Sandia National Laboratories

Exceptional service in the national interest

LESSONS LEARNED FROM DEFINING AN APPLIED SYSTEMS ENGINEERING ONTOLOGY AT SANDIA NATIONAL LABORATORIES

Jaimie Murdock and Ed Carroll
jmmurdo@sandia.gov

INCOSE 2023 International Symposium

July 17, 2023

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

U.S. DEPARTMENT OF ENERGY

NNSA

WHAT IS AN ONTOLOGY?

WHAT IS AN ONTOLOGY?

An ontology is a formal definition of the types and relationships in a domain.

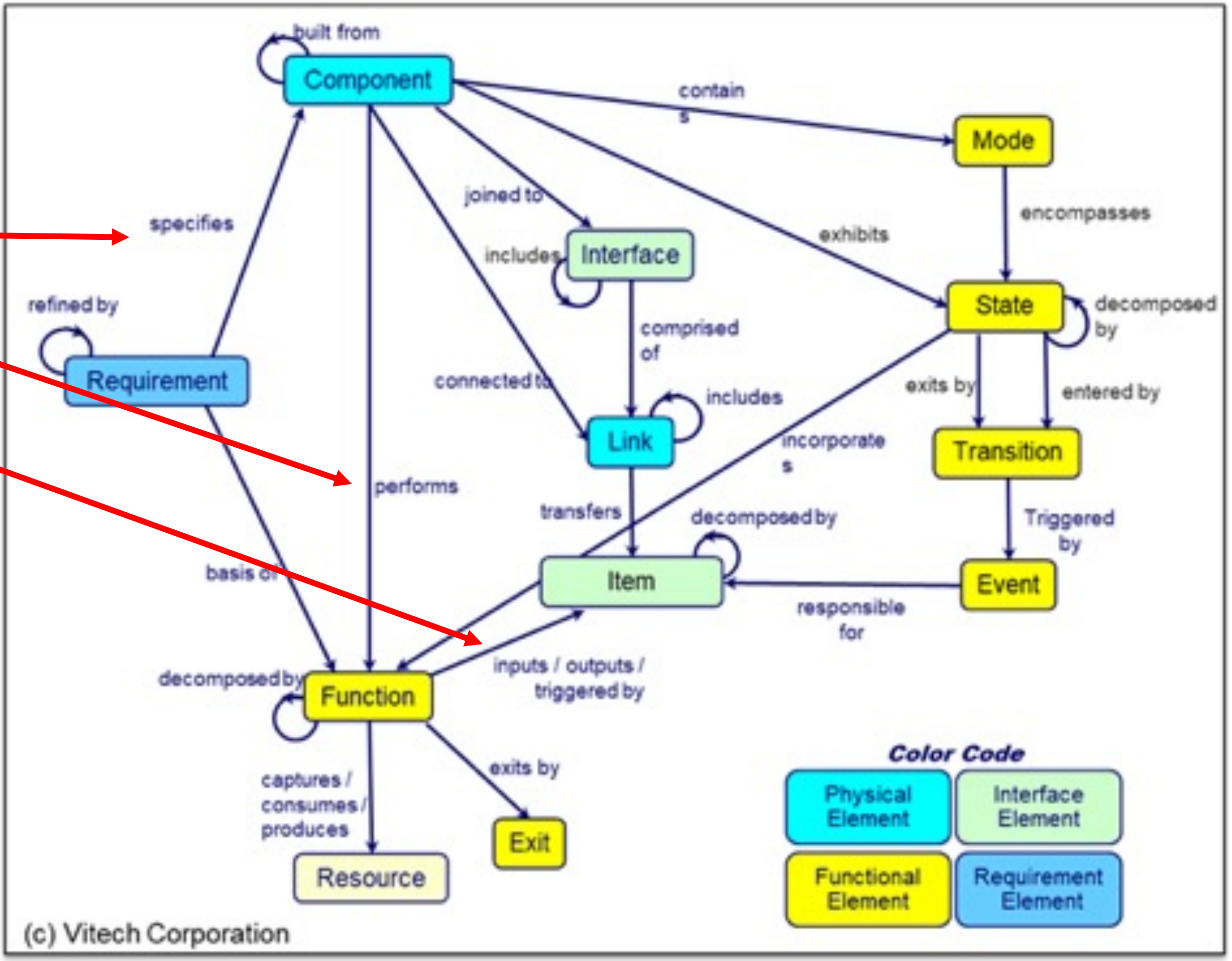
They are defined using "**triples**" based on subject, predicate, object structures.

Requirement – specifies – Component
Component – performs – Function
Function – outputs – Item

Ontologies are a type of knowledge graph, amenable to GOFAI/symbolic analysis.

Ontologies specify a *lexicon* of the types of things in a system and the ways they are related to each other.

A Systems Model is based on an Ontology



(c) Vitech Corporation

ONTOLOGIES MEDIATE MEANING

Make sure we use a Safety Harness to transport the rocket, and transport it on Low-Traffic Roads.

Low-Traffic Roads and a Safety Harness Got it!

Semantic Dissonance

Same words; same data types.
Meaning different things.

An Ontology makes this semantic disconnect explicit.
An Ontology encodes that these two separate meanings are not equivalent.

What he meant!

Low-Traffic Road: Any road with < 5,000 cars a day
Safety Harness: Any suspension system with belts having 5-points or more

What he Understood!

Low-Traffic Road: Any road that is not a highway
Safety Harness: Any harness with 3-points or more

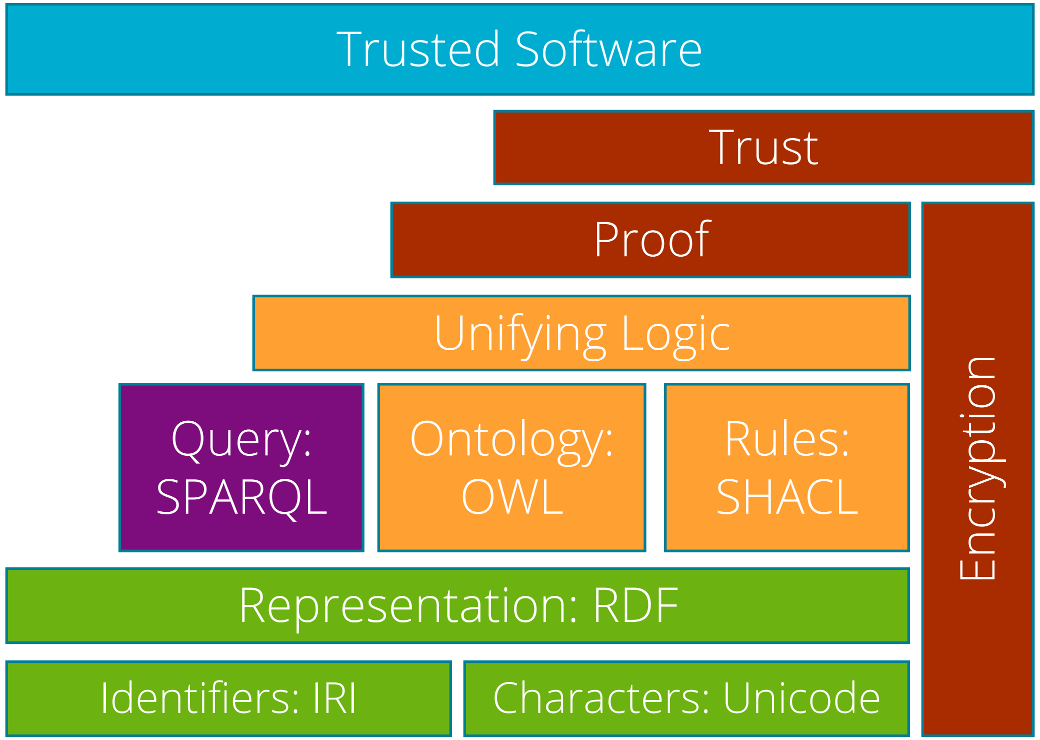
ONTOLOGY IMPLEMENTATIONS

The Semantic Web is the most robust set of technologies implementing an ontology.

The Resource Description Framework (RDF) is a syntax for defining triples. RDF was adopted as an open standard by the W3C in 1999.

Need-to-know concerns are addressed through a federated architecture relying on the use of URIs to identify objects.

Data can be included or excluded easily – triples are atomic.

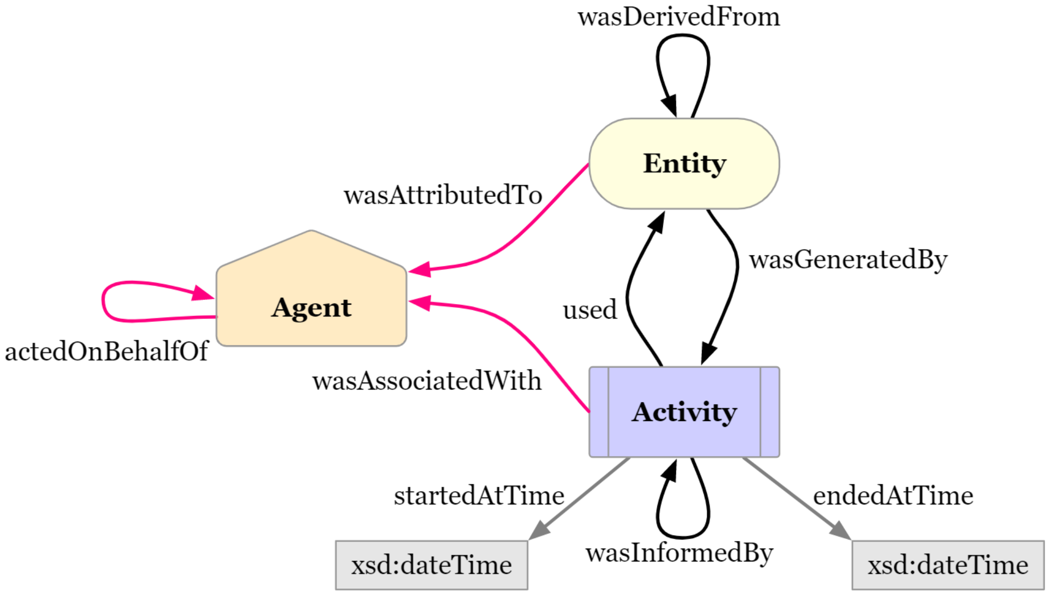


VOCABULARIES NEGOTIATE MEANING

Many standard vocabularies exist and have been open-sourced, addressing many of our needs.

Adopting standards means shared meaning across orgs and disciplines.

A key example is the PROV ontology, which handles information provenance.



Many vocabularies:

- PROV (provenance)
- SKOS (glossaries and lexicons)
- Dublin Core (metadata)
- FOAF (relationships)
- FaBiO (bibliographies)
- Ontology of Chemical Elements
- Basic Formal Ontology (BFO)
- DoD Architecture Framework (DoDAF)

DEFINING AN APPLIED SE ONTOLOGY

APPROACHES TO ONTOLOGY DESIGN

Ontology design driven by two concerns.

Top-down: Model Credibility

The top-down approach is prescriptivist: “this is how SE is done at our organization”

Data from (opinionated) tools are then transformed to match the organization.

This approach makes it easier to evaluate models against business logic, flexible with respect to new tooling.

Bottom-up: Model Interoperability

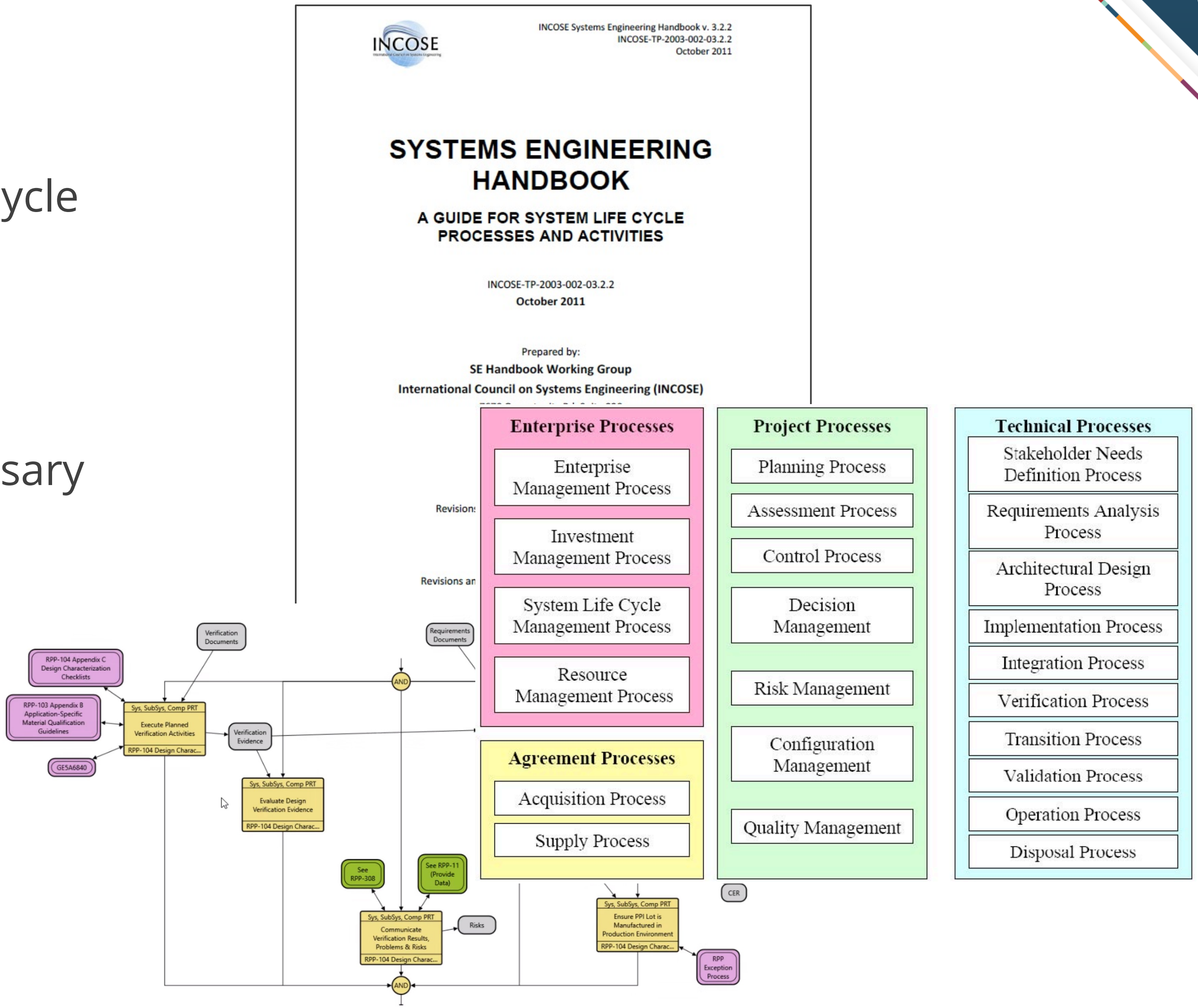
The bottom-up approach is desciptivist: “this is how our SE data is stored”.

Organizational ontology includes tool-specific information (ex: GenesysRequirement, CreoRequirement)

This approach is quicker, but less flexible. Mappings are integrated with central representation.

SOURCE MATERIAL

- ISO 15288:2015 (System Life Cycle Processes)
- INCOSE Handbook
- GENESYS Architecture
- Internal business process glossary
- Work-in-progress SE models



INCOSE

INCOSE Systems Engineering Handbook v. 3.2.2
INCOSE-TP-2003-002-03.2.2
October 2011

SYSTEMS ENGINEERING HANDBOOK

A GUIDE FOR SYSTEM LIFE CYCLE PROCESSES AND ACTIVITIES

INCOSE-TP-2003-002-03.2.2
October 2011

Prepared by:
SE Handbook Working Group
International Council on Systems Engineering (INCOSE)

Revision:

Revisions ar

Enterprise Processes
- Enterprise Management Process
- Investment Management Process
- System Life Cycle Management Process
- Resource Management Process

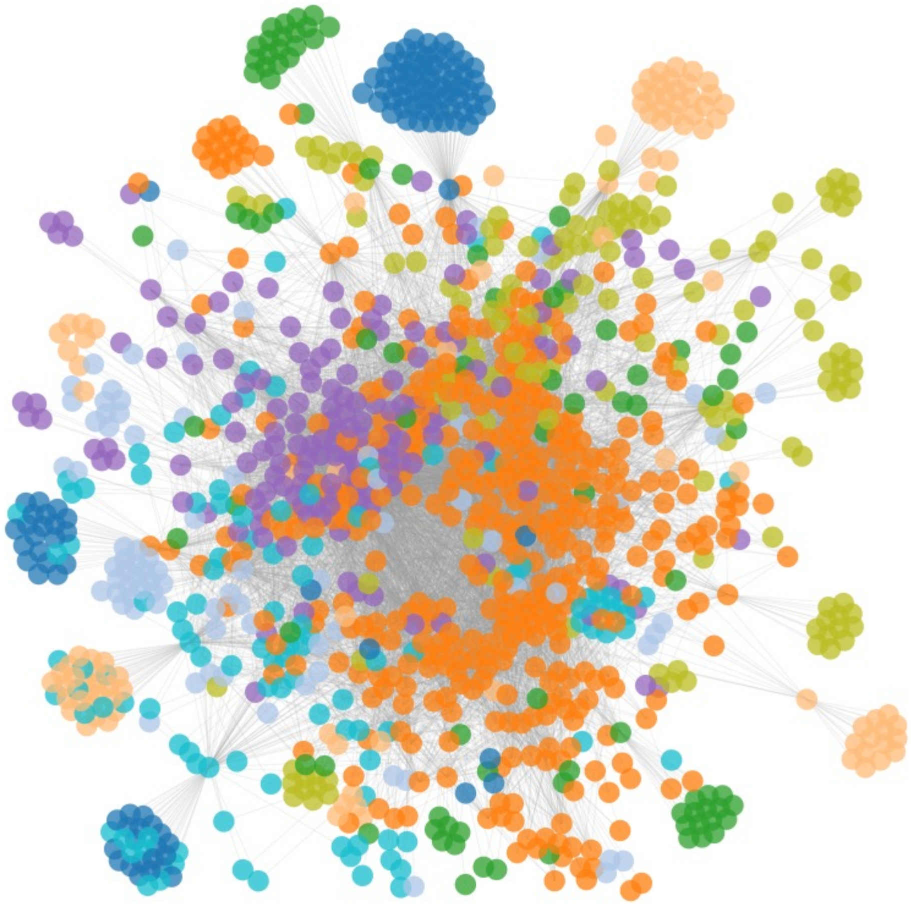
Agreement Processes
- Acquisition Process
- Supply Process

Project Processes
- Planning Process
- Assessment Process
- Control Process
- Decision Management
- Risk Management
- Configuration Management
- Quality Management

Technical Processes
- Stakeholder Needs Definition Process
- Requirements Analysis Process
- Architectural Design Process
- Implementation Process
- Integration Process
- Verification Process
- Transition Process
- Validation Process
- Operation Process
- Disposal Process

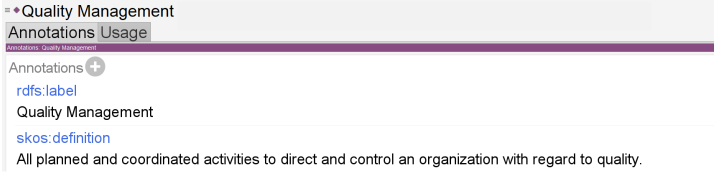
Verification Documents
Requirements Documents
RPP-104 Appendix C Design Characterization Checklists
RPP-103 Appendix B Application-Specific Material Qualification Guidelines
GE5A6840
Sys, SubSys, Comp PRT
Execute Planned Verification Activities
RPP-104 Design Charac...
Verification Evidence
AND
Sys, SubSys, Comp PRT
Evaluate Design Verification Evidence
RPP-104 Design Charac...
See RPP-308
See RPP-11 (Provide Data)
Sys, SubSys, Comp PRT
Communicate Verification Results, Problems & Risks
RPP-104 Design Charac...
Risks
CER
Sys, SubSys, Comp PRT
Ensure PPI Lot is Manufactured in Production Environment
RPP-104 Design Charac...
RPP Exception Process
AND

SANDIA REFERENCE ONTOLOGY (SRO)



- 241 classes
- 414 total relationship types
- 1,104 declared objects
- 26,543 declared relationships

◆Quality Management
◆Quality Management System
◆Quantitative Analysis
◆Quantitative Data
◆R001
◆R001 - 4.1 Recurring Product Realization Requirements - FR15042
◆R001 - 4.1 Recurring Product Realization Requirements - FR29561
◆R001 - 4.1 Recurring Product Realization Requirements - FR34890
◆R001 - 4.1 Recurring Product Realization Requirements - FR52199
◆R001 - 4.1 Recurring Product Realization Requirements - FR60460
◆R001 - 4.1 Recurring Product Realization Requirements - FR64761
◆R001 - 4.1 Recurring Product Realization Requirements - FR98381



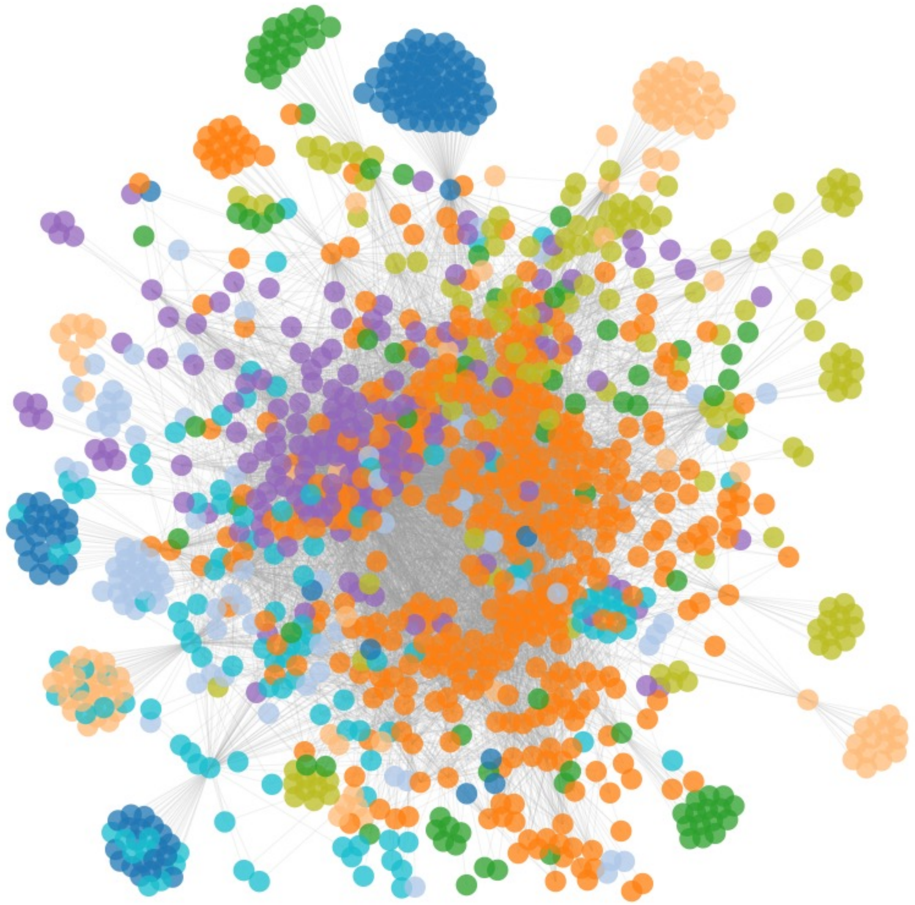
rdfs:label
Quality Management

skos:definition
All planned and coordinated activities to direct and control an organization with regard to quality.

LESSONS LEARNED

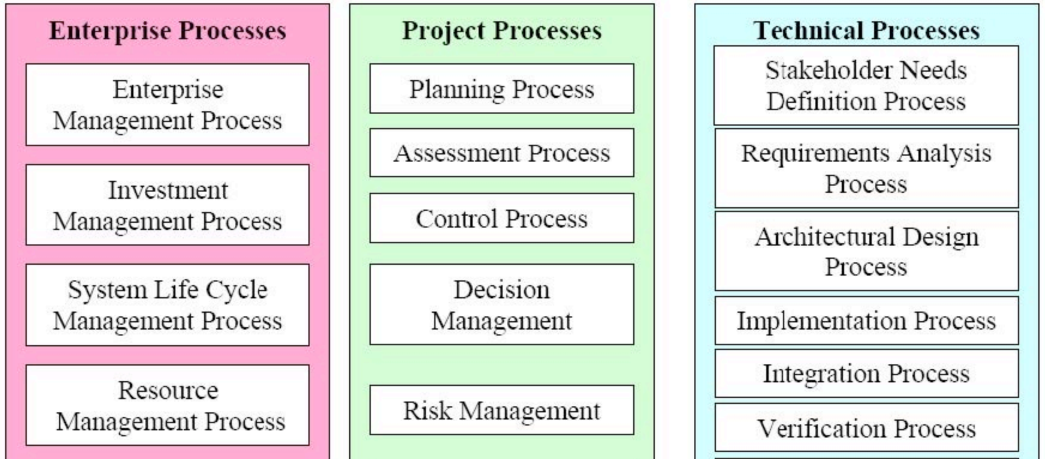
ONTOLOGY DESIGN PROCESS

1. Top-down approach
   - Examined source materials
     - Genesys Architecture
     - ISO 15288
     - INCOSE Handbook
   - Generated high-level structure of SE
   - **Lesson:** Idealized environment did not match development/production data.
2. Bottom-up approach
   - Examined business process definitions and work-in-progress SE models
   - **Lesson:** Tool-based classes may not match ontology-based classes
3. Unification
   - Mapped ontology to SBE Vision Model-Based Engineering (MBE) Ontology
   - **Lesson:** Upper-level ontologies can provide backbone, need to know what is being attached

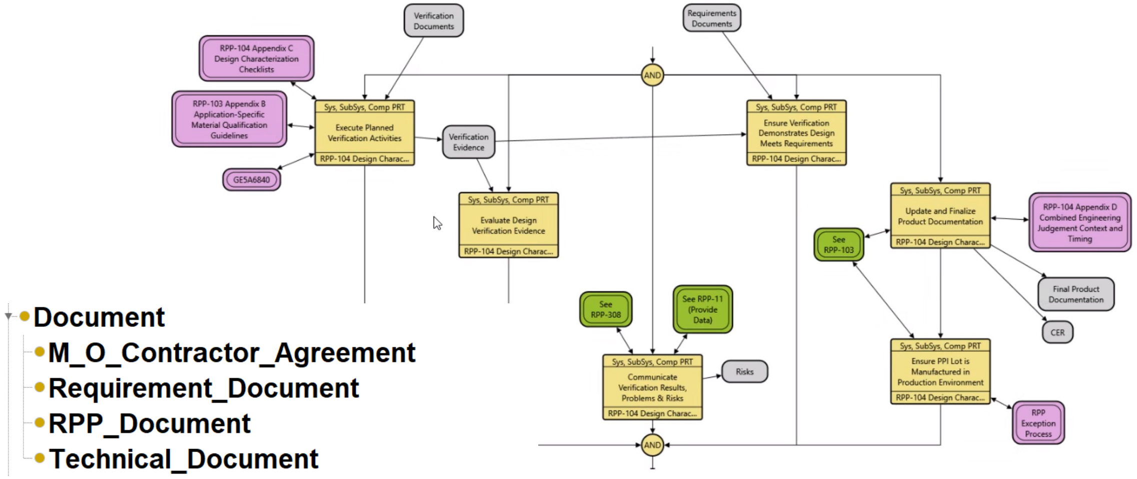


LESSON: IDEALIZED ENVIRONMENT DID NOT MATCH DEVELOPMENT/PRODUCTION DATA.

- By starting with the ISO 15288 and INCOSE Handbook, we quickly learned our internal processes were not organized in the same umbrellas.
  - Alignment of business processes into an idealized ontology was a manual process.
- Also, in-progress models followed schema of tool-based ontologies.
  - Example: Phase, in an idealized sense, refers to the strictly defined lifecycle management phases. In technical models, may refer to phases of a launch, with different operating environments.
- Separation of concerns between business/technical lifecycles.



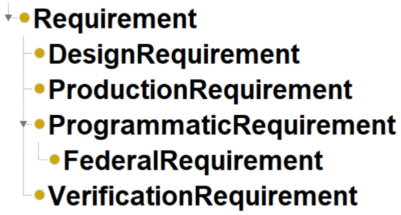
Enterprise Processes	Project Processes	Technical Processes
Enterprise Management Process	Planning Process	Stakeholder Needs Definition Process
Investment Management Process	Assessment Process	Requirements Analysis Process
System Life Cycle Management Process	Control Process	Architectural Design Process
Resource Management Process	Decision Management	Implementation Process
	Risk Management	Integration Process
		Verification Process


Verification Documents
Requirements Documents
RPP-104 Appendix C Design Characterization Checklists
RPP-103 Appendix B Application-Specific Material Qualification Guidelines
GE5A6840
AND
Sys, SubSys, Comp PRT
Execute Planned Verification Activities
RPP-104 Design Charac...
Verification Evidence
Sys, SubSys, Comp PRT
Evaluate Design Verification Evidence
RPP-104 Design Charac...
Sys, SubSys, Comp PRT
Ensure Verification Demonstrates Design Meets Requirements
RPP-104 Design Charac...
Sys, SubSys, Comp PRT
Update and Finalize Product Documentation
RPP-104 Design Charac...
RPP-104 Appendix D Combined Engineering Judgement Context and Timing
See RPP-103
Final Product Documentation
CER
See RPP-308
See RPP-11 (Provide Data)
Sys, SubSys, Comp PRT
Communicate Verification Results, Problems & Risks
RPP-104 Design Charac...
Risks
Sys, SubSys, Comp PRT
Ensure PPI Lot is Manufactured in Production Environment
RPP-104 Design Charac...
RPP Exception Process
AND

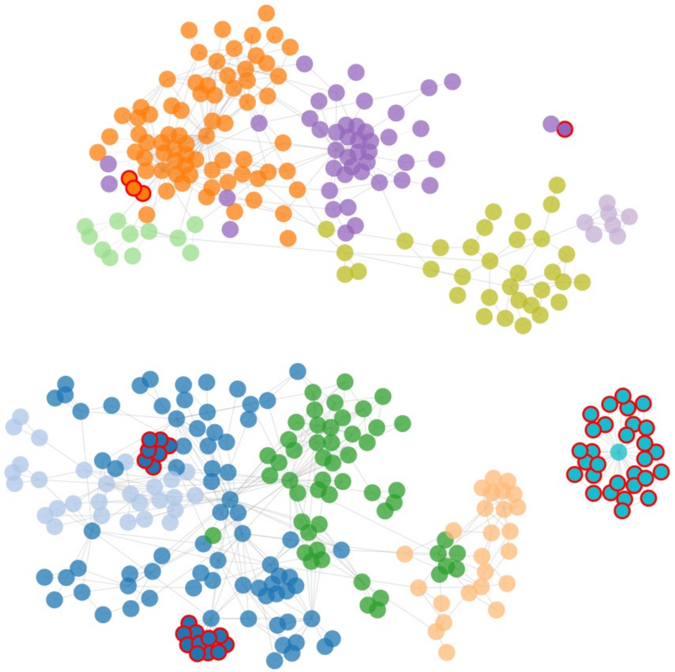
- **Document**
  - **M_O_Contractor_Agreement**
  - **Requirement_Document**
  - **RPP_Document**
  - **Technical_Document**

LESSON: TOOL-BASED CLASSES MAY NOT MATCH ONTOLOGY-BASED CLASSES

- Data coming from different sources may have different associated properties and relationships defined.
- Mappings must be specified between tool and ontology, possibly lossy.
- Do we mix mappings with idealized ontology?
  - GenesysRequirement, CreoRequirement, DNGRequirement, …
  - Each of which may be a ProgrammaticRequirement, VerificationRequirement, …
  - Subtypes un-specified by tools!
- Decision not to mix tool-based classes with idealized classes in SRO.
- Also, models mix and match business and technical lifecycle management by necessity!

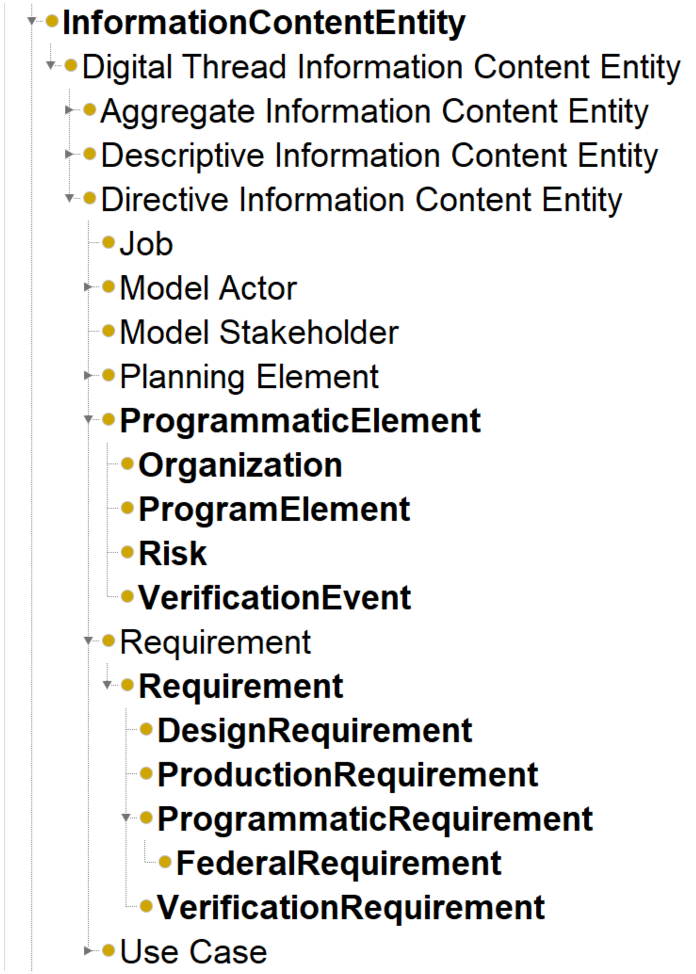


- Requirement
  - DesignRequirement
  - ProductionRequirement
  - ProgrammaticRequirement
    - FederalRequirement
  - VerificationRequirement



LESSON: UPPER-LEVEL ONTOLOGIES CAN PROVIDE BACKBONE, NEED TO KNOW WHAT IS BEING ATTACHED.

- We decided to outsource mapping to the SBE Vision Digital Thread product, leaving the idealized SRO to focus on credibility tasks, separating interoperability concerns.
- Enabled us to keep goal of lossless data transformations between tools.
- Required mapping of SRO to MBE ontology
- Without prior work defining ontological core, would have been lost in abstraction



- **InformationContentEntity**
  - Digital Thread Information Content Entity
    - Aggregate Information Content Entity
    - Descriptive Information Content Entity
    - Directive Information Content Entity
      - Job
      - Model Actor
      - Model Stakeholder
      - Planning Element
      - **ProgrammaticElement**
        - **Organization**
        - **ProgramElement**
        - **Risk**
        - **VerificationEvent**
      - Requirement
        - **Requirement**
          - **DesignRequirement**
          - **ProductionRequirement**
          - **ProgrammaticRequirement**
            - **FederalRequirement**
          - **VerificationRequirement**
      - Use Case

APPLICATIONS

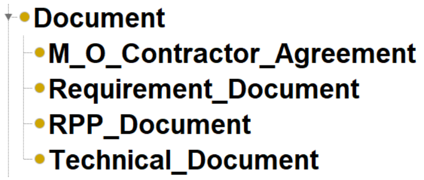
WHY KEEP A SANDIA REFERENCE ONTOLOGY?

After adopting Digital Thread, interoperability – the primary mission concern – has been solved.

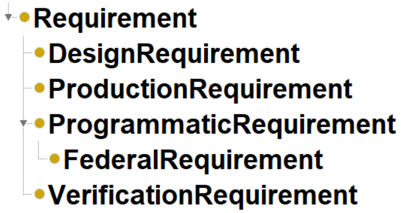
However, SRO provides additional value for assessing credibility. Contains authoritative source for programmatic requirements.

Can use this to ensure compliance with federal requirements.

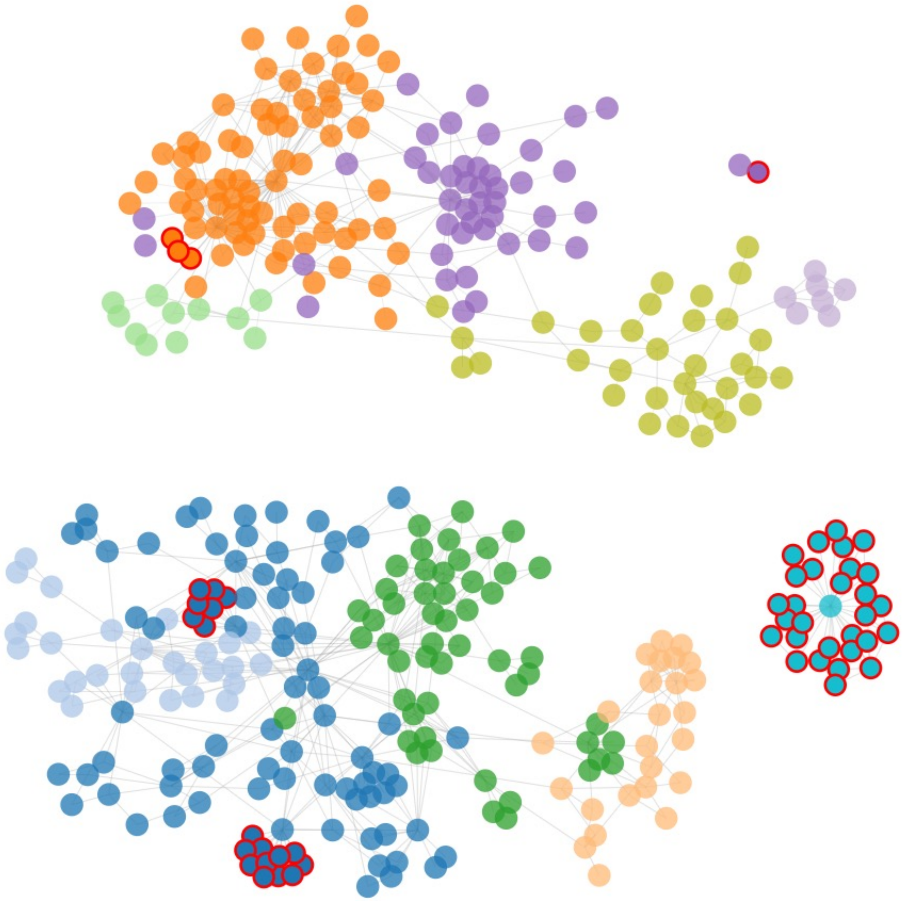
Also enables data science applications like matching requirements across models.



- Document
  - M_O_Contractor_Agreement
  - Requirement_Document
  - RPP_Document
  - Technical_Document



- Requirement
  - DesignRequirement
  - ProductionRequirement
  - ProgrammaticRequirement
    - FederalRequirement
  - VerificationRequirement



USE CASE: REQUIREMENTS MANAGEMENT + DATA MINING

More than just linking sources, this enables **insight**. Ontology increases discoverability.

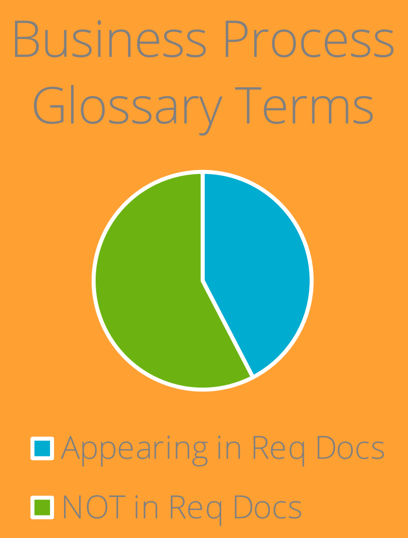
Workflow-based approach means new data sources from particular programs can quickly be added.

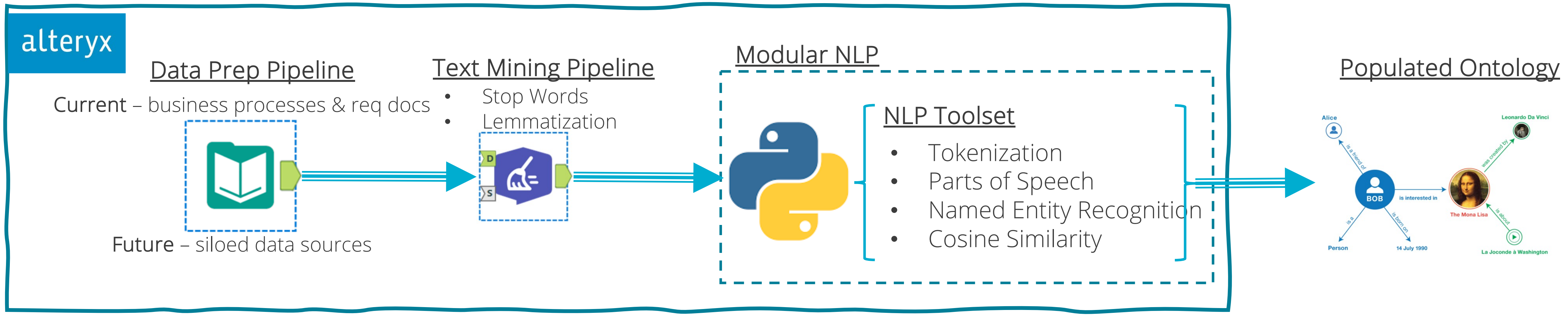
Doesn't require manual review or negotiation of definitions, allows automated evaluation of documents. Can say "Document X is useful to you at 85% based on the following terms…"

Example: 57.6% of terms in the process glossary *do not* appear in a requirements document.

Business process glossary is derived from federal requirements! Are we missing ***requirements*** during design process?

Answer: division of labor among labs, don't have 100% coverage, but now know what to specify.





USE CASE: MODEL CREDIBILITY

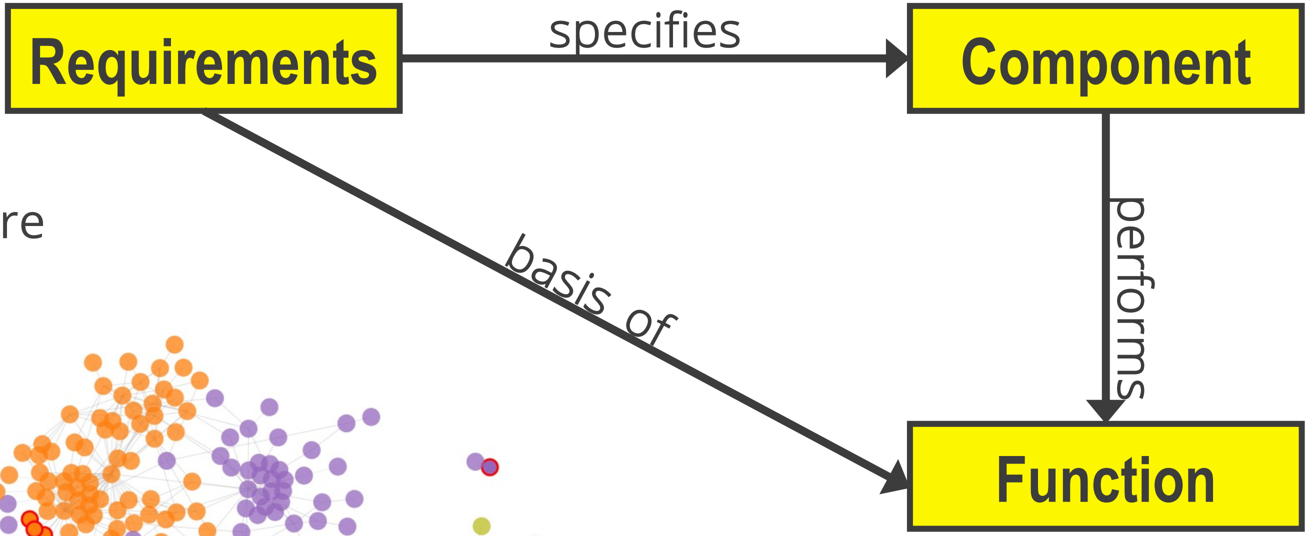
Messy data.

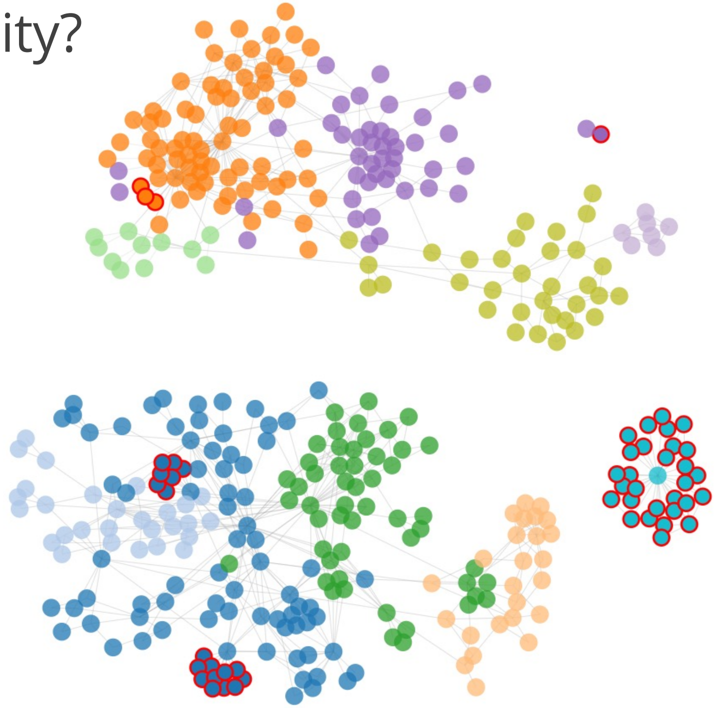
Who has authoritative source?

- Simple example: regulatory definitions are stored in the business process glossary.

What do we do to establish credibility?

- Constraints programming
- Automation increases reliability
- Enables experimentation!

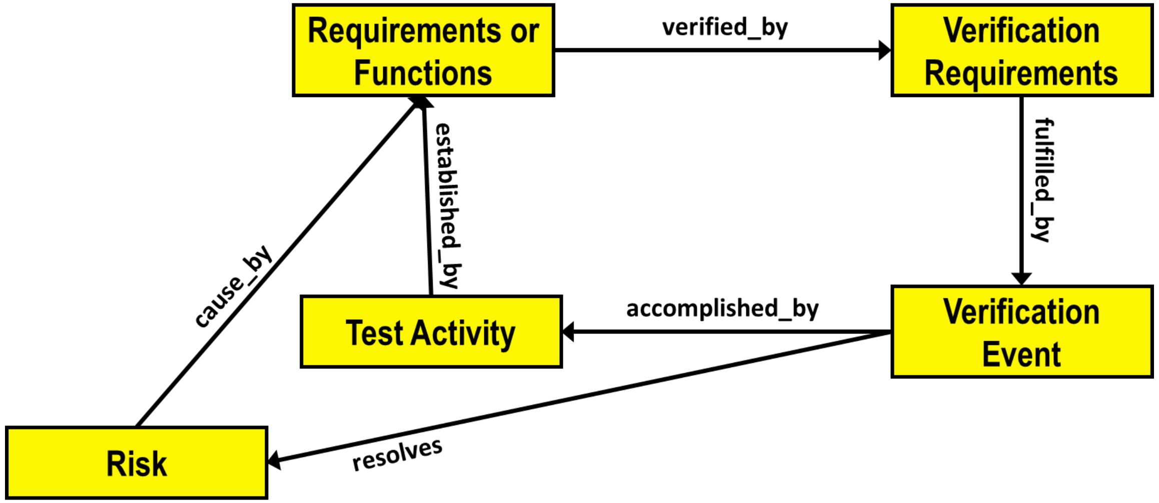




USE CASE: MODEL CREDIBILITY – FUTURE WORK

Reasoning systems can automatically propose fixes.

- Like Intellisense for programming or spell correct. “This Requirement does not specify a Component. Select an existing component or create a new one.”



Defeasible reasoning systems can propose experiments.

- Can use graph theory to highlight central nodes and propose “defeasible” changes that would disrupt system stability.
- “If the tolerance for pressure is reduced by 2 bars, these 20 assumptions will need to be tested.”

Defeasible reasoning is used in medical ontologies to reduce to minimal symptoms set. Searching on partial symptoms may yield a stronger result set.

- Think about early COVID recommendations. Gradually reduced to persistent fever and dry cough to reduce conflation with allergies & cold/flu.
- Root cause analysis: “Increasing the size of the controller impacts the following 53 objects, which need to be adjusted to accommodate the size change.”

THANK YOU!

SUMMARY

1. Top-down approach
   - Easier to evaluate models against business logic, flexible with respect to new tooling, longer time to production.
   - **Lesson:** Idealized environment did not match development/production data.
2. Bottom-up approach
   - Quicker, but less flexible. Mappings are integrated with central representation.
   - **Lesson:** Tool-based classes may not match ontology-based classes
3. Unification
   - Separation of concerns between interoperability and credibility.
   - **Lesson:** Upper-level ontologies can provide backbone, need to know what is being attached