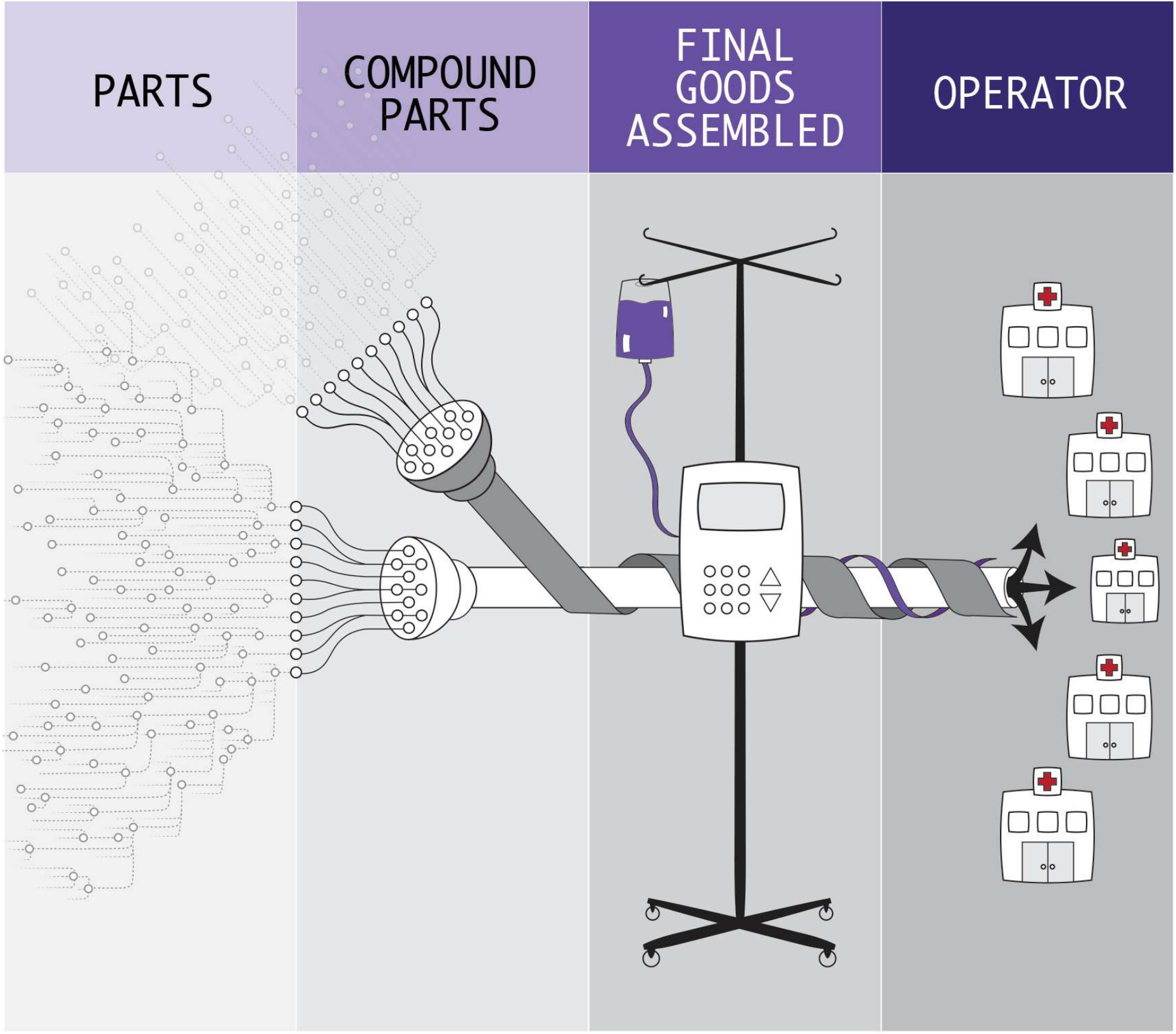
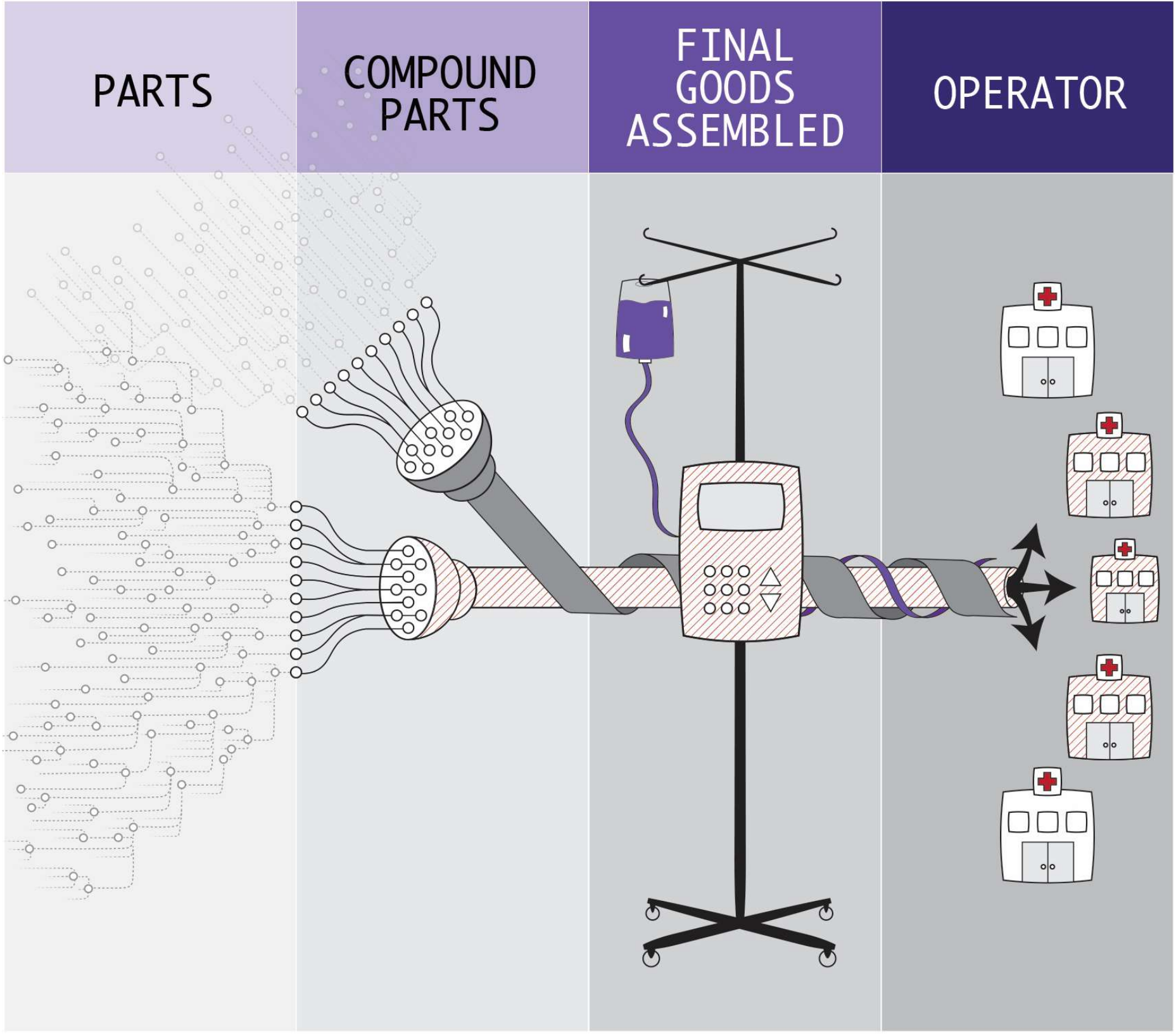
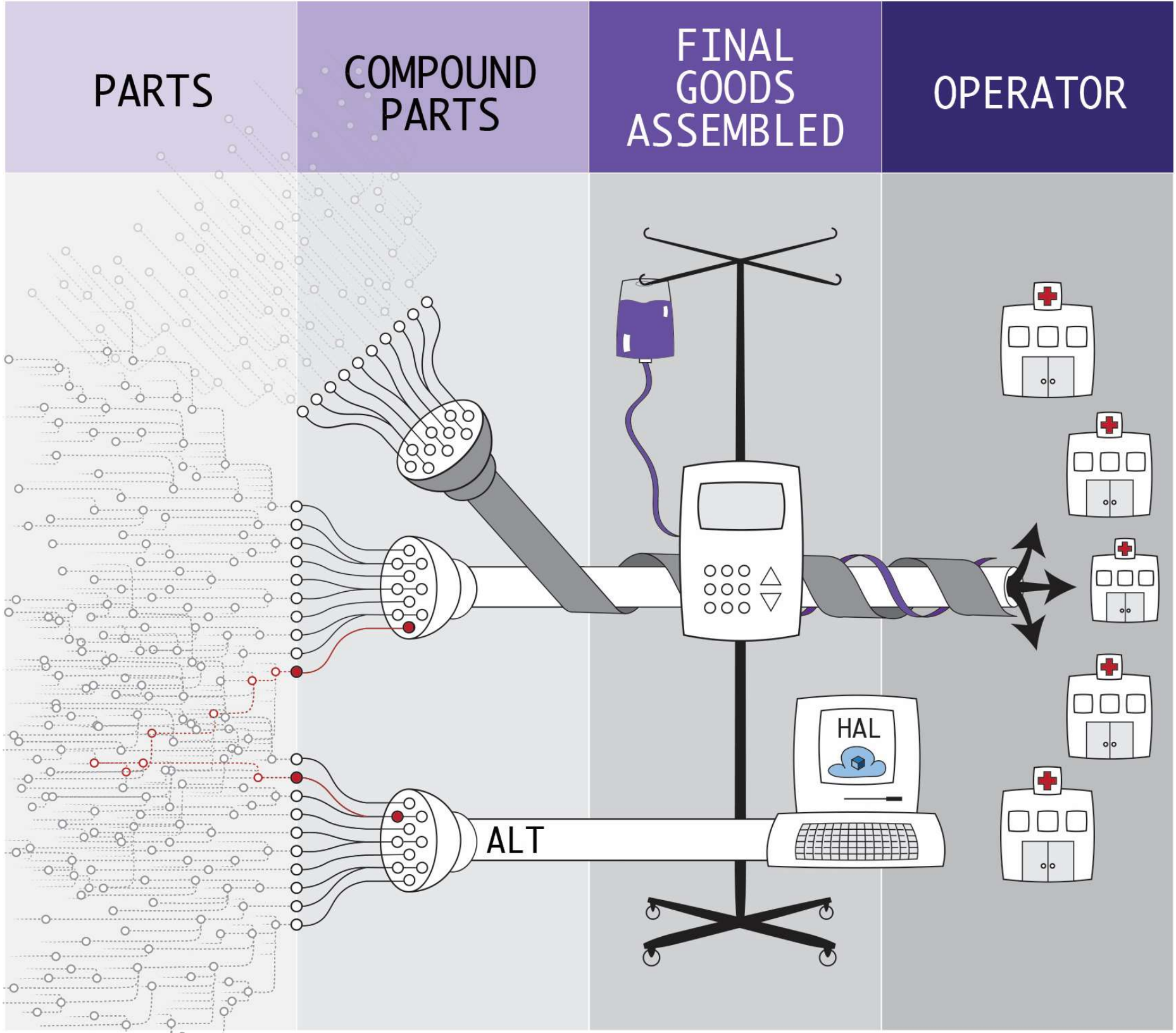
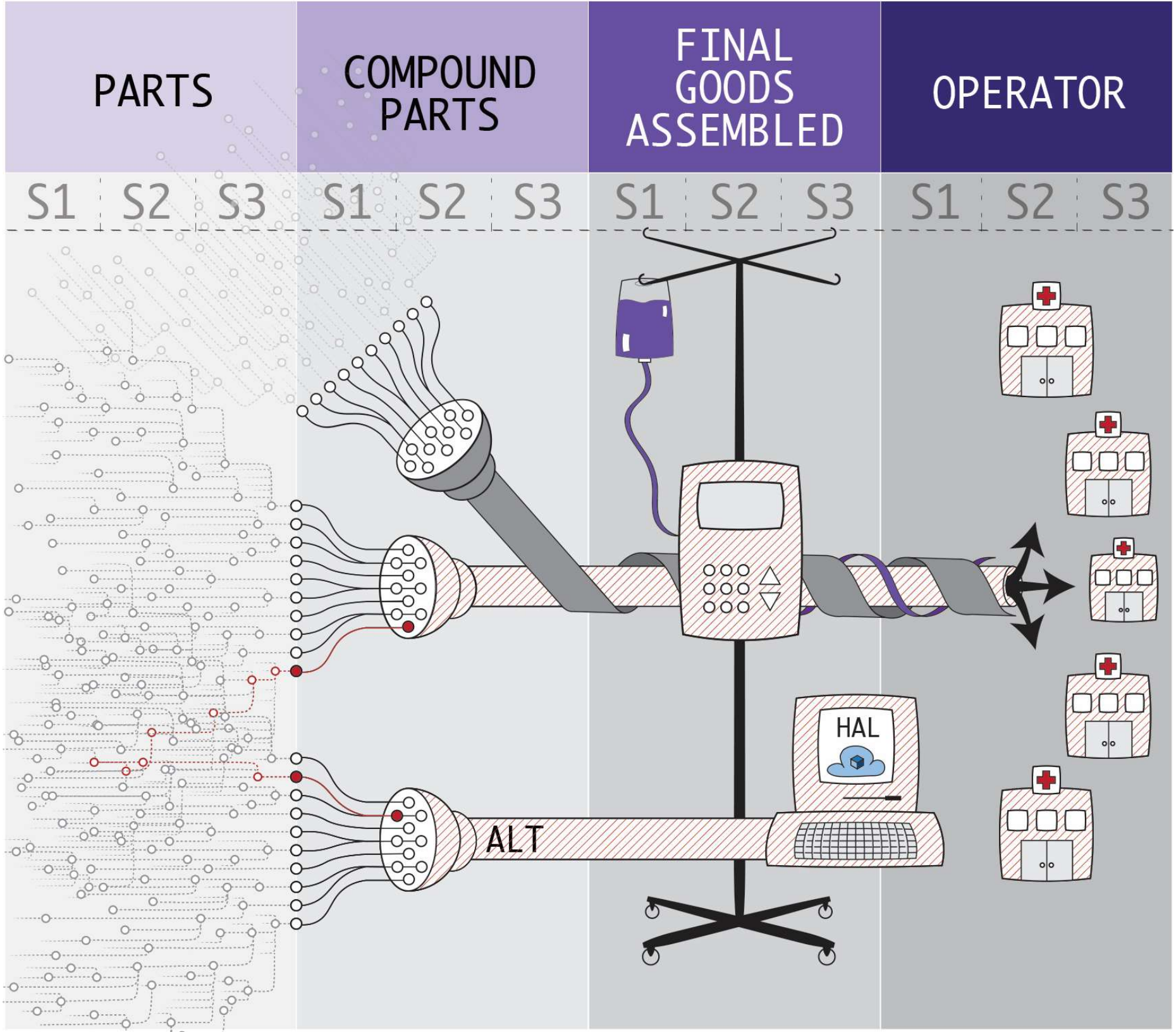
NTIA SBoM Practices WG

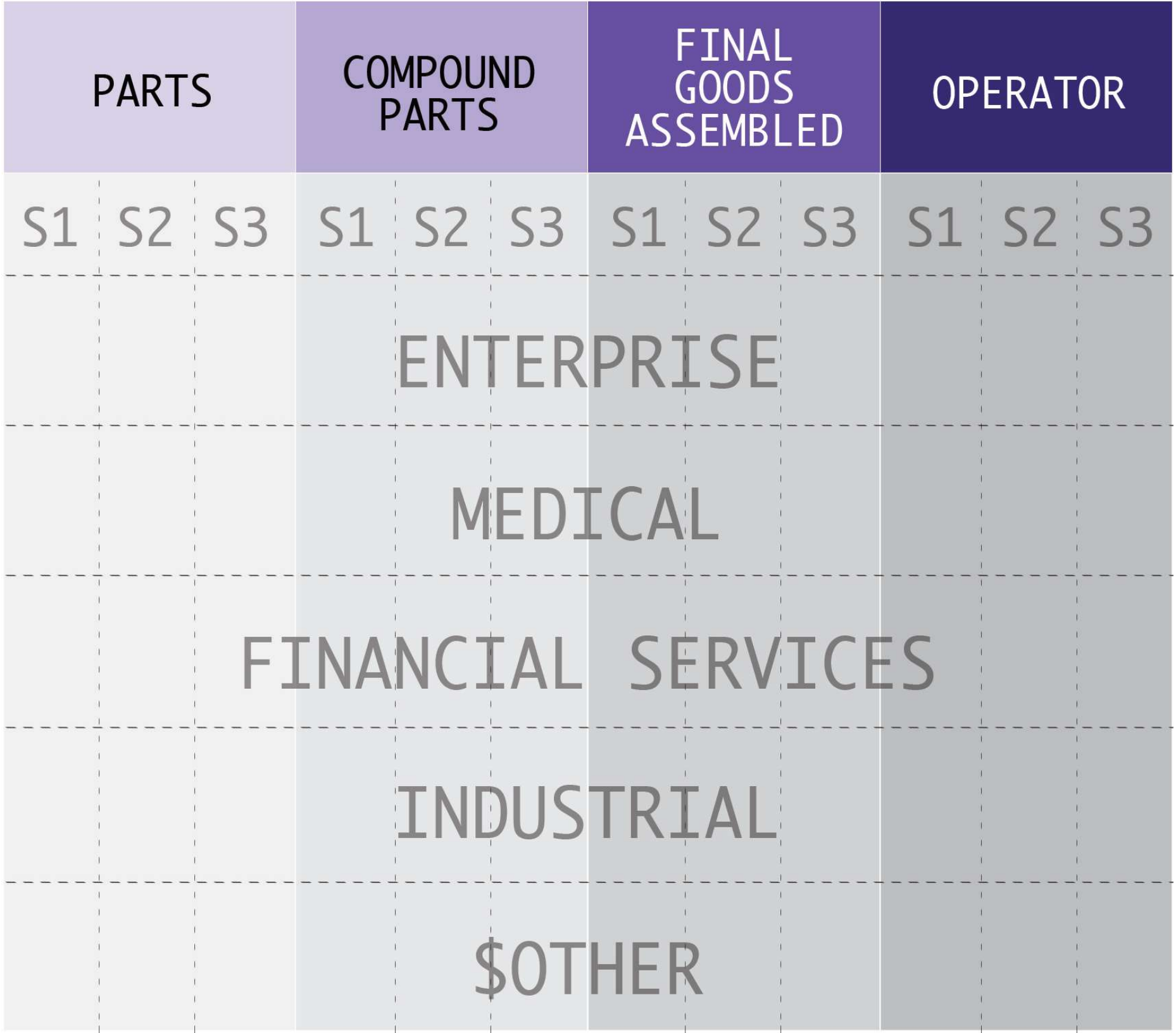
April 11, 2019

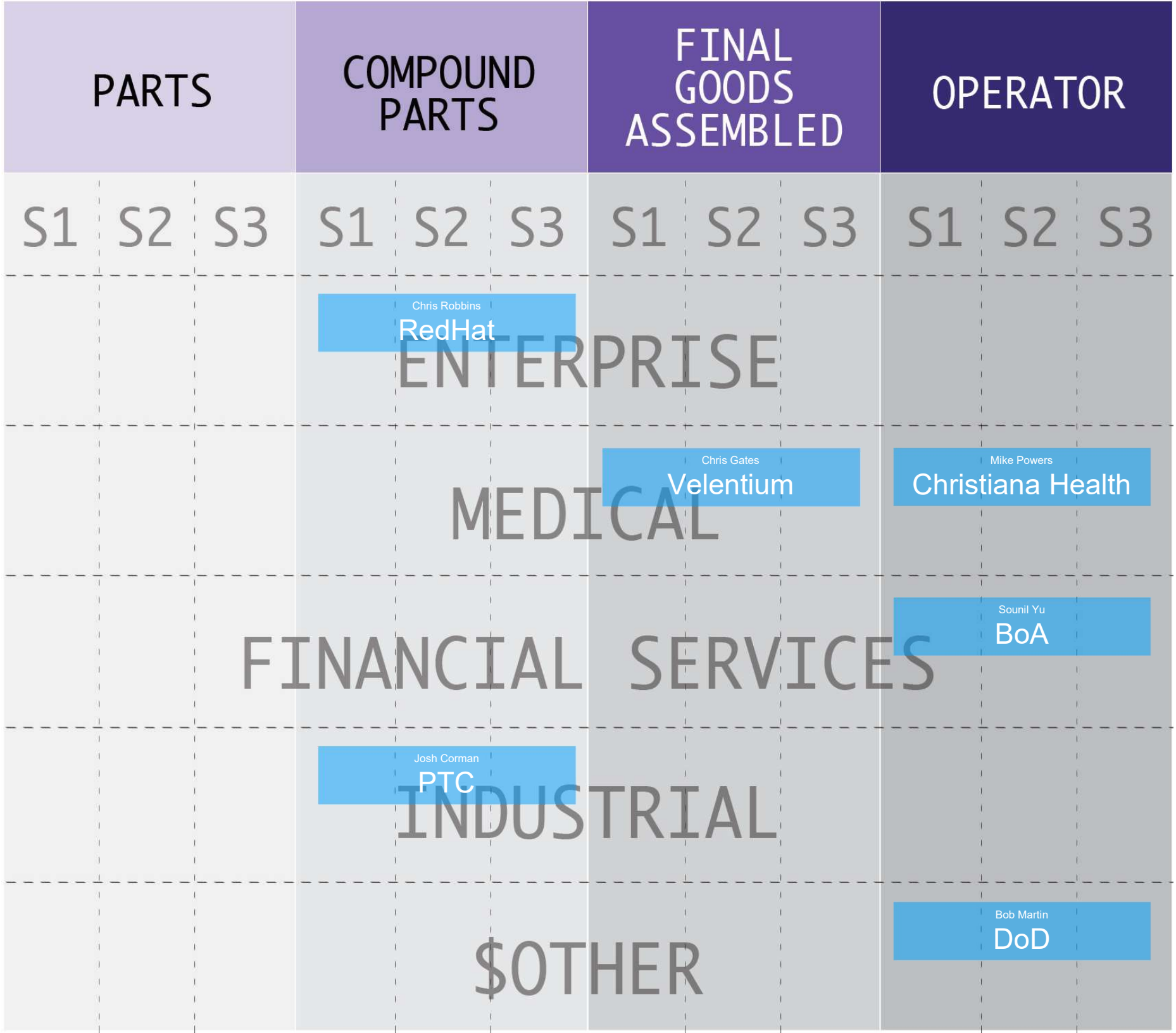

PARTS
COMPOUND PARTS
FINAL GOODS ASSEMBLED
OPERATOR


PARTS
COMPOUND PARTS
FINAL GOODS ASSEMBLED
OPERATOR

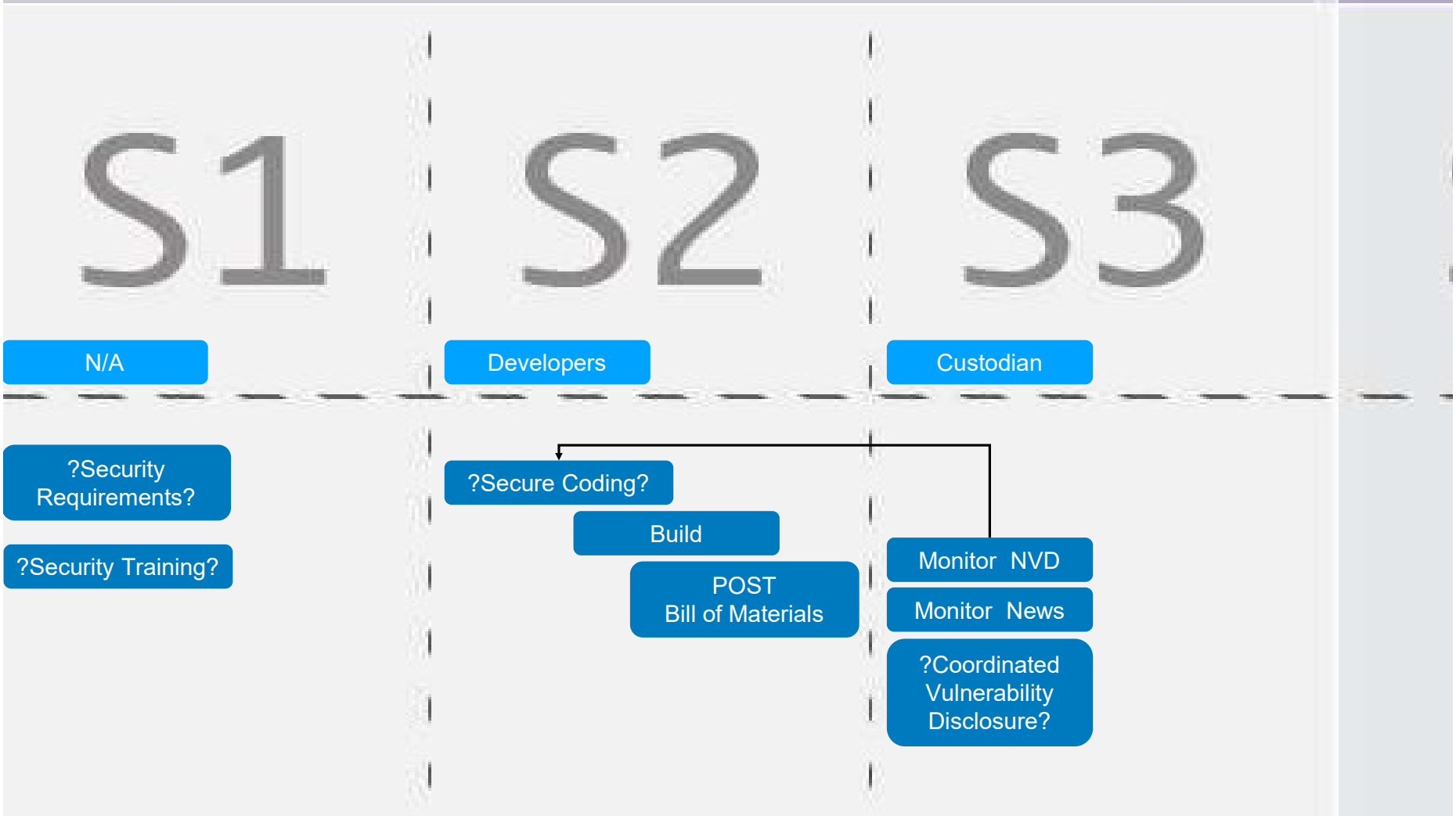

PARTS
COMPOUND PARTS
FINAL GOODS ASSEMBLED
OPERATOR
HAL
ALT

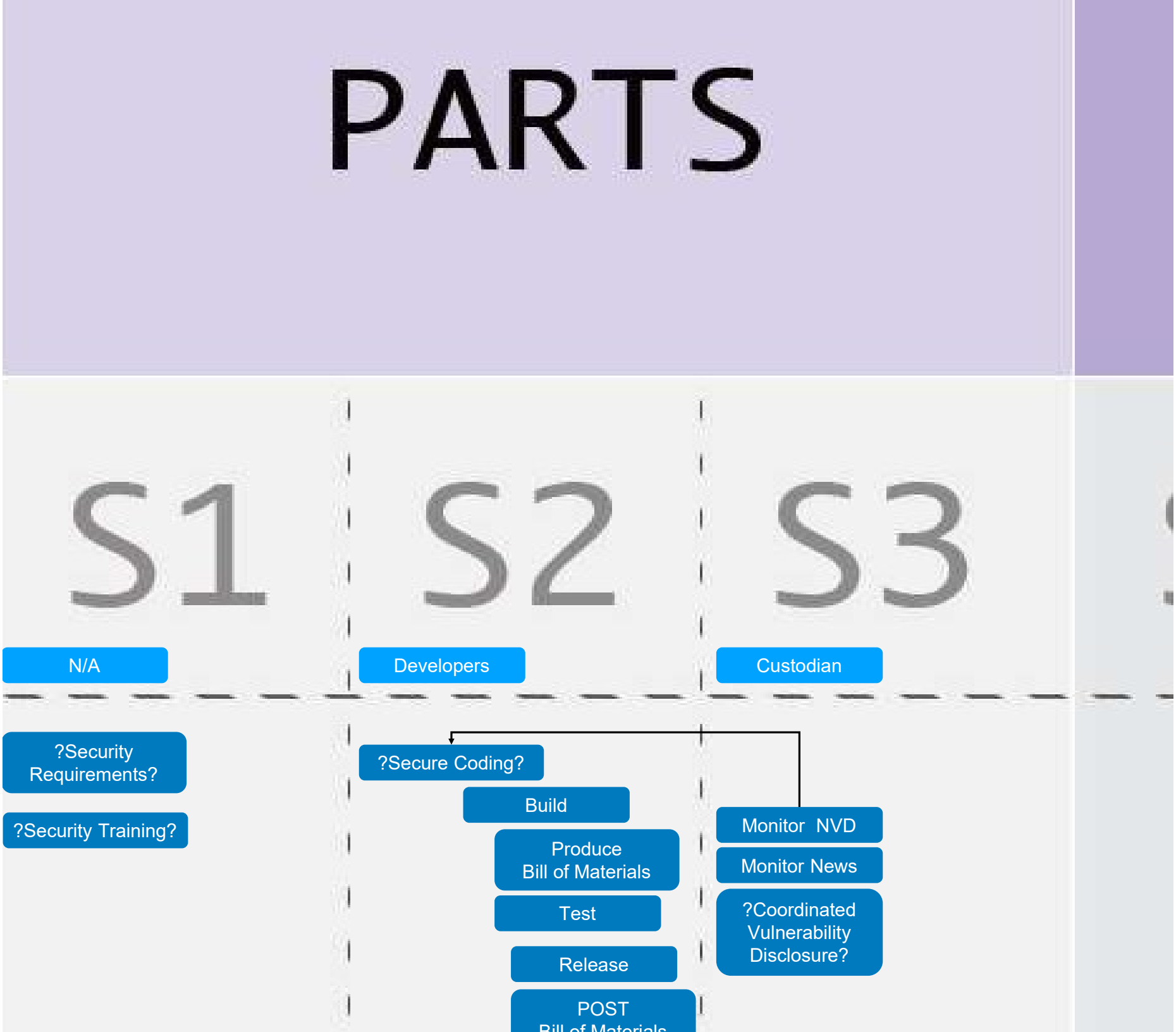

PARTS
COMPOUND PARTS
FINAL GOODS ASSEMBLED
OPERATOR
S1
S2
S3
S1
S2
S3
S1
S2
S3
S1
S2
S3
HAL
ALT


PARTS
COMPOUND PARTS
FINAL GOODS ASSEMBLED
OPERATOR
S1 S2 S3 S1 S2 S3 S1 S2 S3 S1 S2 S3
ENTERPRISE
MEDICAL
FINANCIAL SERVICES
INDUSTRIAL
$OTHER

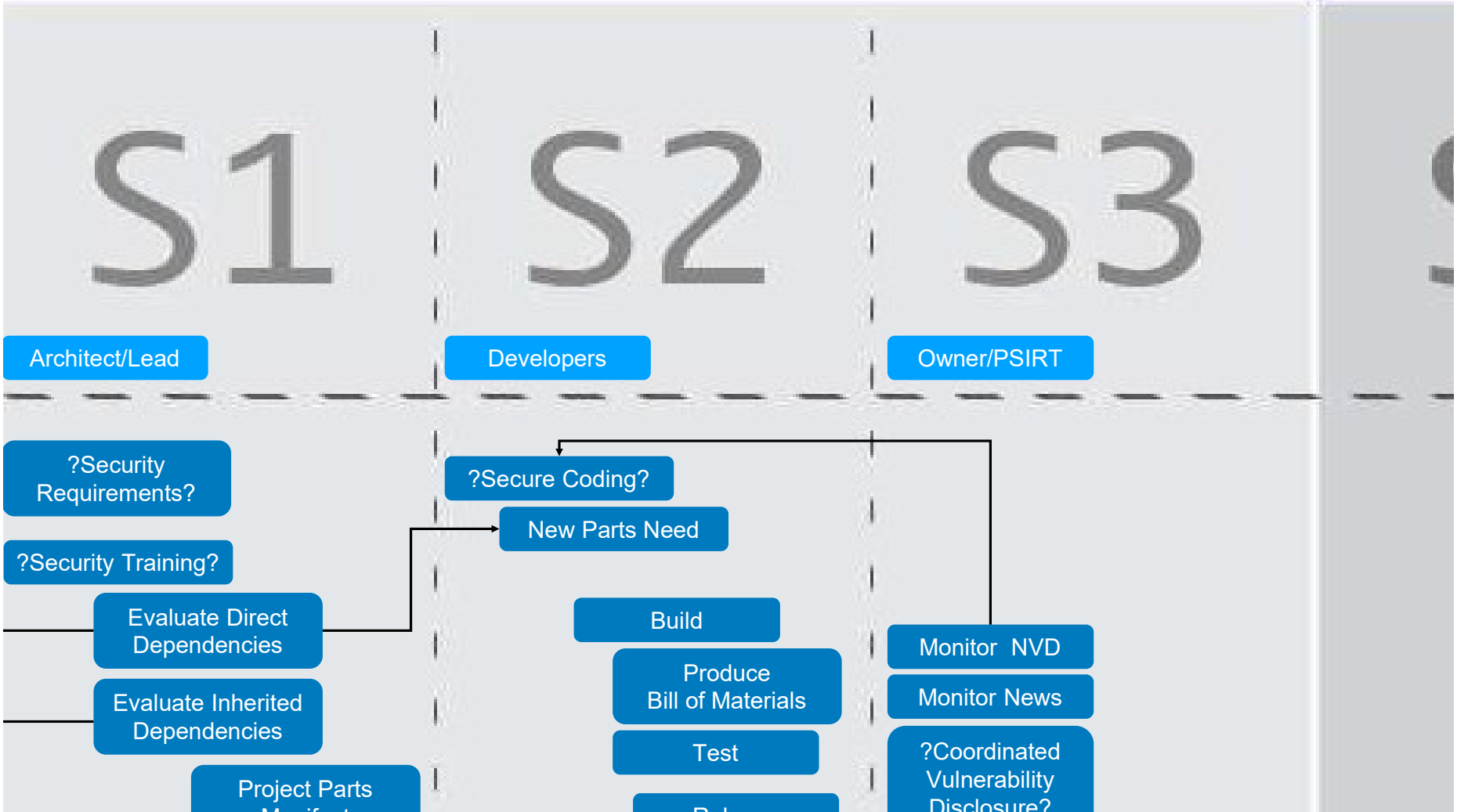

PARTS
COMPOUND PARTS
FINAL GOODS ASSEMBLED
OPERATOR
S1 S2 S3 S1 S2 S3 S1 S2 S3 S1 S2 S3
Chris Robbins
RedHat
ENTERPRISE
Chris Gates
Velentium
Mike Powers
Christiana Health
MEDICAL
Sounil Yu
BoA
FINANCIAL SERVICES
Josh Corman
PTC
INDUSTRIAL
Bob Martin
DoD
$OTHER

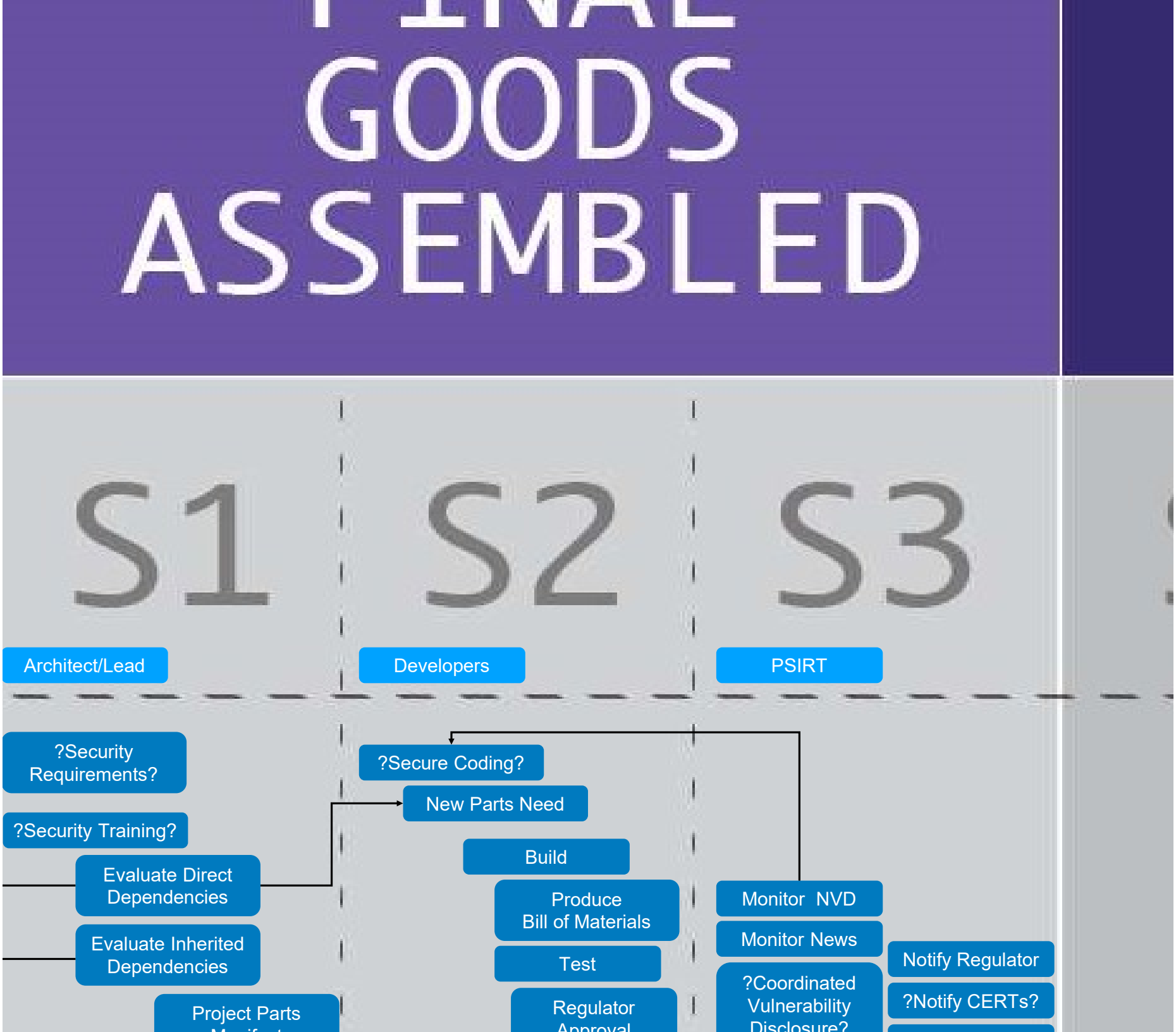
PARTS


S1
S2
S3
N/A
Developers
Custodian
?Security Requirements?
?Security Training?
?Secure Coding?
Build
POST Bill of Materials
Monitor NVD
Monitor News
?Coordinated Vulnerability Disclosure?

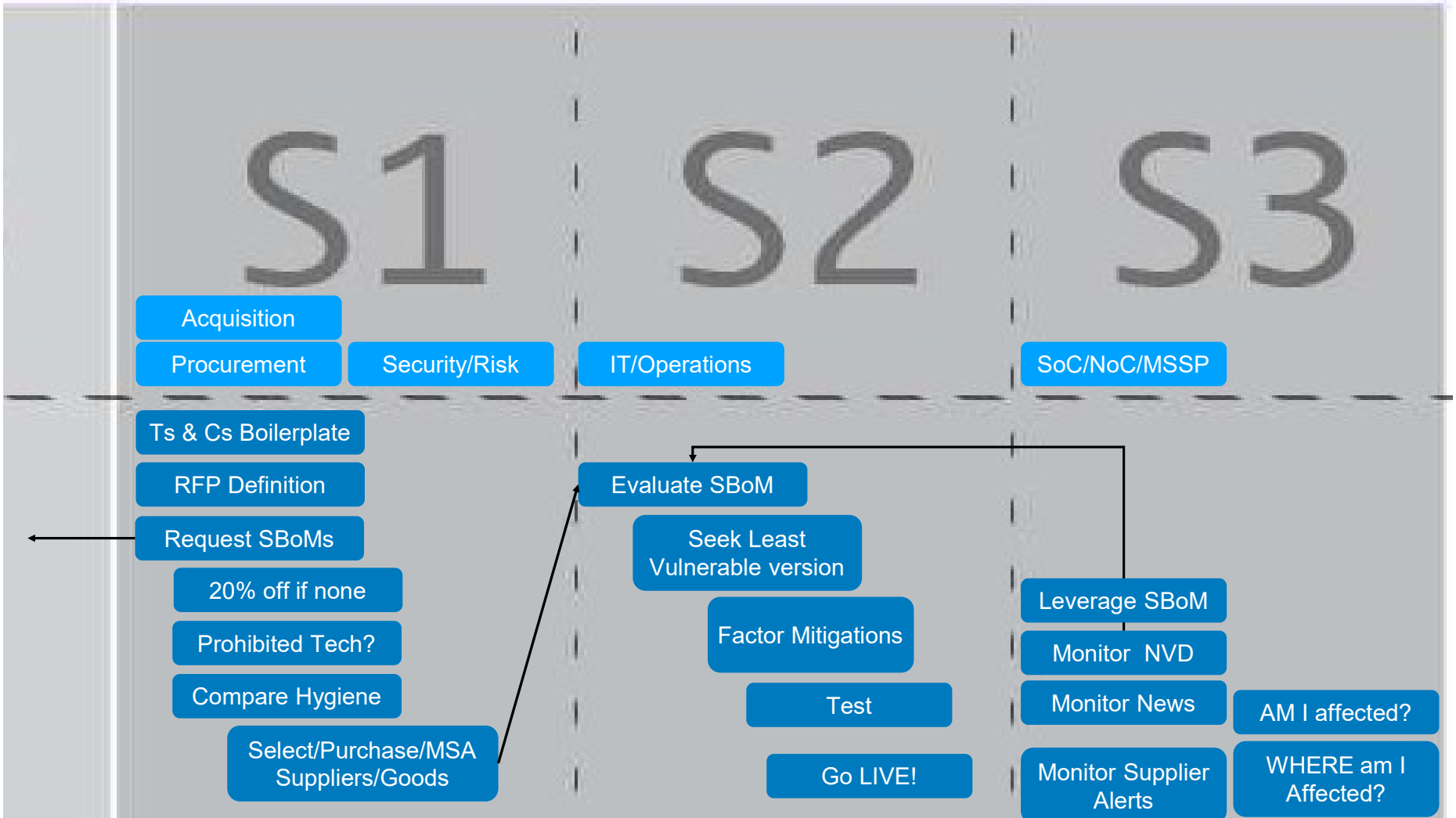

PARTS
S1
S2
S3
N/A
Developers
Custodian
?Security Requirements?
?Security Training?
?Secure Coding?
Build
Produce Bill of Materials
Test
Release
POST
Monitor NVD
Monitor News
?Coordinated Vulnerability Disclosure?

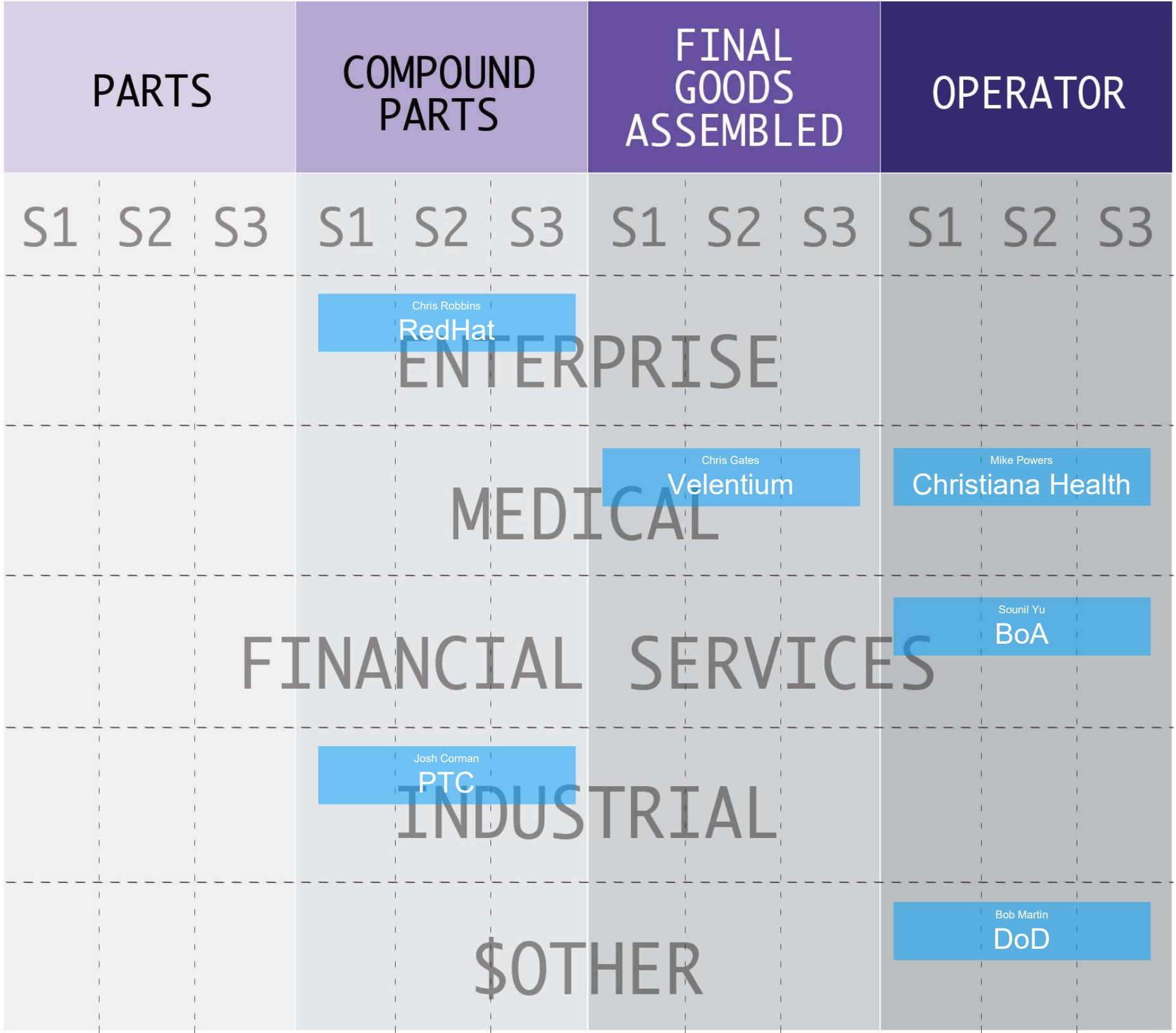
COMPOUND PARTS




FINAL
GOODS
ASSEMBLED
S1
S2
S3
Architect/Lead
Developers
PSIRT
?Security Requirements?
?Security Training?
Evaluate Direct Dependencies
Evaluate Inherited Dependencies
Project Parts
?Secure Coding?
New Parts Need
Build
Produce Bill of Materials
Test
Regulator
Monitor NVD
Monitor News
?Coordinated Vulnerability Disclosure?
Notify Regulator
?Notify CERTs?

OPERATOR


S1
S2
S3
Acquisition
Procurement
Security/Risk
IT/Operations
SoC/NoC/MSSP
Ts & Cs Boilerplate
RFP Definition
Request SBoMs
20% off if none
Prohibited Tech?
Compare Hygiene
Select/Purchase/MSA Suppliers/Goods
Evaluate SBoM
Seek Least Vulnerable version
Factor Mitigations
Test
Go LIVE!
Leverage SBoM
Monitor NVD
Monitor News
Monitor Supplier Alerts
AM I affected?
WHERE am I Affected?


PARTS
COMPOUND PARTS
FINAL GOODS ASSEMBLED
OPERATOR
S1 S2 S3 S1 S2 S3 S1 S2 S3 S1 S2 S3
Chris Robbins
RedHat
ENTERPRISE
Chris Gates
Velentium
Mike Powers
Christiana Health
MEDICAL
Sounil Yu
BoA
FINANCIAL SERVICES
Josh Corman
PTC
INDUSTRIAL
Bob Martin
DoD
$OTHER

Overall thrust

Crawl

Learn to what degree people are using SBoM & friends

Suss out common obstacles

Walk

Learn **how** people are using SBoM:

- What works
- What doesn't work
- How has it helped or hindered?

Run

Understand near misses: what could SBoM unlock if it met your use cases better?

Understand "rainbow scenarios"

Q: Are people using SBoM today?

A: In some industries, yes!

Less mature: healthcare end users, manufacturers w/ huge product catalogs

More mature: DoD, OS packaging, automotive, some medical device manufacturers

Doing their best: middle parts of the supply chain

“We need to know what we’re defending.” —healthcare end user interviewee

Common obstacles to SBoM use

Heavy vetting workload (e.g., Red Hat's curation of packages)

Uncooperative or clueless vendors

Developer inertia ("this is QA's problem")

No way to ingest/manage SBoM even if we had it

How are people using SBoM concepts today?

In what forms?

- Listing of filesystem directories & files (“manifest” or text dump)
- Folder full of software manuals
- Tool outputs from executable/source analysis (Software Composition Analysis)

At what stages of the software supply chain?

- Manufacturer, compound parts assembler, final goods assembler, end user
- End users (except DoD) often have the least leverage

What could SBoM unlock for our interviewees?

Effective incident response via quick search

Richer asset records for inventory management

Tune security tools according to what systems say they're running

Graceful phasing out of end-of-life/aging systems

SBoM as forcing function: vendors can streamline their own processes

Insights from interviews (n = ~7)

Supplier selection is **not** a universal use case for our interviewees. Typically, lack of an SBoM does not disqualify a vendor (except in DoD)

Vulnerability matching & vuln management is a major use case for end users

Ability to ingest/handle SBoMs decreases toward end of supply chain

Demand for features beyond SW name & version number is **low** among our interviewees (except DoD)

Frameworks (e.g., Java) are important to divulge, not just libraries/packages