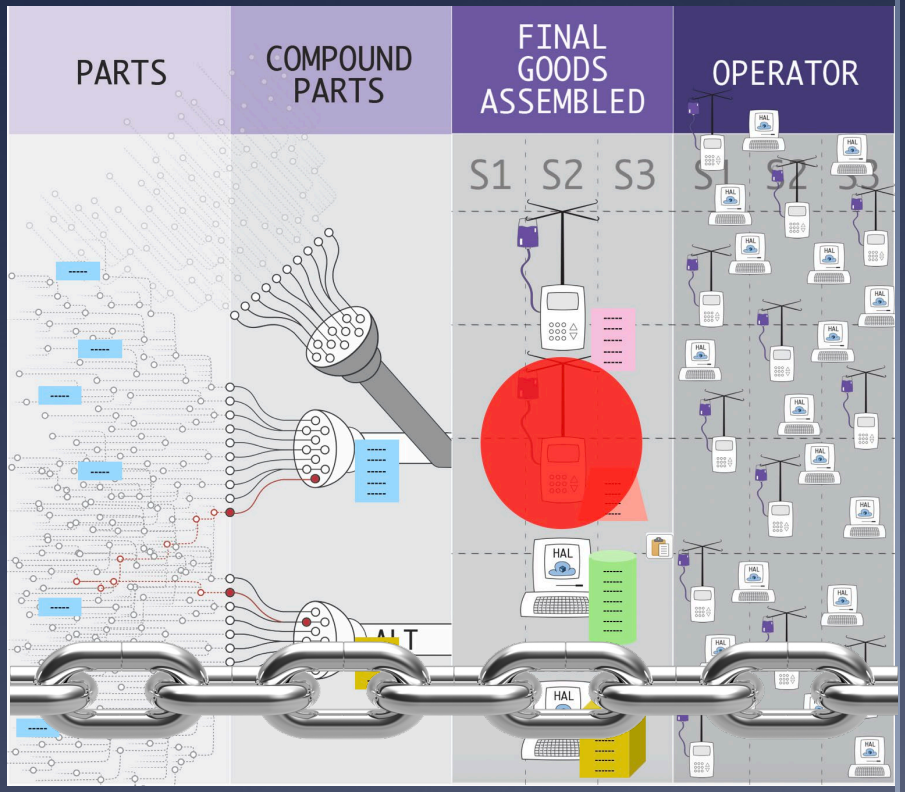
Less mature:
No SBOM penetration
No tooling, no readiness
SBOM not a factor in selection
"Our vendors are clueless!"
"SBOM is QA's problem!"
"Vetting is too much work!"

More mature:
Consistent SBOM Everywhere
Mature tooling
SBOM contract language
"We can respond to incidents."
"Let's phase out EoL assets."
"SBOM is a forcing function."

Vuln mgmt!

Next (1 of 2) : System-Wide / Full Chain

Patient Health vs Public Health



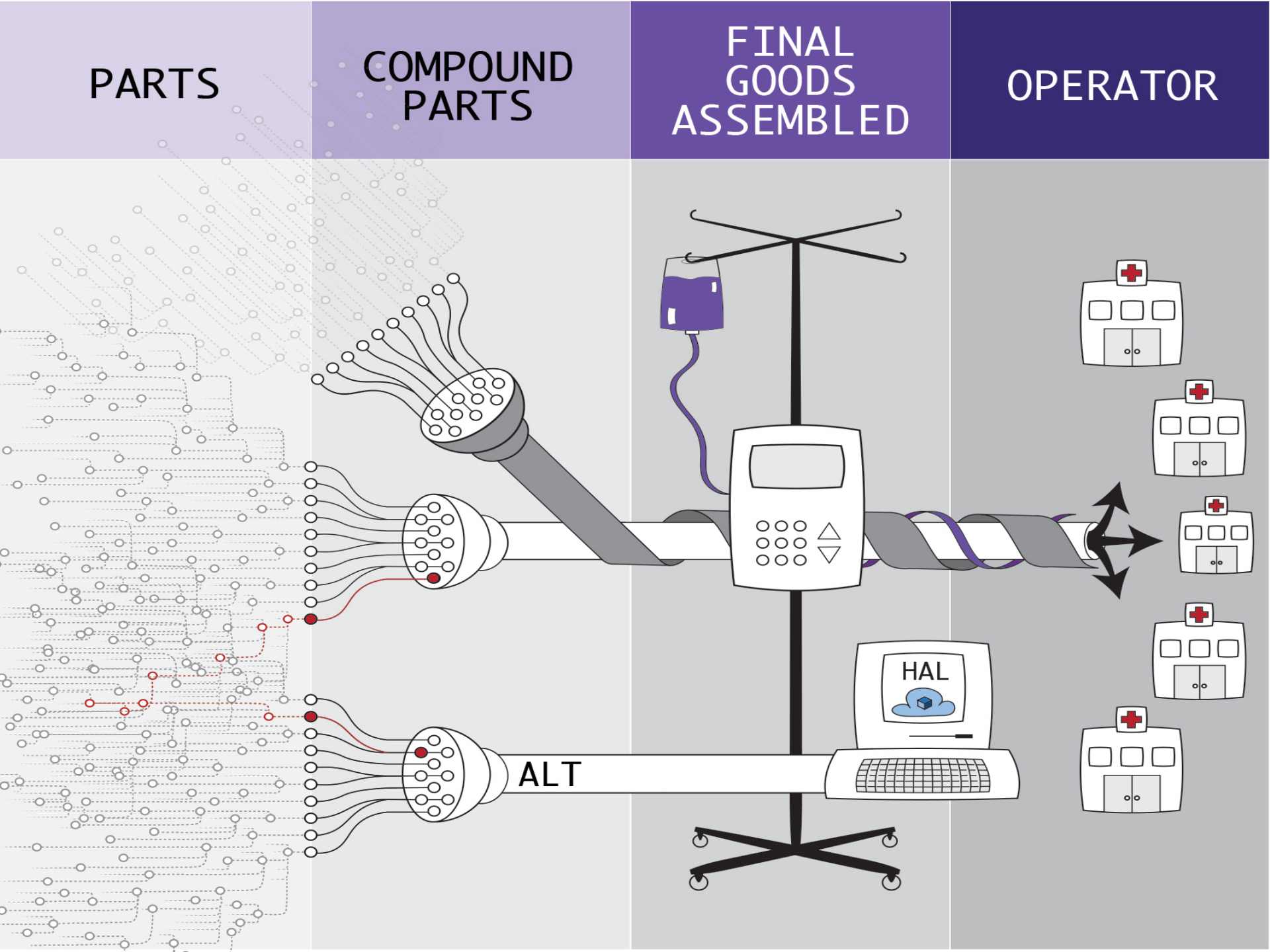
- Network Effects
- Population Impact Analysis
- Faster Vulnerability Visibility
- Market Incentives
- Supplier Darwinism
- "Out-of-Business Proof"

Next (2 of 2) : Advanced / High Assurance

Advanced

High Assurance DoD

* Provenance
* Pedigree
* Integrity
* “Deliver Uncompromised”


PARTS
COMPOUND PARTS
FINAL GOODS ASSEMBLED
OPERATOR
HAL
ALT