Boosting D3FEND: Ontological Analysis and Recommendations

Ítalo Oliveira[1,3], Gal Engelberg[2], Pedro Paulo F. Barcelos[1], Tiago Prince Sales[3], Mattia Fumagalli[1], Riccardo Baratella[1], Dan Klein[2], and Giancarlo Guizzardi[3,4]

[1]Free University of Bozen-Bolzano, Bolzano, Italy

[2]Accenture Israel Cyber R&D Lab, Tel Aviv, Israel

[3]University of Twente, Enschede, The Netherlands

[4]Stockholm University, Stockholm, Sweden

My Blog: https://notsoshortnotes.wordpress.com/

Content

It is well-known that ontological foundations support the development of ontologies as information artifacts.

It is well-known that ontological foundations support the development of ontologies as information artifacts.

Still, in academia and the industry, people often develop those ontologies from scratch. 🤦

It is well-known that ontological foundations support the development of ontologies as information artifacts.

Still, in academia and the industry, people often develop those ontologies from scratch. 🤦

- Can an ontology be widely adopted without foundations?

It is well-known that ontological foundations support the development of ontologies as information artifacts.

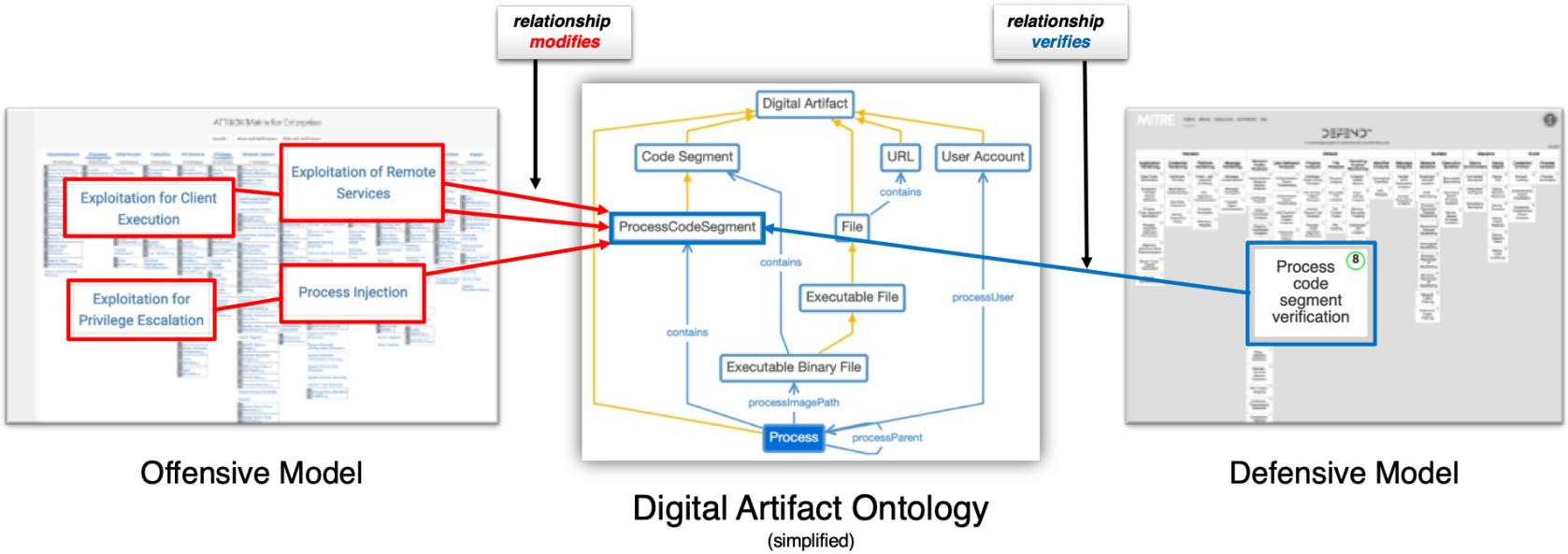
Still, in academia and the industry, people often develop those ontologies from scratch. 🤦

- Can an ontology be widely adopted without foundations?
- Can an ontology even be useful without foundations?

It is well-known that ontological foundations support the development of ontologies as information artifacts.

Still, in academia and the industry, people often develop those ontologies from scratch. 🤦

- Can an ontology be widely adopted without foundations?
- Can an ontology even be useful without foundations?
- But what happens in case of lack of foundations? Is this a problem? 🤔



"D3FEND is (...) a knowledge graph of cybersecurity countermeasure techniques. (...) it is a catalog of defensive cybersecurity techniques and their relationships to offensive/adversary techniques. The primary goal of the initial D3FEND release is to help standardize the vocabulary used to describe defensive cybersecurity technology functionality."
(`https://d3fend.mitre.org/faq/`)

D3FEND is getting more popular in cybersecurity

Swimlane
https://swimlane.com › blog › clou... · Vertaal deze pagina

5 Essential Steps for Stronger Cloud Security

22 aug 2023 — The **MITRE ATT&CK** and **D3FEND** frameworks can be valuable tools for organizations looking to **secure** their **cloud** environments.

Business Wire

RangeForce Adds MITRE D3fend and ATT&CK Frameworks to Cyber Defense Readiness Platform

RangeForce now provides individual learning modules, advanced reporting and live team-based threat exercises that map to MITRE D3FEND and...

10 Nov 2022

Best Windows network hardening advice from MITRE D3FEND

The new **MITRE D3FEND** knowledge graph of cybersecurity countermeasures offers solid **guidance** for **Windows** admins. Follow…

YouTube · IDG TECHtalk · 21 jul 2021

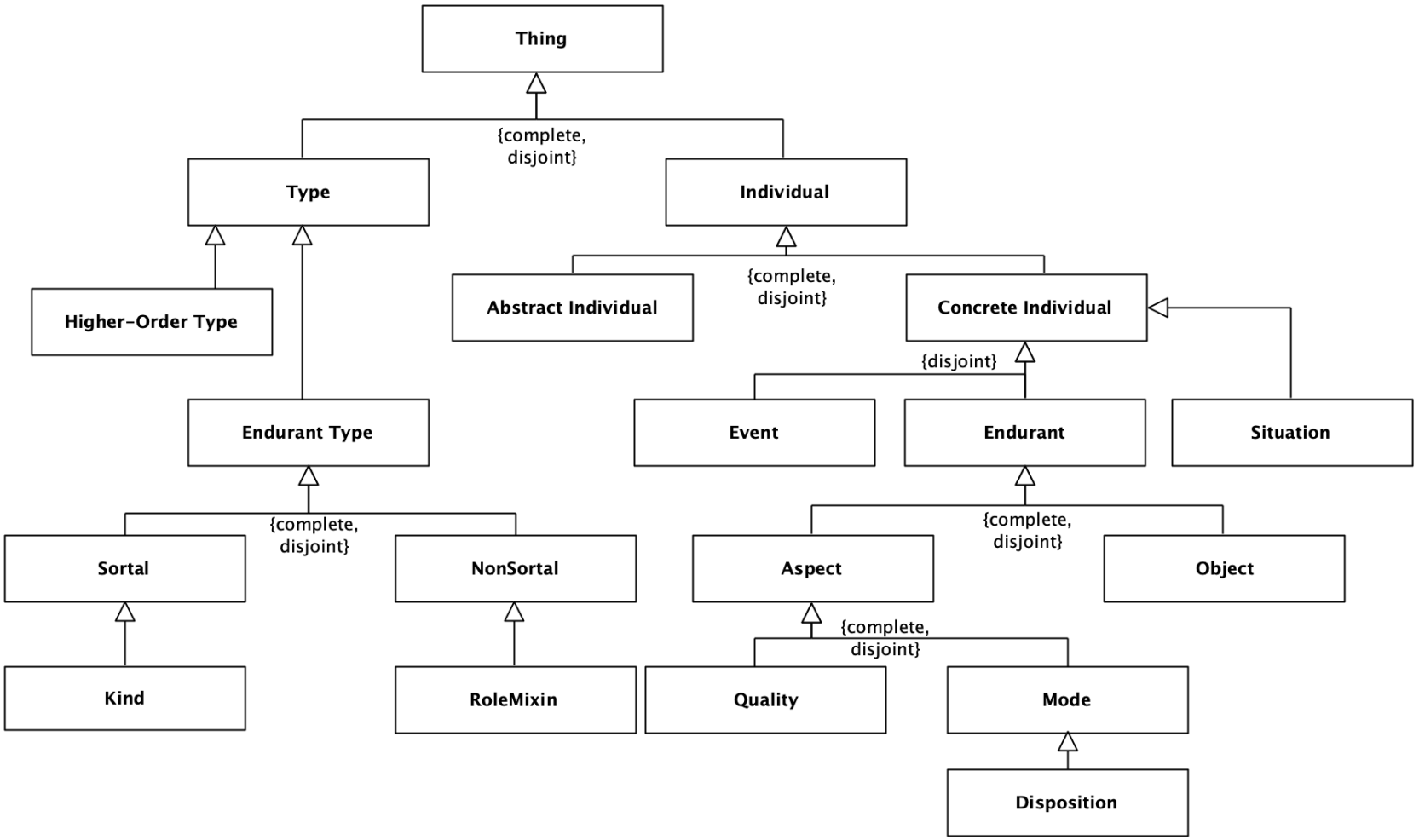
SecurityWeek

Three Ways to Improve Defense Readiness Using MITRE D3FEND

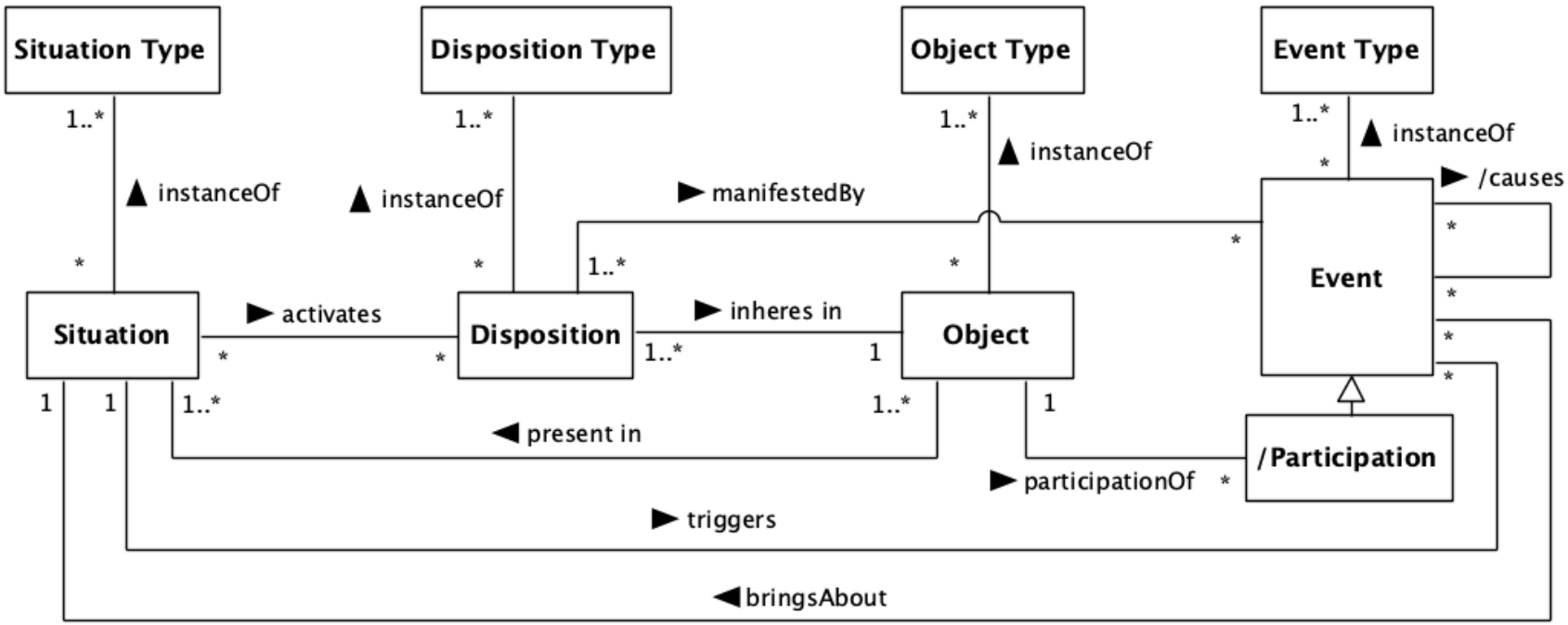
Created and maintained by MITRE, MITRE D3FEND is a framework that provides a library of defensive cybersecurity countermeasures and...

6 Dec 2022

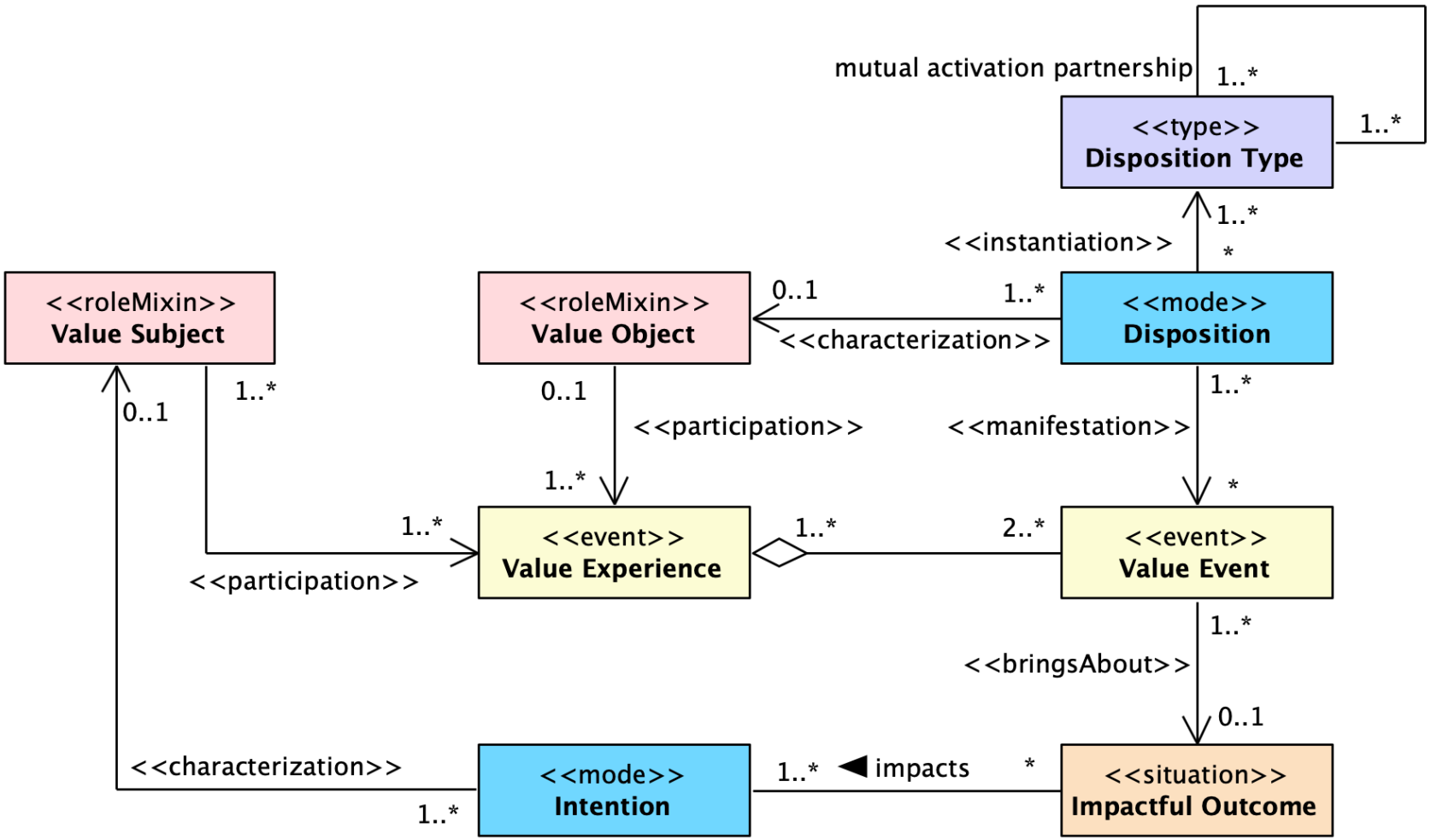
Unified Foundational Ontology (UFO)



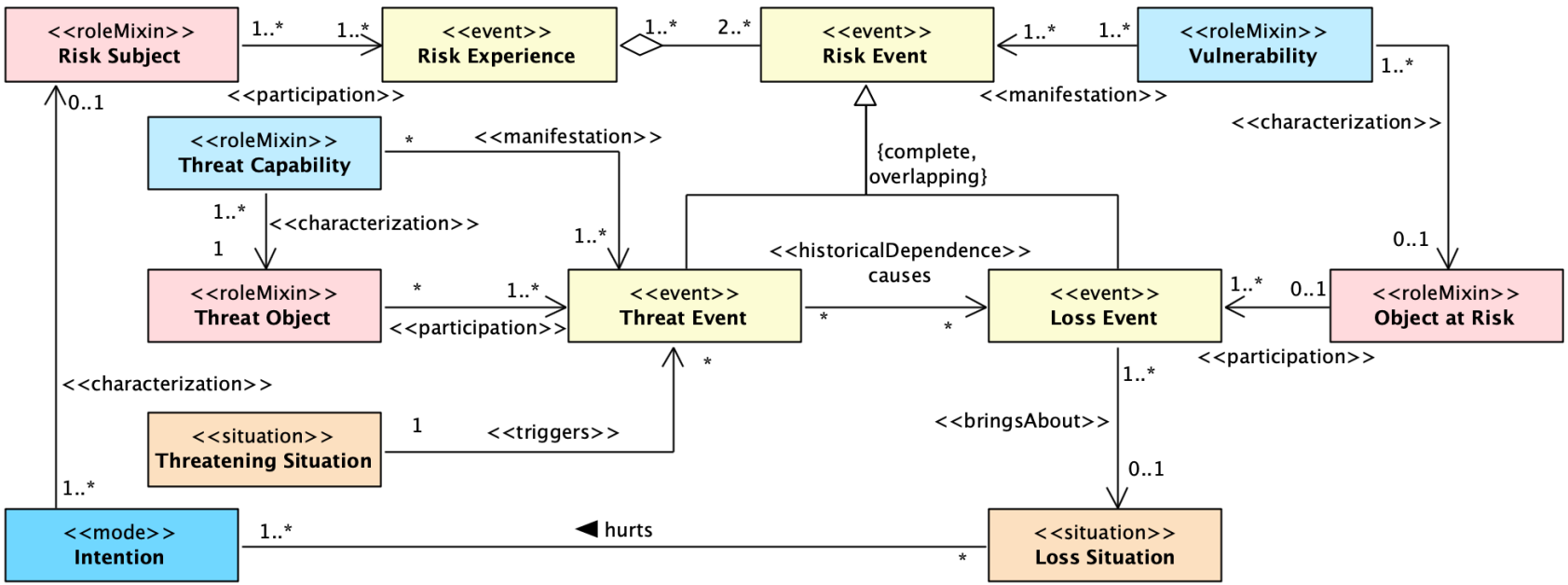
UFO-B: Ontology of Events



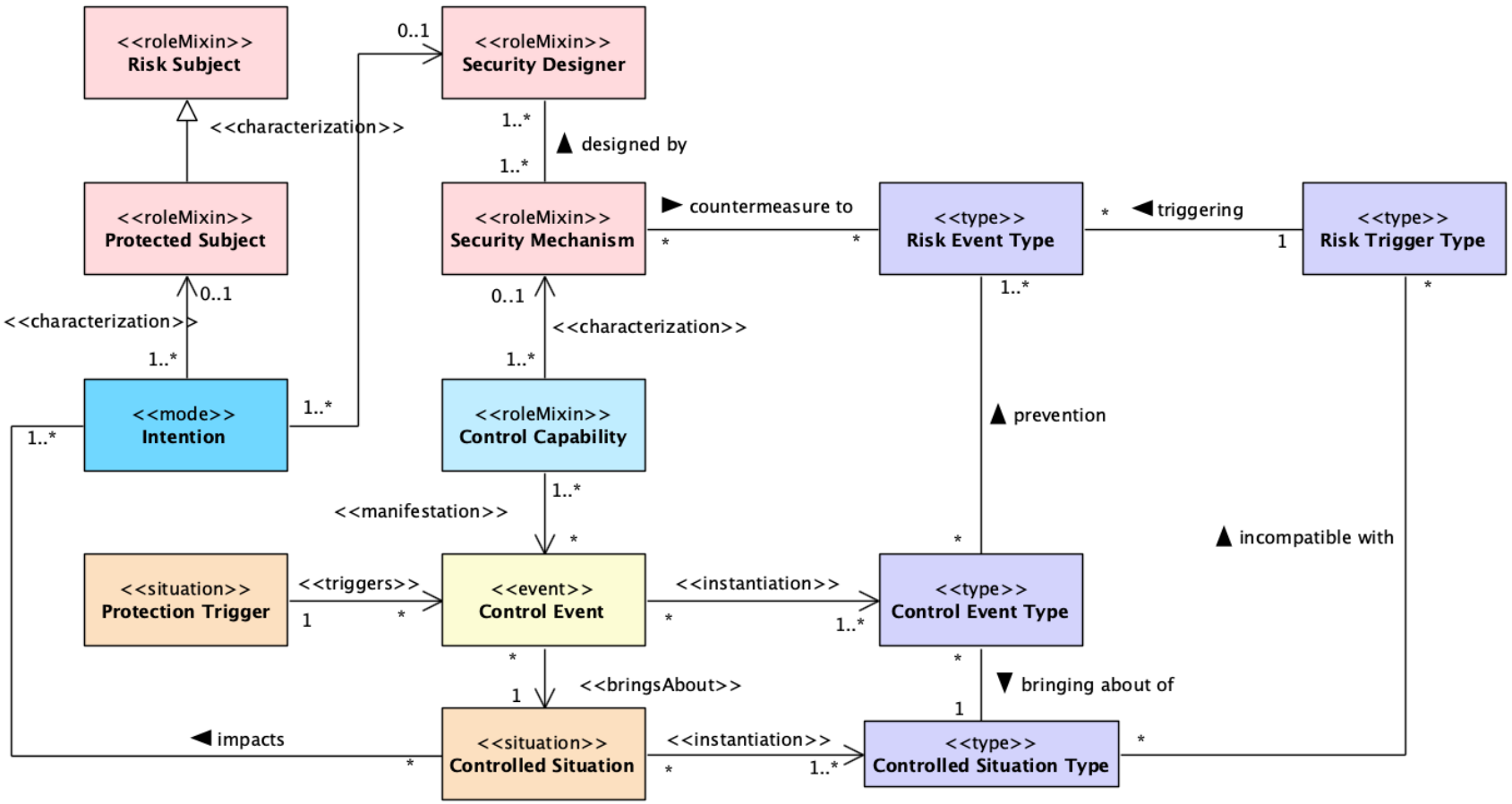
Reference Ontology for Security Engineering (ROSE)



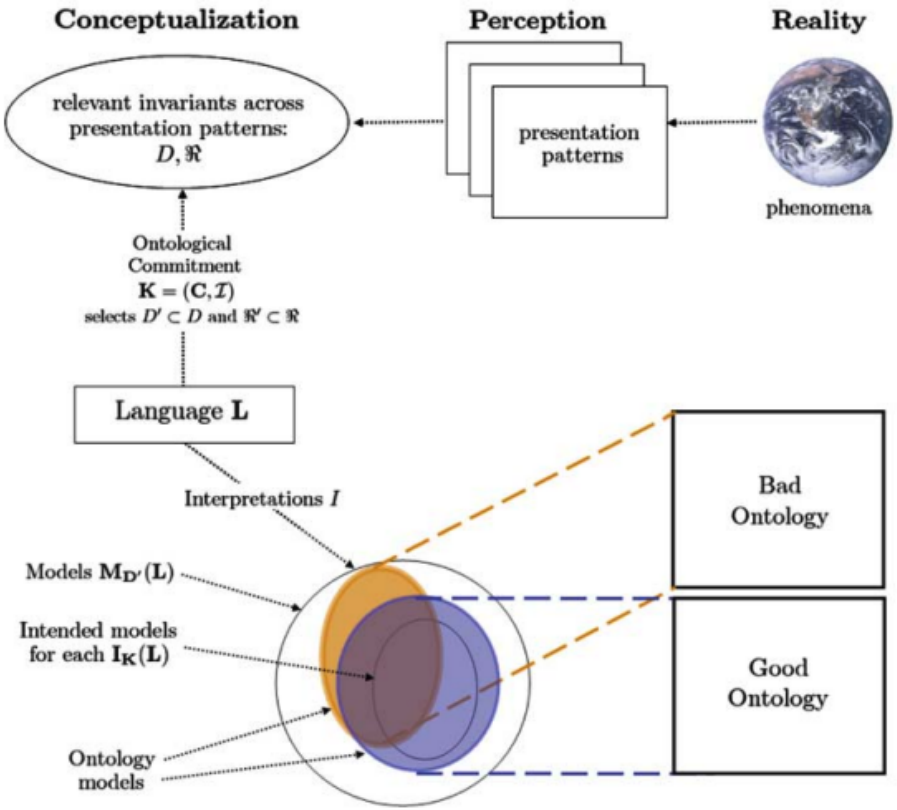
Reference Ontology for Security Engineering (ROSE)



Reference Ontology for Security Engineering (ROSE)

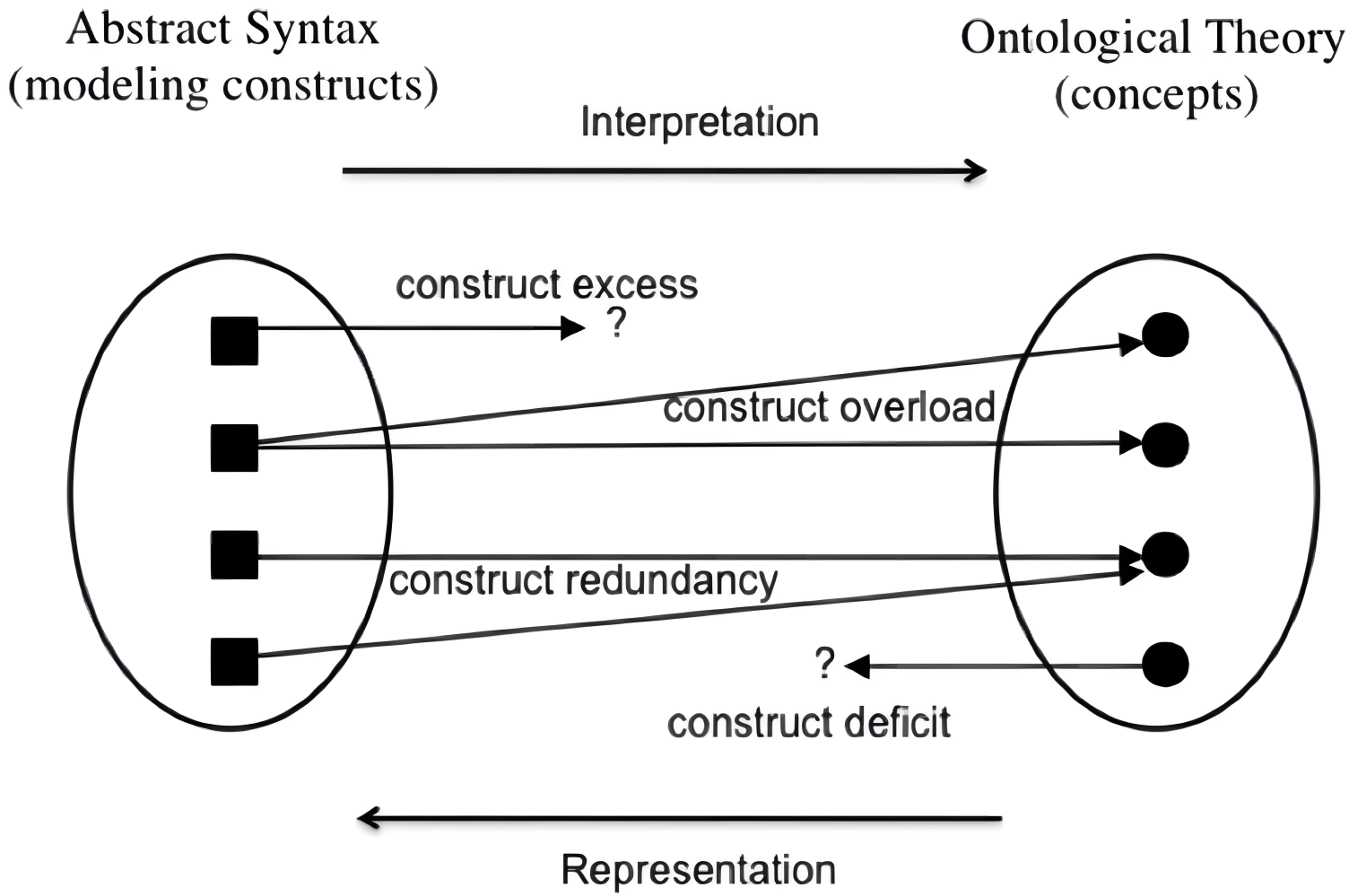


A good ontology should not only capture intended instances but also exclude unintended ones.



GUARINO et al. What is an ontology? (2009)

Ontological Analysis



***Conjecture**: without the aid of the systematic taxonomy of a foundational ontology, ontology engineers tend to drop constraints to avoid inconsistencies as the ontology gets bigger, consequently admitting more and more unintended instances.*

Versions of D3FEND

- Version 0.11.0-BETA, October 2022, is *logically inconsistent*.

Versions of D3FEND

- Version 0.11.0-BETA, October 2022, is *logically inconsistent*.
- We use the previous one, 0.10.1-BETA, June 2022.

Versions of D3FEND

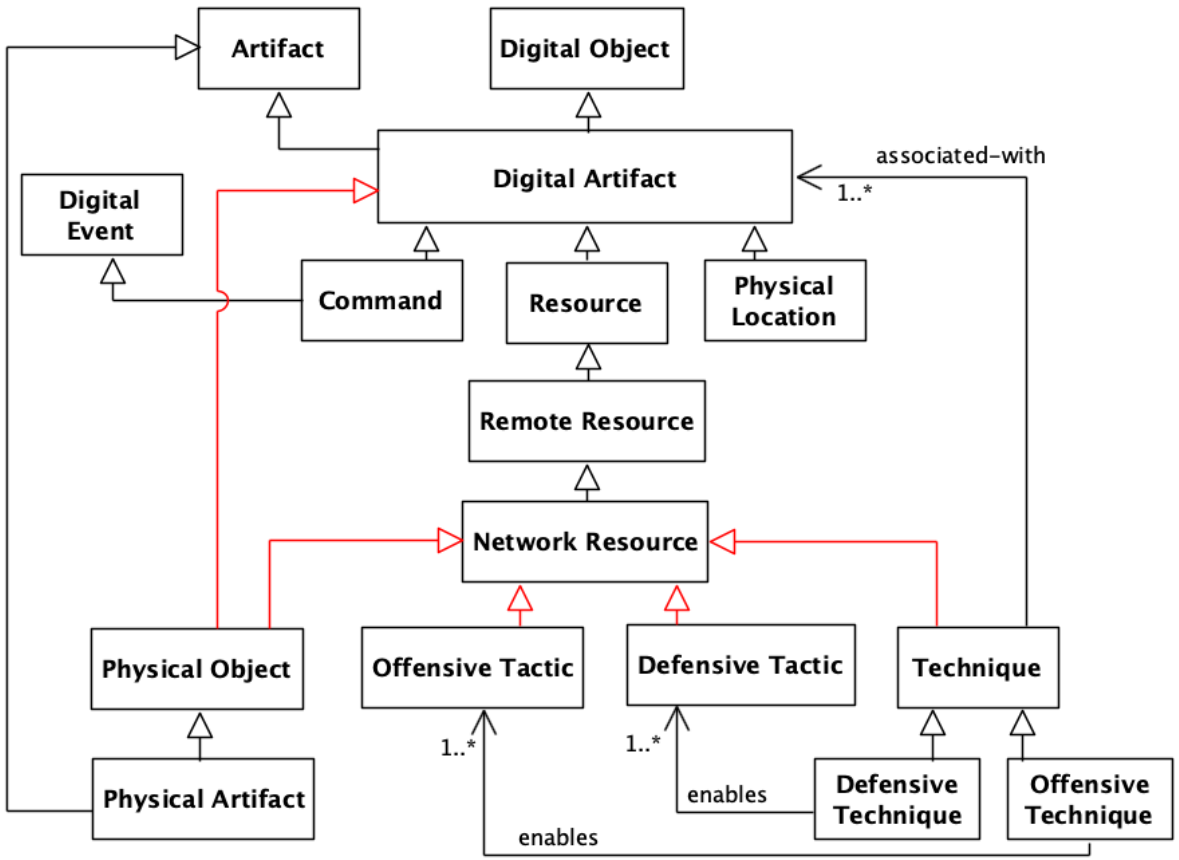
- Version 0.11.0-BETA, October 2022, is *logically inconsistent*.
- We use the previous one, 0.10.1-BETA, June 2022.
- Currently, there is version 0.12.0-BETA, January 2023.

Versions of D3FEND

- Version 0.11.0-BETA, October 2022, is *logically inconsistent*.
- We use the previous one, 0.10.1-BETA, June 2022.
- Currently, there is version 0.12.0-BETA, January 2023.
- All related files at: `https://purl.org/d3fend-analysis`

General Ontological Issues Within D3FEND

Systematic problem of ontological imprecision, particularly regarding its *lack of disjointness* among classes.



General Ontological Issues Within D3FEND

- Physical Objects and Locations and Digital Artifacts

General Ontological Issues Within D3FEND

- Physical Objects and Locations and Digital Artifacts
- Tactic and Technique

General Ontological Issues Within D3FEND

- Physical Objects and Locations and Digital Artifacts
- Tactic and Technique
- Types and Instances

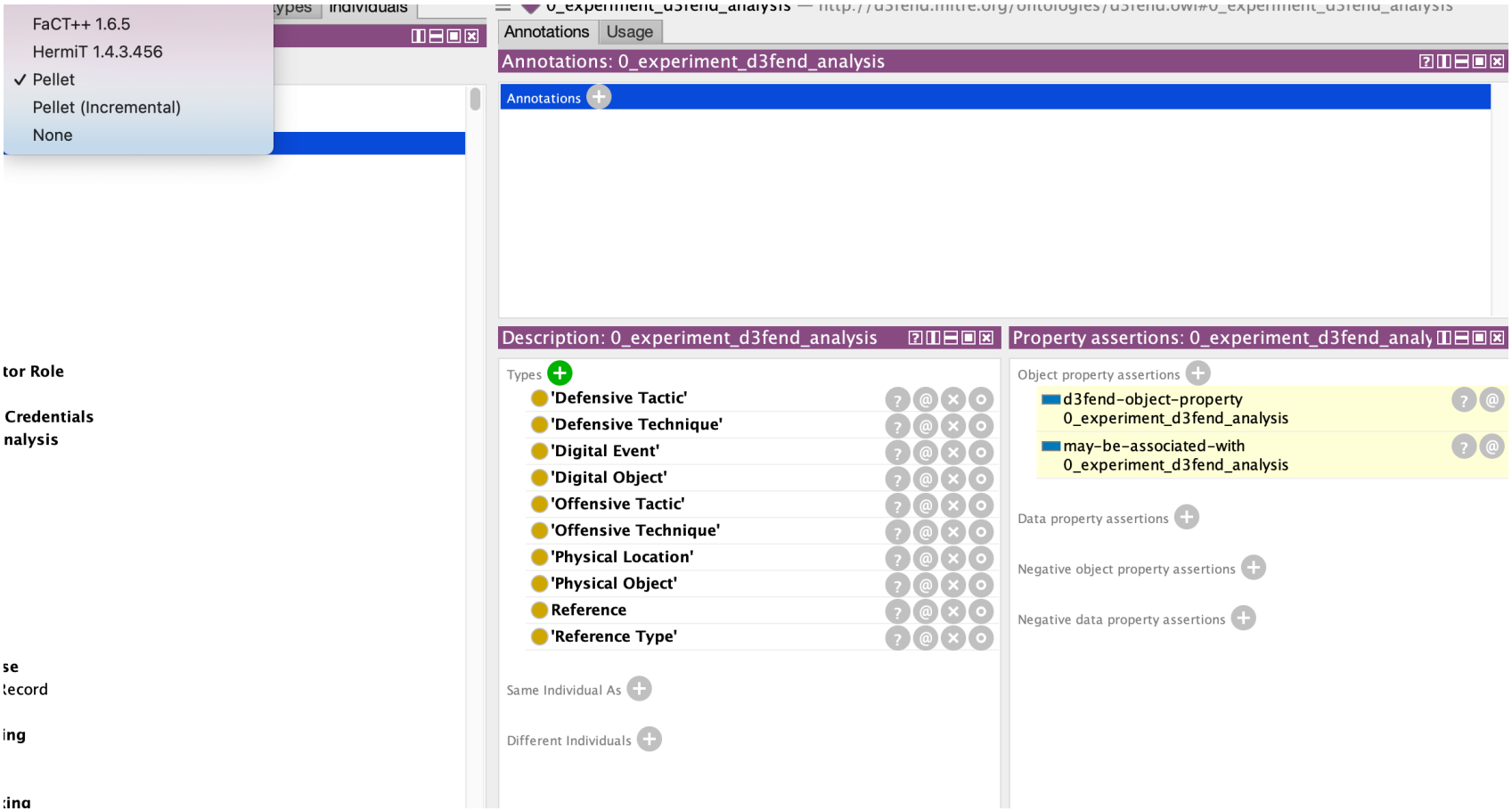
General Ontological Issues Within D3FEND

- Physical Objects and Locations and Digital Artifacts
- Tactic and Technique
- Types and Instances
- Digital Artifacts and Digital Events

General Ontological Issues Within D3FEND

- Physical Objects and Locations and Digital Artifacts
- Tactic and Technique
- Types and Instances
- Digital Artifacts and Digital Events
- As final evidence of the systematic lack of constraints of D3FEND, we made an experiment by creating an individual that is, *concomitantly*, everything at once.

Lack of constraints



Domain-Specific Ontological Issues Within D3FEND

- Artifact Ontology $\Leftrightarrow$ Value Ontology

Domain-Specific Ontological Issues Within D3FEND

- Artifact Ontology $\Leftrightarrow$ Value Ontology
- Attack Ontology $\Leftrightarrow$ Risk Ontology

Domain-Specific Ontological Issues Within D3FEND

- Artifact Ontology $\Leftrightarrow$ Value Ontology
- Attack Ontology $\Leftrightarrow$ Risk Ontology
- Defense Ontology $\Leftrightarrow$ Security Ontology

Domain-Specific Ontological Issues Within D3FEND

- Ontological incompleteness: Value Subject, Risk Subject, Protected Subject, and Security Designer.

Domain-Specific Ontological Issues Within D3FEND

- Ontological incompleteness: Value Subject, Risk Subject, Protected Subject, and Security Designer.
- Threat Object and Attacker are missing, so it is not possible to identify the Objects that are sources of a Risk Event or a Attack.

Domain-Specific Ontological Issues Within D3FEND

- The conditions that favor the appearance of a Risk Event (Threatening Situation) or the conditions that favor the occurrence of a Control Event (Protection Trigger) are absent. As a result, we cannot properly describe and assess the situations associated with risk or security.

Domain-Specific Ontological Issues Within D3FEND

- The conditions that favor the appearance of a Risk Event (Threatening Situation) or the conditions that favor the occurrence of a Control Event (Protection Trigger) are absent. As a result, we cannot properly describe and assess the situations associated with risk or security.
- The notion of Technique obfuscates the distinction between an Object (say, a Security Mechanism, its capability (say, a Control Capability), the event or process that is the manifestation of this capability (Control Event), and the resulting state of the world (Controlled Situation) that impacts (positively or negatively) an Intention of a subject.
- Vulnerability?

Takeaways

- Can an ontology be widely adopted without foundations?

Takeaways

- Can an ontology be widely adopted without foundations?
  YES! 😐

Takeaways

- Can an ontology be widely adopted without foundations?
  YES! 😐
- Can an ontology even be useful without foundations?

Takeaways

- Can an ontology be widely adopted without foundations? YES! 😐
- Can an ontology even be useful without foundations? YES! 🤨

Takeaways

- Can an ontology be widely adopted without foundations? YES! 😐
- Can an ontology even be useful without foundations? YES! 🤨
- But what happens in case of lack of foundations? Is this a problem? 🤔

Takeaways

- Can an ontology be widely adopted without foundations? YES! 😐
- Can an ontology even be useful without foundations? YES! 🤨
- But what happens in case of lack of foundations? Is this a problem? 🤔 Ontological imprecision 🤦

Takeaways

- Can an ontology be widely adopted without foundations? YES! 😐
- Can an ontology even be useful without foundations? YES! 🤨
- But what happens in case of lack of foundations? Is this a problem? 🤔 Ontological imprecision 🤦
- Motto: No ontology without Ontology! 🙃

Takeaways

- Can an ontology be widely adopted without foundations? YES! 😐
- Can an ontology even be useful without foundations? YES! 🤨
- But what happens in case of lack of foundations? Is this a problem? 🤔 Ontological imprecision 🤦
- Motto: No ontology without Ontology! 🙃
- Foundational ontologies and reference domain ontologies work as ontology engineering frameworks. 🥰

Future Work

- Specializing ROSE to capture the cybersecurity domain, following D3FEND's artifact, attack, and defense ontologies.

Future Work

- Specializing ROSE to capture the cybersecurity domain, following D3FEND's artifact, attack, and defense ontologies.
- List of threat groups, registered by MITRE: https://attack.mitre.org/groups/.

Future Work

- Specializing ROSE to capture the cybersecurity domain, following D3FEND's artifact, attack, and defense ontologies.
- List of threat groups, registered by MITRE: https://attack.mitre.org/groups/.
- "CIA triad": *Confidentiality*, *Integrity*, and *Availability*. They can be used not only to specialize the subjects' Intentions (security goals) but also to specialize Loss Event and Loss Situation–Loss of Confidentiality, Loss of Integrity, and Loss of Integrity.)

Thank you! Questions?

Get in touch: 😇

- i.j.dasilvaoliveira@utwente.nl
- https://sites.google.com/view/italojsoliveira
- Semantics, Cybersecurity, and Services Group: `https://www.utwente.nl/en/eemcs/scs/`