34th Annual INCOSE international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

Securing Your Eggs in Multiple Baskets – Assuring a Resilient and Secure Supply Chain

Matthew Hause, System Strategy Inc.
MHause@SystemXI.com
Mitchell Brooks, System Strategy Inc.
MBrooks@ SystemXI.com
Robert Kennedy, Clearfield, Inc.
RKennedy@SEECLEARFIELD.COM

Abstract

The global supply chain is a complex system of system relying on other complex systems of systems (SoS) to achieve their goals. To take a typical example, Enterprise A is supplied essential parts on a regular basis to manufacture its products. To place the order requires global financial systems, integrated email systems, the internet, multiple telecommunications systems, supply software provided by large companies. To deliver the parts may require air and maritime transportation systems, the rail network, interstate highway systems, road haulage companies, and state and local transportation systems. When these complex systems fail, the impact can be global, and the results catastrophic. Recent examples were the shortage of Personal Protective Equipment (PPI) during the COVID pandemic, computer chip shortages delaying the assembly and sales of cars, and most recently the baby formula shortage. These were due to disruptions in the supply chain caused by an overreliance on single sourced suppliers who failed to deliver, transportation disruptions, outsourcing of critical parts, supplies, and medicines to distant countries, and an overreliance on "Just In Time" for inventory management. This is the case of placing too many eggs in too few baskets, and often just one basket. In addition, counterfeit or substandard parts and products can enter the supply chain. This has included critical mechanical parts on aircraft, chips containing spyware, and substandard or out of date medicines substituted for the real thing resulting in serious illness and death. This complex SoS needs to be examined, studied and understood in the same way as a mission critical system: threats, vulnerabilities, and risks need to be identified and mitigated and assurance cases defined to ensure a solid and reliable supply chain. This paper will look at the supply chain of an example factory system to determine how some of these problems can be predicted, prevented, mitigated, and solved using the UAF, RAAML and assurance case techniques.

Agenda

- The Global Supply Chain
- Supply Chain Issues
- Modeling Systems of Systems and Enterprises
- Security Controls and Mitigations
- Example Supply Chain Model
- Conclusions
- Questions?

History of the Global Supply Chain

History of the Global Supply Chain

- Keith Oliver, coined the terms "Supply Chain" and "Supply Chain Management“ in 1982.
- “Supply chain management (SCM) is the process of planning, implementing, and controlling the operations of the supply chain with the purpose to satisfy customer requirements as efficiently as possible. Supply chain management spans all movement and storage of raw materials, work-in-process inventory, and finished goods from point-of-origin to point-of-consumption”. (Oliver, 1982).
- In reality, supply chains have always existed.
- Early humans gathered in tribes and family units and started to cooperate and specialize their skills.
  - Usually one-on-one transactions, with people who knew and trusted one another.
  - Over time the supply chain expanded attempting to remove inefficiencies by circumventing middlemen, taxes/tariffs, or reducing the number of suppliers.
  - Exchanges occurred between multiple suppliers and transporters, often incurring taxes by the governments, and danger from bandits in route to the destinations.

The Dynamic Supply Chain

- The driving principle behind the supply chain and all commerce is to provide value for stakeholders and to remain profitable.
- Throughout the evolution of the supply chain, the enabling principles were transportation, supply, communication, and trust.
- Currently the global supply chain has problems in all these categories.

Current Supply Chain Issues

- Trust/ Certification
  - Lack of proper supplier qualification
  - Counterfeit or substandard parts
  - Substandard or out of date medicines
  - Fake critical mechanical parts on aircraft
  - Chips containing spyware
  - Certification of prevenance of products, organic, no child/slave labor, sustainably sourced, USA sourced, Fair Trade, etc.
- Supply
  - Capacity constraints
  - Container shortages
  - Single sources products: Chips, medicine, PPE, etc.
- Transportation
  - Port Congestion
  - Labor Shortages
  - Infrastructure bottlenecks
  - Regulatory changes
  - Technological disruptions
- Communication
  - Data silos
  - Inconsistent data standards
  - Information gaps
  - Manual processes
  - Ransomware, phishing, insider threats, etc.
  - Lack of collaborative tools

So, what do we do now?

- Transportation
  - Limit the distance between buyers and providers
  - Ensure backup routes and strategies are in place
- Supply
  - Minimize single sourced parts
  - Increase local warehousing
  - Adopt condition-based maintenance
- Communication
  - Ensure visibility throughout the links of the supply chain
  - Increase production metrics to properly gage demand
- Trust/ Certification
  - Establish assurance cases for all parts of the supply chain
  - Apply risk management at all levels
- Accept that the global supply chain is a complex system of systems that cannot be controlled but can be managed if understood.

Supply Chain Risk Management (SCRM)

- SCRM is a systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain. SCRM will be applied to all information systems and weapons systems that are designated as, or comprised of, any of the following:
  - a. National Security Systems, Automated Tactical Systems, and automated weapon systems as defined by Army regulation 25–2.
  - b. Mission Assurance Category I systems, as defined by Department of Defense Instruction 5200.44.
  - c. Systems registered as mission critical in Army portfolio management system or the Department of Defense's information technology repository.
  - d. Other systems that the Army Acquisition Executive or CIO/G–6 determines are critical to the direct fulfillment of military or intelligence missions.

Modeling Systems of Systems and Enterprises

The Supply Chain as an SoS

- Operational independence
  - The supply chain is a collection of independent operators, government institutions, and international conglomerates. They operate independently to support their individual customers. Support of the overall is of secondary importance.
- Managerial independence
  - Each of the supply chain entities must comply with a variety of different standards, rules, laws and regulations. There are various government institutions that oversee different companies. However, they maintain their operational independence separate from that of the supply chain.
- Evolutionary development
  - New systems, technologies or ConOps may be introduced by any of the companies as required to evolve and adapt to the changing environment, latest technology needs or stakeholder requirements. This will affect both the individual system as well as the SoS.
- Geographical distribution
  - The global supply chain is geographically distributed by its very definition.
- Lifecycle independence
  - Even within the individual companies there will be multiple system lifecycles across asynchronous acquisition and development efforts, involving legacy systems, developmental systems, and technology insertion to meet their customer needs.

Importance of the SoS to the Supply Chain

- Multiple levels of stakeholders
  - Changes cannot simply be mandated but must be negotiated.
  - Changes will take time to negotiate and implement
- Multiple, and contradictory, objectives and purpose
  - There is no “Common Good”. Benefits for one can adversely affect others
  - Proposed changes can cause infighting delaying implementation
- Multiple, different, operational priorities
  - Owners, stakeholders, shareholders, customers, regulators must be consulted
  - Competition is fierce between and across different entities.
- Multiple System lifecycles
  - Production cycles may not match demand
  - ROI to replace newly installed systems is difficult
- Multiple owners making independent resourcing decisions
  - Competition has cut operating margins limiting discretionary funds
  - In a distributed, global, supply chain, enforcement can be impossible

Unified Architecture Framework (UAF)

- The UAF is used for defining system architectures and system of systems architectures
- It is focused on the scope, needs, strategy, expectations, stakeholders, and long-term plans
- It is built on SysML, so has built-in traceability to system development in SysML.

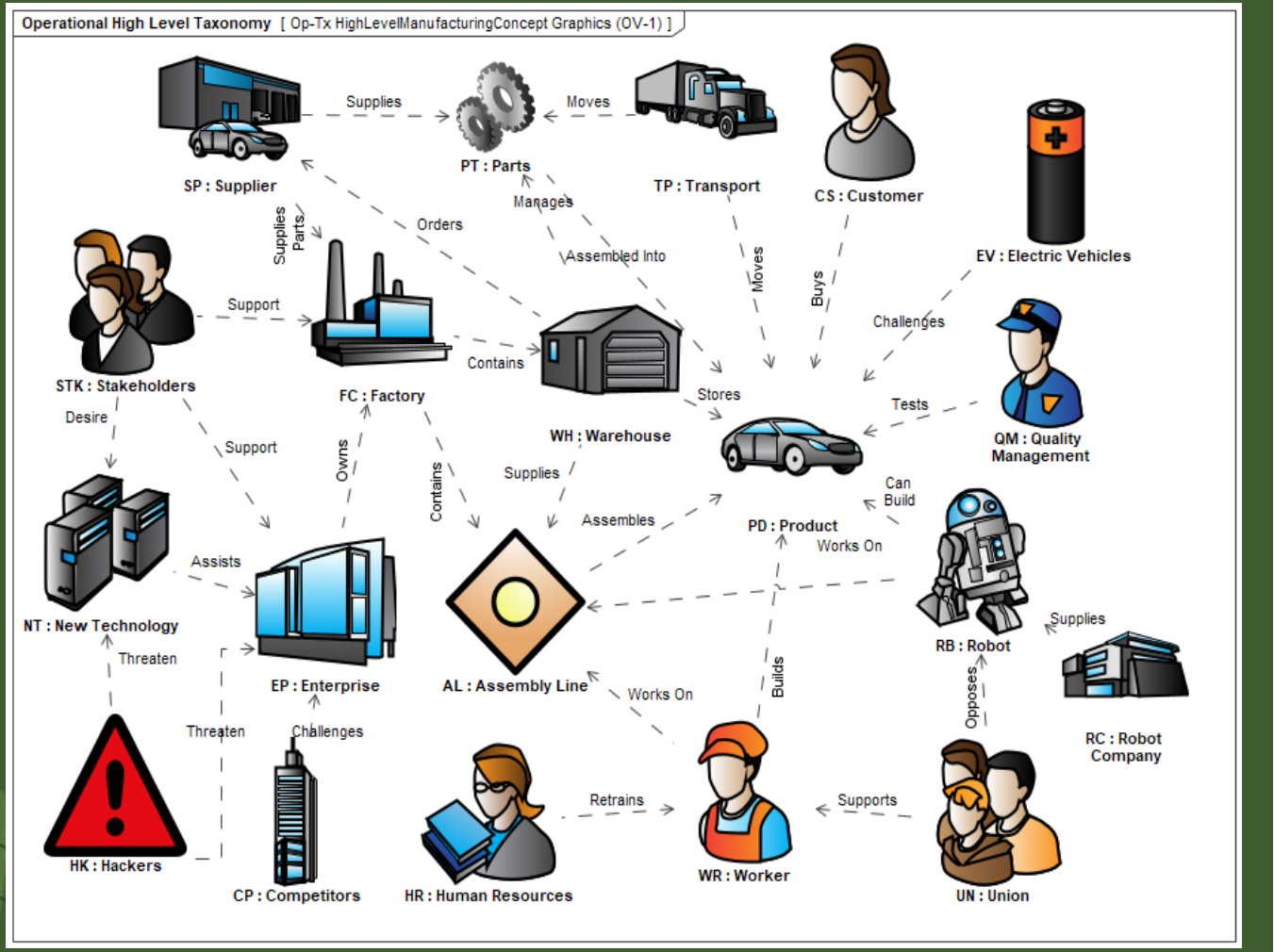
	Taxonomy Tx	Structure Sr	Connectivity Cn	Processes Pr	States St	Interaction Scenarios Is	Information If	Parameters Pm	Constraints Ct	Roadmap Rm	Traceability Tr
Metadata Md	Metadata Taxonomy Md-Tx	Architecture Viewpoints [a] Md-Sr	Metadata Connectivity Md-Cn	Metadata Processes [a] Md-Pr	-	-			Metadata Constraints [a] Md-Ct		Metadata Traceability Md-Tr
Strategic St	Strategic Taxonomy St-Tx	Strategic Structure St-Sr	Strategic Connectivity St-Cn	-	Strategic States St-St	-			Strategic Constraints St-Ct	Strategic Deployment, St-Rm Stategic Phasing St-Rm	Strategic Traceability St-Tr
Operational 0p	Operational Taxonomy Op-Tx	Operational Structure Op-Sr	Operational Connectivity Op-Cn	Operational Processes Op-Pr	Operational States Op-St	Operational Interaction Scenarios Op-Is			Operational Constraints Op-Ct	-	-
Services Sv	Service Taxonomy Sv-Tx	Service Structure Sv-Sr	Service Connectivity Sv-Cn	Service Processes Sv-Pr	Service States Sv-St	Service Interaction Scenarios Sv-Is	Conceptual Data Model,	Environment Pm-En	Service Constraints Sv-Ct	Service Roadmap Sv-Rm	Service Traceability Sv-Tr
Personnel Pr	Personnel Taxonomy Pr-Tx	Personnel Structure Pr-Sr	Personnel Connectivity Pr-Cn	Personnel Processes Pr-Pr	Personnel States Pr-St	Personnel Interaction Scenarios Pr-Is	Logical Data Model,		Competence, Drivers, Performance Pr-Ct	Personnel Availability, Personnel Evolution, Personnel Forecast Pr-Rm	Personnel Traceability Pr-Tr
Resources Rs	Resource Taxonomy Rs-Tx	Resource Structure Rs-Sr	Resource Connectivity Rs-Cn	Resource Processes Rs-Pr	Resource States Rs-St	Resource Interaction Scenarios Rs-Is	Physical schema, real world results		Resource Constraints Rs-Ct	Resource evolution, Resource forecast Rs-Rm	Resource Traceability Rs-Tr
Security Sc	Security Taxonomy Sc-Tx	Security Structure Sc-Sr	Security Connectivity Sc-Cn	Security Processes Sc-Pr	-	-		Measurements Pm-Me	Security Constraints Sc-Ct	-	-
Projects Pj	Project Taxonomy Pj-Tx	Project Structure Pj-Sr	Project Connectivity Pj-Cn	-	-	-			-	Project Roadmap Pj-Rm	Project Traceability Pj-Tr
Standards Sd	Standard Taxonomy Sd-Tx	Standards Structure Sd-Sr	-	-	-	-			-	Standards Roadmap Sr-Rm	Standards Traceability Sr-Tr
Actuals Resources Ar		Actual Resources Structure, Ar-Sr	Actual Resources Connectivity, Ar-Cn	Simulation [b]					Parametric Execution/ Evaluation [b]	-	-
Dictionary * Dc											
Summary & Overview SmOv											
Requirements Rq											

Example Automotive Factory Model

- Problem Statement: Powerhouse Engines (PE Inc.) is an automotive supply company providing internal combustion engines. PE Inc. finds that it has gradually become less competitive over the years largely due to their outdated technology and largely manual processes. Foreign and domestic competitors have started to cut into their business and the stakeholders are concerned that the company's loss of market share will accelerate and that they will eventually become insolvent. To combat this, the shareholders have proposed an investigation into strategies and technologies such as Augmented reality, Robotic assembly systems, 5G, AI, Additive manufacturing, outsourcing of select manufacturing and IT systems, Battery technology, Data analytics, Hybrid/electric engines, etc. These technologies will be rolled out over a 3-phase technology deployment plan.

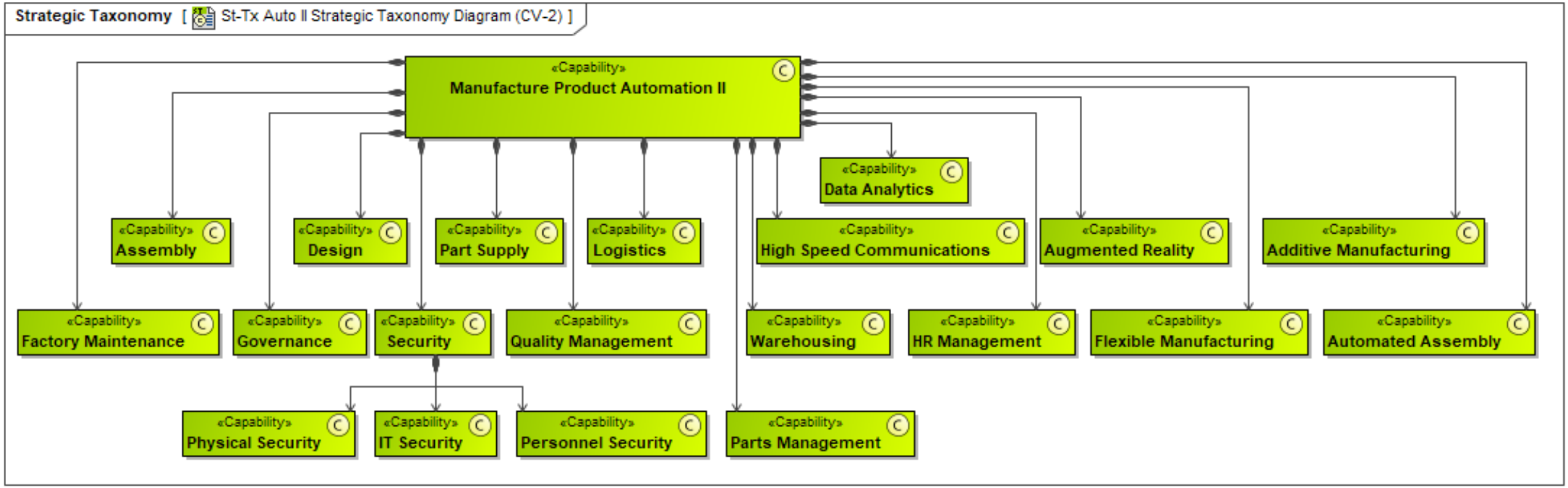
High Level Manufacturing Concept for Powerhouse Engines

- Solution independent concepts in the architecture
- The part supplier could be an external company, an internal casting department, or an in-house 3D printer.
- All supply parts, and each has advantages and disadvantages regarding supply chain delays, cost, flexibility, etc.
- All 3 will be deployed over the 3 phases of technology introduction.



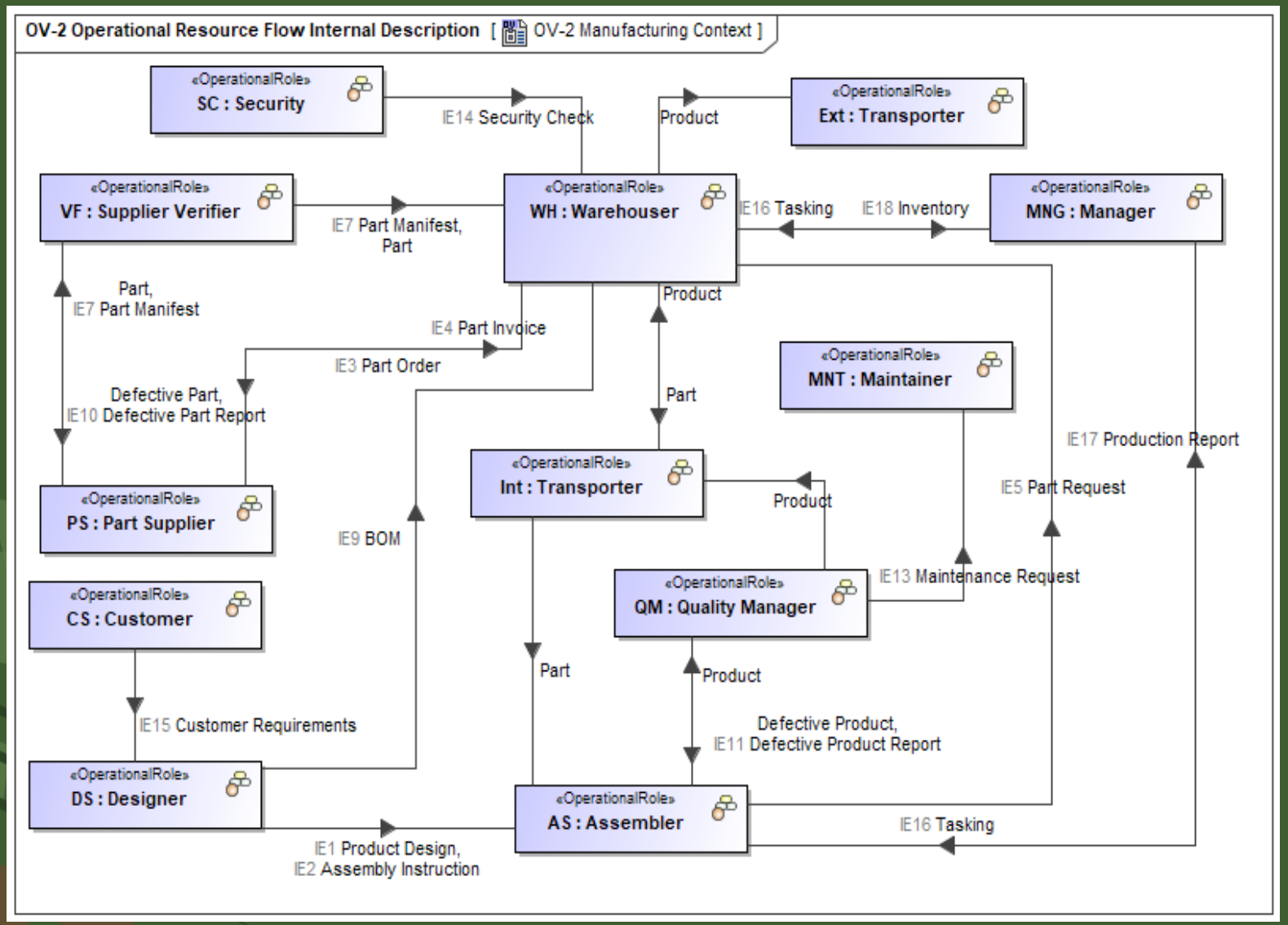
Powerhouse Engines Enterprise Capabilities

- Defines what the enterprise can do, not how it does it.
- Linked to effects accomplished by the implementing systems



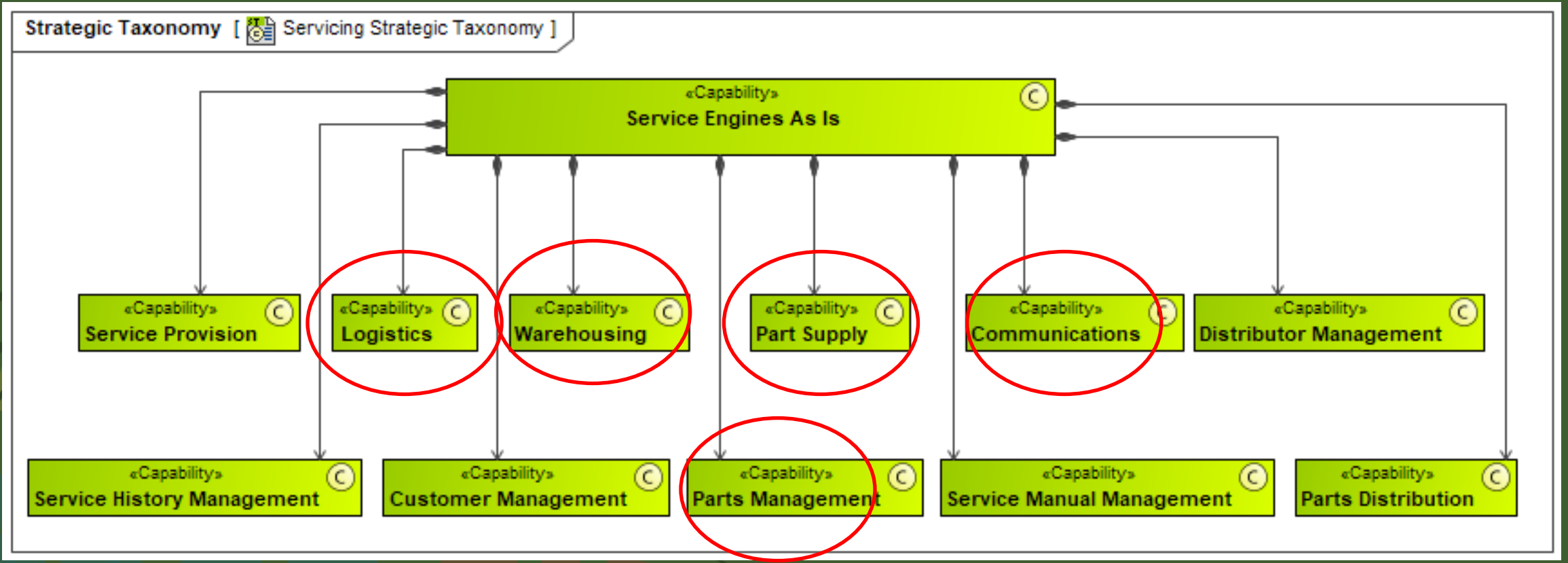
Manufacturing Logical Performers

- Operational activities are grouped together to define operational performers
- Deriving performers from their activities concentrates on behavior before structure
- Helps prevent “Solutioneering”



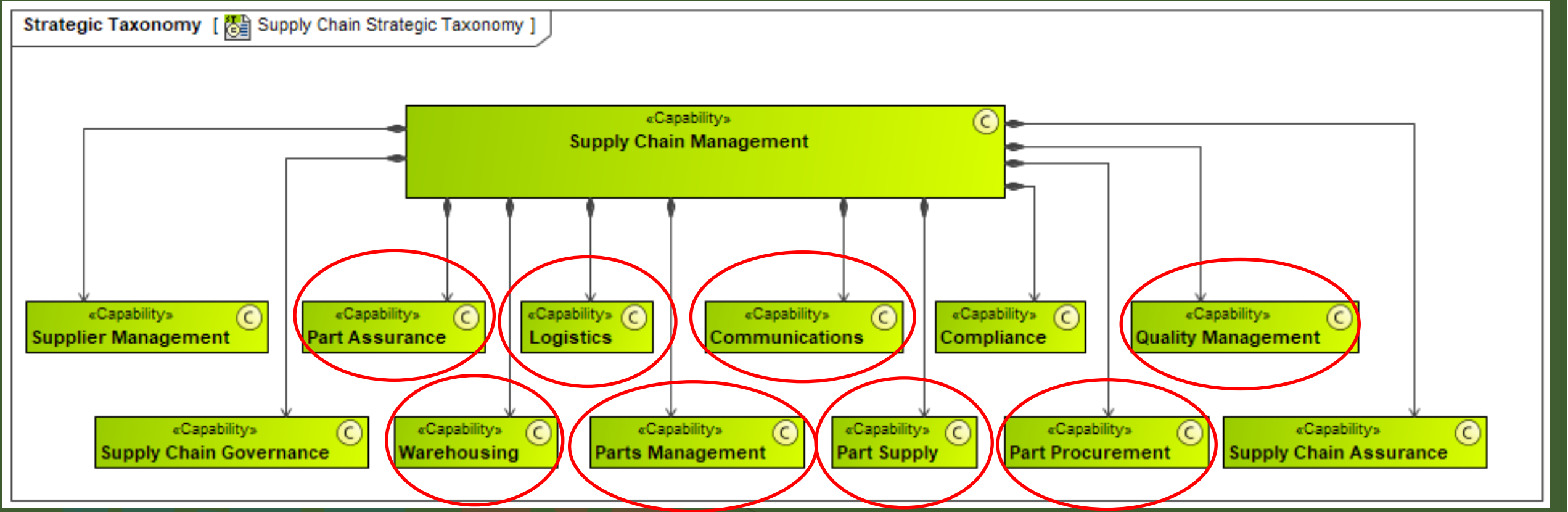
Servicing Capabilities

- Many capabilities in common

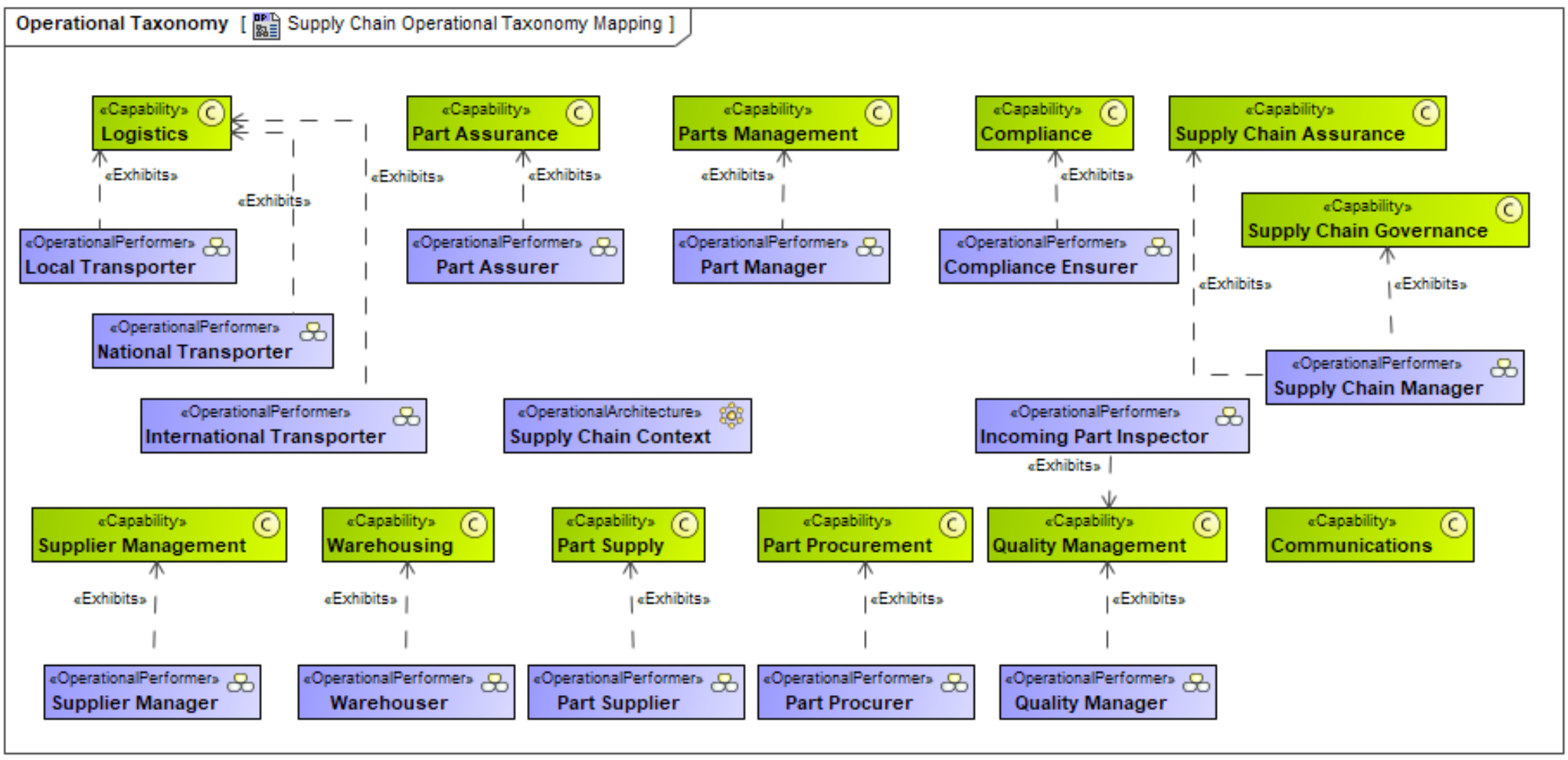


Supply Chain Management Capabilities

- Multiple capabilities in common, therefore reuse of implementing systems, but also constrains changes

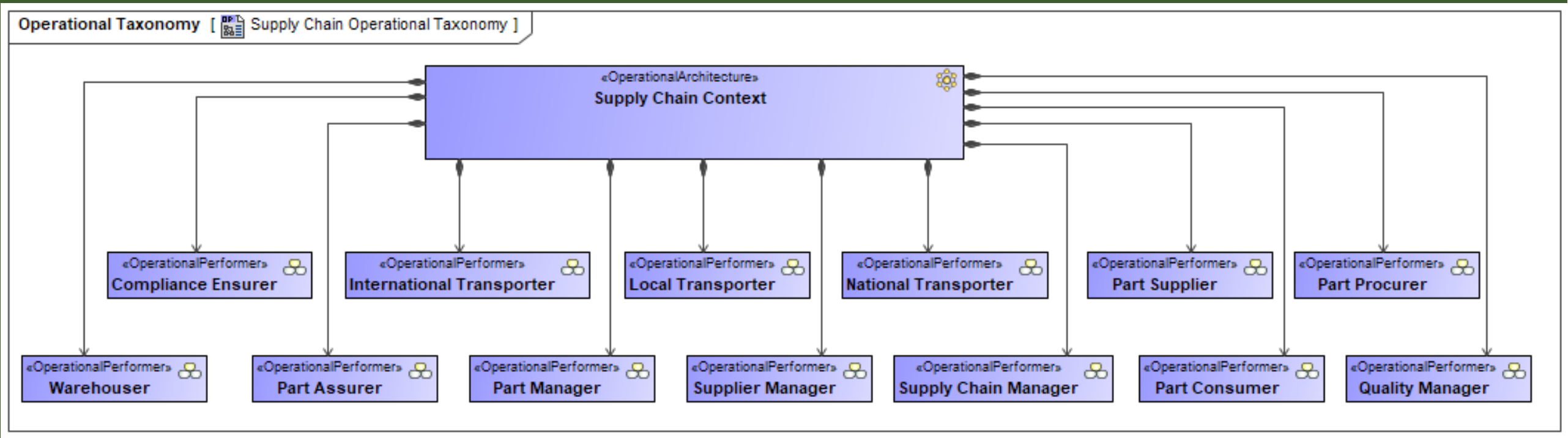


Supply Chain Operational Performers

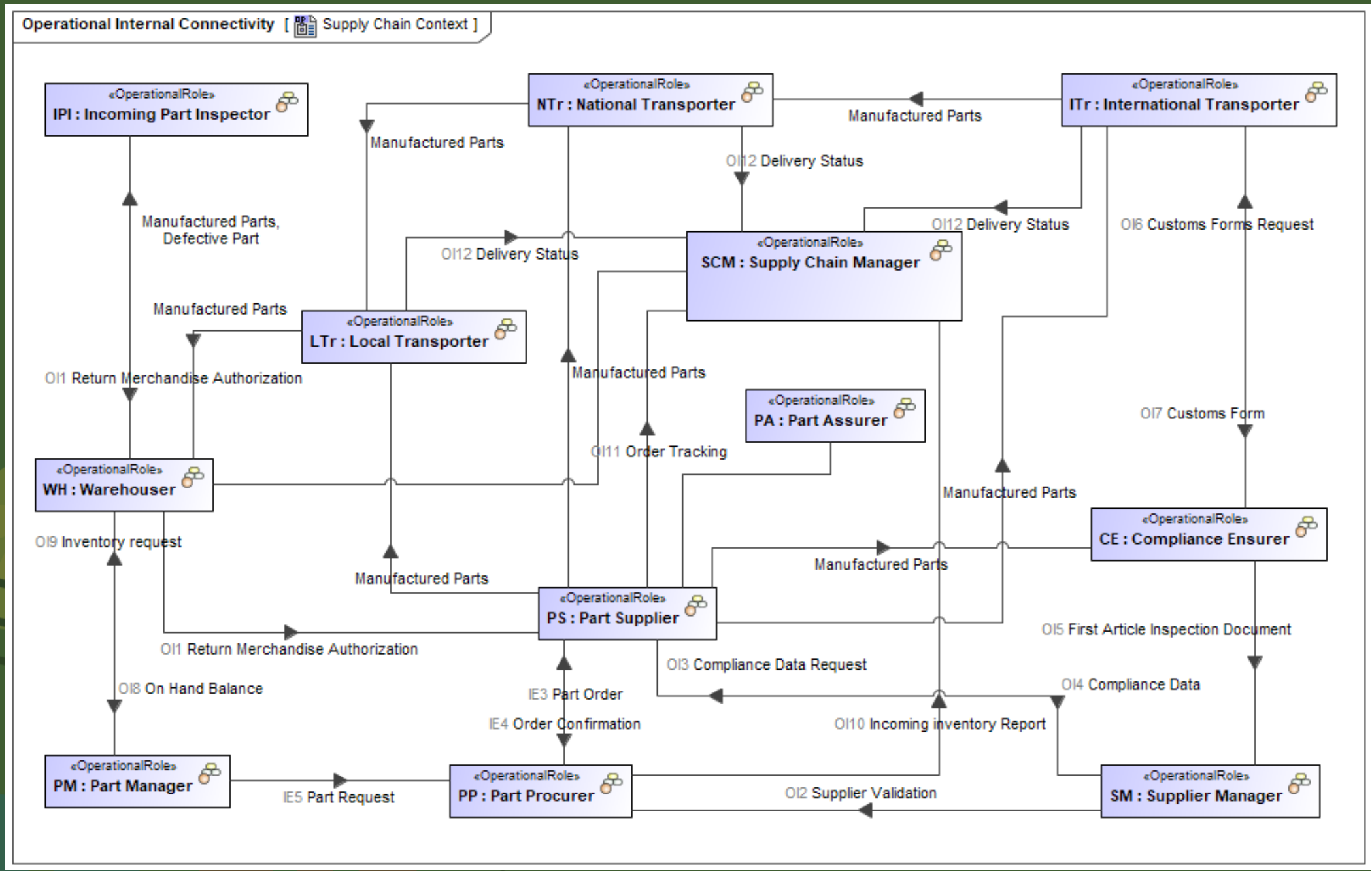


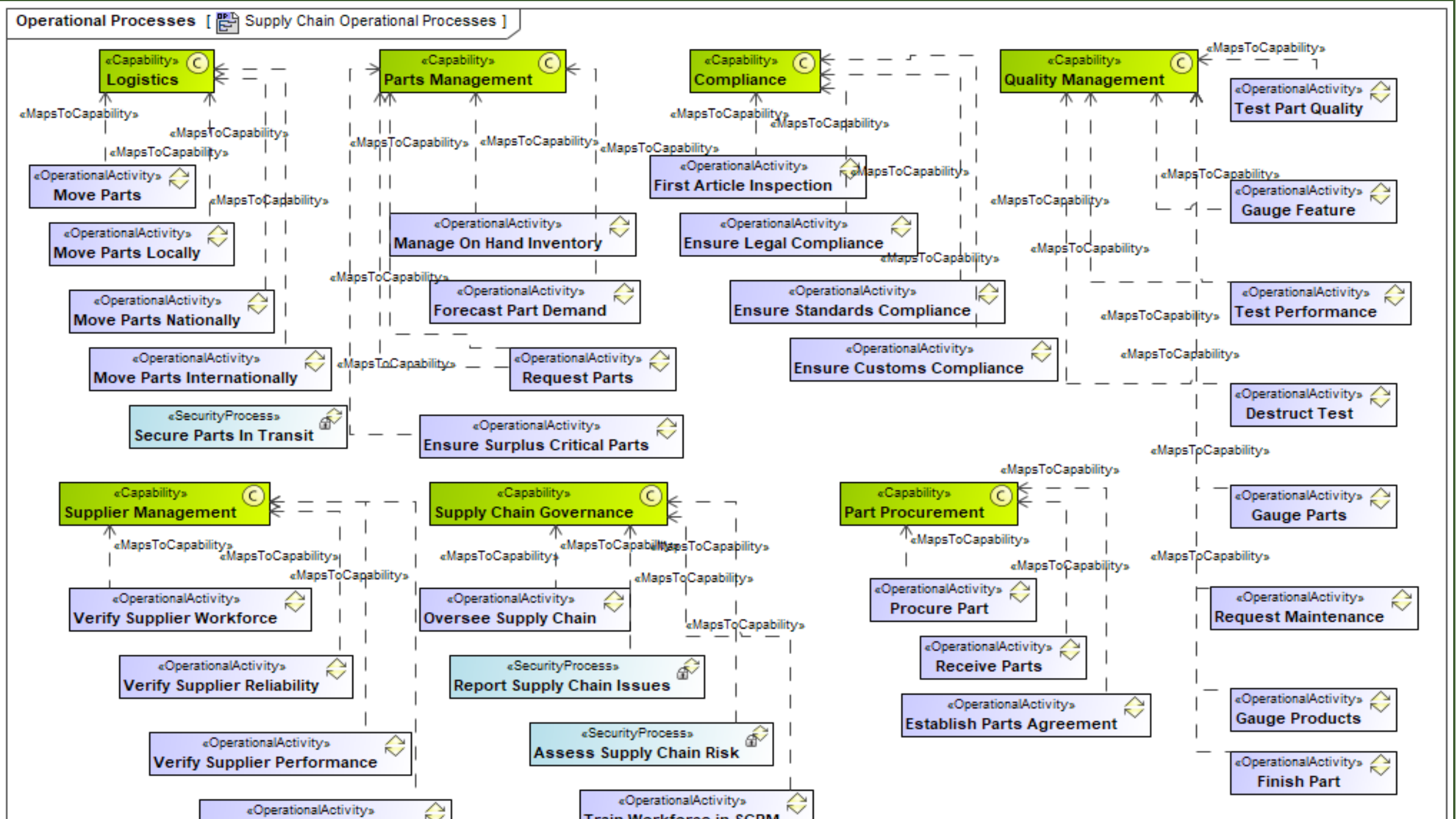
Supply Chain Structure

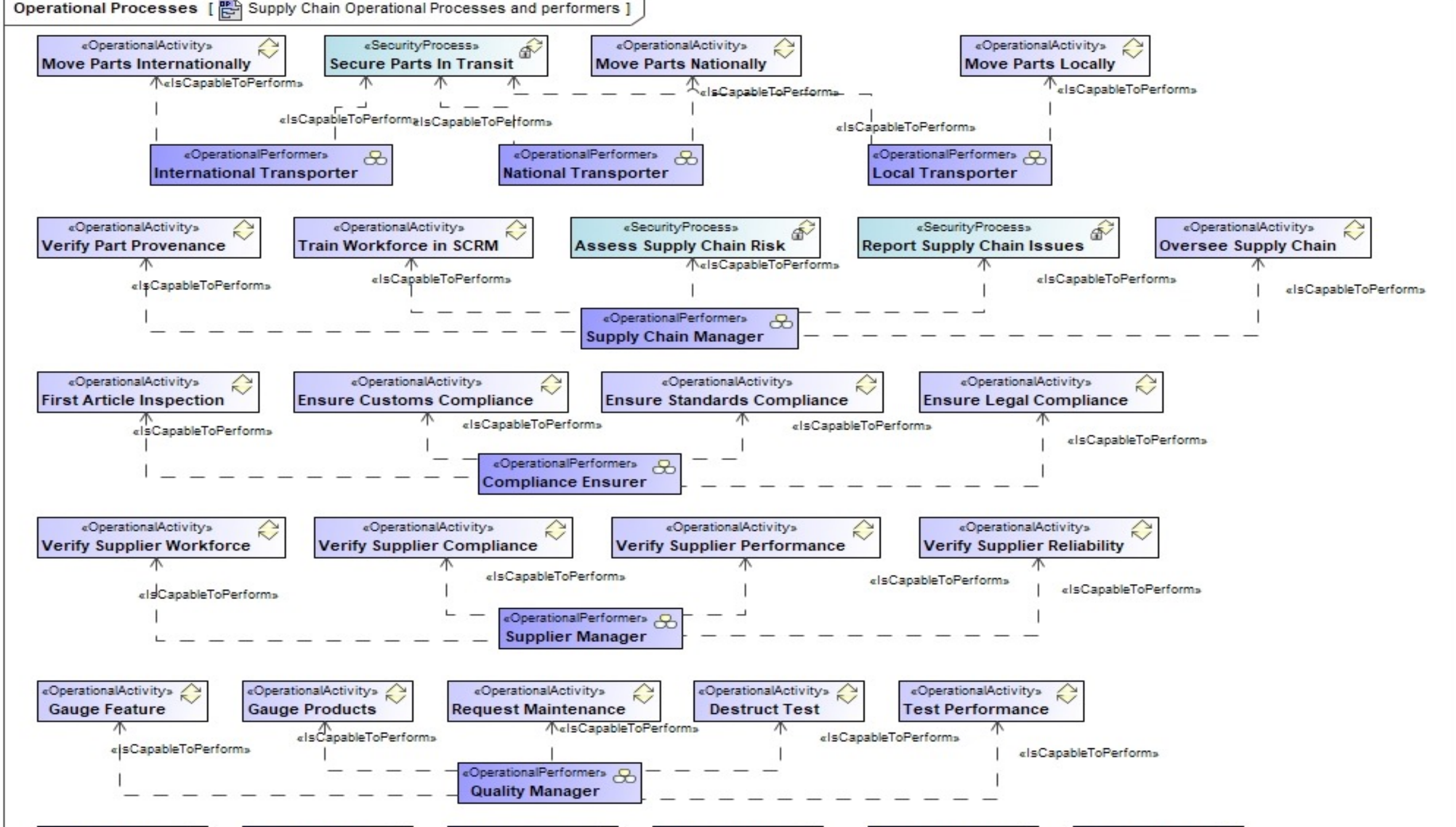
- The mapped elements are gathered into a context



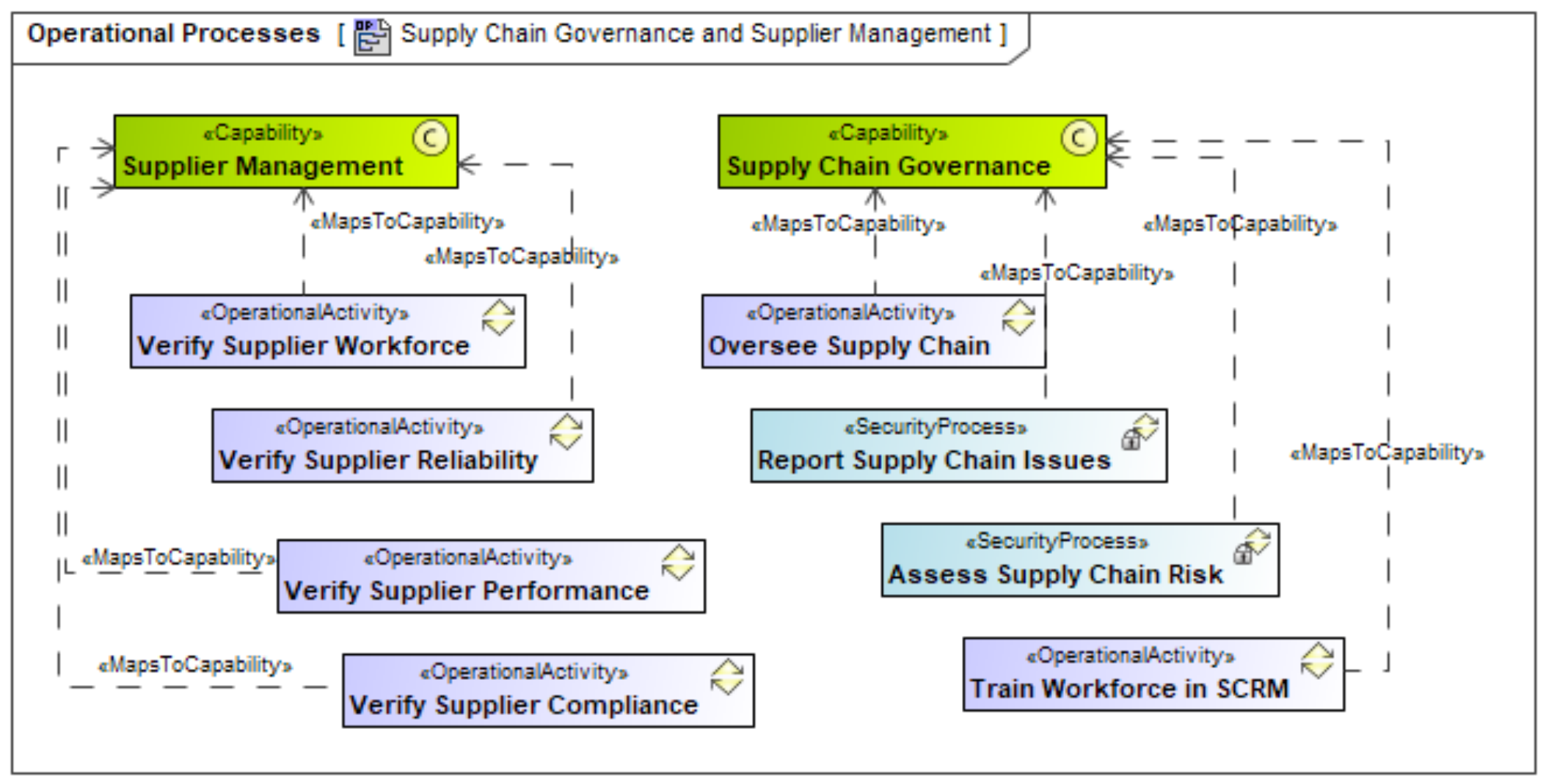
Supply Chain Interactions



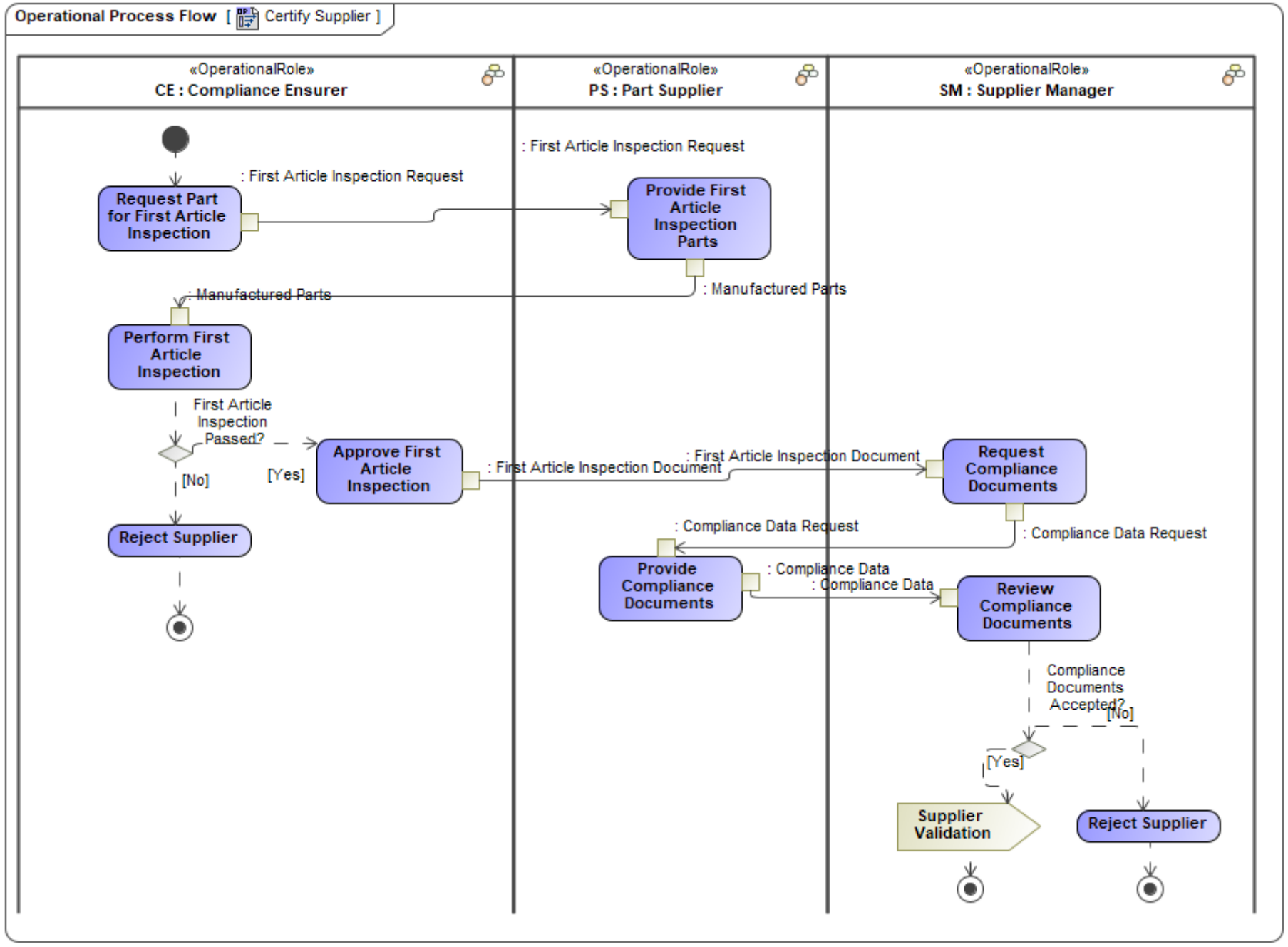

Operational Processes [Supply Chain Operational Processes]
«Capability» Logistics
«Capability» Parts Management
«Capability» Compliance
«Capability» Quality Management
«MapsToCapability»
«OperationalActivity» Move Parts
«OperationalActivity» Move Parts Locally
«OperationalActivity» Move Parts Nationally
«OperationalActivity» Move Parts Internationally
«OperationalActivity» Manage On Hand Inventory
«OperationalActivity» Forecast Part Demand
«OperationalActivity» Request Parts
«SecurityProcess» Secure Parts In Transit
«OperationalActivity» Ensure Surplus Critical Parts
«OperationalActivity» First Article Inspection
«OperationalActivity» Ensure Legal Compliance
«OperationalActivity» Ensure Standards Compliance
«OperationalActivity» Ensure Customs Compliance
«OperationalActivity» Test Part Quality
«OperationalActivity» Gauge Feature
«OperationalActivity» Test Performance
«OperationalActivity» Destruct Test
«Capability» Supplier Management
«Capability» Supply Chain Governance
«Capability» Part Procurement
«OperationalActivity» Verify Supplier Workforce
«OperationalActivity» Verify Supplier Reliability
«OperationalActivity» Verify Supplier Performance
«OperationalActivity» Oversee Supply Chain
«SecurityProcess» Report Supply Chain Issues
«SecurityProcess» Assess Supply Chain Risk
«OperationalActivity» Procure Part
«OperationalActivity» Receive Parts
«OperationalActivity» Establish Parts Agreement
«OperationalActivity» Gauge Parts
«OperationalActivity» Request Maintenance
«OperationalActivity» Gauge Products
«OperationalActivity» Finish Part

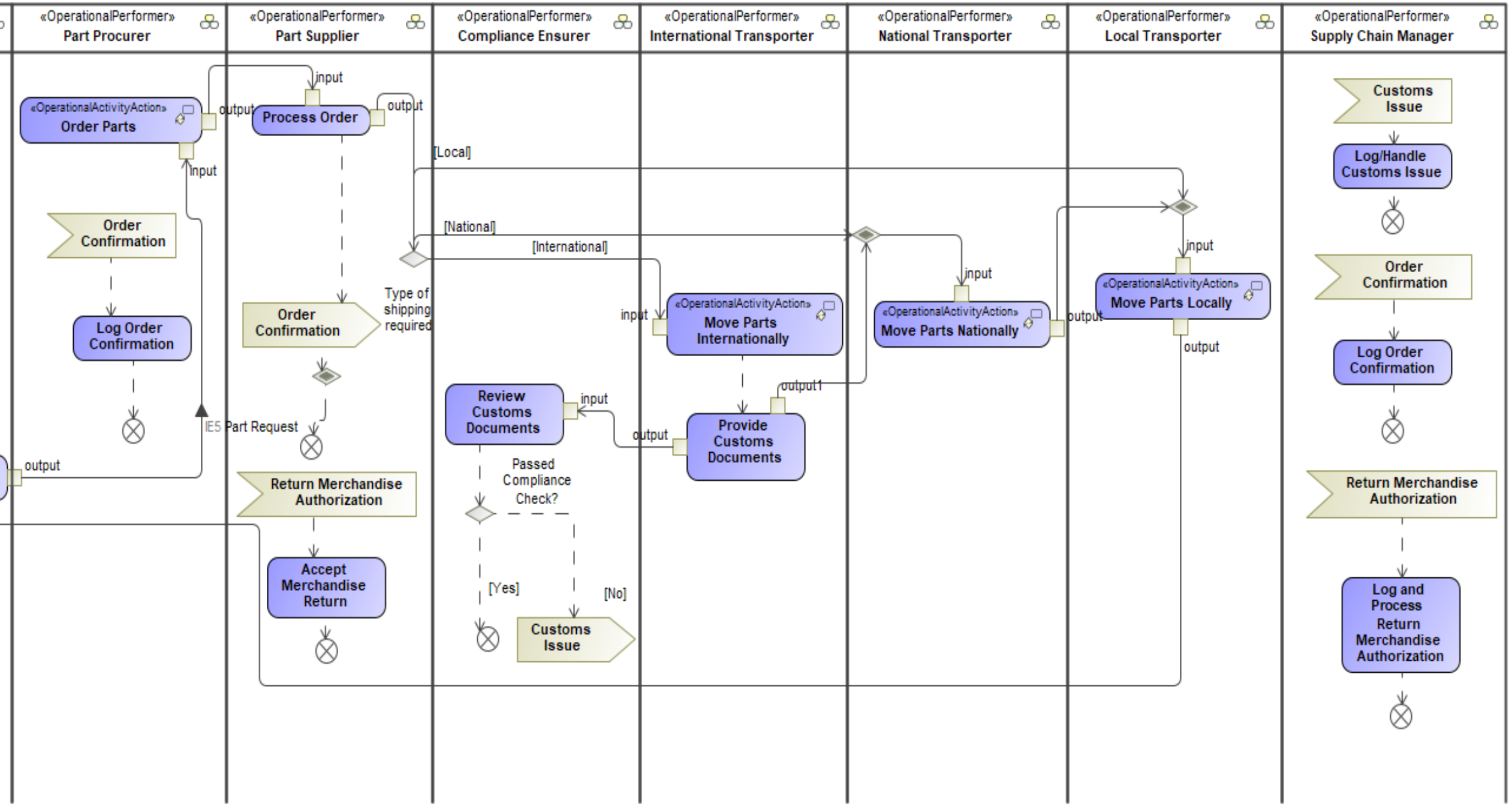

Operational Processes [Supply Chain Operational Processes and performers]
«OperationalActivity»
Move Parts Internationally
«SecurityProcess»
Secure Parts In Transit
«OperationalActivity»
Move Parts Nationally
«OperationalActivity»
Move Parts Locally
«IsCapableToPerform»
«OperationalPerformer»
International Transporter
«OperationalPerformer»
National Transporter
«OperationalPerformer»
Local Transporter
«OperationalActivity»
Verify Part Provenance
«OperationalActivity»
Train Workforce in SCRM
«SecurityProcess»
Assess Supply Chain Risk
«SecurityProcess»
Report Supply Chain Issues
«OperationalActivity»
Oversee Supply Chain
«OperationalPerformer»
Supply Chain Manager
«OperationalActivity»
First Article Inspection
«OperationalActivity»
Ensure Customs Compliance
«OperationalActivity»
Ensure Standards Compliance
«OperationalActivity»
Ensure Legal Compliance
«OperationalPerformer»
Compliance Ensurer
«OperationalActivity»
Verify Supplier Workforce
«OperationalActivity»
Verify Supplier Compliance
«OperationalActivity»
Verify Supplier Performance
«OperationalActivity»
Verify Supplier Reliability
«OperationalPerformer»
Supplier Manager
«OperationalActivity»
Gauge Feature
«OperationalActivity»
Gauge Products
«OperationalActivity»
Request Maintenance
«OperationalActivity»
Destruct Test
«OperationalActivity»
Test Performance
«OperationalPerformer»
Quality Manager

Governance and Supplier Management



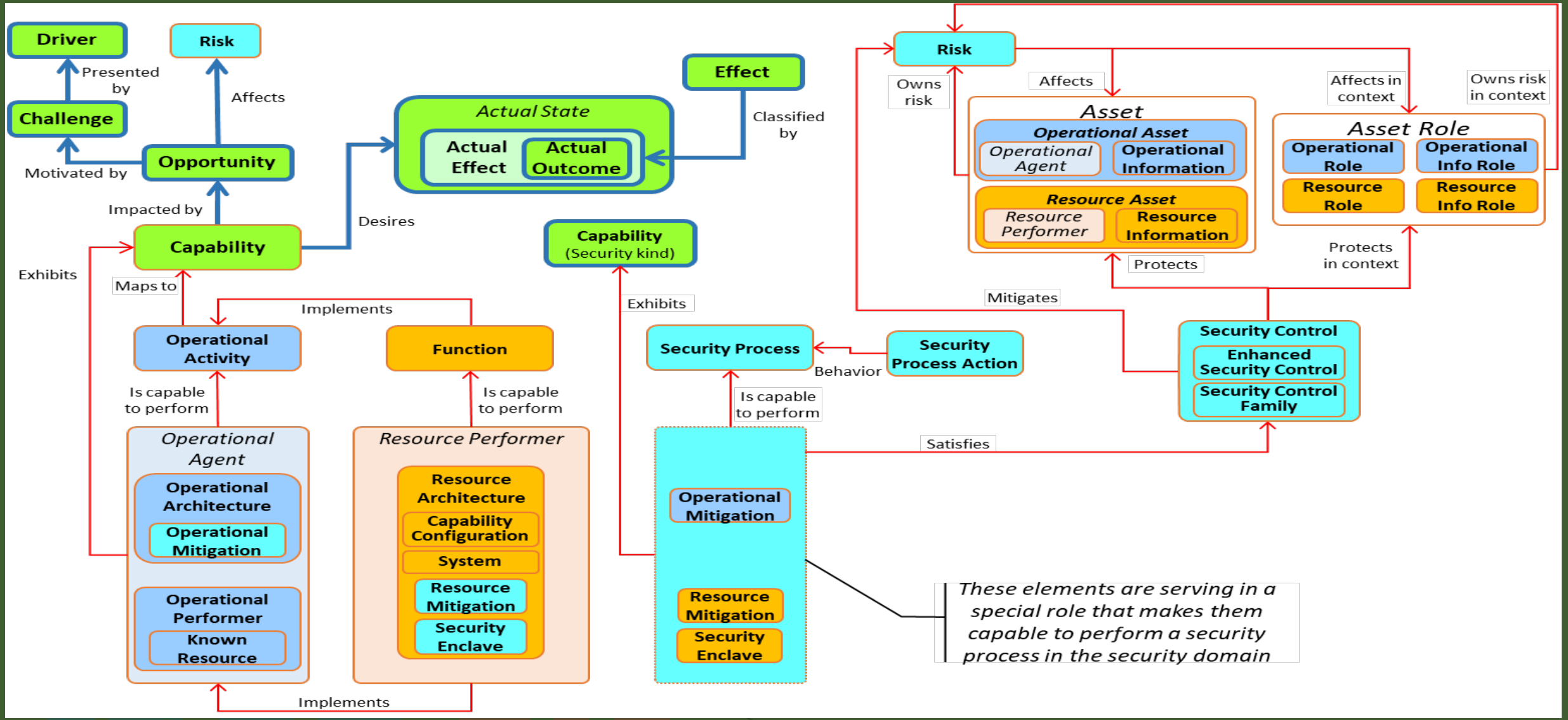
Certify Supplier Process




«OperationalPerformer»
Part Procurer
«OperationalPerformer»
Part Supplier
«OperationalPerformer»
Compliance Ensurer
«OperationalPerformer»
International Transporter
«OperationalPerformer»
National Transporter
«OperationalPerformer»
Local Transporter
«OperationalPerformer»
Supply Chain Manager
«OperationalActivityAction»
Order Parts
input
output
Process Order
output
input
[Local]
Order Confirmation
Log Order Confirmation
[National]
[International]
Order Confirmation
Type of shipping required
input
«OperationalActivityAction»
Move Parts Internationally
input
«OperationalActivityAction»
Move Parts Nationally
input
«OperationalActivityAction»
Move Parts Locally
output
output
output
output1
IE5 Part Request
Review Customs Documents
input
output
Provide Customs Documents
output
Return Merchandise Authorization
Passed Compliance Check?
Accept Merchandise Return
[Yes]
[No]
Customs Issue
Customs Issue
Log/Handle Customs Issue
Order Confirmation
Log Order Confirmation
Return Merchandise Authorization
Log and Process Return Merchandise Authorization

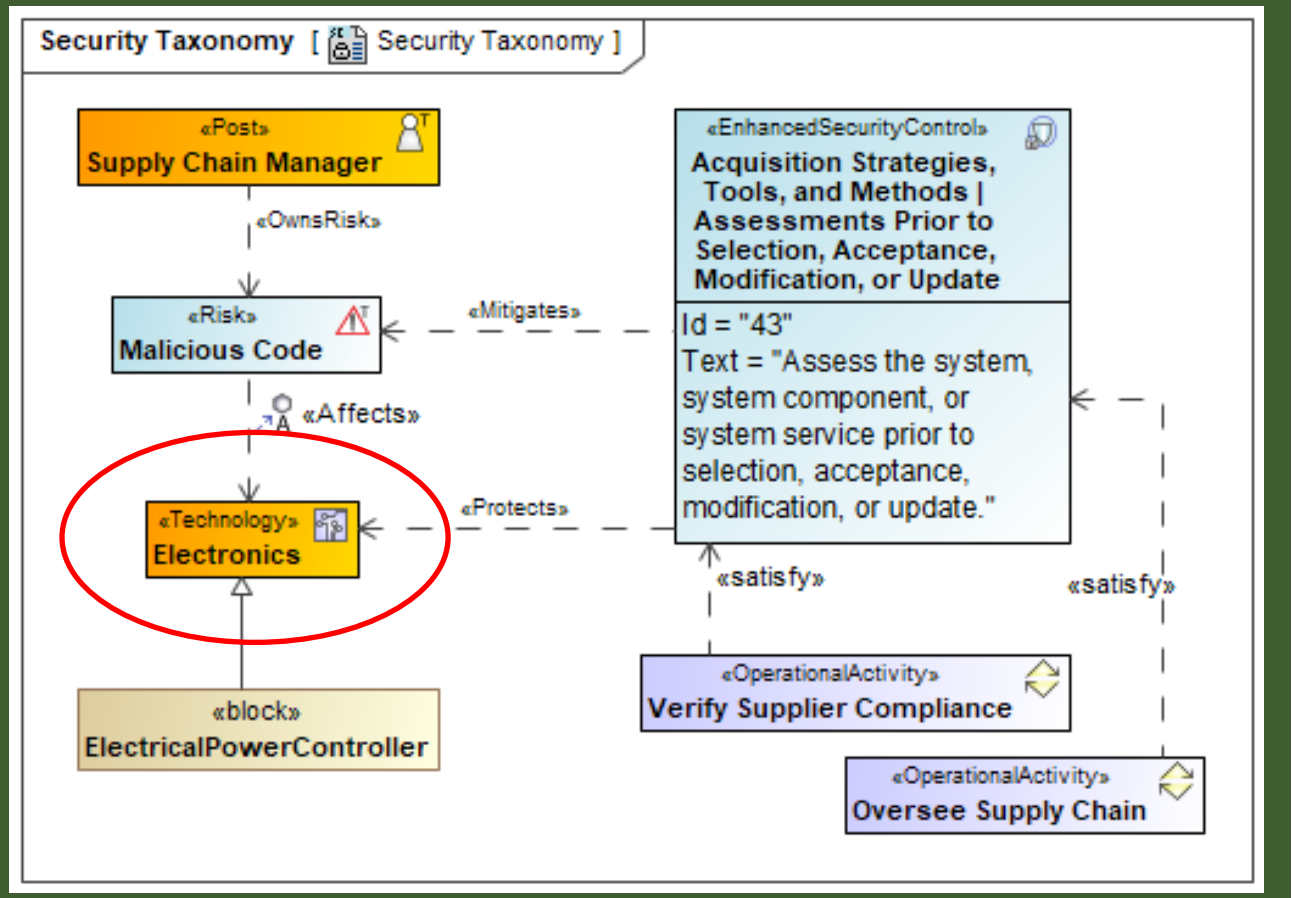
UAF Security Libraries

UAF Security Views Conceptual Meta-Model



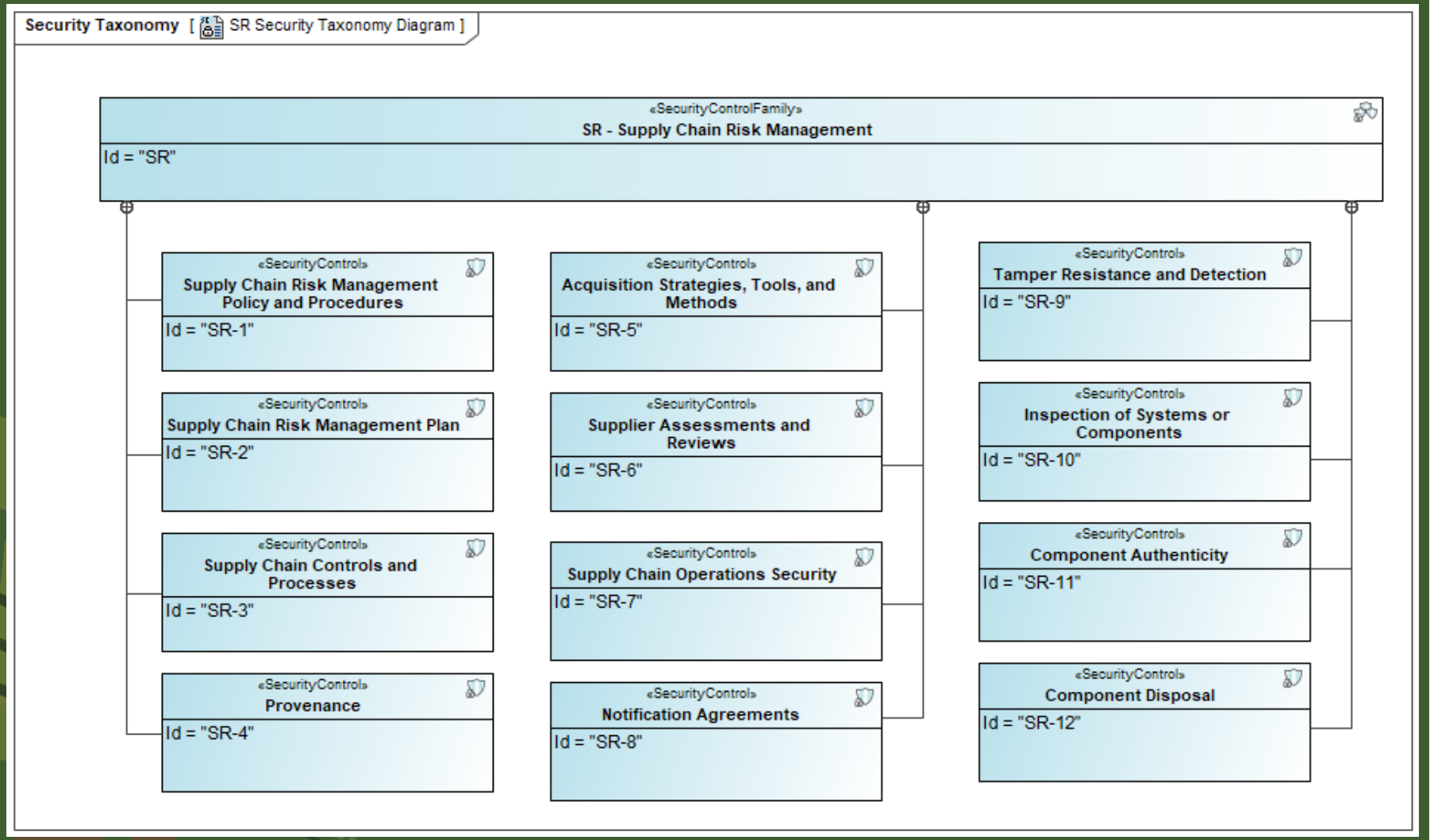
Sc-Tx Security Taxonomy

- This figure shows the taxonomy for some of the security elements
- Risks are the possibility of an adverse effect and its likelihood of occurrence
  - Risks affect resource artifacts, capability configurations, etc.
- Security Controls are a management, operational, or technical control (e.g., safeguard or countermeasure) which Protects an asset.
  - They mitigate risks and protect assets
- Resource Mitigations are a set of performers established to manage operational or resource Risks.
  - They are represented as an overall strategy or through techniques (mitigation configurations) and procedures (Security Processes)and other assets to satisfy security controls



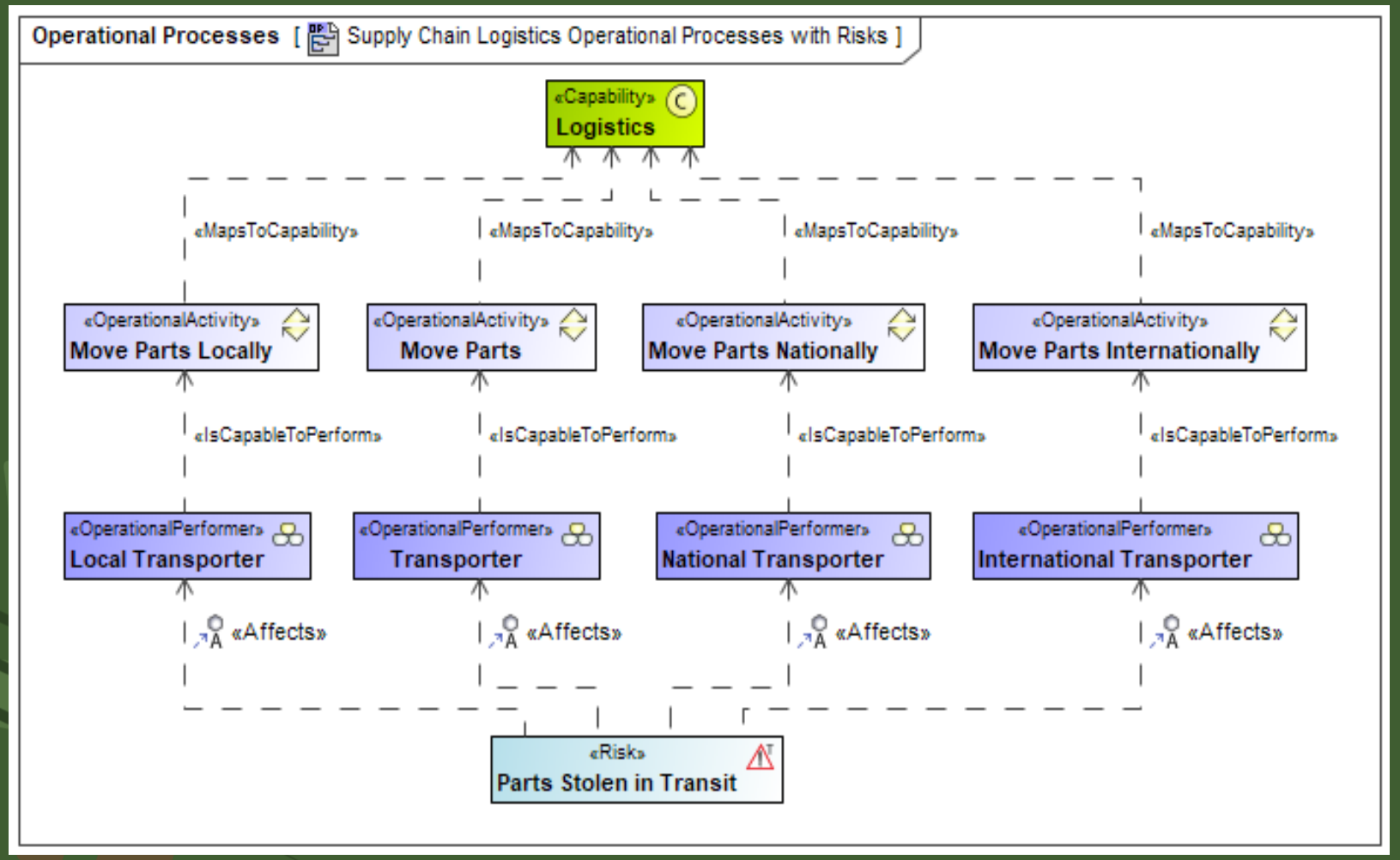
NIST SP 800-53 Security Controls Library

- UAF Reference Library
- Captures Security Controls, Families, Enhanced, Etc.
- Can combine with risks, mitigations, to find solutions

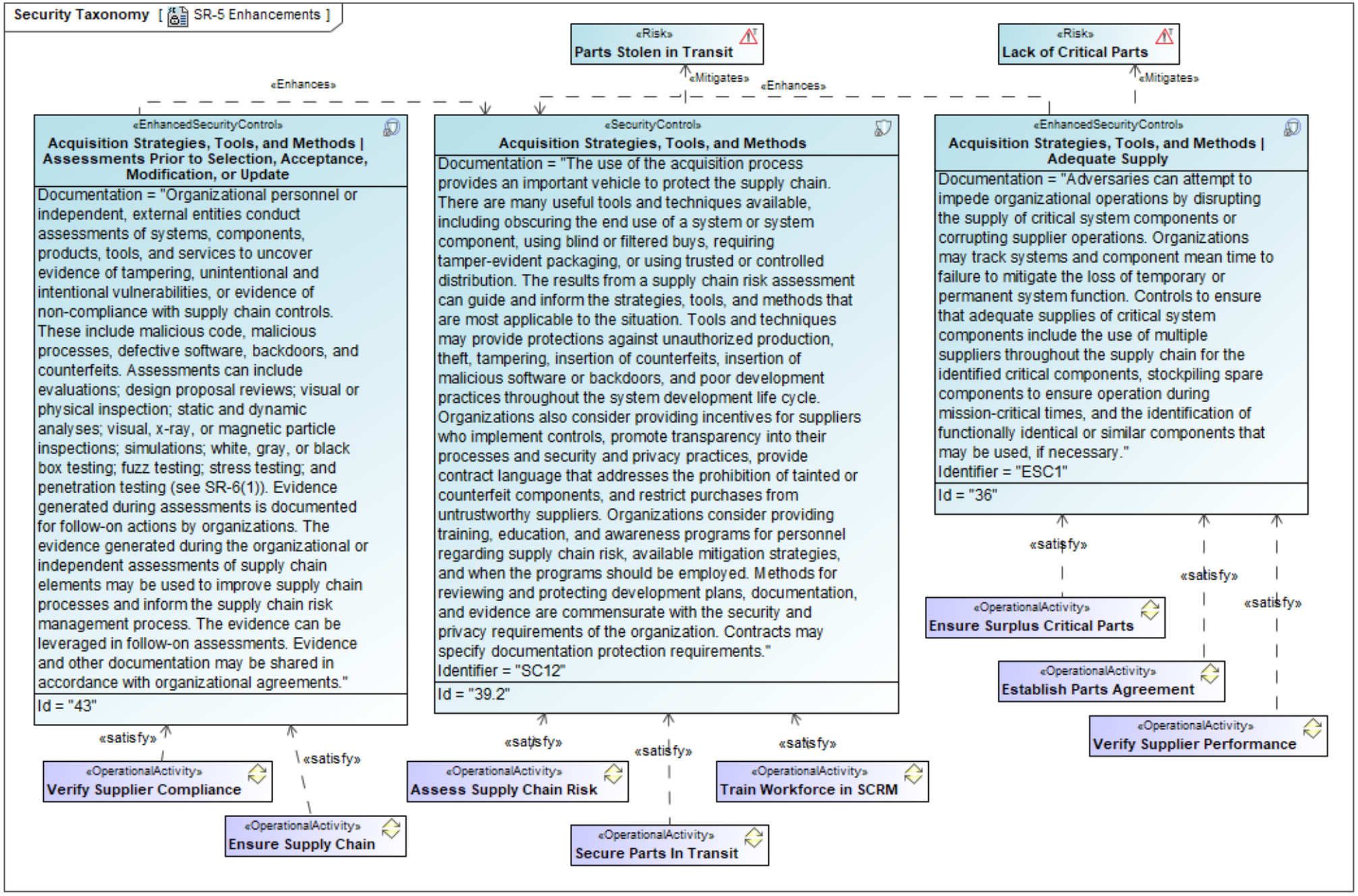


Example Risk and Affected Element

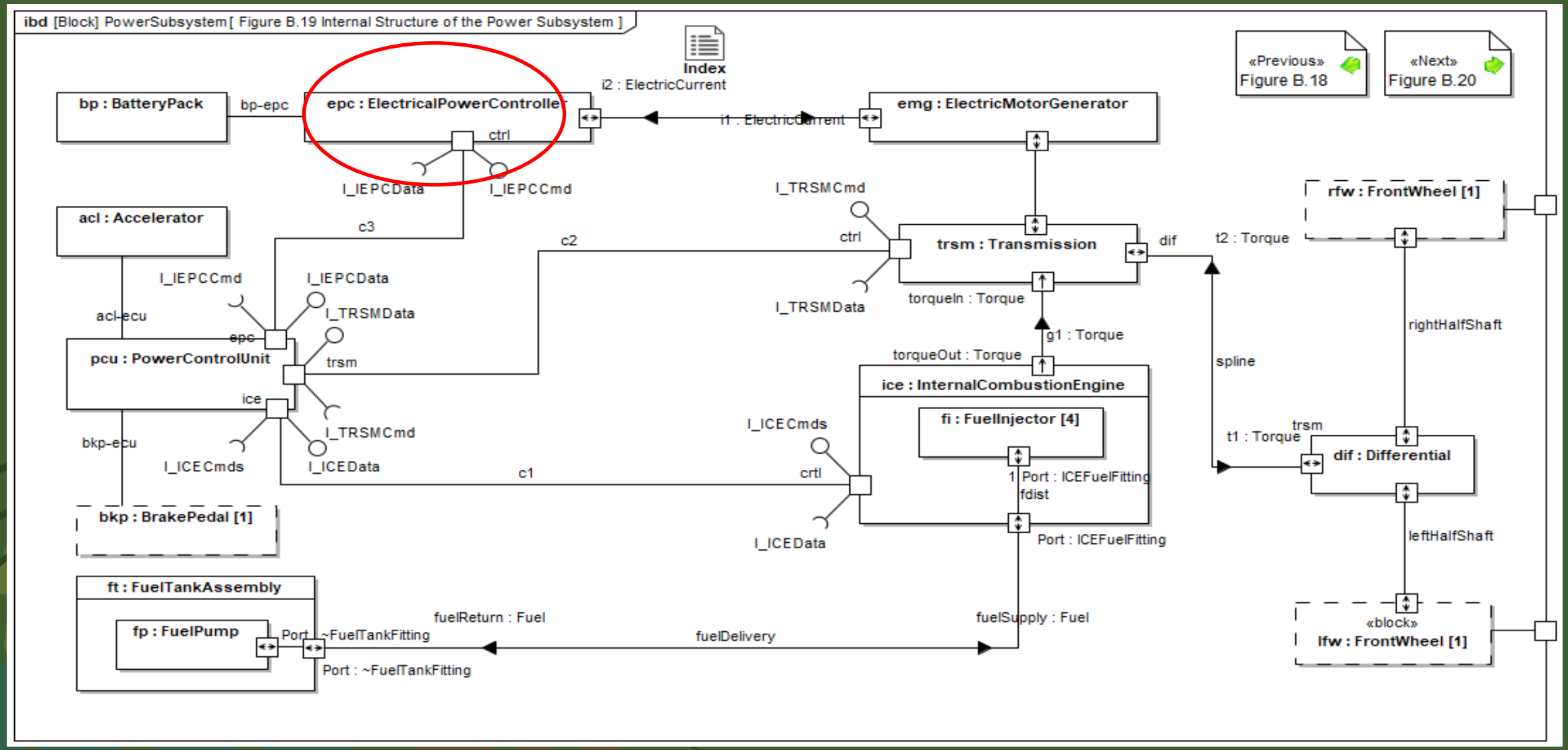
- The risk of Parts Stolen in Transit affects the Transporters
- These eventually map to the Logistics capability



Security Controls and mitigating elements

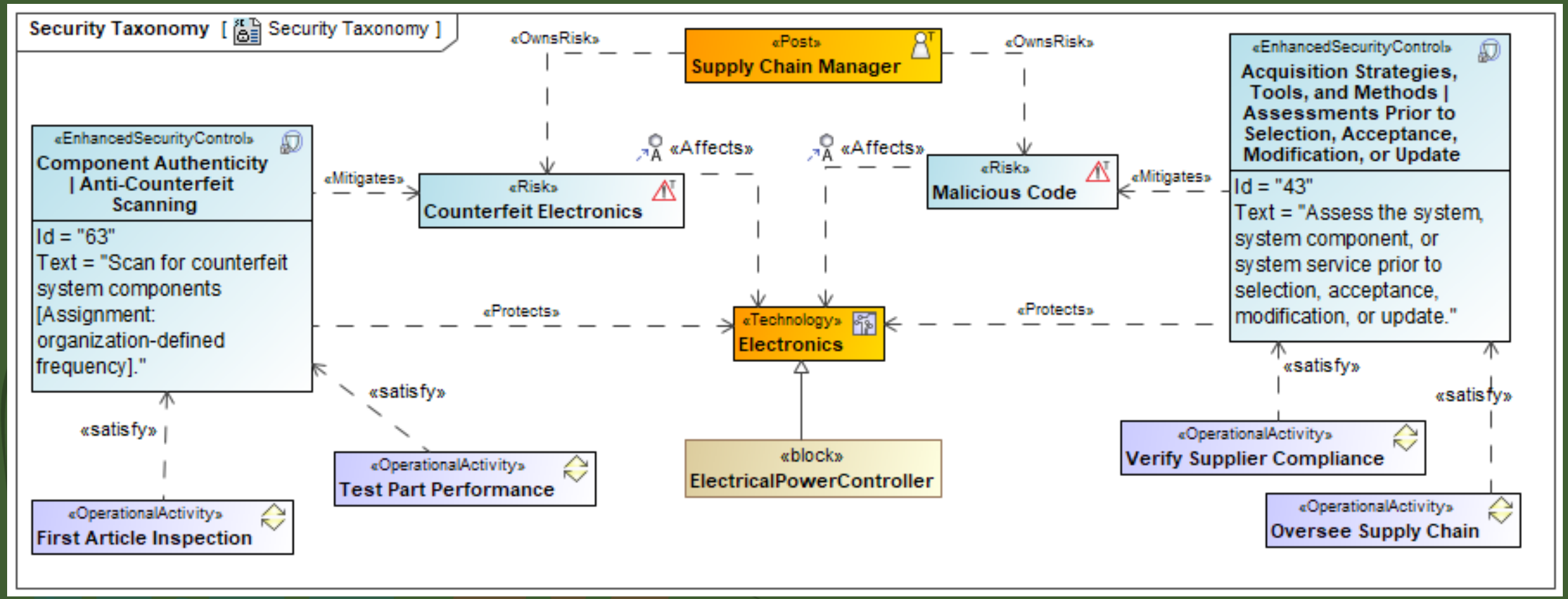


Traceability from the System Design



Links From SysML Elements to Supply Chain

- The Electrical Power Controller is a type of Electronics.
- The Risk, Security Control, Mitigating Elements and Satisfying Processes define the necessary Supply Chain processes.



Why is This Useful?

- Although supply chain simulation software exists, a SoS POV is still useful
- Looking outside the existing context is always helpful
- Provides SCRM earlier in the cycle

MH&L Material Handling & Logistics

GLOBAL SUPPLY CHAIN

80% of Supply Chain Not Accounted for in Current Digital Decision Models

Digital models are missing the vast majority of the supply chain environment.

MH&L Staff

Digital models are missing the vast majority of the supply chain environment, according to analyst firm Gartner.

This incomplete view of the supply chain results in digital trade-off analysis failing to improve decision makers' outcomes, despite the potentially transformative capabilities of these new tools. Digital trade-off analysis includes things such as what-if analysis, scenario modeling, or simulations. Digital trade-off analysis offers improvements in analytical power and clarity when processes are adhered to and enabled with high-quality data.

"The 'digital-to-reality gap' will continue to hamper supply chain performance

Future Work

- Create additional risks and mitigations
- Add RAAML relationships to verify assurance case
- Generate traceability tables for SysML parts list
- Further investigation of Supply Chain Tools for gap analysis
- Decompose existing controls into atomic controls or requirements
- Add links to standards and guidance

Questions?