unibz
Fakultät für Ingenieurwesen
Facoltà di Ingegneria
Faculty of Engineering

An Ontological Approach to Security Modeling

Ítalo José da Silva Oliveira

https://italojsoliveira.github.io/

Supervisors:

Enrico Franconi (Free University of Bozen-Bolzano)

Giancarlo Guizzardi (University of Twente)

Tiago Prince Sales (University of Twente)

External Reviewers:

Manfred Jeusfeld (University of Skövde)

Raimundas Matulevičius (University of Tartu)

28/06/2024

"Conceptual Modeling is the activity of **representing the** physical or social **world for** the purposes of communication, problem-solving and meaning negotiation among **humans**"

(Guarino, Mylopoulos & Guizzardi, 2019)
Philosophical Foundations for Conceptual Modeling

Security is pervasive

asset, something of value

vulnerability

threat

reduced risk level

constitutes a security risk

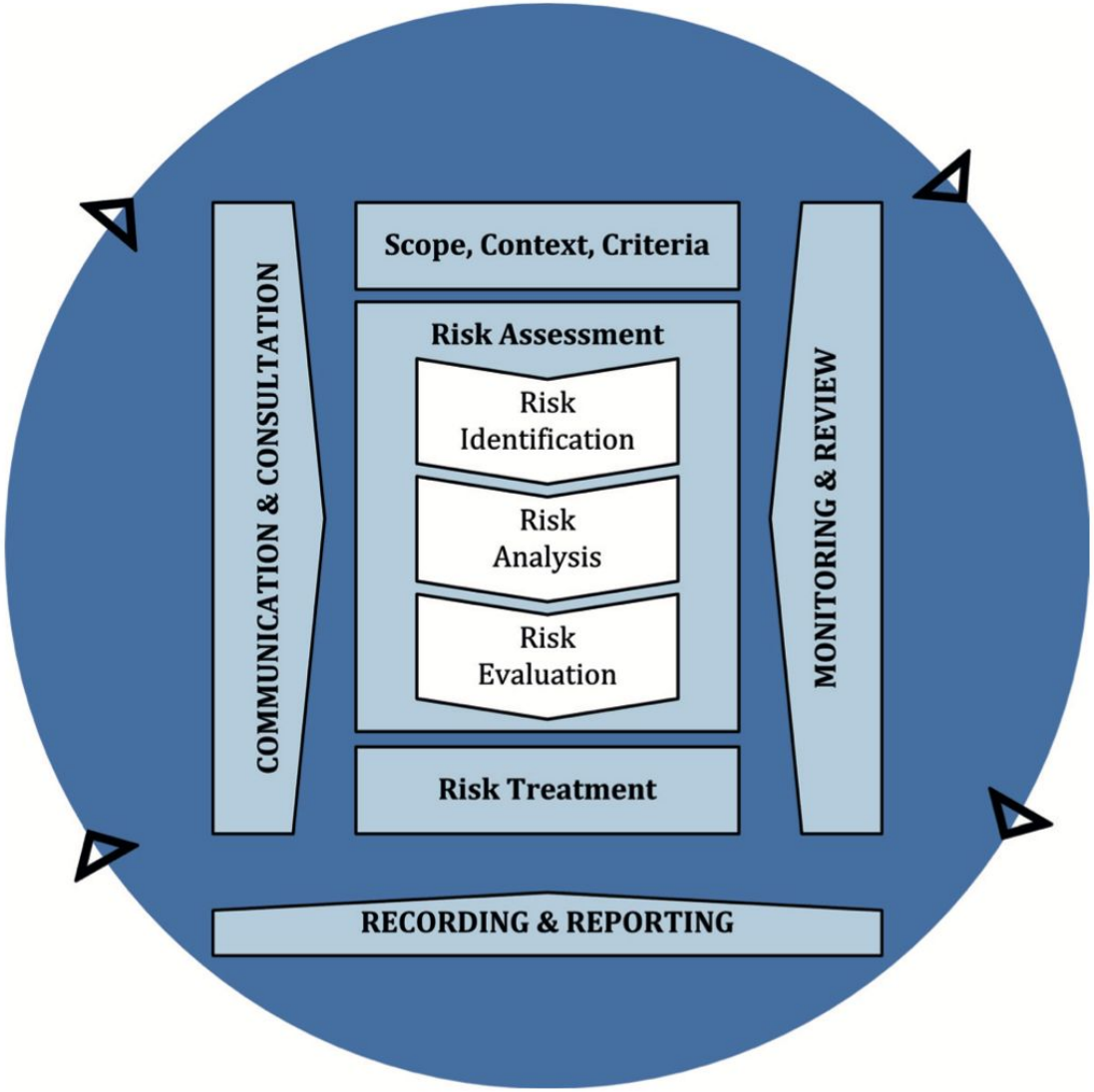
we need to introduce security mechanisms

Context & Motivation

Risk Management, ISO 31000:2018

- The purpose of risk management is the creation and protection of value.

- Complex relations among objects and agents, their capabilities and vulnerabilities, events and goals, assets and risks, security mechanisms, and safety measures, all that occurs transversely in multiple domains.

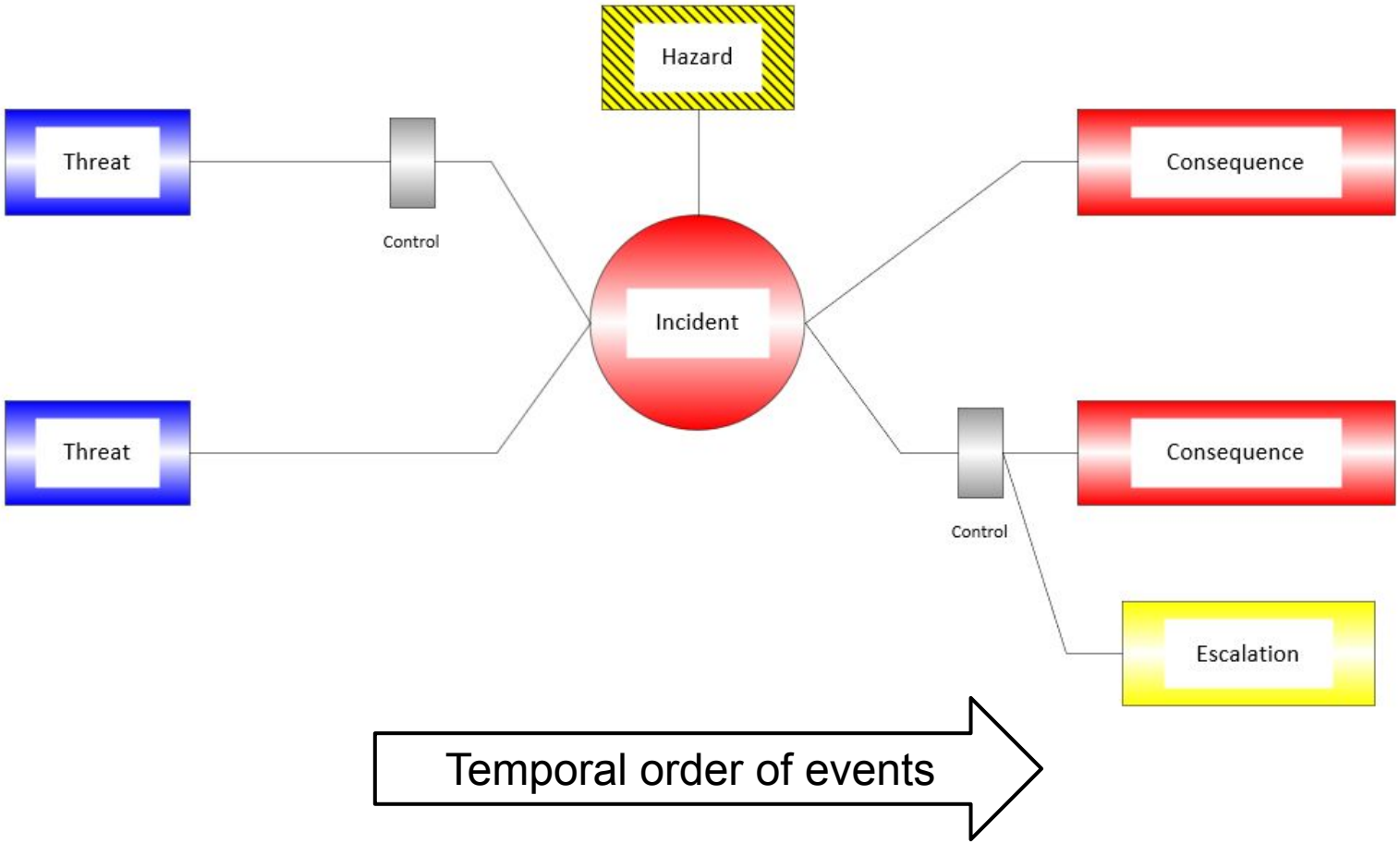


Risk Management Process, ISO 31000

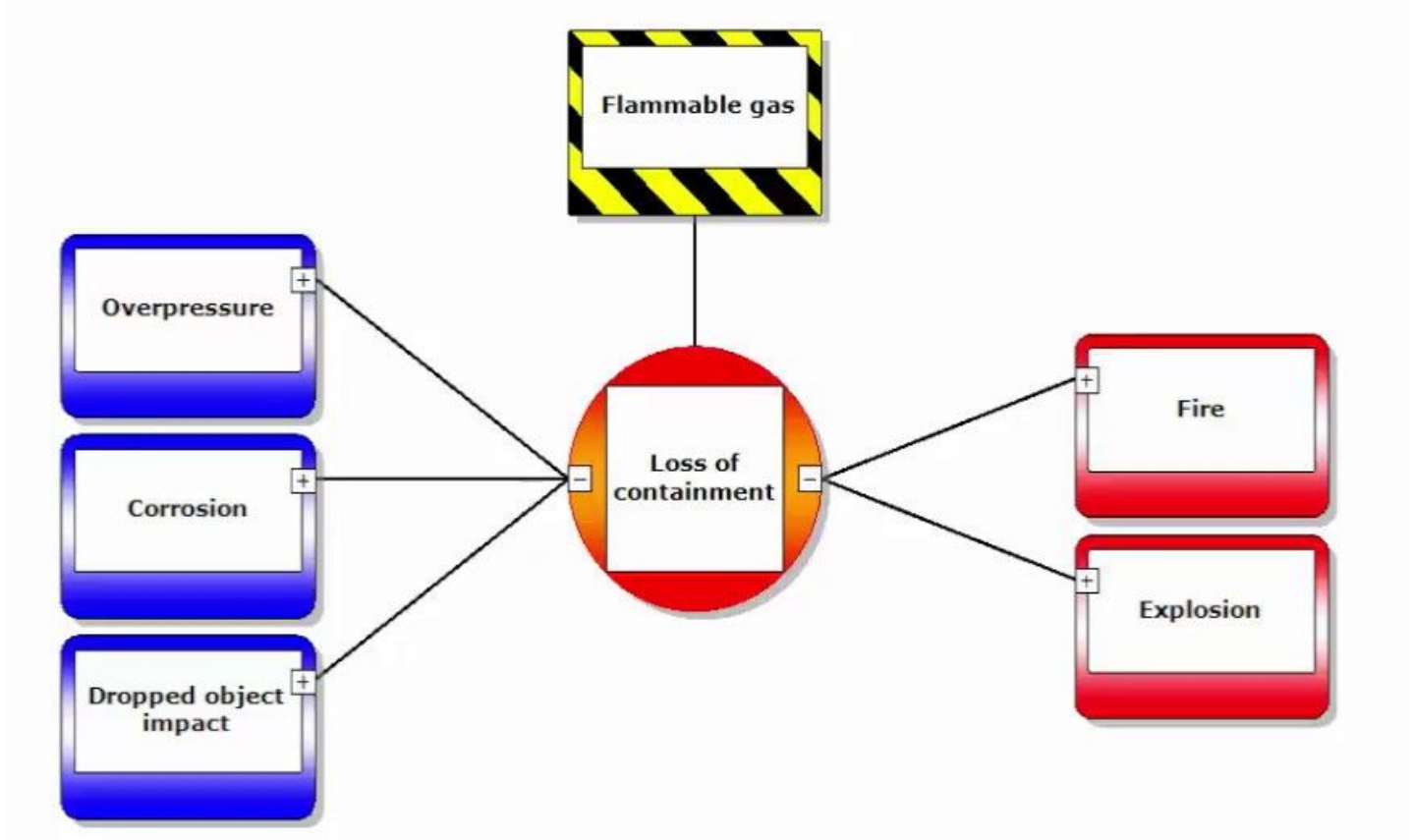
Risk Assessment Techniques, ISO/IEC 31010:2019

- It mentions more than 40 risk assessment techniques, all of which require, explicitly or implicitly, a conceptualization of risk and security entities.
    - Bowtie analysis
    - Failure mode and effects analysis (FMEA)
    - Fault tree analysis (FTA)
    - Event tree analysis (ETA)
    - Risk Matrix
    - …

Bowtie Model of the Risk and Security Domains



Example of a Bowtie Model



- A common risk assessment technique.

There's no sense in being precise when you don't even know what you're talking about.

John von Neumann

Problem:

How can we define an adequate conceptualization of the risk and security domain?

It is a matter of:

- Domain analysis.
- Conceptual clarification.
- Meaning negotiation.

It is a matter of Ontology!

Understanding and Modeling Prevention


R
I
S
K

General Research Goal

Understanding and modeling the security domain.

General Research Goal

Understanding and modeling the security domain.

To provide ontological foundations for modeling information in risk management.

Research Objectives

1. To identify the state of the art and gaps in security ontologies.
2. …
3. …

Research Objectives

1. To identify the state of the art and gaps in security ontologies.
2. To propose a general theory of prevention to support our security ontology.
3. …

Research Objectives

1. To identify the state of the art and gaps in security ontologies.

2. To propose a general theory of prevention to support our security ontology.

3. To propose a *Reference Ontology for Security Engineering* (*ROSE*) from a risk treatment perspective, according to ISO 31000.

Research Objectives

4. To show how to specialize this ontology of security in a more specific domain. In this case, phishing attacks.

5. …

6. …

Research Objectives

4. To show how to specialize this ontology of security in a more specific domain. In this case, phishing attacks.

5. Application 1: an ontological analysis of the D3FEND cybersecurity model based on ROSE.

6. …

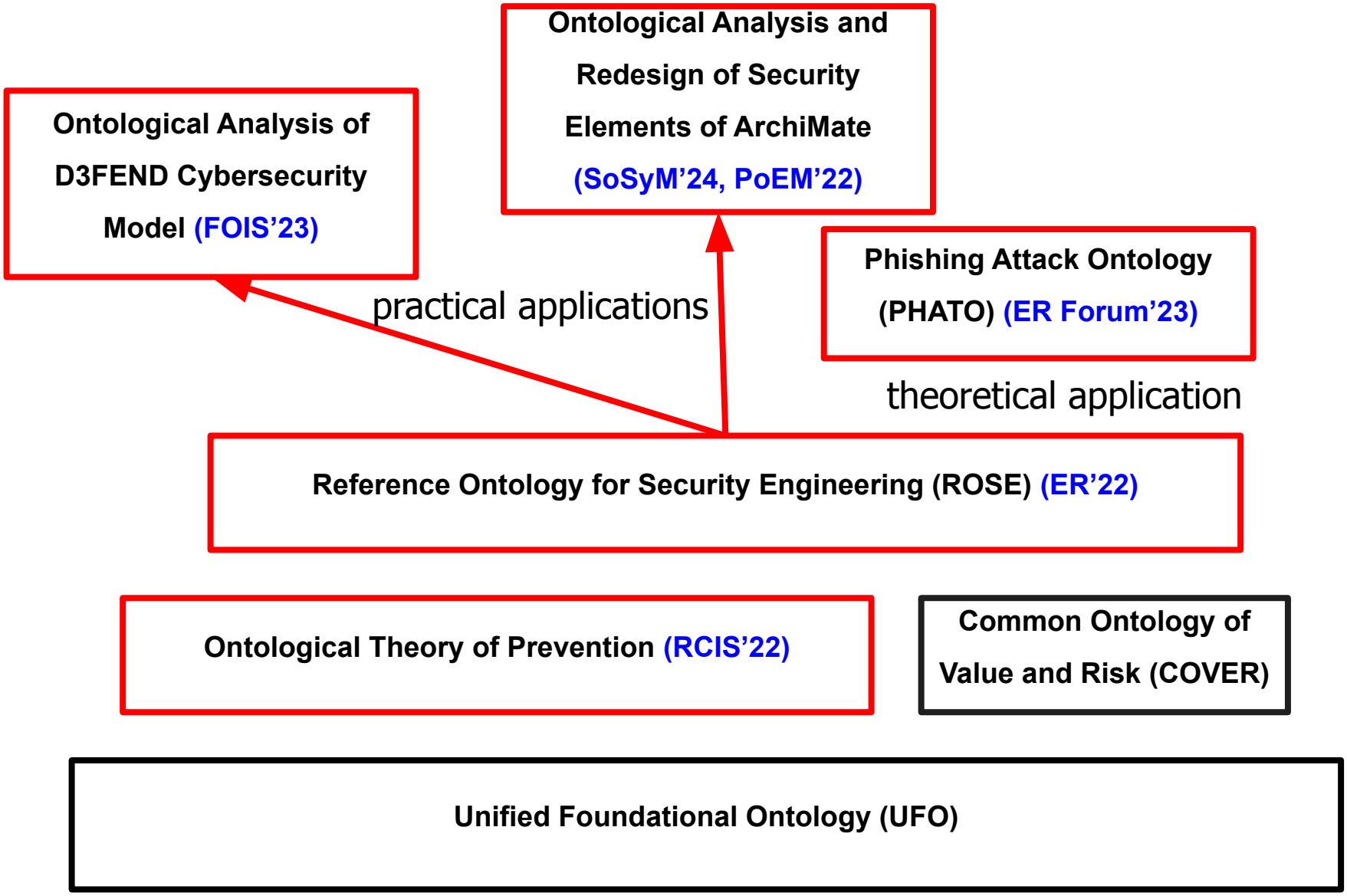
Research Objectives

4. To show how to specialize this ontology of security in a more specific domain. In this case, phishing attacks.

5. Application 1: an ontological analysis of the D3FEND cybersecurity model based on ROSE.

6. Application 2: an ontological analysis and redesign of the ArchiMate's Risk and Security Overlay based on ROSE.

Research Outcomes



Design Science Research Methodology

(a) Concrete artifacts (ontologies and languages);

(b) …

(c) …

(d) …

(e) …

Design Science Research Methodology

(a) Concrete artifacts (ontologies and languages);

(b) to support technology-based solutions to business problems (modeling information in risk management);

(c) …

(d) …

(e) …

Design Science Research Methodology

(a) Concrete artifacts (ontologies and languages);

(b) to support technology-based solutions to business problems (modeling information in risk management);

(c) Solid foundations (ontology-driven conceptual modeling) in the process of construction and…

(d) …

(e) …

Design Science Research Methodology

(a) Concrete artifacts (ontologies and languages);

(b) to support technology-based solutions to business problems (modeling information in risk management);

(c) Solid foundations (ontology-driven conceptual modeling) in the process of construction and…

(d) evaluation of the artifacts (expressiveness, consistency, FAIRness, etc.).

(e) …

Design Science Research Methodology

(a) Concrete artifacts (ontologies and languages);

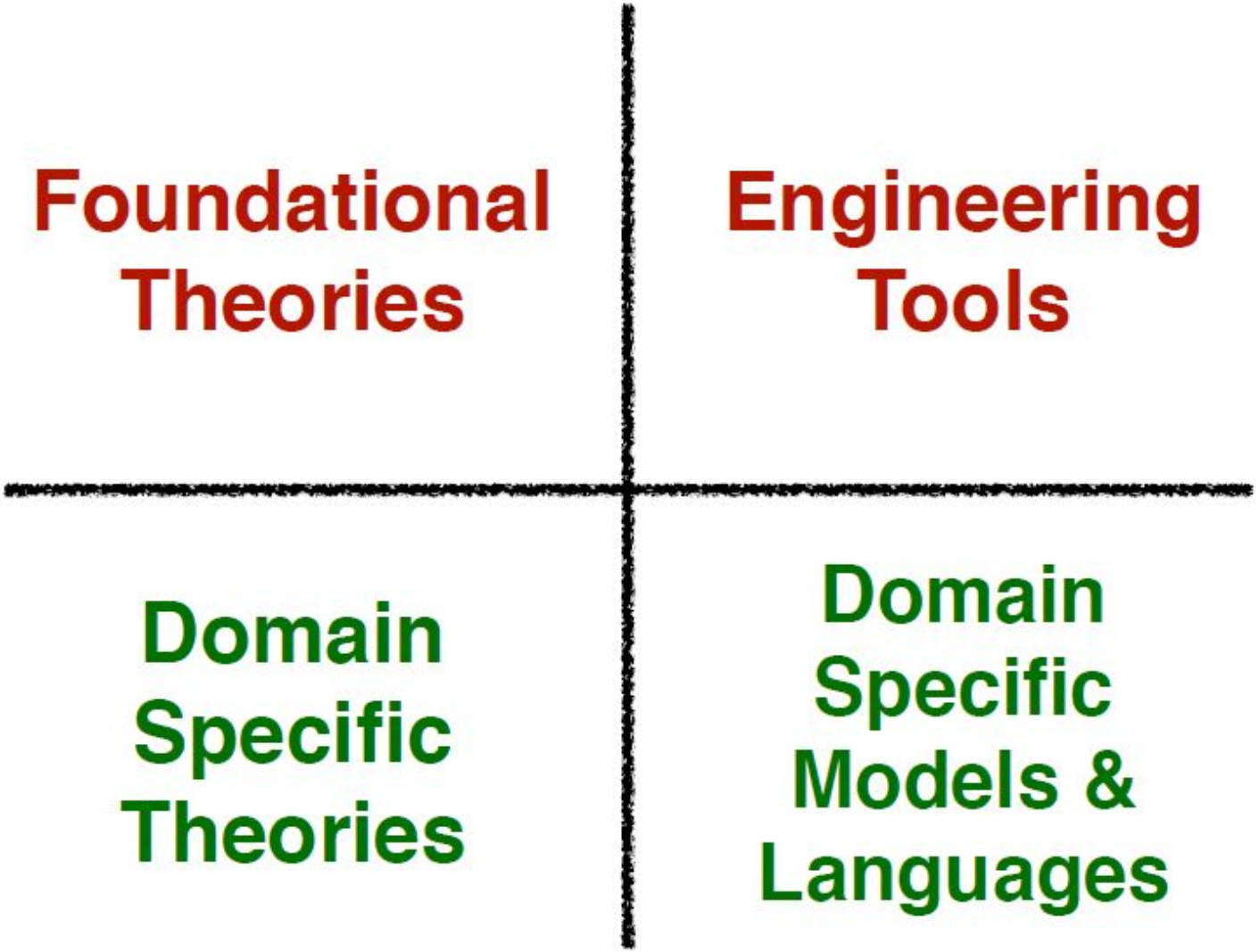
(b) to support technology-based solutions to business problems (modeling information in risk management);

(c) Solid foundations (ontology-driven conceptual modeling) in the process of construction and…

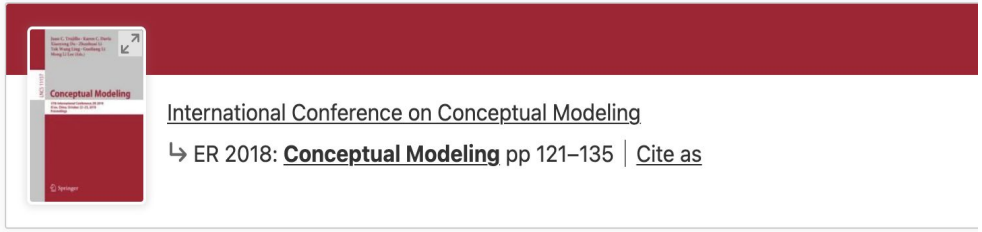
(d) evaluation of the artifacts (expressiveness, consistency, FAIRness, etc.).

(e) Proper communication to reach stakeholders.

Ontology-driven Conceptual Modeling



An Ontological Approach



International Conference on Conceptual Modeling

↳ ER 2018: **Conceptual Modeling** pp 121–135 | Cite as

Home › Conceptual Modeling › Conference paper

The Common Ontology of Value and Risk

Tiago Prince Sales ✉, Fernanda Baião, Giancarlo Guizzardi, João Paulo A. Almeida, Nicola Guarino & John Mylopoulos

Conference paper | First Online: 26 September 2018

2704 Accesses | **38** Citations

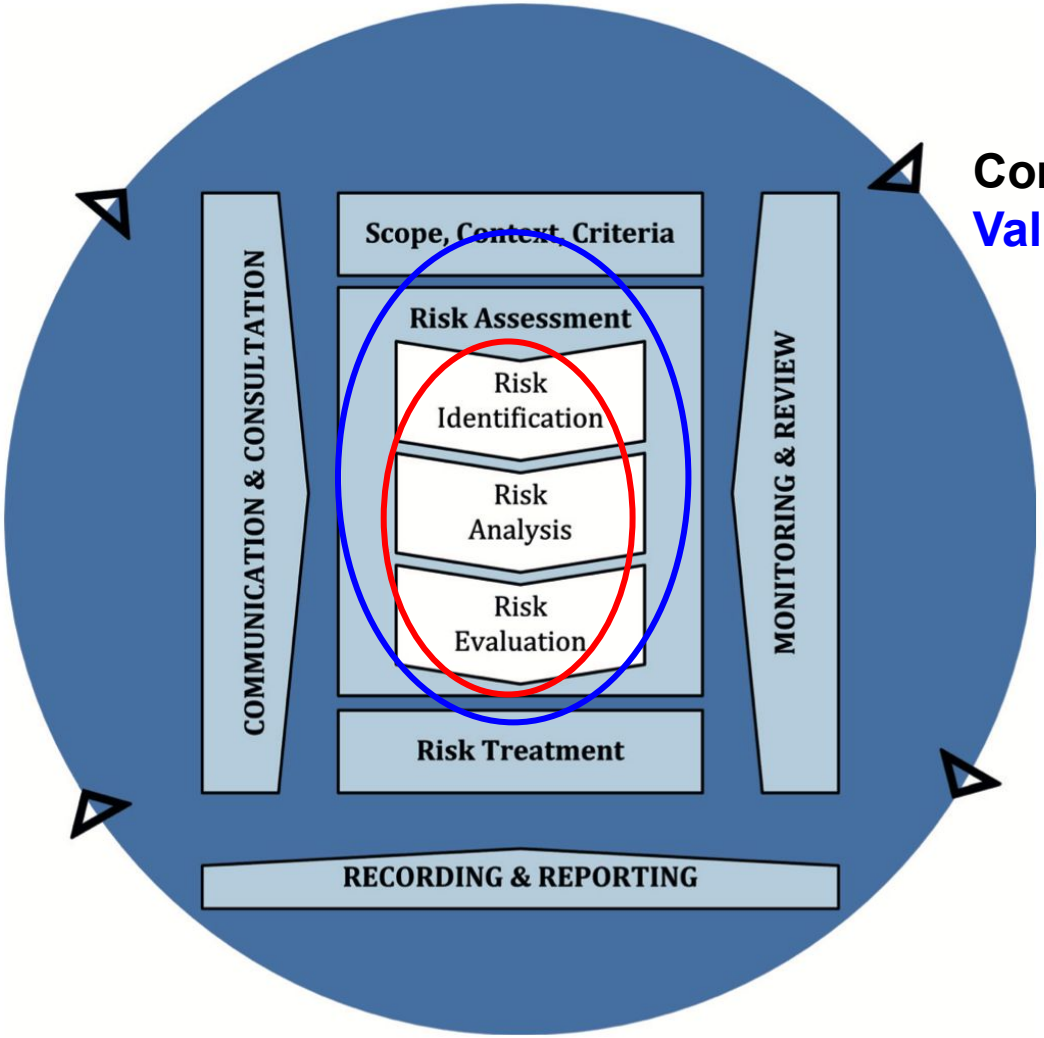
Part of the Lecture Notes in Computer Science book series (LNISA,volume 11157)

ONTOUML

UFO

Unified Foundational Ontology

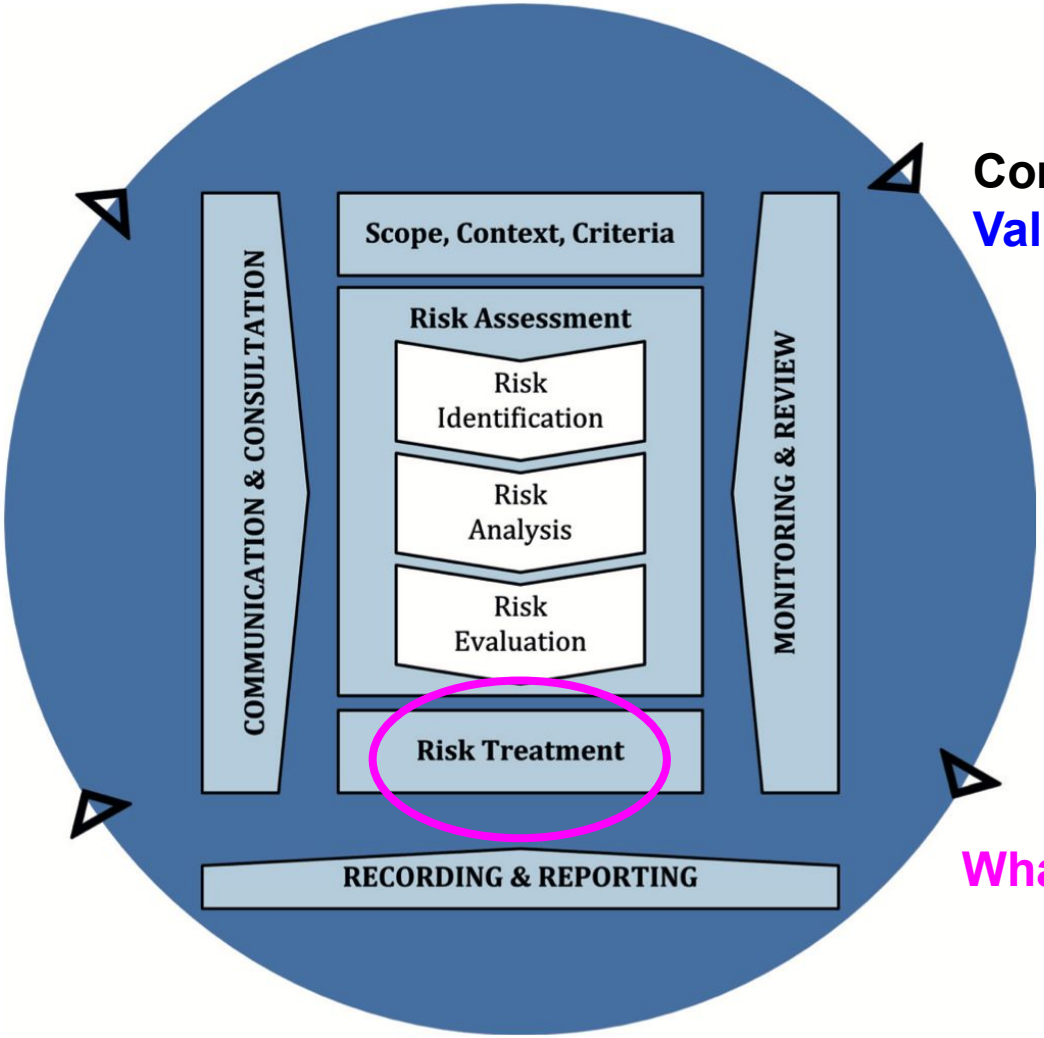
Scope



Common Ontology of Value and Risk

Risk Management Process, ISO 31000

Scope

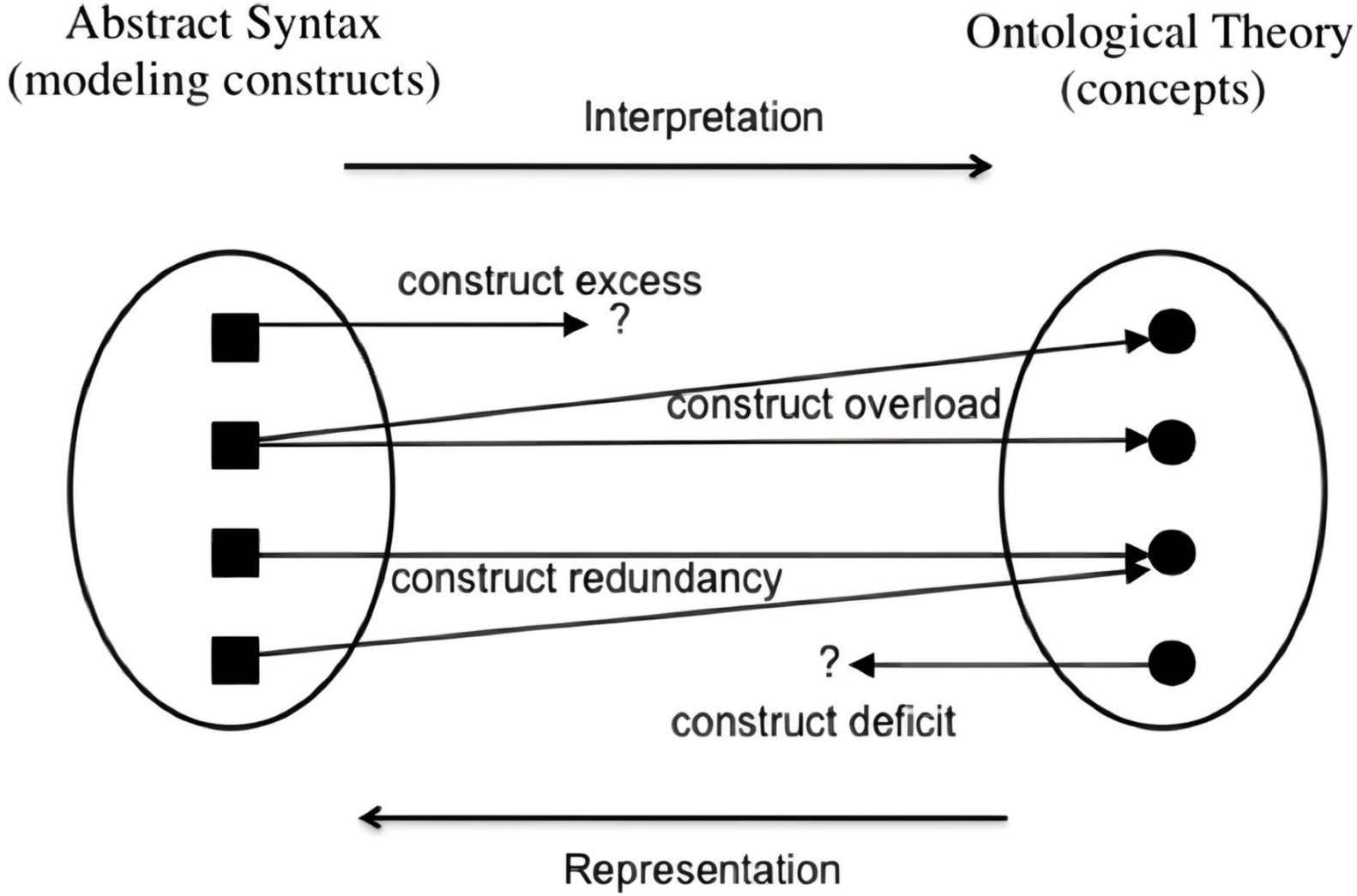


Common Ontology of Value and Risk

What about security?

Risk Management Process, ISO 31000

An Ontological Approach



Identifying the gaps

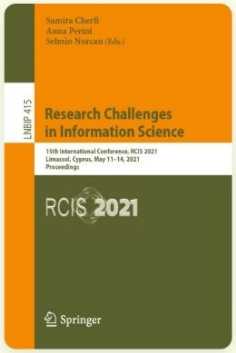
How FAIR are Security Core Ontologies? A Systematic Mapping Study

Conference paper | First Online: 08 May 2021

pp 107–123 | Cite this conference paper

Download book PDF

Download book EPUB



Research Challenges in Information Science

(RCIS 2021)

Ítalo Oliveira, Mattia Fumagalli, Tiago Prince Sales & Giancarlo Guizzardi

Part of the book series: Lecture Notes in Business Information Processing ((LNBIP,volume 415))

Included in the following conference series:
International Conference on Research Challenges in Information Science

Sections | Figures | References

Findings

- Lack of a common ontology of security.
- Lack of ontological foundations among security ontologies.
- Lack of FAIRness (not even findable!).
- Most common concepts: vulnerability, asset, threat, countermeasure, attack, risk, attacker, control, stakeholder, consequence.

A theory of prevention to ground a security ontology

Home > Research Challenges in Information Science > Conference paper

Understanding and Modeling Prevention

Conference paper | First Online: 14 May 2022

pp 389–405 | Cite this conference paper

Download book PDF Download book EPUB

Research Challenges in Information Science

(RCIS 2022)

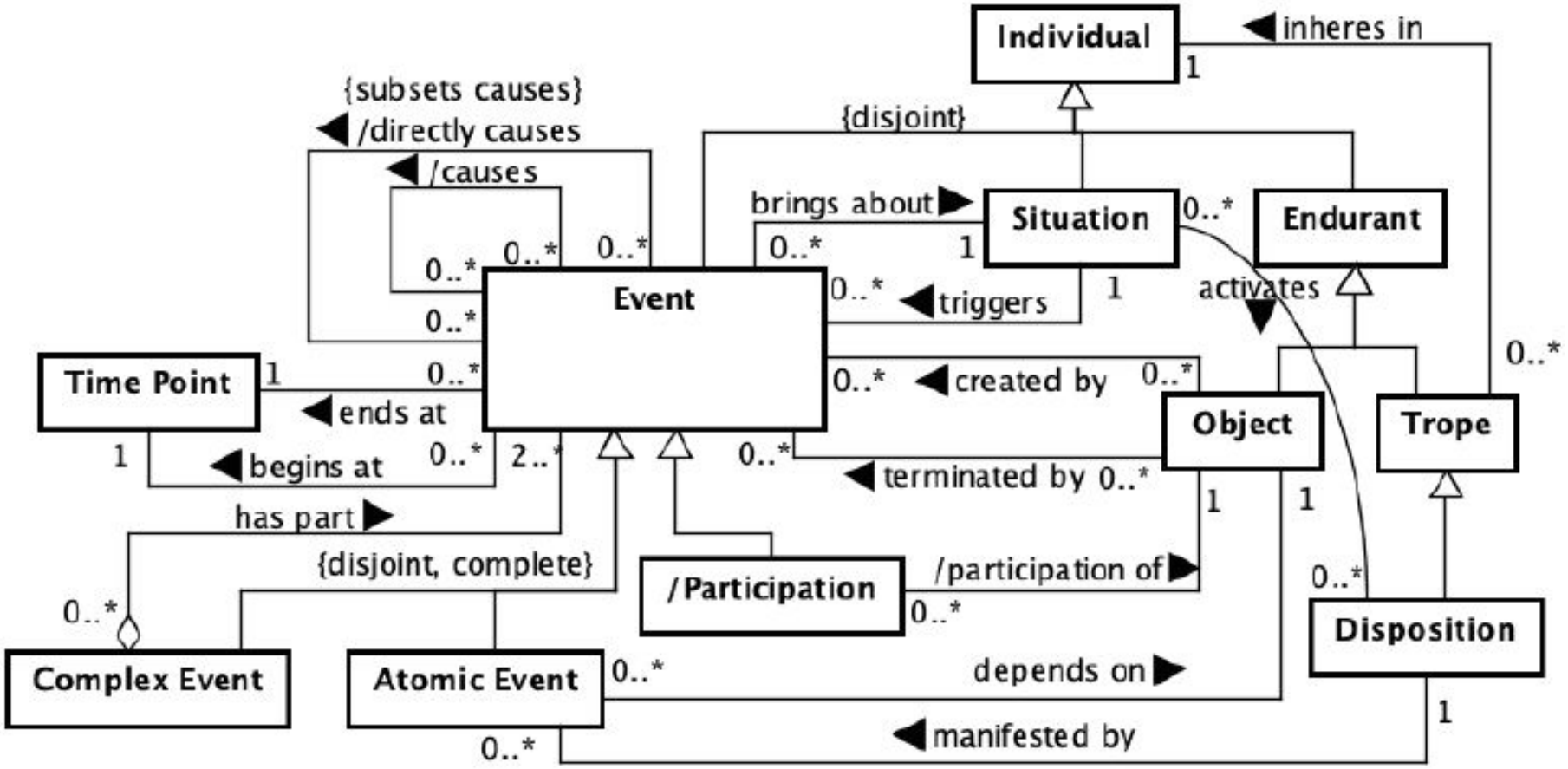
Riccardo Baratella, Mattia Fumagalli, Ítalo Oliveira & Giancarlo Guizzardi

Part of the book series: Lecture Notes in Business Information Processing ((LNBIP,volume 446))

Included in the following conference series:
International Conference on Research Challenges in Information Science

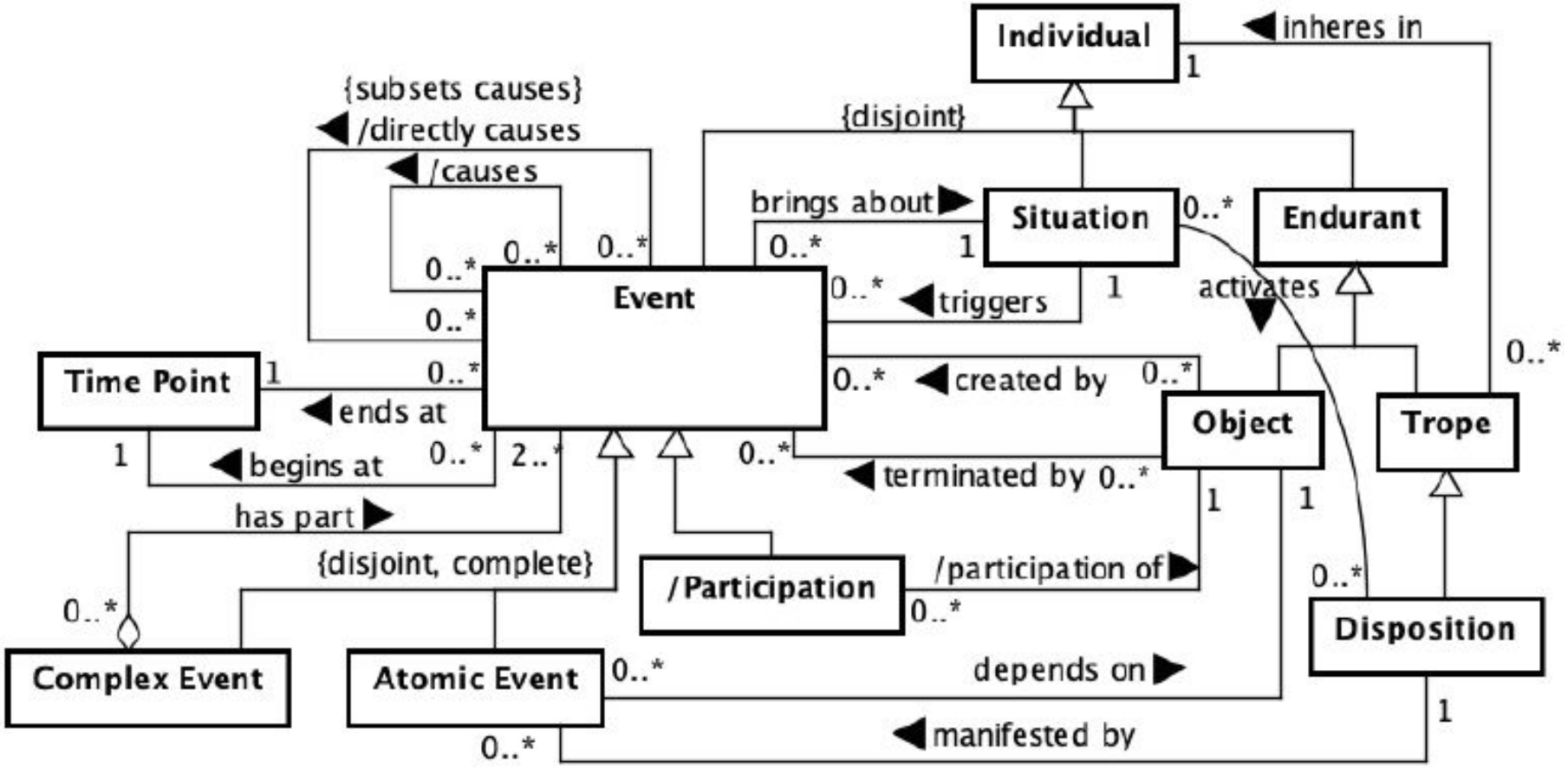
Sections | Figures | References

UFO-B: an ontology of events

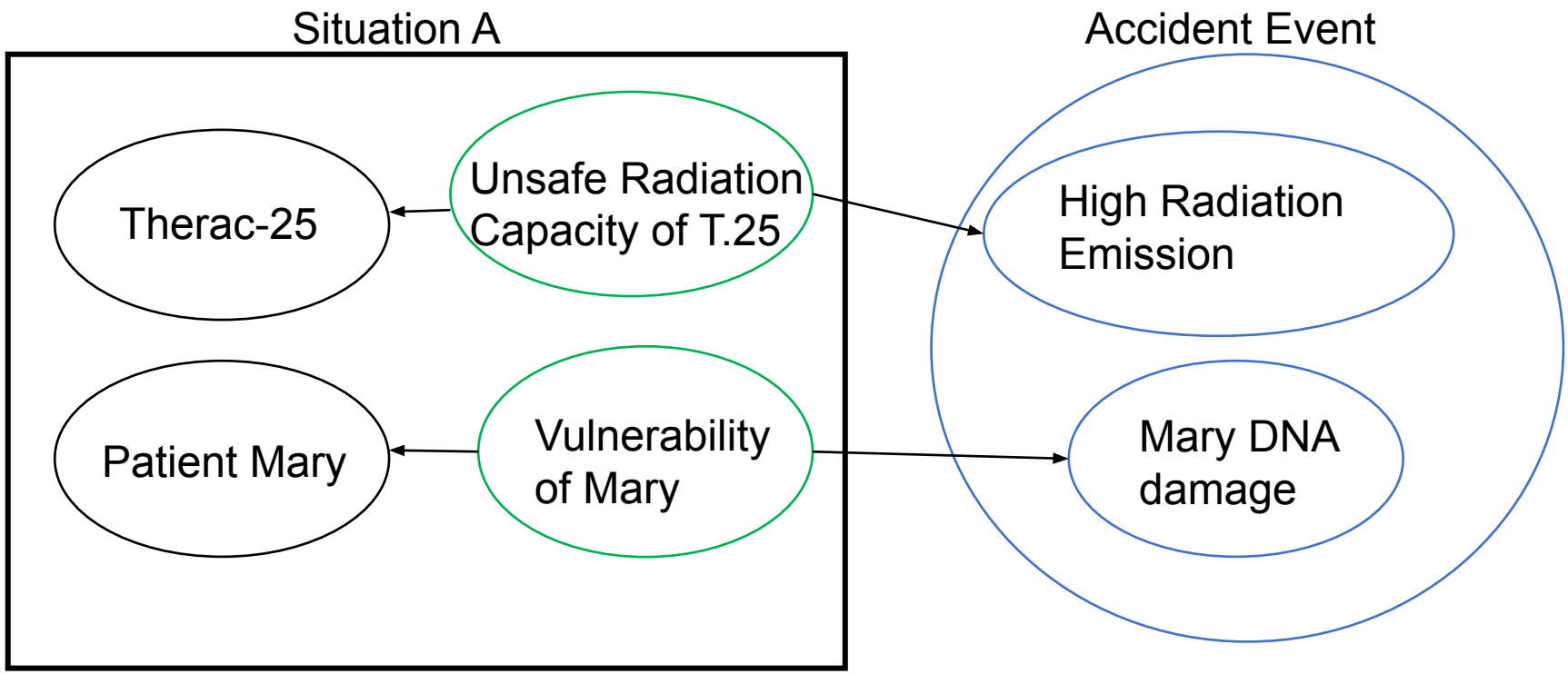


UFO-B: an ontology of events

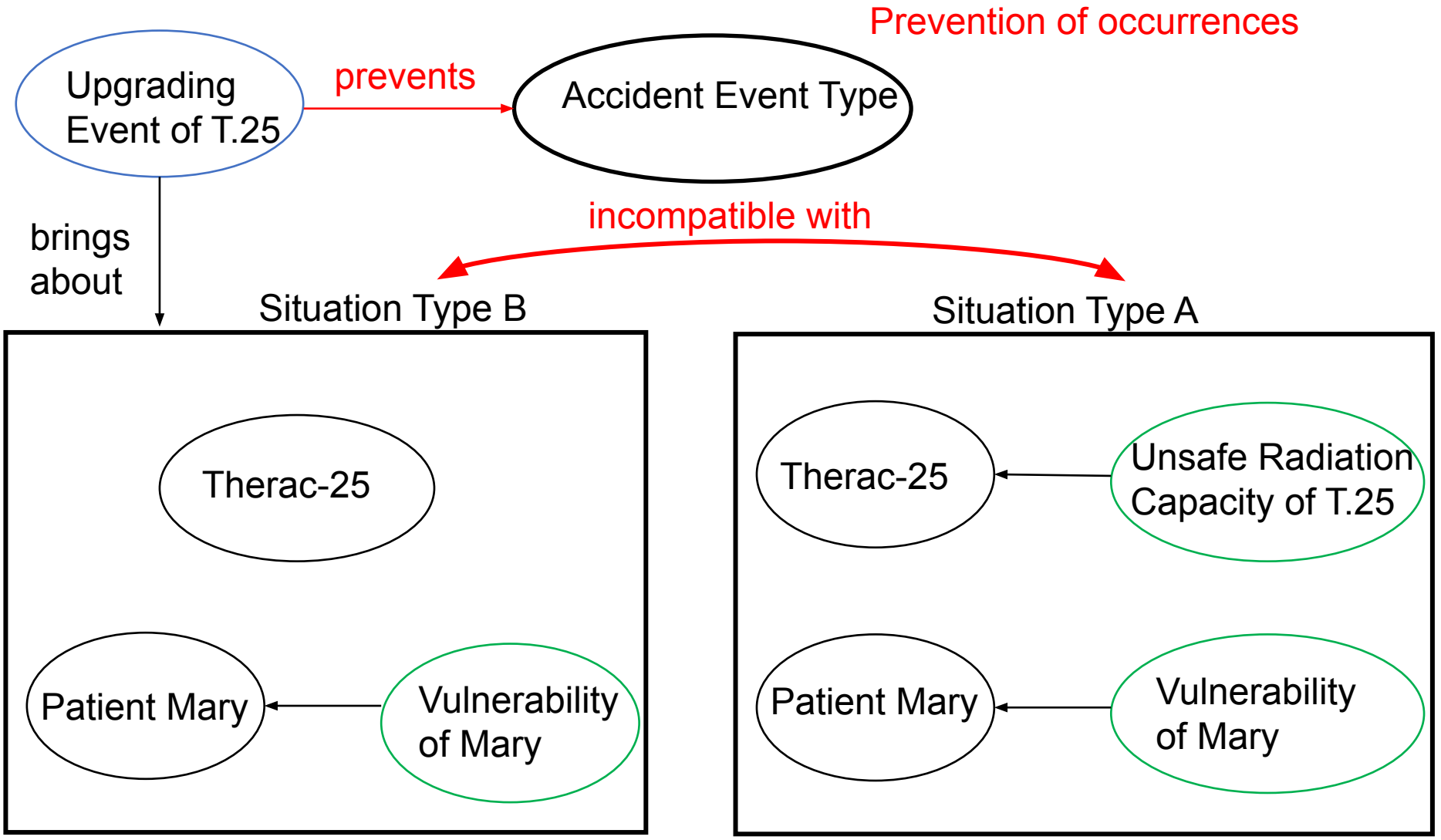
What about prevention?

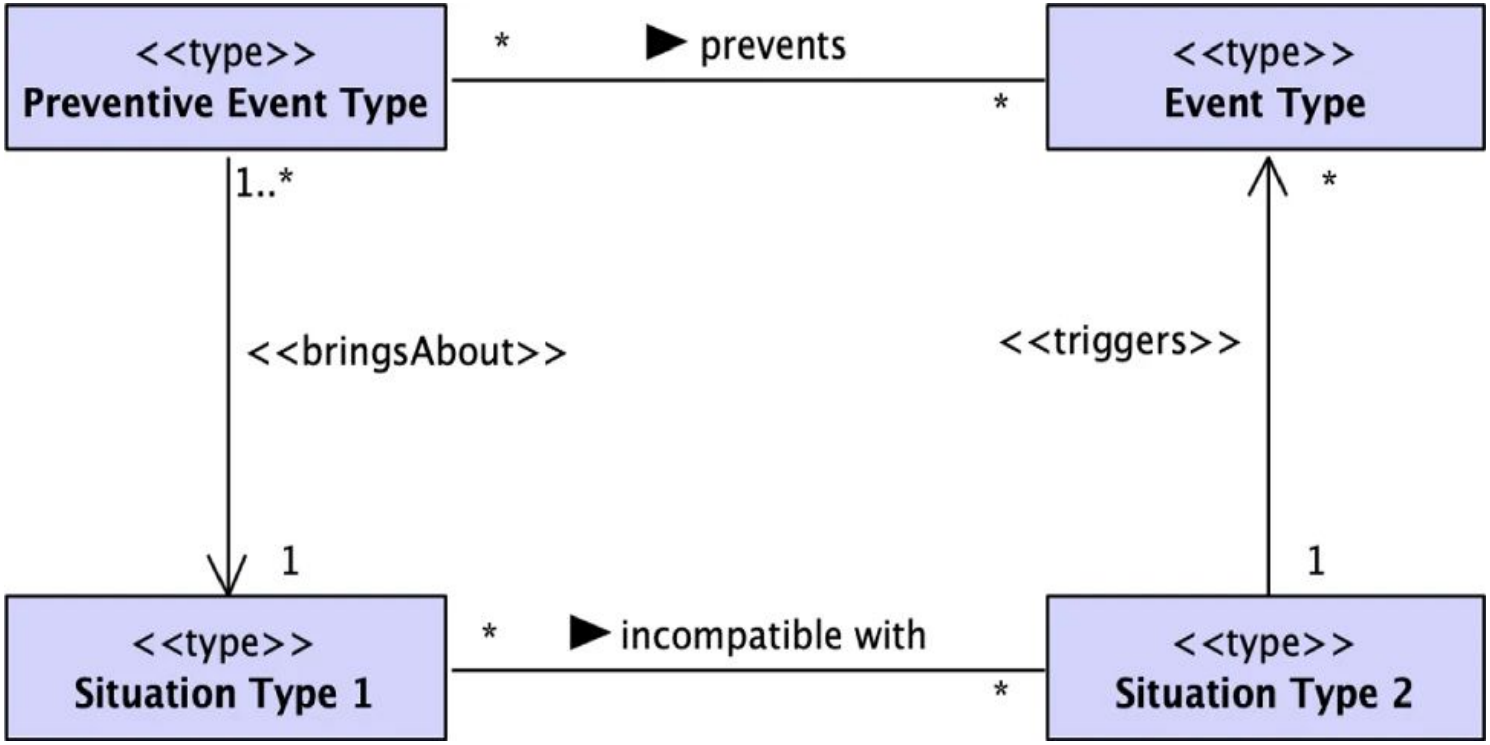


Occurrences



The combination of capabilities and vulnerabilities *in certain situations* gives raise to complex manifestation events.


Prevention of occurrences
Upgrading Event of T.25
prevents
Accident Event Type
brings about
incompatible with
Situation Type B
Situation Type A
Therac-25
Patient Mary
Vulnerability of Mary
Therac-25
Unsafe Radiation Capacity of T.25
Patient Mary
Vulnerability of Mary



Prevention schema: certain types of events bring about situations of a given type, such that other types of situations are impossible, resulting in the prevention of the types of events that are triggered by these situations

Reference Ontology for Security Engineering (ROSE)

Home > Conceptual Modeling > Conference paper

An Ontology of Security from a Risk Treatment Perspective

Conference paper | First Online: 10 October 2022
pp 365–379 | Cite this conference paper

Download book PDF Download book EPUB

Conceptual Modeling

(ER 2022)

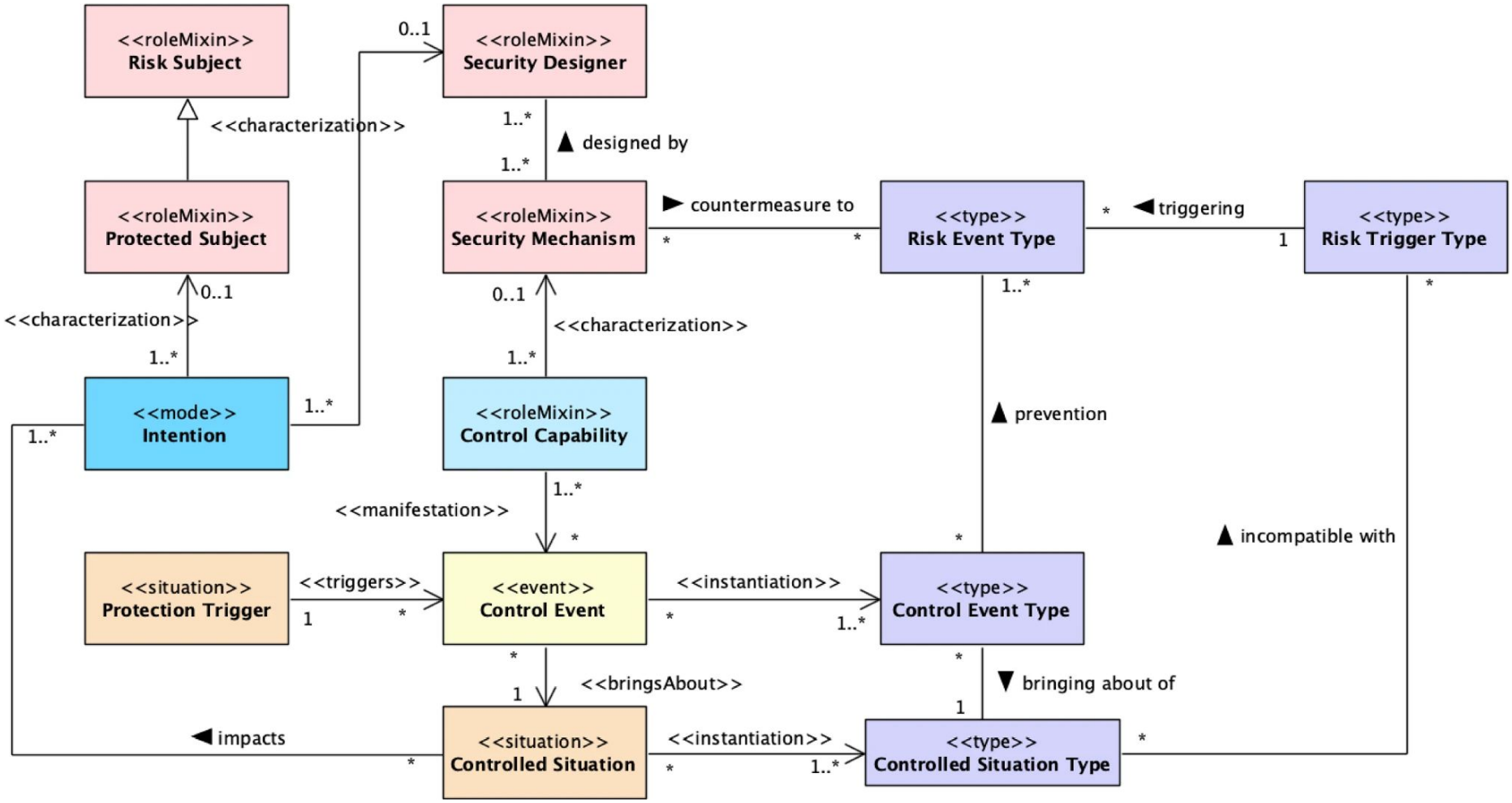
Ítalo Oliveira, Tiago Prince Sales, Riccardo Baratella, Mattia Fumagalli & Giancarlo Guizzardi

Part of the book series: Lecture Notes in Computer Science ((LNCS,volume 13607))

Included in the following conference series:
International Conference on Conceptual Modeling

Sections | Figures | References

The concept of security mechanism



Toward a phishing attack ontology

Ítalo Oliveira*, Rodrigo F. Calhau, Giancarlo Guizzardi

*Corresponding author for this work

Semantics, Cybersecurity & Services, Digital Society Institute

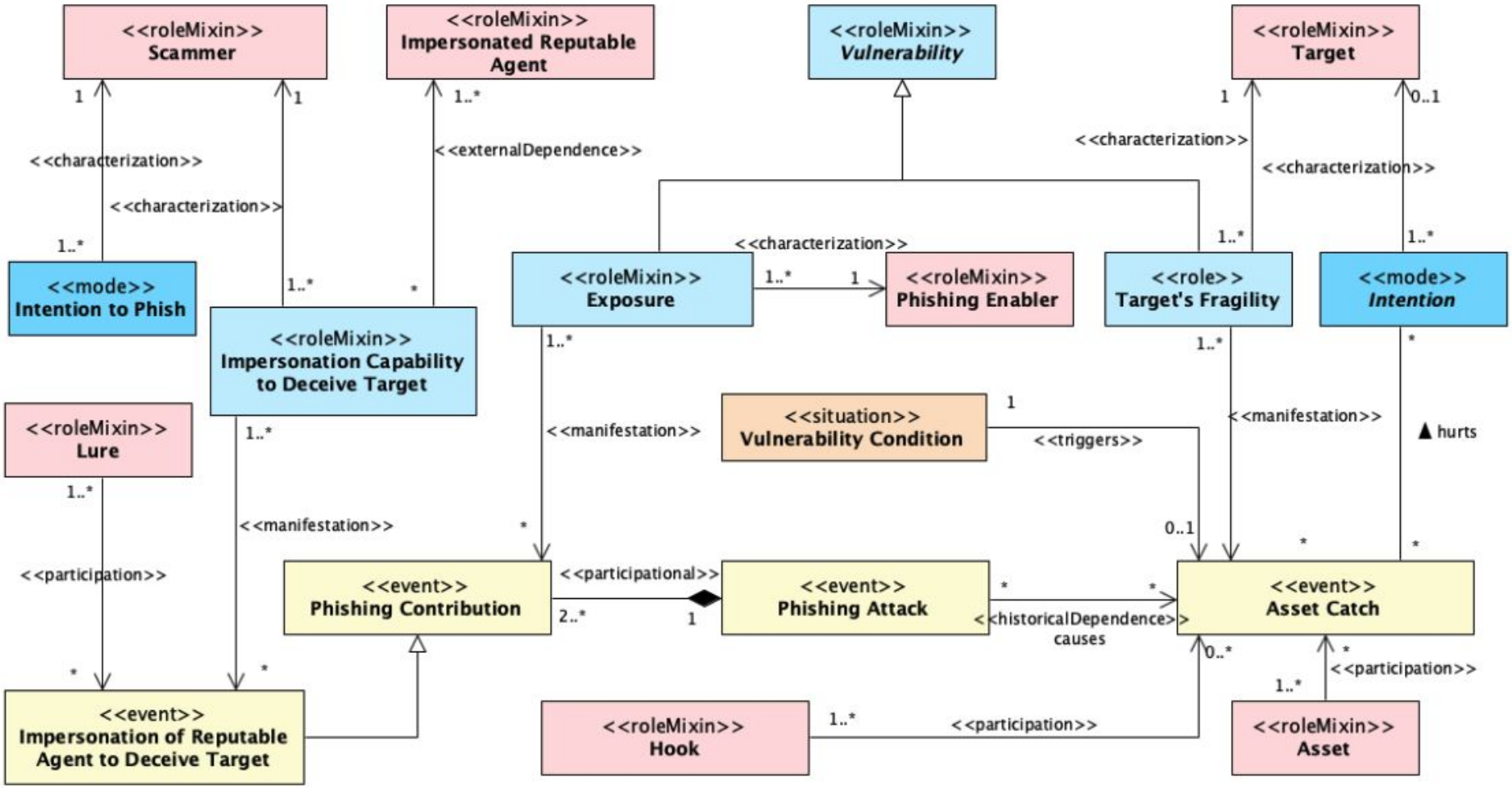
Research output: Chapter in Book/Report/Conference proceeding › Conference contribution › Academic › peer-review

Abstract

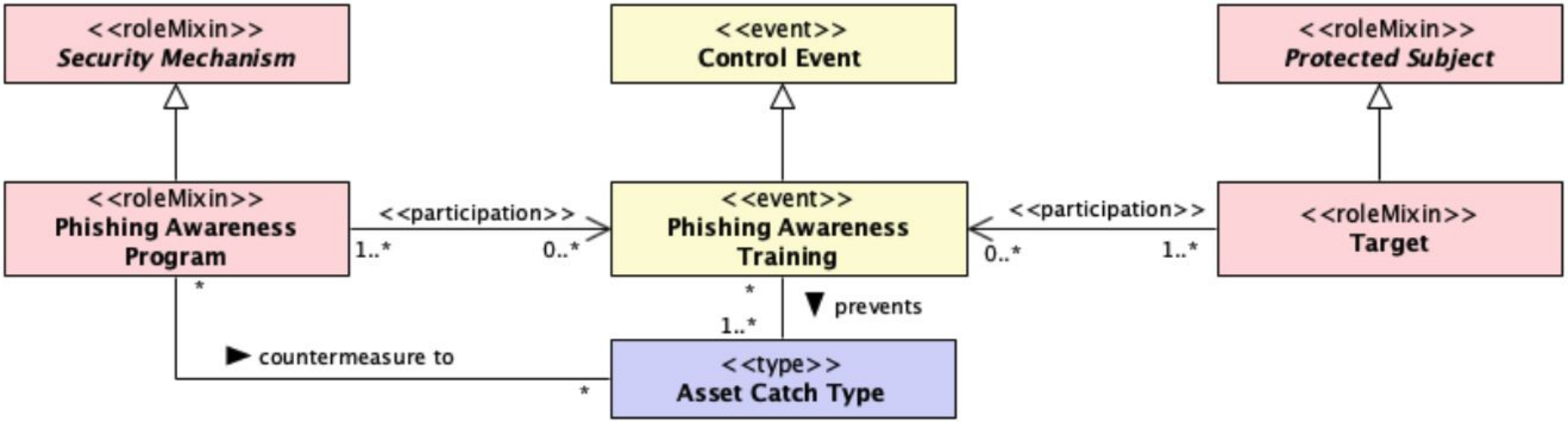
Phishing attacks are the most common form of social engineering where attackers intend to deceive targeted people into revealing sensitive information or installing malware. To understand the dynamics of phishing attacks and design suitable countermeasures, particularly the promotion of phishing awareness, cybersecurity researchers have proposed several domain conceptual models and lightweight ontologies. Despite the growing literature in ontology engineering highlighting the advantages of employing upper and reference ontologies for domain modeling, current phishing attack models lack ontological foundations. As a result, they suffer from a number of shortcomings, such as false agreements, informality, and limited interoperability. To address this gap, we propose a Phishing Attack Ontology (PHATO) grounded in the Reference Ontology for Security Engineering (ROSE) and the Common Ontology of Value and Risk (COVER), which are both founded in the Unified Foundational Ontology (UFO). Our proposal is represented through the OntoUML ontology-driven conceptual modeling language, benefiting from its ecosystem of tools and domain ontologies. We also discuss some implications of PHATO for the design of anti-phishing countermeasures.

Original language	English
Title of host publication	ER-Companion 2023
Subtitle of host publication	Companion Proceedings of the 42nd International Conference on Conceptual Modeling: ER Forum, 7th SCME, Project Exhibitions, Posters and Demos, and Doctoral Consortium co-located with ER 2023 Lisbon, Portugal, November 06-09, 2023
Editors	Claudenir M. Fonseca, José Borbinha, Giancarlo Guizzardi
Place of Publication	Aachen
Publisher	CEUR

Phishing Attack Ontology (PHATO)



Designing anti-phishing measures



Ontology-based security modeling patterns

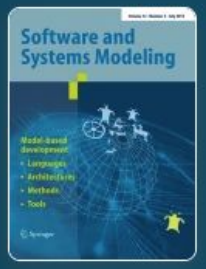
Home > Software and Systems Modeling > Article

Ontology-based security modeling in ArchiMate

Special Section Paper | Open access | Published: 16 February 2024
(2024) Cite this article

Download PDF

You have full access to this open access article



Ítalo Oliveira, Tiago Prince Sales, João Paulo A. Almeida, Riccardo Baratella, Mattia Fumagalli & Giancarlo Guizzardi

ArchiMate's Risk and Security Overlay

There are at least the following ways of action of a CONTROL EVENT, so that THREAT EVENTS or LOSS EVENTS are ultimately prevented:

1. The THREAT AGENT can be disabled by losing its THREAT CAPABILITY. For example, when tranquilizer darts temporarily disable the threatening capacities of large animals.

2. …

3. …

There are at least the following ways of action of a CONTROL EVENT, so that THREAT EVENTS or LOSS EVENTS are ultimately prevented:

1. The THREAT AGENT can be disabled by losing its THREAT CAPABILITY. For example, when tranquilizer darts temporarily disable the threatening capacities of large animals.

2. The very THREAT AGENT can be destroyed or moved away from the scene. For instance, when missiles intercept dangerous projectiles or when inspections enforce regulations about the replacement of defective components.

3. …

There are at least the following ways of action of a CONTROL EVENT, so that THREAT EVENTS or LOSS EVENTS are ultimately prevented:

1. The THREAT AGENT can be disabled by losing its THREAT CAPABILITY. For example, when tranquilizer darts temporarily disable the threatening capacities of large animals.

2. The very THREAT AGENT can be destroyed or moved away from the scene. For instance, when missiles intercept dangerous projectiles or when inspections enforce regulations about the replacement of defective components.

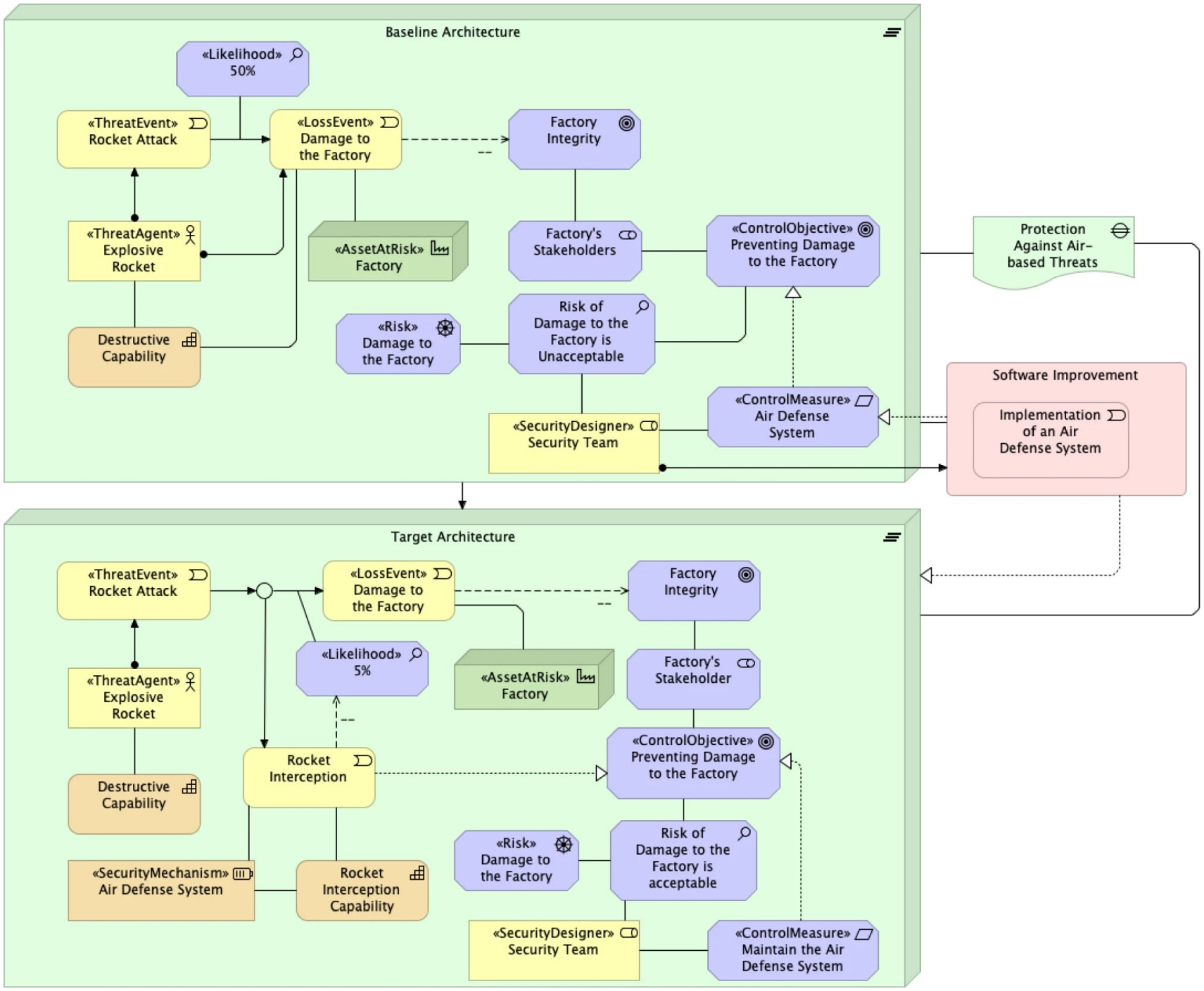
3. The THREAT AGENT can be dissuaded from its GOALS. For example, warnings, security cameras, and walls that demotivate thieves from starting their criminal activities against a facility.

4. The ASSETS AT RISK can be hardened, that is, their VULNERABILITIES can be removed. Say, when a piece of software provides updates for a given program by removing potentially problematic code.

5. …

4. The ASSETS AT RISK can be hardened, that is, their VULNERABILITIES can be removed. Say, when a piece of software provides updates for a given program by removing potentially problematic code.

5. The very ASSET AT RISK can be moved away from the scene. For instance, when customers and employees are blocked from accessing certain dangerous spaces in a factory.


Baseline Architecture
«Likelihood» 50%
«ThreatEvent» Rocket Attack
«LossEvent» Damage to the Factory
Factory Integrity
«ThreatAgent» Explosive Rocket
«AssetAtRisk» Factory
Factory's Stakeholders
«ControlObjective» Preventing Damage to the Factory
Protection Against Air-based Threats
Destructive Capability
«Risk» Damage to the Factory
Risk of Damage to the Factory is Unacceptable
Software Improvement
«ControlMeasure» Air Defense System
Implementation of an Air Defense System
«SecurityDesigner» Security Team
Target Architecture
«ThreatEvent» Rocket Attack
«LossEvent» Damage to the Factory
Factory Integrity
«Likelihood» 5%
«AssetAtRisk» Factory
Factory's Stakeholder
«ThreatAgent» Explosive Rocket
«ControlObjective» Preventing Damage to the Factory
Rocket Interception
Destructive Capability
«Risk» Damage to the Factory
Risk of Damage to the Factory is acceptable
«SecurityMechanism» Air Defense System
Rocket Interception Capability
«SecurityDesigner» Security Team
«ControlMeasure» Maintain the Air Defense System

Shortcomings of the D3FEND cybersecurity model

IOS Press Ebooks

Your cart is empty

Welcome Universiteit | My account | Log off

IOS Press

Home | Ebooks | Open Access | About IOS Press | Contact | FAQ | My Access

Search

> SEARCH

Browse by subject

- Computer Sciences, Mathematics & Statistics
- Environmental & Energy Sciences
- Humanities & Social Sciences
- Medicine & Health
- Natural Sciences
- Technology, Engineering & Architecture

Boosting D3FEND: Ontological Analysis and Recommendations

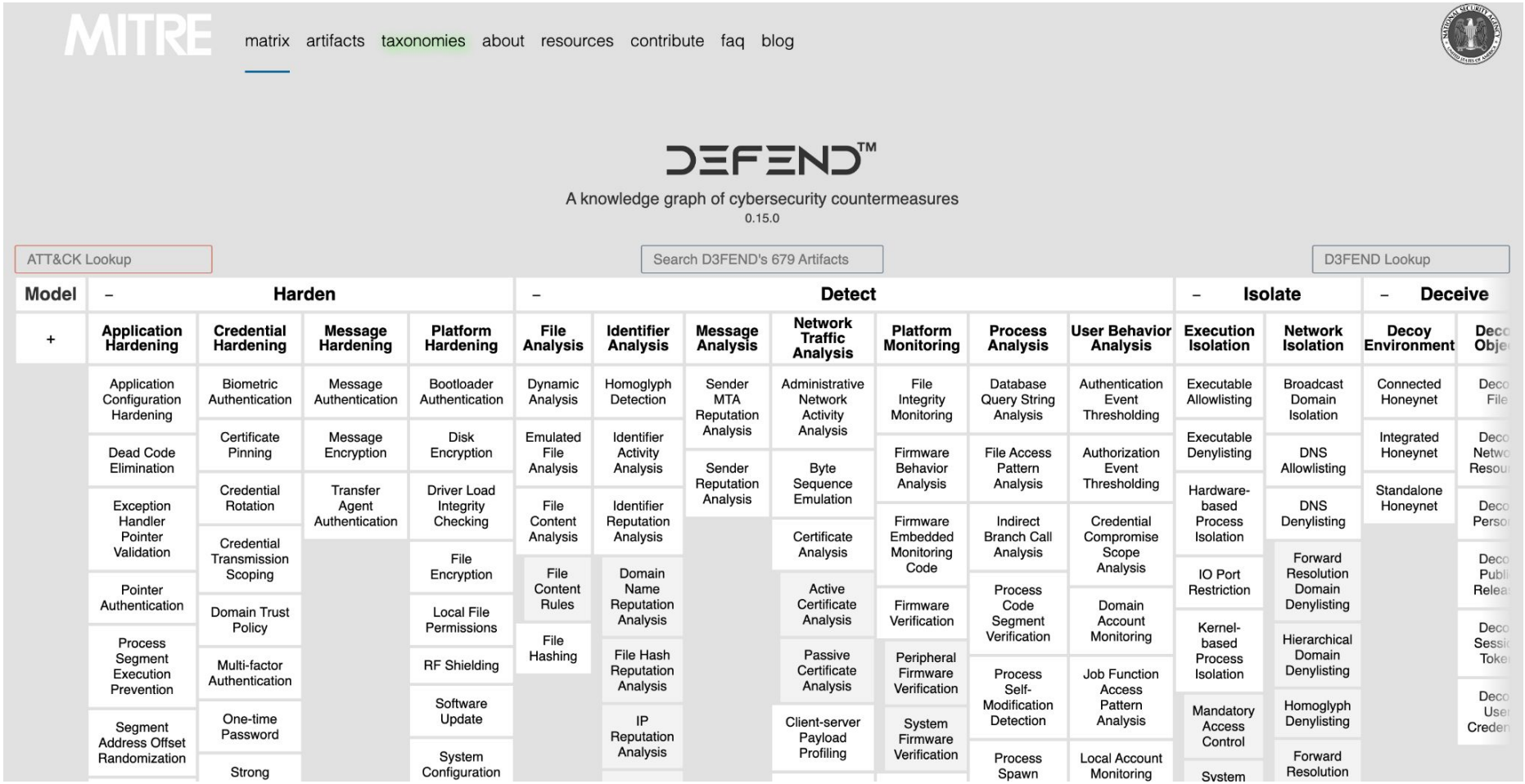
Authors	Ítalo Oliveira, Gal Engelberg, Pedro Paulo F. Barcelos, Tiago Prince Sales, Mattia Fumagalli, Riccardo Baratella, Dan Klein, Giancarlo Guizzardi
Pages	334 - 348
DOI	10.3233/FAIA231138
Category	Research Article
Series	Frontiers in Artificial Intelligence and Applications
Ebook	Volume 377: Formal Ontology in Information Systems

Download

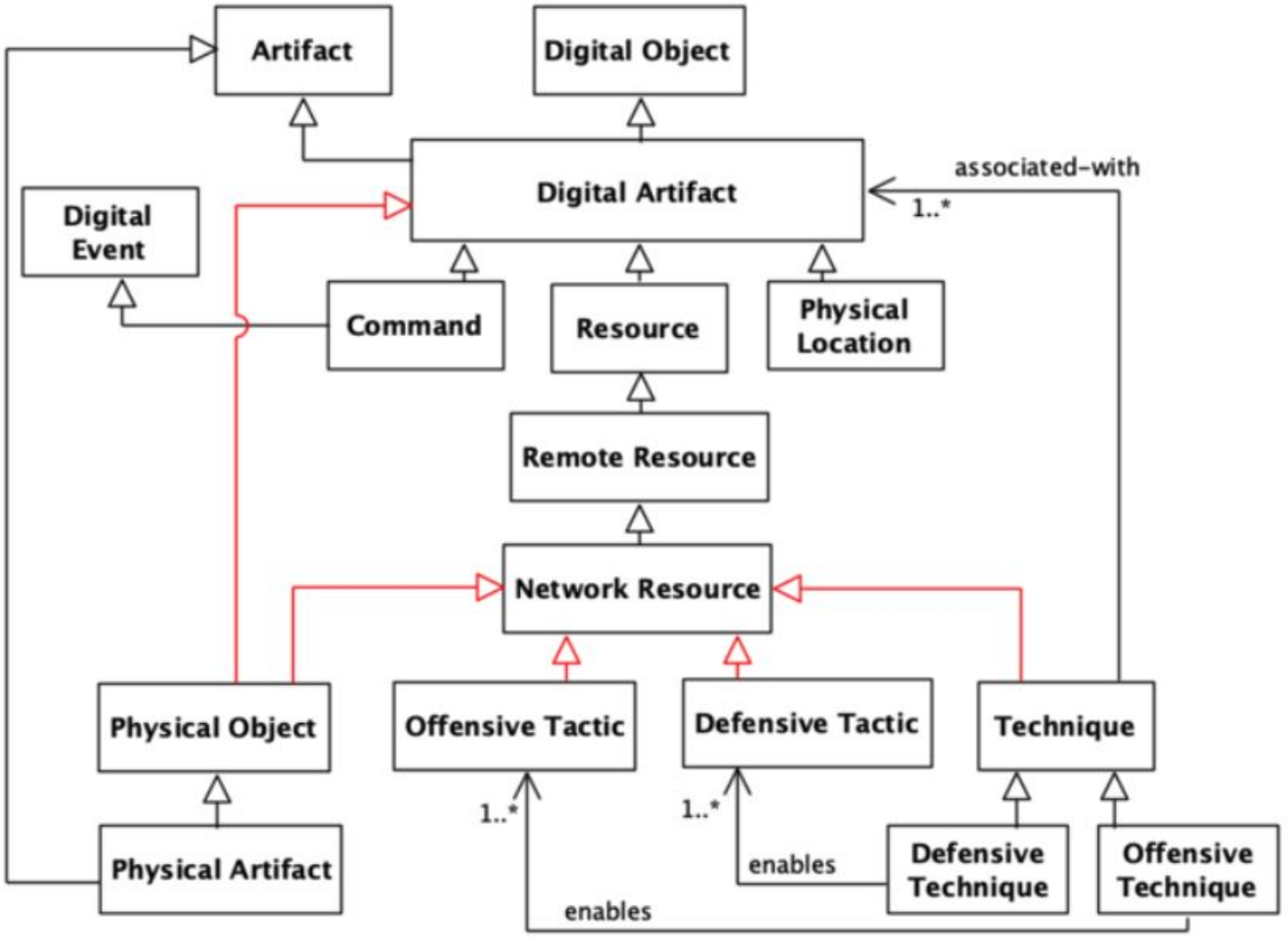
(cc) BY-NC

Abstract

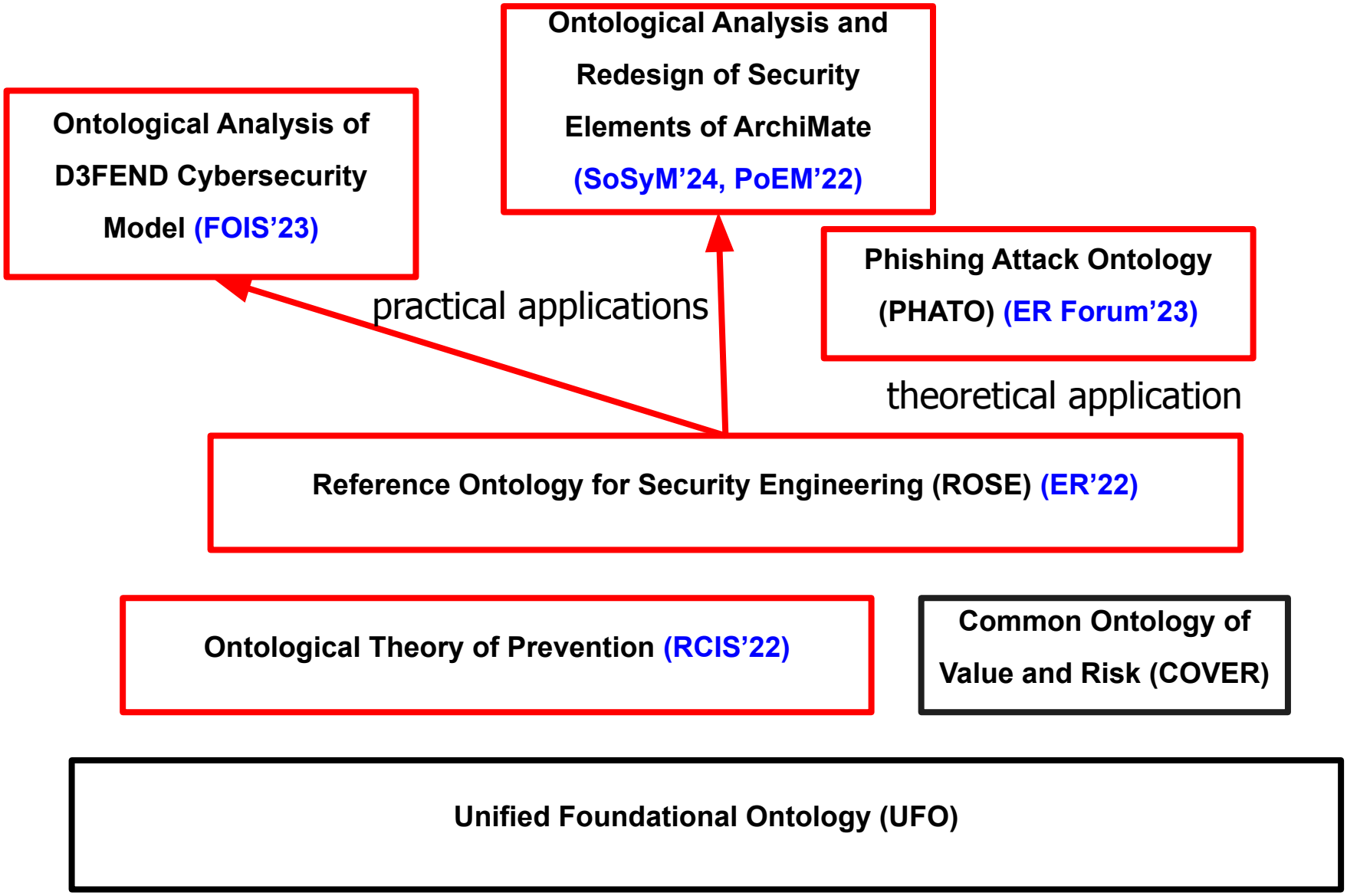
Formal Ontology is a discipline whose business is to develop formal theories about general aspects of reality such as identity, dependence, parthood, truthmaking, causality, etc. A foundational ontology is a specific consistent set of these ontological theories that support activities such as domain analysis, conceptual clarification, and meaning negotiation. A (well-founded) core ontology specifies, under a foundational ontology, the central concepts and relations of a given domain. Foundational and core ontologies can be seen as ontology engineering frameworks to systematically address the laborious task of building large (more specific) domain ontologies. However, both


MITRE
matrix artifacts taxonomies about resources contribute faq blog
D3FEND™
A knowledge graph of cybersecurity countermeasures
0.15.0
ATT&CK Lookup
Search D3FEND's 679 Artifacts
D3FEND Lookup
Model
Harden
Application Hardening
Application Configuration Hardening
Dead Code Elimination
Exception Handler Pointer Validation
Pointer Authentication
Process Segment Execution Prevention
Segment Address Offset Randomization
Credential Hardening
Biometric Authentication
Certificate Pinning
Credential Rotation
Credential Transmission Scoping
Domain Trust Policy
Multi-factor Authentication
One-time Password
Strong
Message Hardening
Message Authentication
Message Encryption
Transfer Agent Authentication
Platform Hardening
Bootloader Authentication
Disk Encryption
Driver Load Integrity Checking
File Encryption
Local File Permissions
RF Shielding
Software Update
System Configuration
Detect
File Analysis
Dynamic Analysis
Emulated File Analysis
File Content Analysis
File Content Rules
File Hashing
Identifier Analysis
Homoglyph Detection
Identifier Activity Analysis
Identifier Reputation Analysis
Domain Name Reputation Analysis
File Hash Reputation Analysis
IP Reputation Analysis
Message Analysis
Sender MTA Reputation Analysis
Sender Reputation Analysis
Network Traffic Analysis
Administrative Network Activity Analysis
Byte Sequence Emulation
Certificate Analysis
Active Certificate Analysis
Passive Certificate Analysis
Client-server Payload Profiling
Platform Monitoring
File Integrity Monitoring
Firmware Behavior Analysis
Firmware Embedded Monitoring Code
Firmware Verification
Peripheral Firmware Verification
System Firmware Verification
Process Analysis
Database Query String Analysis
File Access Pattern Analysis
Indirect Branch Call Analysis
Process Code Segment Verification
Process Self-Modification Detection
Process Spawn
User Behavior Analysis
Authentication Event Thresholding
Authorization Event Thresholding
Credential Compromise Scope Analysis
Domain Account Monitoring
Job Function Access Pattern Analysis
Local Account Monitoring
Isolate
Execution Isolation
Executable Allowlisting
Executable Denylisting
Hardware-based Process Isolation
IO Port Restriction
Kernel-based Process Isolation
Mandatory Access Control
Network Isolation
Broadcast Domain Isolation
DNS Allowlisting
DNS Denylisting
Forward Resolution Domain Denylisting
Hierarchical Domain Denylisting
Homoglyph Denylisting
Forward Resolution
Deceive
Decoy Environment
Connected Honeynet
Integrated Honeynet
Standalone Honeynet

A slice of the D3FEND model



Research Outcomes



Transparency, Reproducibility, and Documentation

Ontology of Prevention

- PURL: https://purl.org/prevention-ontology

Reference Ontology for Security Engineering (ROSE)

- PURL: https://purl.org/security-ontology

Ontological Analysis of D3FEND Cybersecurity Model

- PURL: https://purl.org/d3fend-analysis

Phishing Attack Ontology (PHATO)

- PURL: https://purl.org/phishing-ontology

Ontology-based Security Modeling in ArchiMate

- DOI: https://doi.org/10.5281/zenodo.10005209
- Website: https://unibz-core.github.io/security-archimate/

Core Publications

In peer-reviewed journal

- Oliveira, Í., Sales, T.P., Almeida, J.P.A., Baratella, R., Fumagalli, M., Guizzardi, G. (2024). *Ontology-based Security Modeling in ArchiMate*. Software and Systems Modeling. https://doi.org/10.1007/s10270-024-01149-1

In peer-reviewed international conference proceedings

- Oliveira, Í., Fumagalli, M., Prince Sales, T., Guizzardi, G. (2021). *How FAIR are Security Core Ontologies? A Systematic Mapping Study*. In: Cherfi, S., Perini, A., Nurcan, S. (eds) Research Challenges in Information Science. RCIS 2021. Lecture Notes in Business Information Processing, vol 415. Springer, Cham. https://doi.org/10.1007/978-3-030-75018-3_7

- Baratella, R., Fumagalli, M., Oliveira, Í., Guizzardi, G. (2022). *Understanding and Modeling Prevention*. In: Guizzardi, R., Ralyté, J., Franch, X. (eds) Research Challenges in Information Science. RCIS 2022. Lecture Notes in Business Information Processing, vol 446. Springer, Cham. https://doi.org/10.1007/978-3-031-05760-1_23

Core Publications

In peer-reviewed international conference proceedings

- Oliveira, Í., Sales, T.P., Baratella, R., Fumagalli, M., Guizzardi, G. (2022). *An Ontology of Security from a Risk Treatment Perspective*. In: Ralyté, J., Chakravarthy, S., Mohania, M., Jeusfeld, M.A., Karlapalem, K. (eds) Conceptual Modeling. ER 2022. Lecture Notes in Computer Science, vol 13607. Springer, Cham. https://doi.org/10.1007/978-3-031-17995-2_26

- Oliveira, Í., Sales, T.P., Almeida, J.P.A., Baratella, R., Fumagalli, M., Guizzardi, G. (2022). *Ontological Analysis and Redesign of Security Modeling in ArchiMate*. In: Barn, B.S., Sandkuhl, K. (eds) The Practice of Enterprise Modeling. PoEM 2022. Lecture Notes in Business Information Processing, vol 456. Springer, Cham. https://doi.org/10.1007/978-3-031-21488-2_6

- Oliveira, Ítalo., Engelberg, G., Barcelos, P.P.F., Sales, T.P., Fumagalli, M., Baratella, R., Klein, D., Guizzardi, G., (2023) *Boosting D3FEND: Ontological analysis and recommendations*. In: Formal Ontology in Information Systems: Proceedings of the Thirteenth International Conference (FOIS 2023). Vol. 377. Frontiers in Artificial Intelligence and Applications. IOS Press. https://ebooks.iospress.nl/doi/10.3233/FAIA231138

Core Publications

In peer-reviewed international workshop

- Oliveira, Ítalo, Calhau, R. F., Guizzardi, G. (2023). *Toward a phishing attack ontology*. In: ER2023: Companion Proceedings of the 42nd International Conference on Conceptual Modeling: ER Forum, 7th SCME, Project Exhibitions, Posters and Demos, and Doctoral Consortium, November 06-09, 2023, Lisbon, Portugal. https://ceur-ws.org/Vol-3618/forum_paper_25.pdf

Additional Publications

In peer-reviewed journal

- Mário de Oliveira Rodrigues, C., Bezerra, C., Freitas, F. and Oliveira, I., 2020. *Handling Crimes of Omission by reconciling a criminal core ontology with UFO*. Applied Ontology, 15(1), pp.7-39. https://doi.org/10.3233/AO-200223

In peer-reviewed international conference proceedings

- Calhau, R.F., Prince Sales, T., Oliveira, Í., Kokkula, S., Ferreira Pires, L., Cameron, D., Guizzardi, G. and Almeida, J.P.A. (2024). *A System Core Ontology for Capability Emergence Modeling*. In: Proper, H.A., Pufahl, L., Karastoyanova, D., van Sinderen, M., Moreira, J. (eds) Enterprise Design, Operations, and Computing. EDOC 2023. Lecture Notes in Computer Science, vol 14367. Springer, Cham. https://doi.org/10.1007/978-3-031-46587-1_1
- Fumagalli, M., Engelberg, G., Sales, T.P., Oliveira, Í., Klein, D., Soffer, P., Baratella, R. and Guizzardi, G. (2023). *On the Semantics of Risk Propagation*. In: Nurcan, S., Opdahl, A.L., Mouratidis, H., Tsohou, A. (eds) Research Challenges in Information Science: Information Science and the Connected World. RCIS 2023. Lecture Notes in Business Information Processing, vol 476. Springer, Cham. https://doi.org/10.1007/978-3-031-33080-3_5

Future work (ongoing)

- Complete formalization and testing of the theory of prevention along with UFO. With:
  - Giancarlo Guizzardi, Claudenir Fonseca, Tiago Prince Sales (University of Twente),
  - Enrico Franconi (Free University of Bozen-Bolzano),
  - Daniele Porello (Università degli Studi di Genova).

- Discrete event simulations of Enterprise Risk Management models with ROSE & PHATO. With:
  - Prof. Gerd Wagner (Brandenburg University of Technology).
  - Glenda Amaral (University of Twente, Brazilian Central Bank).

- Well-founded cybersecurity model for threat intelligence. With:
  - Andrea Continella and Thijs van Ede (University of Twente),
  - Dan Klein and Gal Engelberg (Accenture Labs, Israel).

… and much more.

An Ontological Approach to Security Modeling

Ítalo José da Silva Oliveira

https://italojsoliveira.github.io/

Supervisors:

Enrico Franconi (Free University of Bozen-Bolzano)

Giancarlo Guizzardi (University of Twente)

Tiago Prince Sales (University of Twente)

External Reviewers:

Manfred Jeusfeld (University of Skövde)

Raimundas Matulevičius (University of Tartu)

28/06/2024