Semantics, Cybersecurity, and Services (SCS)

Faculty of Electrical Engineering, Mathematics, and Computer Science (EEMCS)

AN ONTOLOGICAL LENS ON ATTACK TREES:

TOWARD ADEQUACY AND INTEROPERABILITY

Ítalo Oliveira, University of Twente & Y.digital

Stefano Nicoletti, University of Twente

Mattia Fumagalli, Free University of Bozen-Bolzano

Gal Engelberg, University of Haifa

Dan Klein, Accenture EMEA

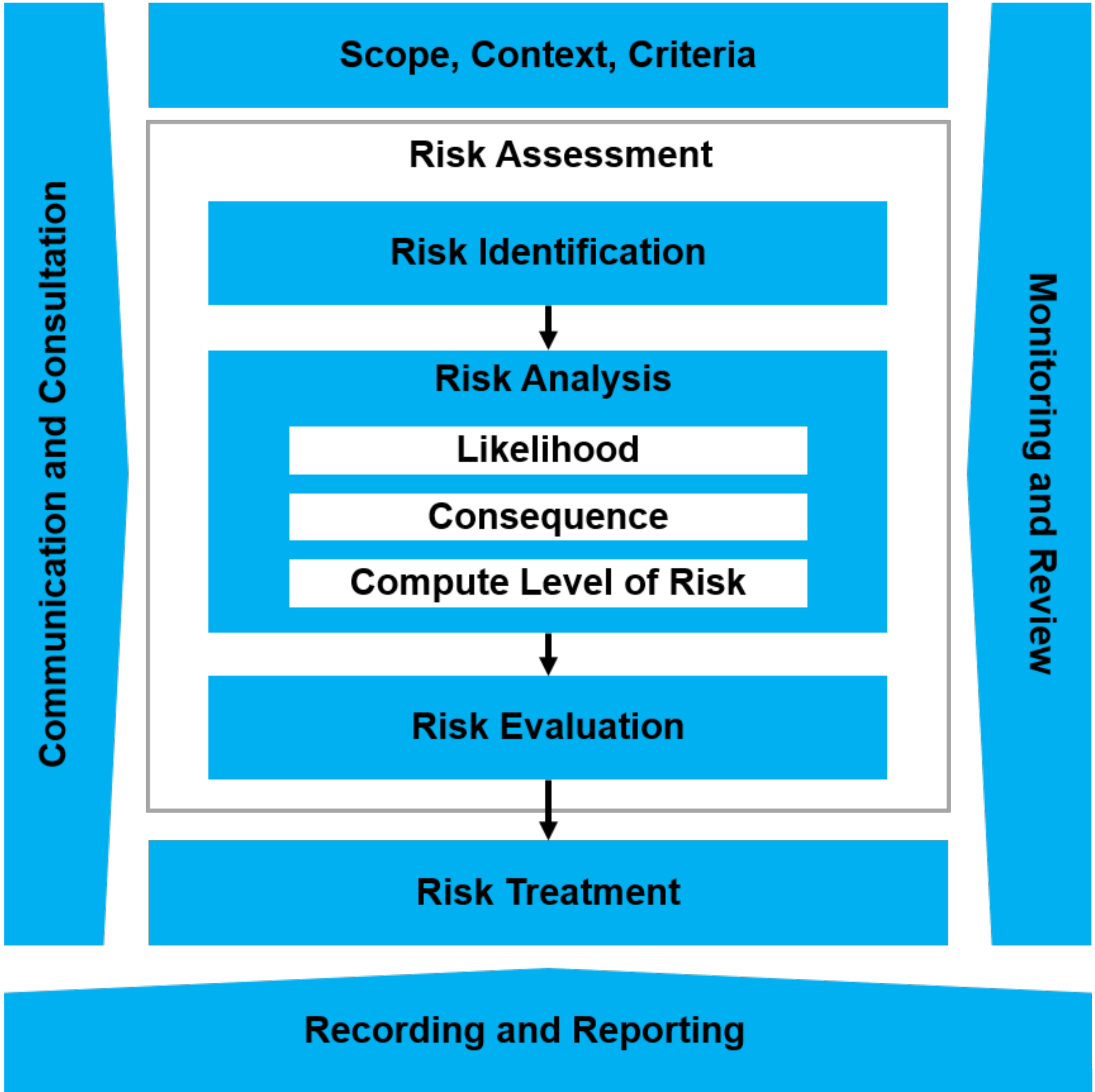
Giancarlo Guizzardi, University of Twente

https://italojsoliveira.github.io

digital
empowering humans

UNIVERSITY
OF TWENTE.

Risk Management Process - ISO 31000



Scope, Context, Criteria

Risk Assessment

Risk Identification

Risk Analysis

Likelihood

Consequence

Compute Level of Risk

Risk Evaluation

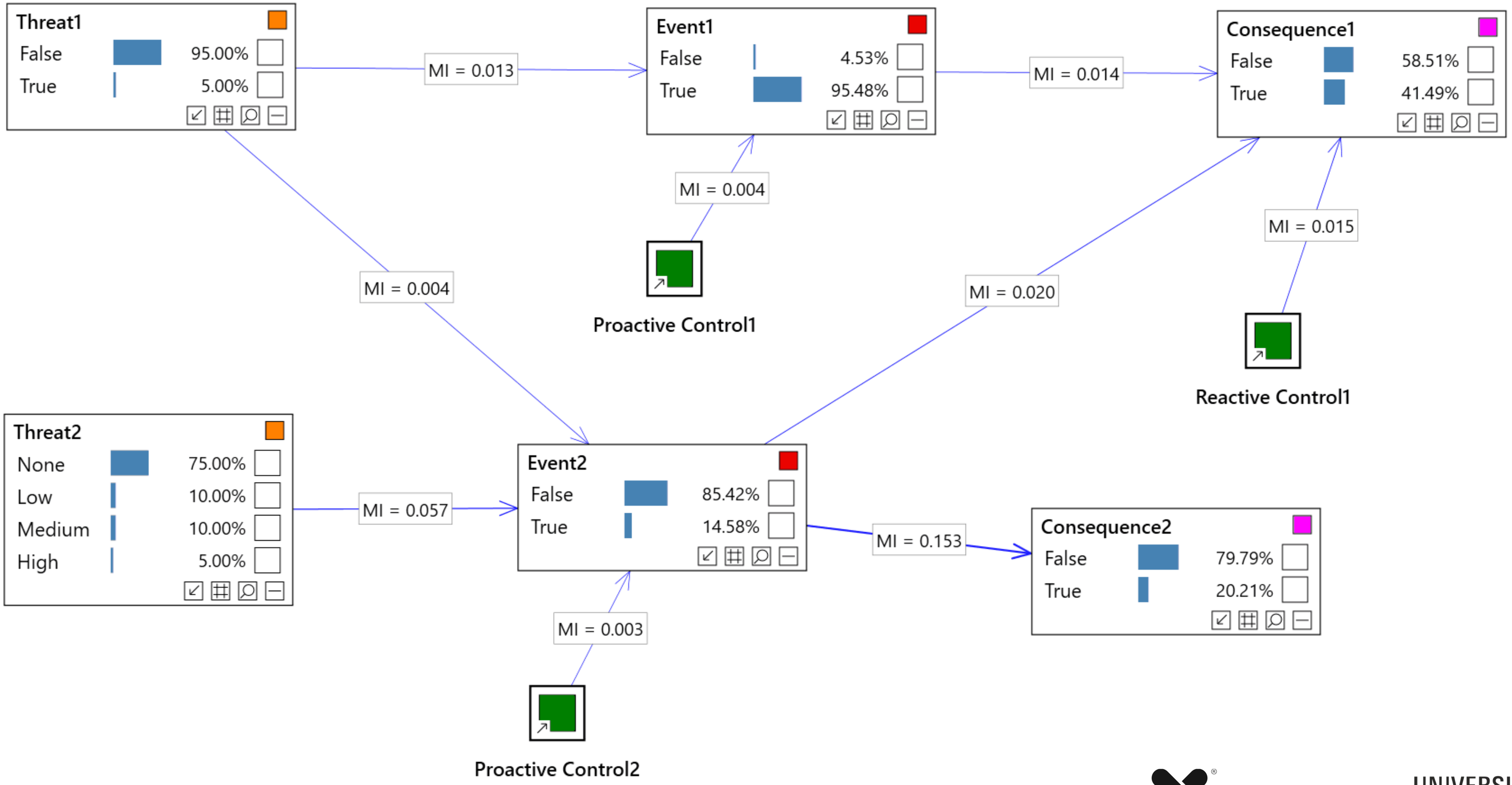
Risk Treatment

Communication and Consultation

Monitoring and Review

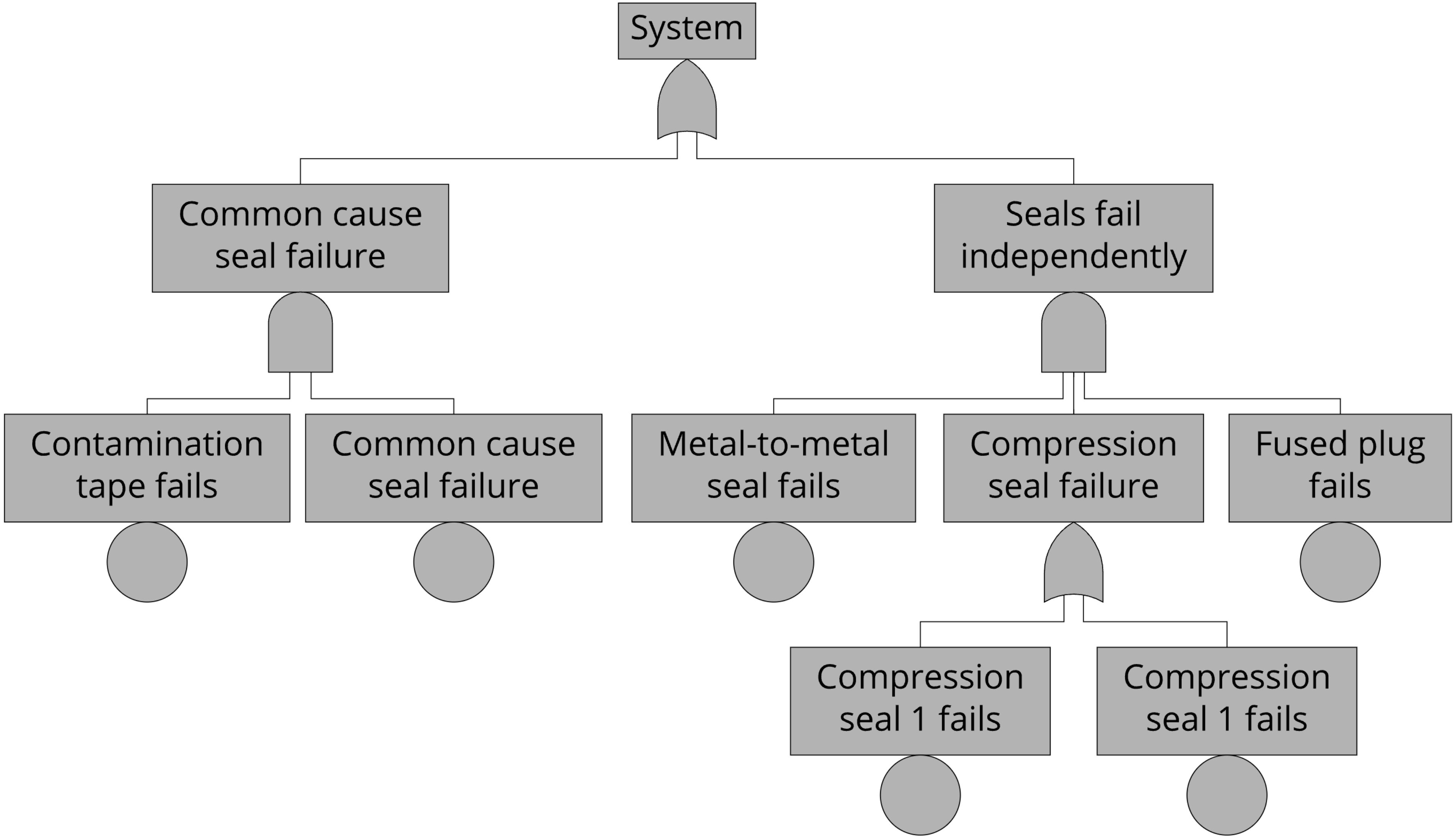
Recording and Reporting

Risk Modeling with Bayesian Networks



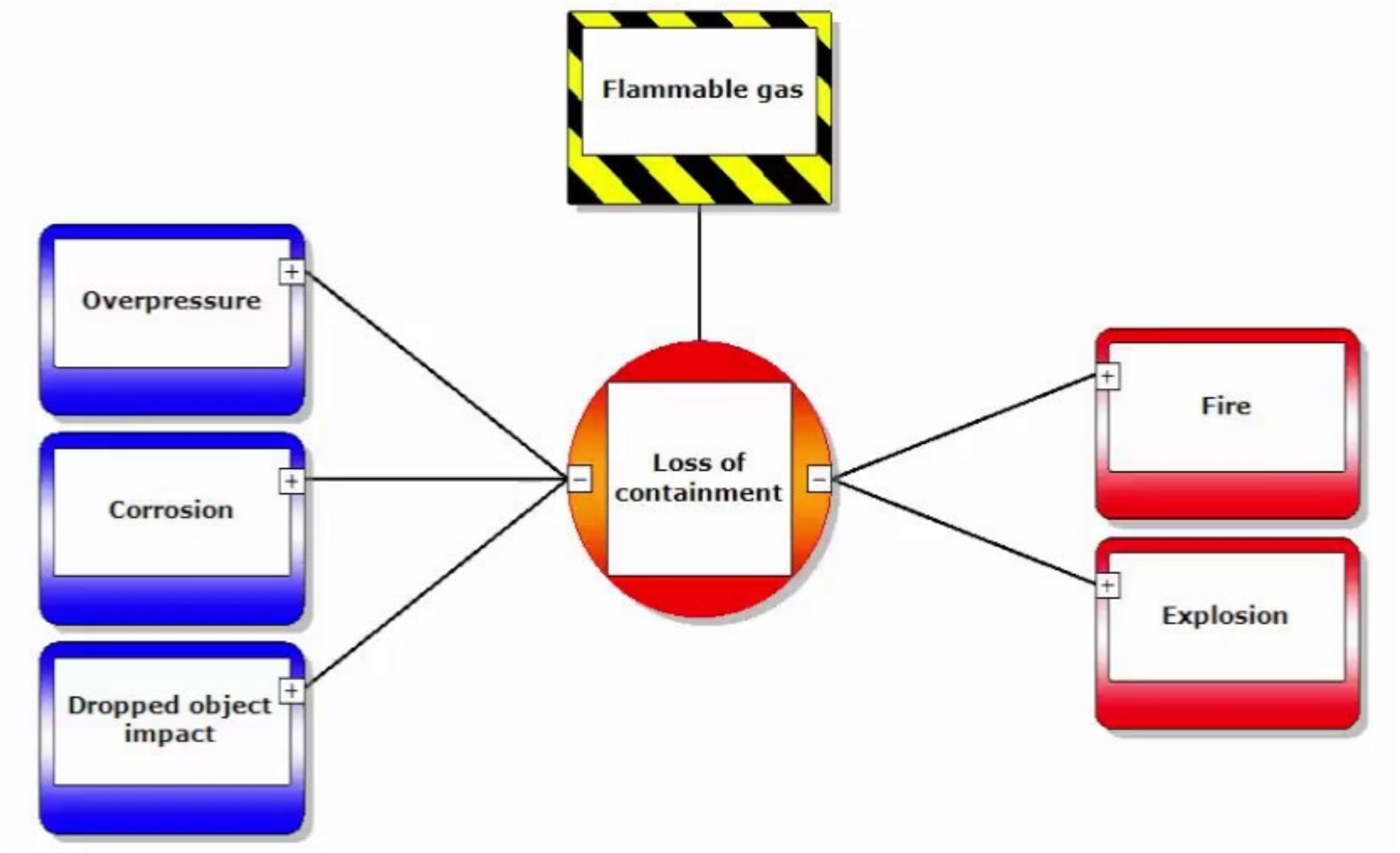
https://www.bayesserver.com/docs/modeling/risk

Fault Tree: How can a system fail?

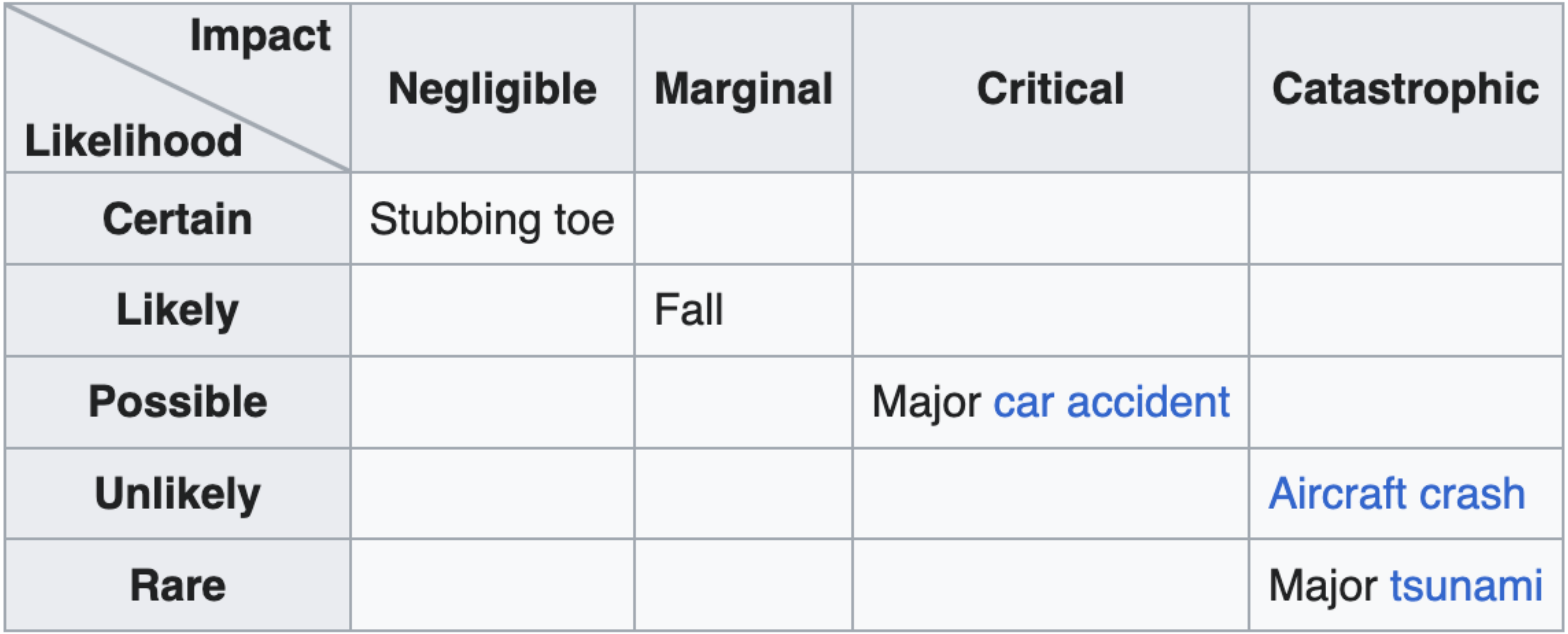


M. Stamatelatos, W. Vesely, J. Dugan, J. Fragola, J. Minarick, and J. Railsback: Fault tree handbook with aerospace applications, 2002

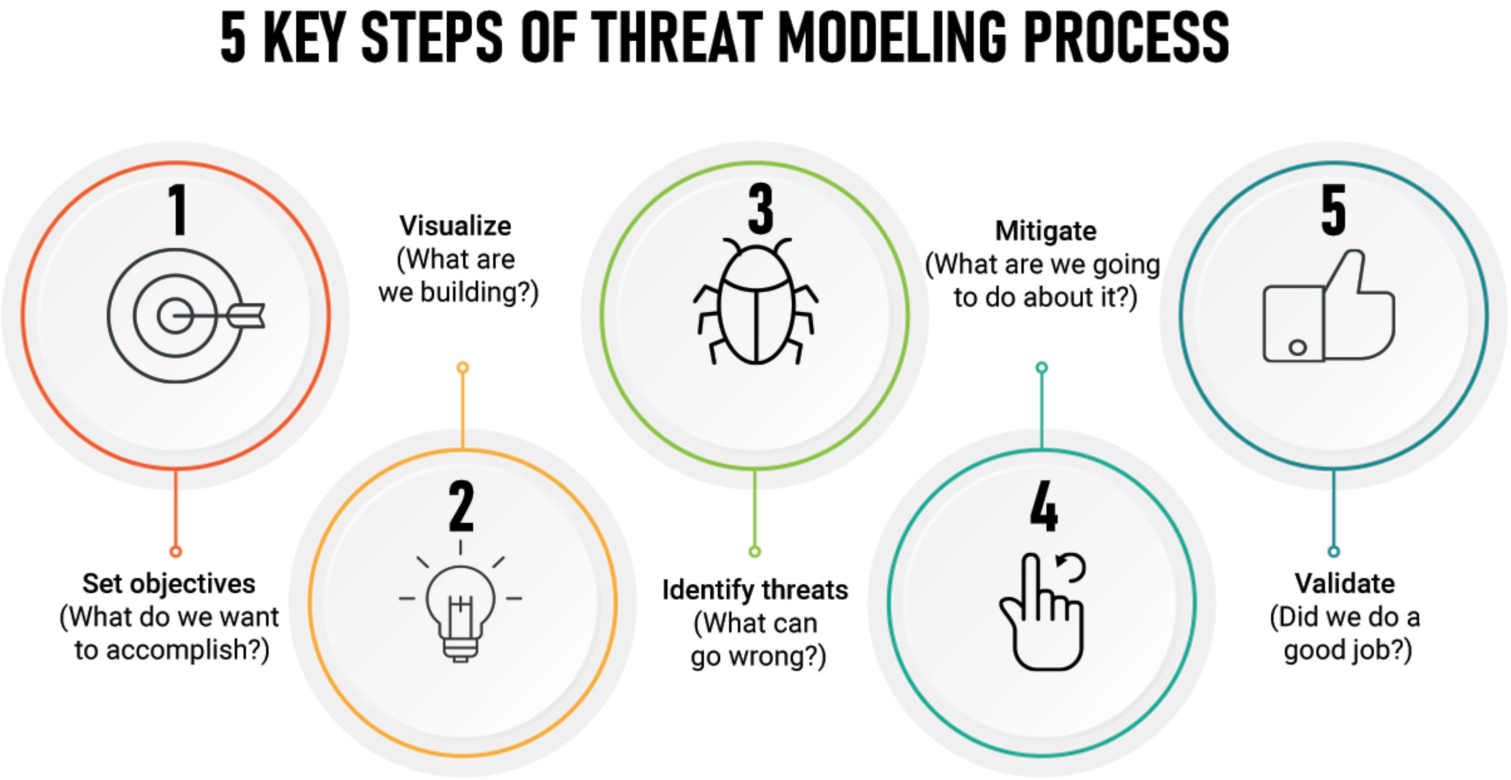
Bowtie diagram



Risk Matrix for Risk Assessment

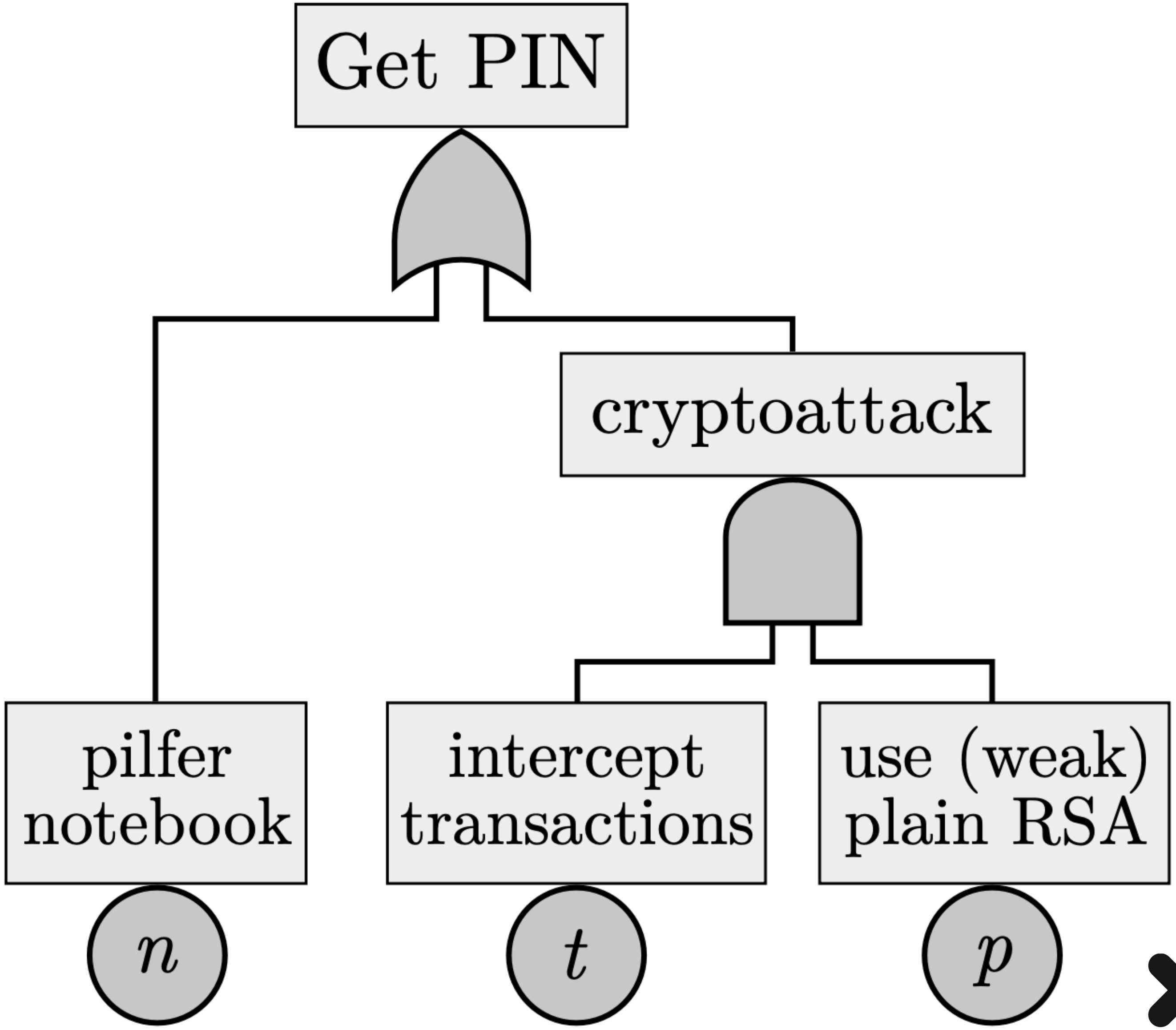


Impact Likelihood	Negligible	Marginal	Critical	Catastrophic
Certain	Stubbing toe			
Likely		Fall		
Possible			Major car accident	
Unlikely				Aircraft crash
Rare				Major tsunami

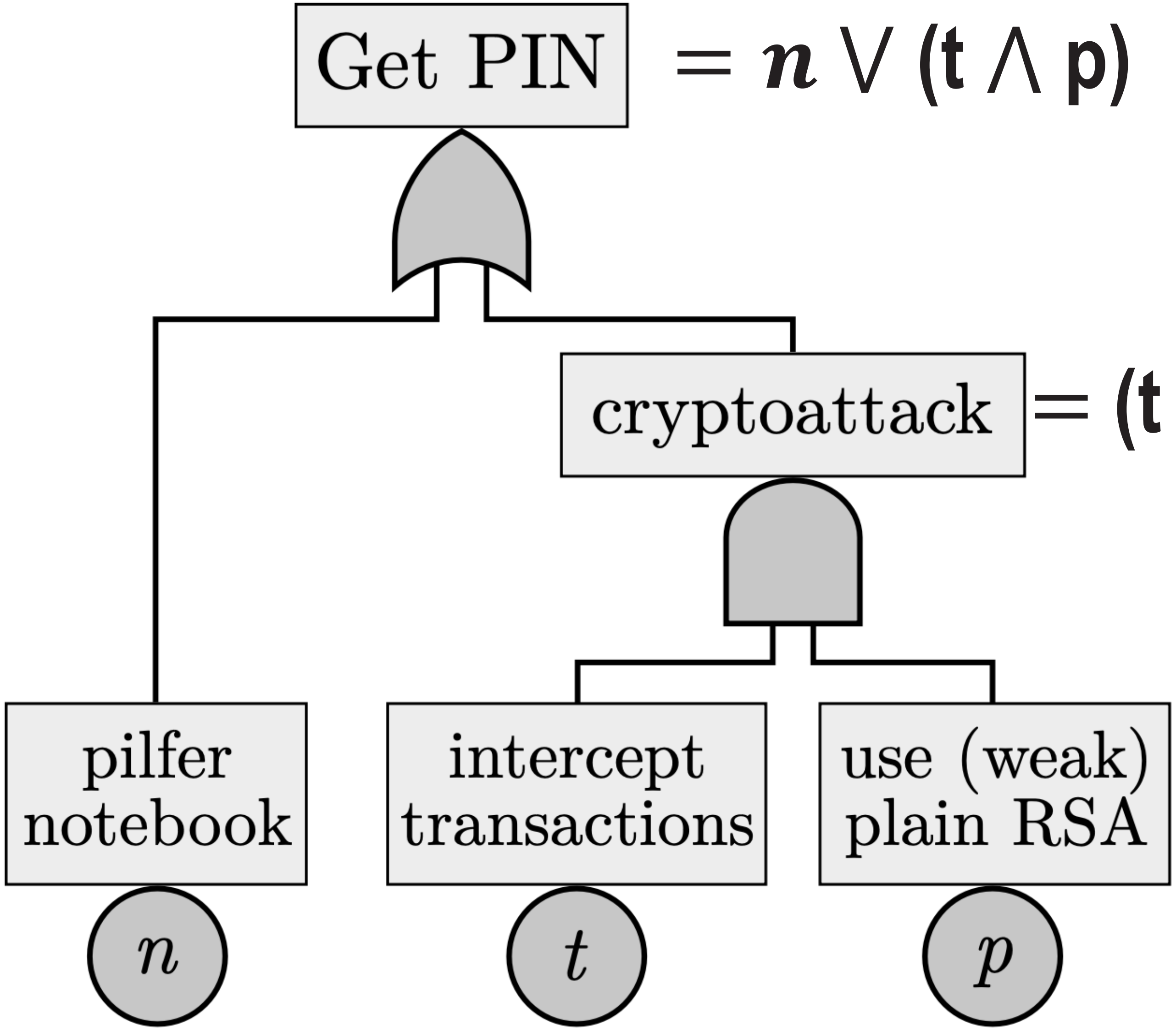


- securiCAD – https://www.bitcyber.com.sg/foreseeti-securicad
- ThreatModeler – https://www.threatmodeler.com
- IriusRisk – https://www.iriusrisk.com
- OWASP Threat Dragon – https://owasp.org/www-project-threat-dragon
- Microsoft Threat Modeling Tool – https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
- CORAS language – https://coras.sourceforge.net/index.html

Attack Trees are rooted Directed Acyclic Graphs with typed nodes.

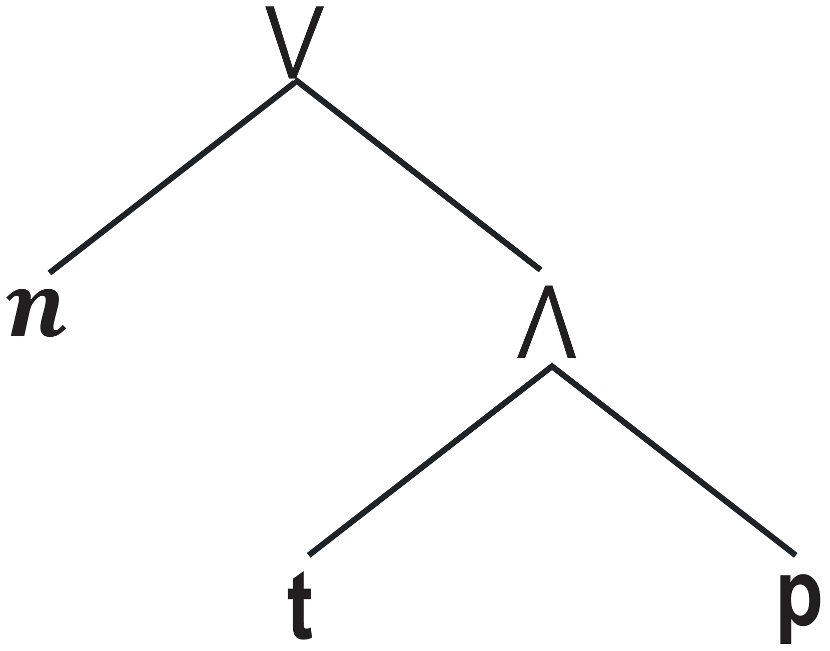


Attack Trees are rooted Directed Acyclic Graphs with typed nodes.



$$= \boldsymbol{n} \vee (\mathbf{t} \wedge \mathbf{p})$$

$$= (\mathbf{t} \wedge \mathbf{p})$$



- Successful attacks: {n}, {t, p}, {n, t, p}
- Minimal (successful) attacks: {n}, {t, p}
- Security metrics are value assignments to attacks.

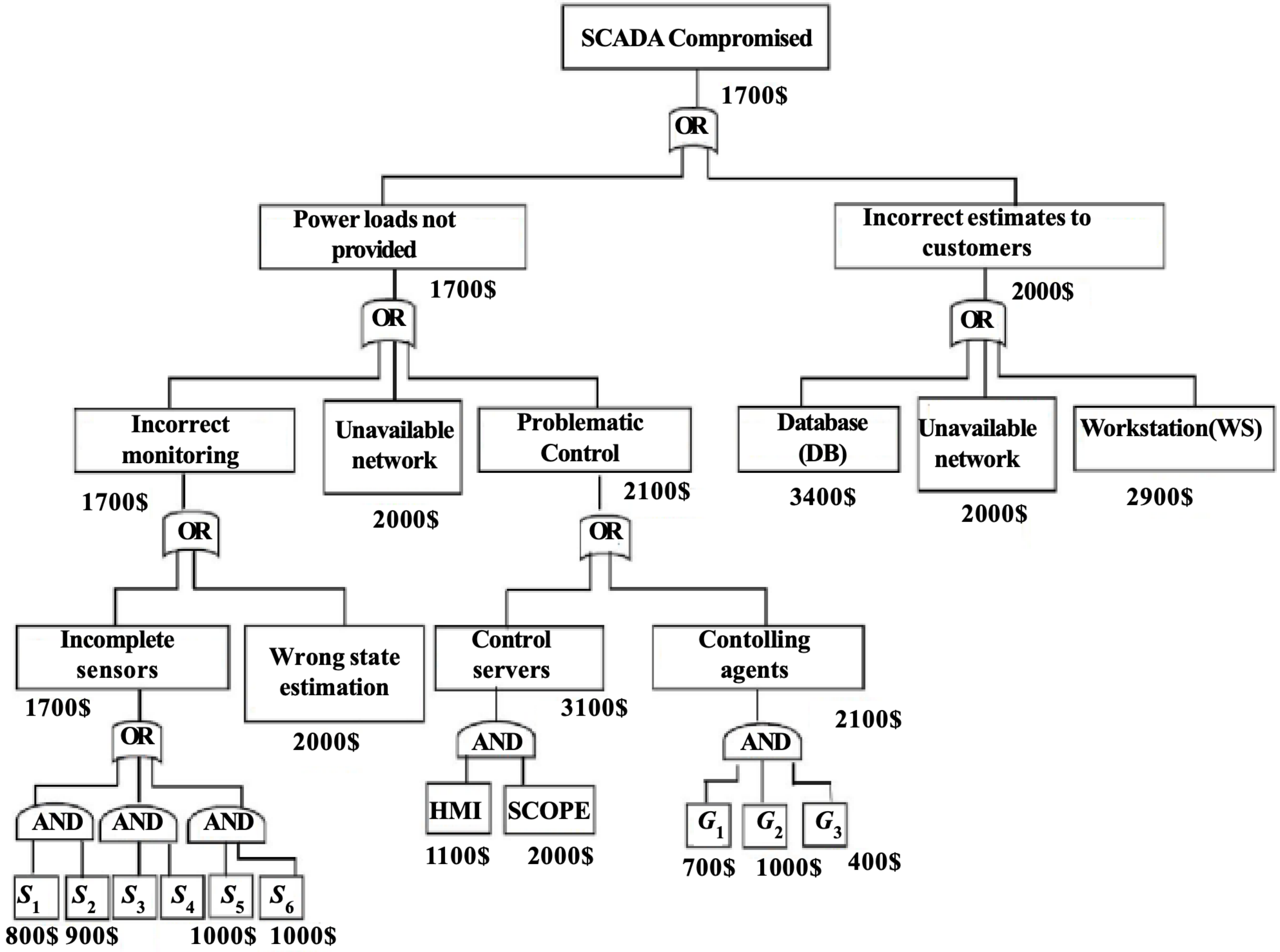
Attack trees offer three important services:

1. **CONCEPTUAL MODELING capabilities for representing security risk management scenarios.**

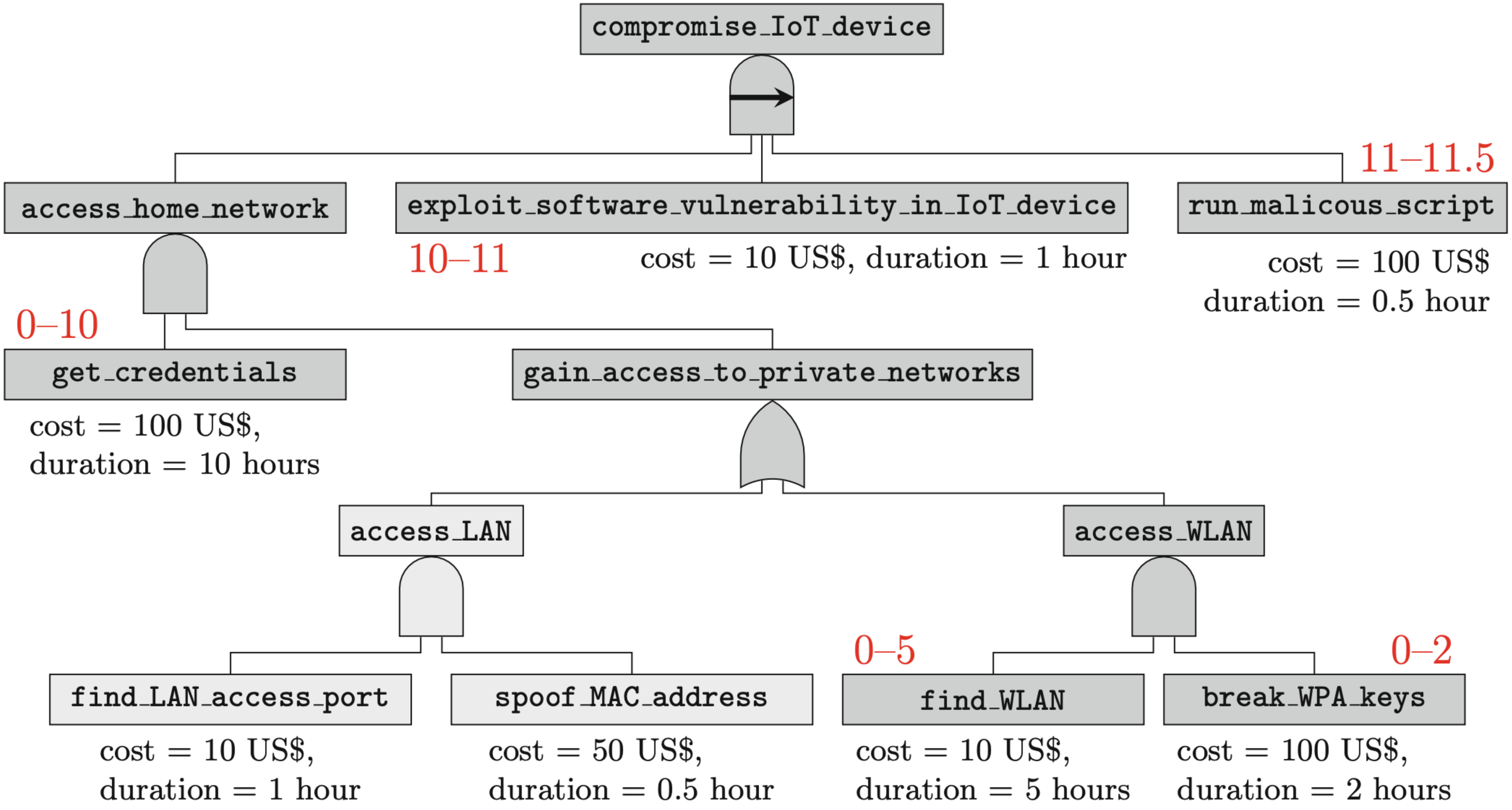
2. **Qualitative analysis to find root causes and minimal conditions of successful attacks.**

3. **Quantitative analysis to compute security metrics, such as minimal time and cost among all attacks.**

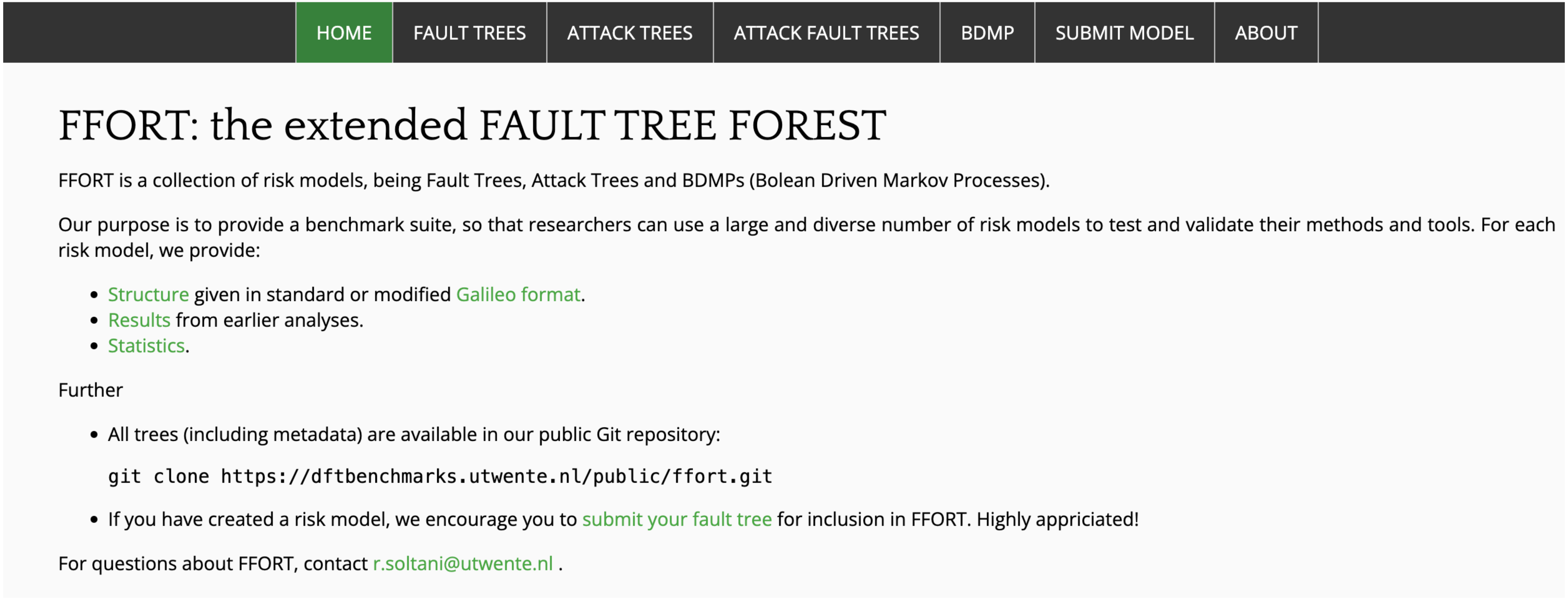
Kumar, R. et al. (2018). Effective Analysis of Attack Trees: A Model-Driven Approach. In: Russo, A., Schürr, A. (eds) Fundamental Approaches to Software Engineering. FASE 2018. Lecture Notes in Computer Science, vol 10802. Springer, Cham. https://doi.org/10.1007/978-3-319-89363-1_4



El Bouchti A, Haqiq A. Modeling cyber-attack for SCADA systems using CoPNet approach. In: 2012 IEEE International Conference on Complex Systems (ICCS). IEEE; 2012. p. 1-6.



Kumar, R. et al. (2018). Effective Analysis of Attack Trees: A Model-Driven Approach. In: Russo, A., Schürr, A. (eds) Fundamental Approaches to Software Engineering. FASE 2018. Lecture Notes in Computer Science, vol 10802. Springer, Cham. https://doi.org/10.1007/978-3-319-89363-1_4



FFORT: the extended FAULT TREE FOREST

FFORT is a collection of risk models, being Fault Trees, Attack Trees and BDMPs (Bolean Driven Markov Processes).

Our purpose is to provide a benchmark suite, so that researchers can use a large and diverse number of risk models to test and validate their methods and tools. For each risk model, we provide:

- Structure given in standard or modified Galileo format.
- Results from earlier analyses.
- Statistics.

Further

- All trees (including metadata) are available in our public Git repository:

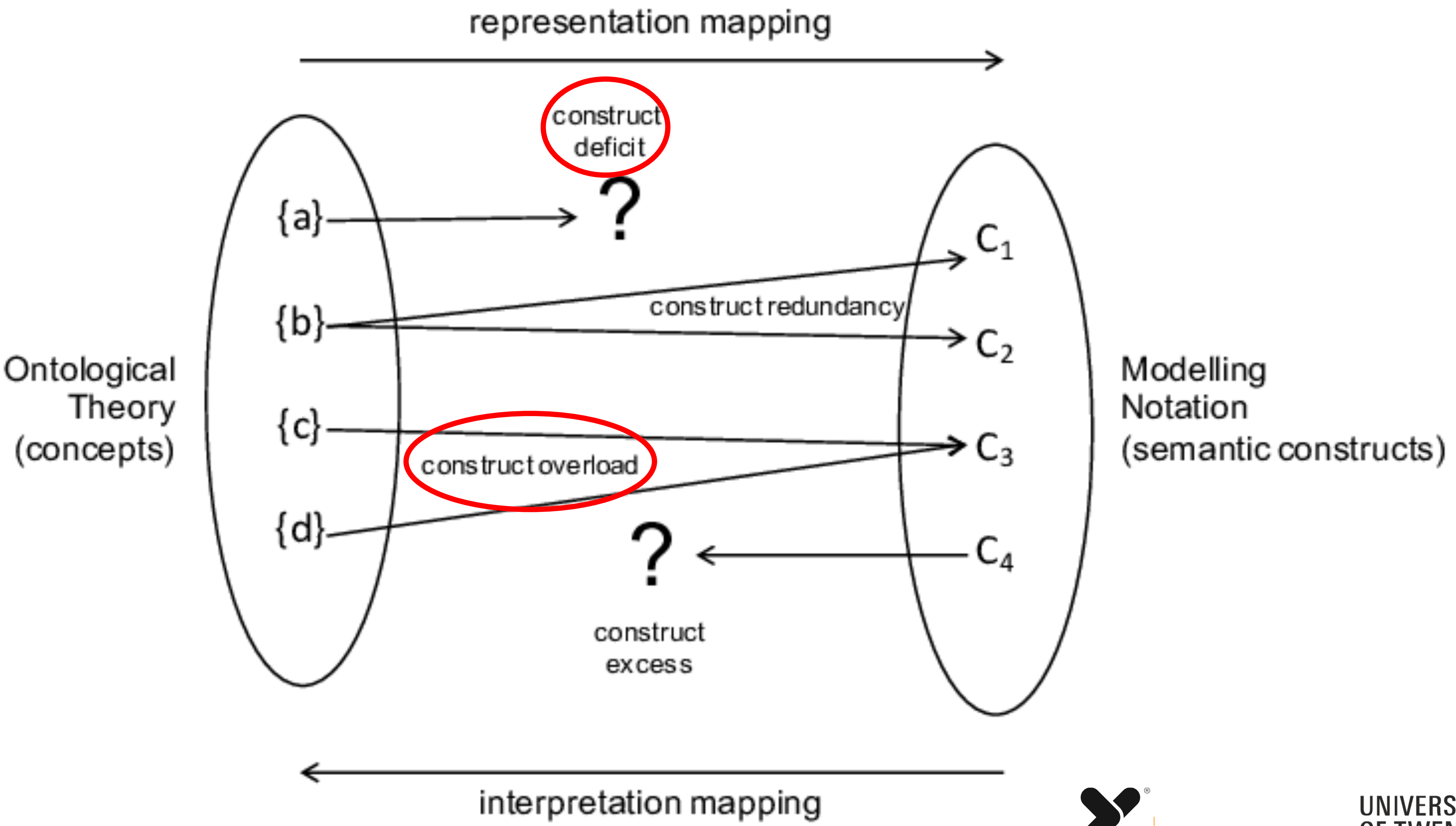
  ```
  git clone https://dftbenchmarks.utwente.nl/public/ffort.git
  ```

- If you have created a risk model, we encourage you to submit your fault tree for inclusion in FFORT. Highly appriciated!

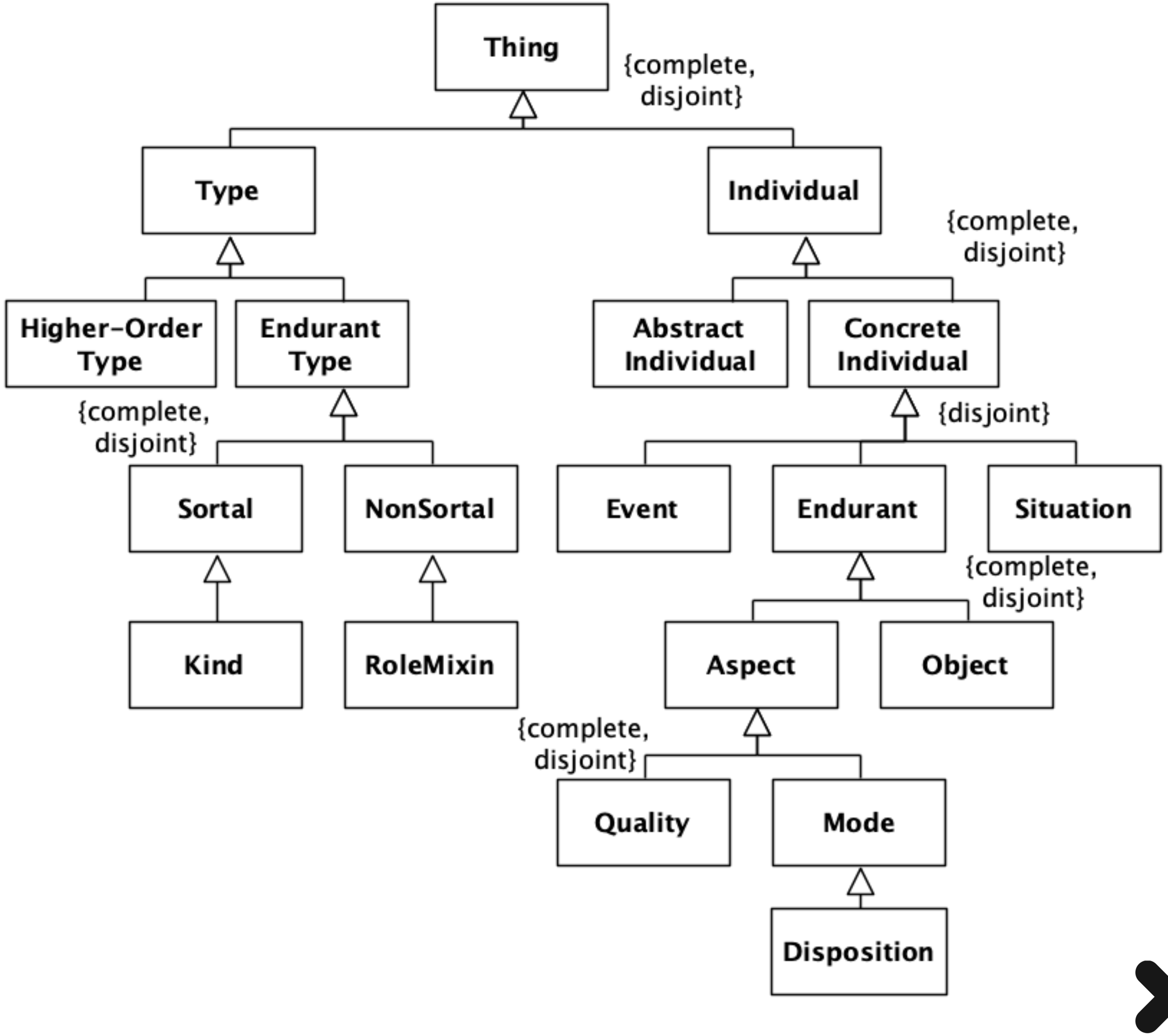
For questions about FFORT, contact r.soltani@utwente.nl .

Website: https://dftbenchmarks.utwente.nl

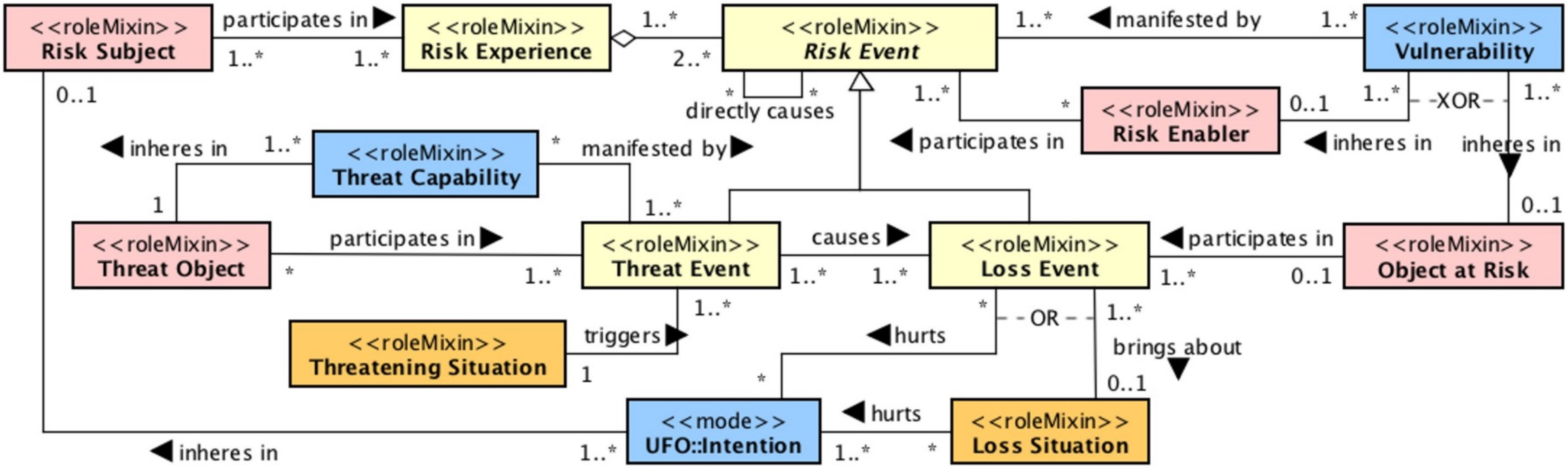
Ontological Analysis Method



A Fragment of the Unified Foundational Ontology

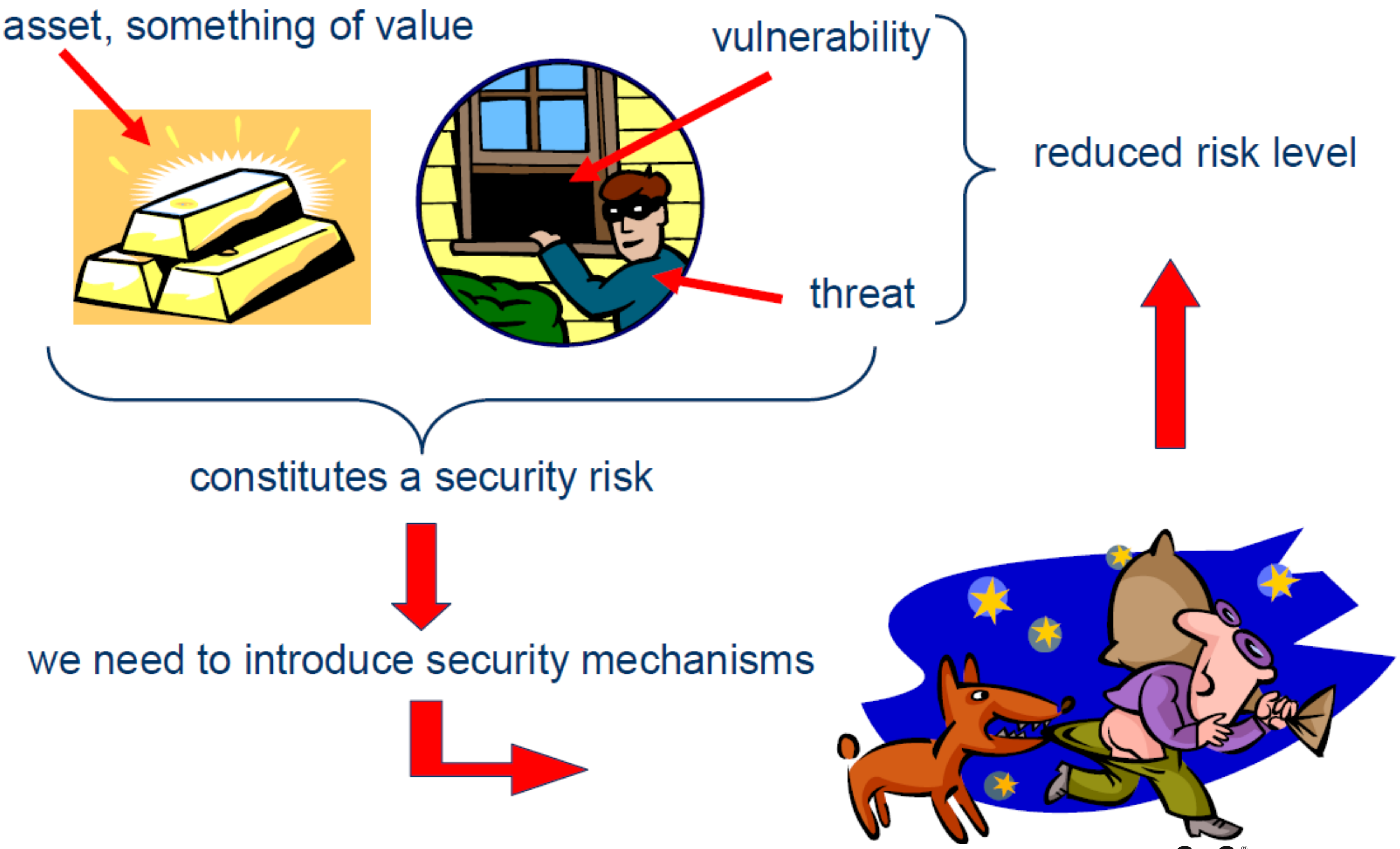


The Common Ontology of Value and Risk



Sales, T.P., Baião, F., Guizzardi, G., Almeida, J.P.A., Guarino, N., Mylopoulos, J. (2018). The Common Ontology of Value and Risk. In: Trujillo, J., et al. Conceptual Modeling. ER 2018. Lecture Notes in Computer Science(), vol 11157. Springer, Cham. https://doi.org/10.1007/978-3-030-00847-5_11

Elements of Value, Risk, and Security



asset, something of value

vulnerability

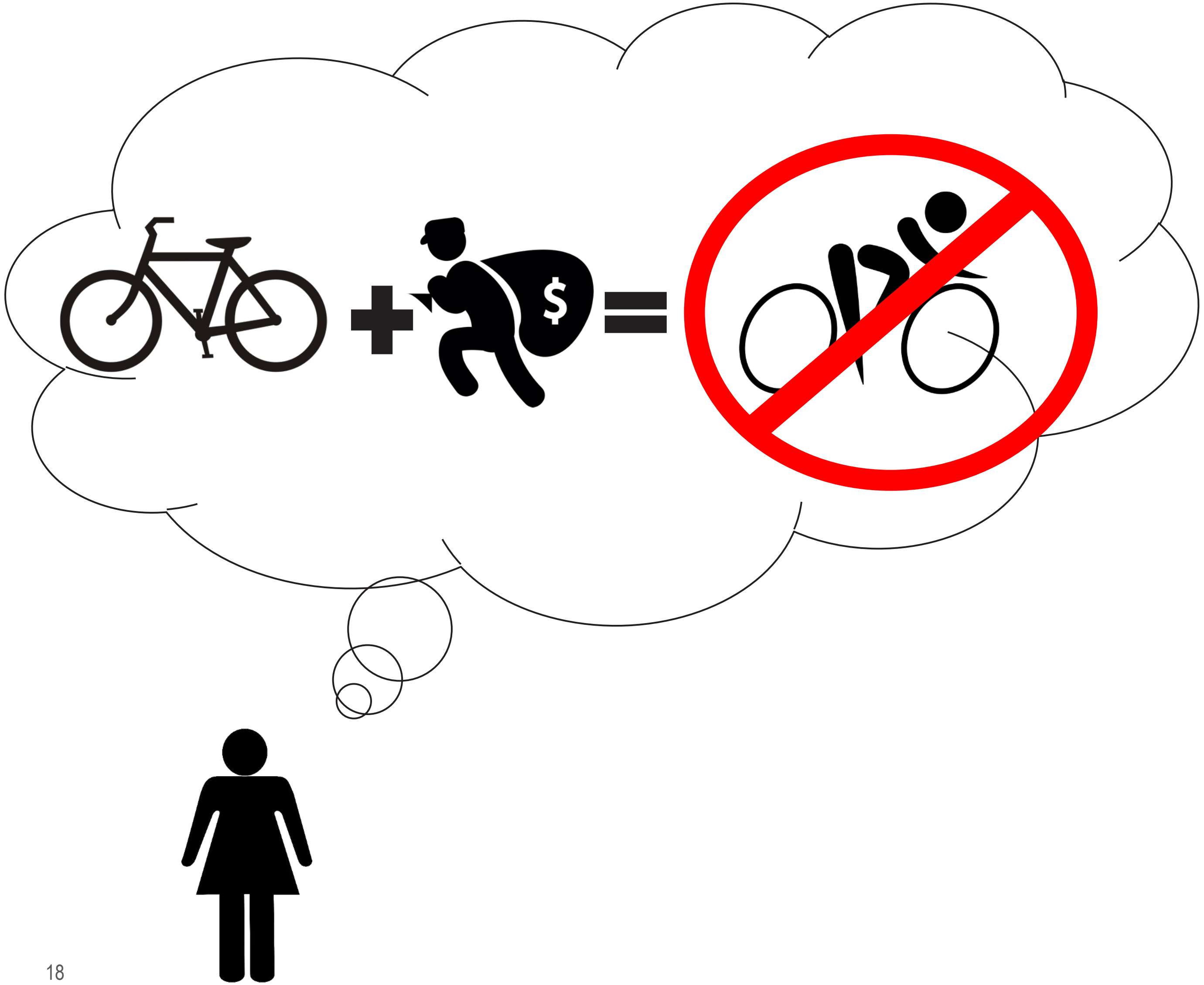
threat

reduced risk level

constitutes a security risk

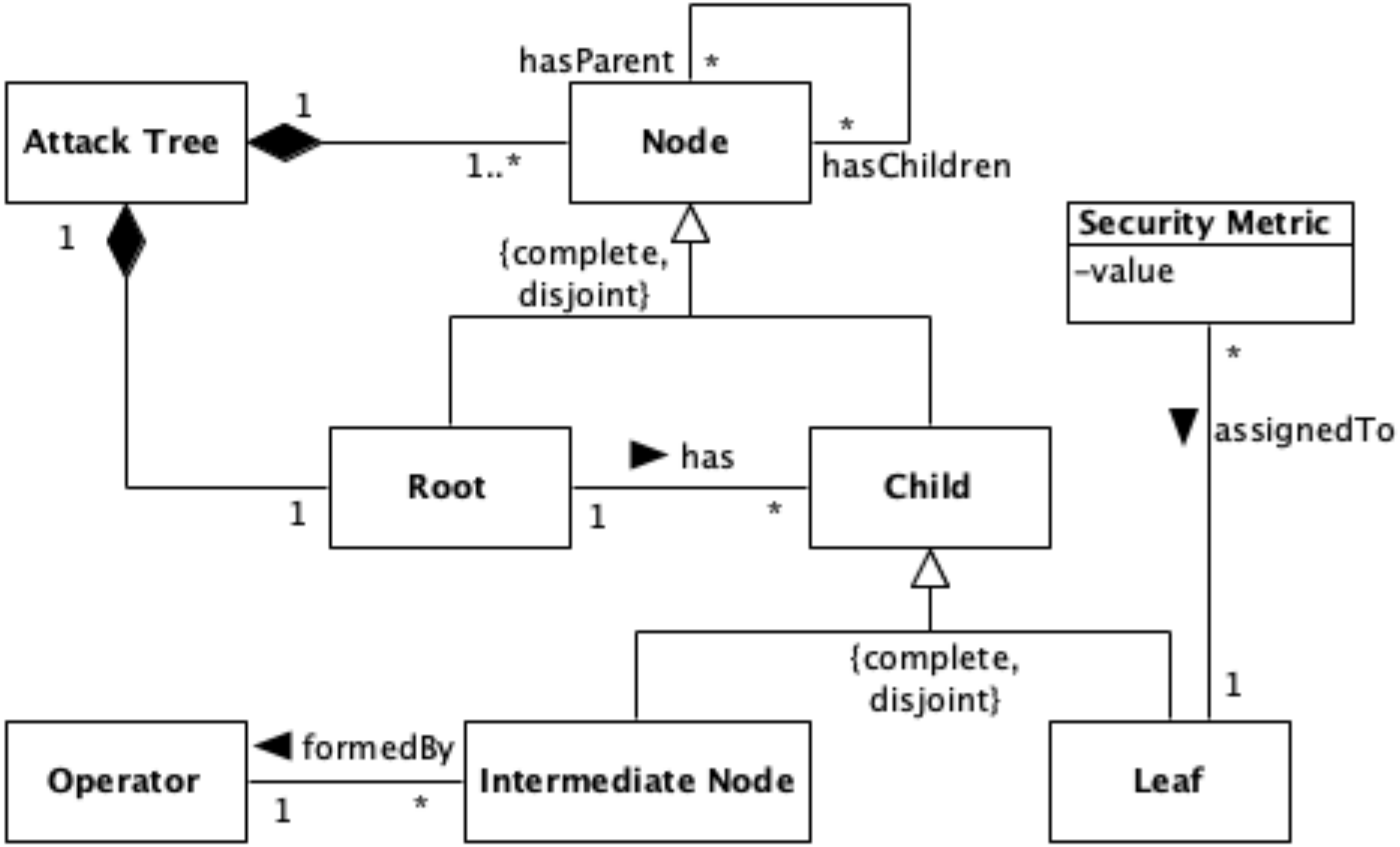
we need to introduce security mechanisms

Elements of Value, Risk, and Security



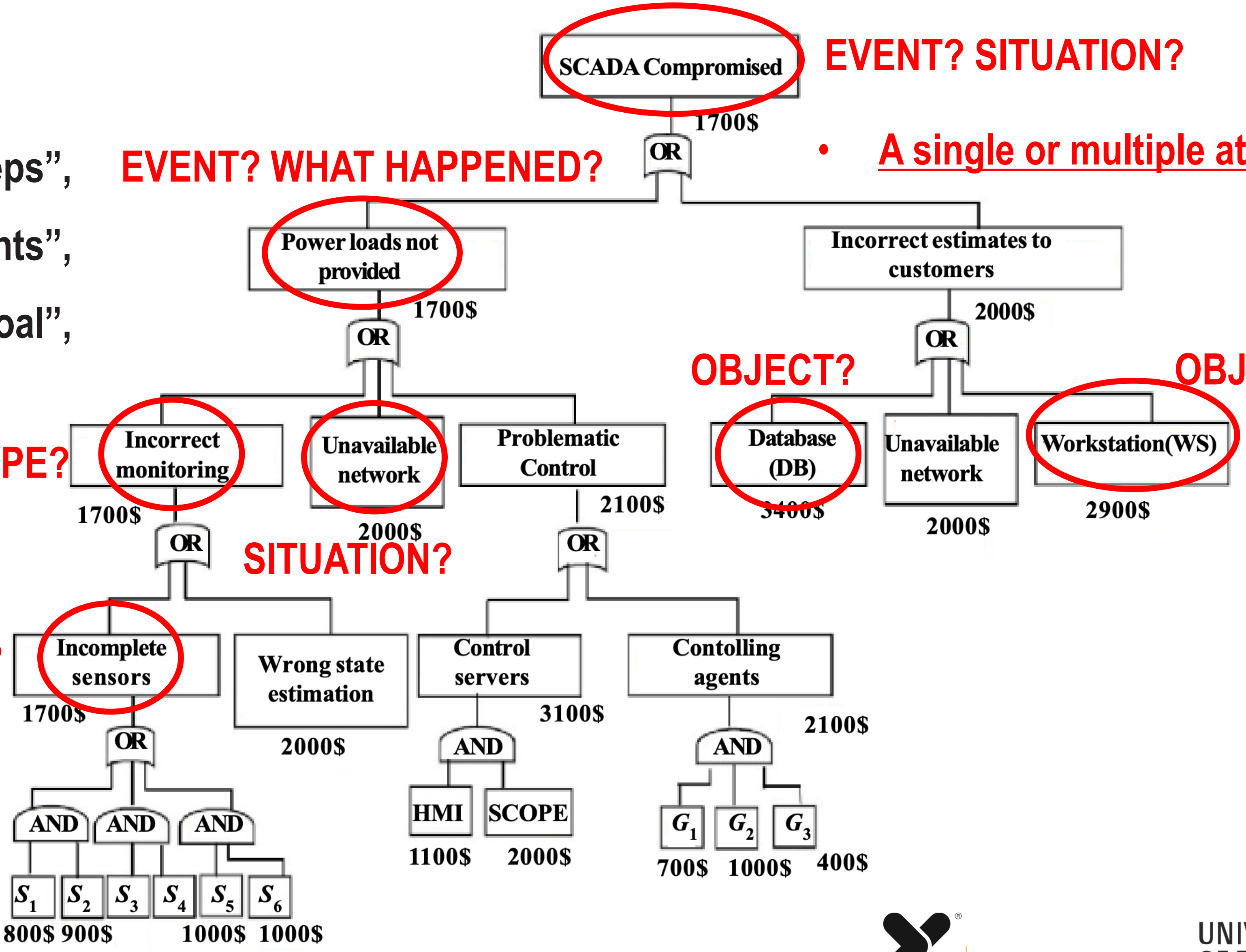
- Subjects
- Assets
- Goals and intentions
- Capabilities and vulnerabilities
- Events and situations
- Threats and attackers
- Chances and impacts

Attack Tree Metamodel



Semantic Overload

- ROOT: “Goal”, “Top Level Event”.
- NODE: “steps”, “attack steps”, “subgoals”, “undesired events”, “ways of achieving the goal”, “attacker actions”.



EVENT? SITUATION?

EVENT? WHAT HAPPENED?

- <u>A single or multiple attackers?</u>

OBJECT?

OBJECT?

EVENT TYPE?

SITUATION?

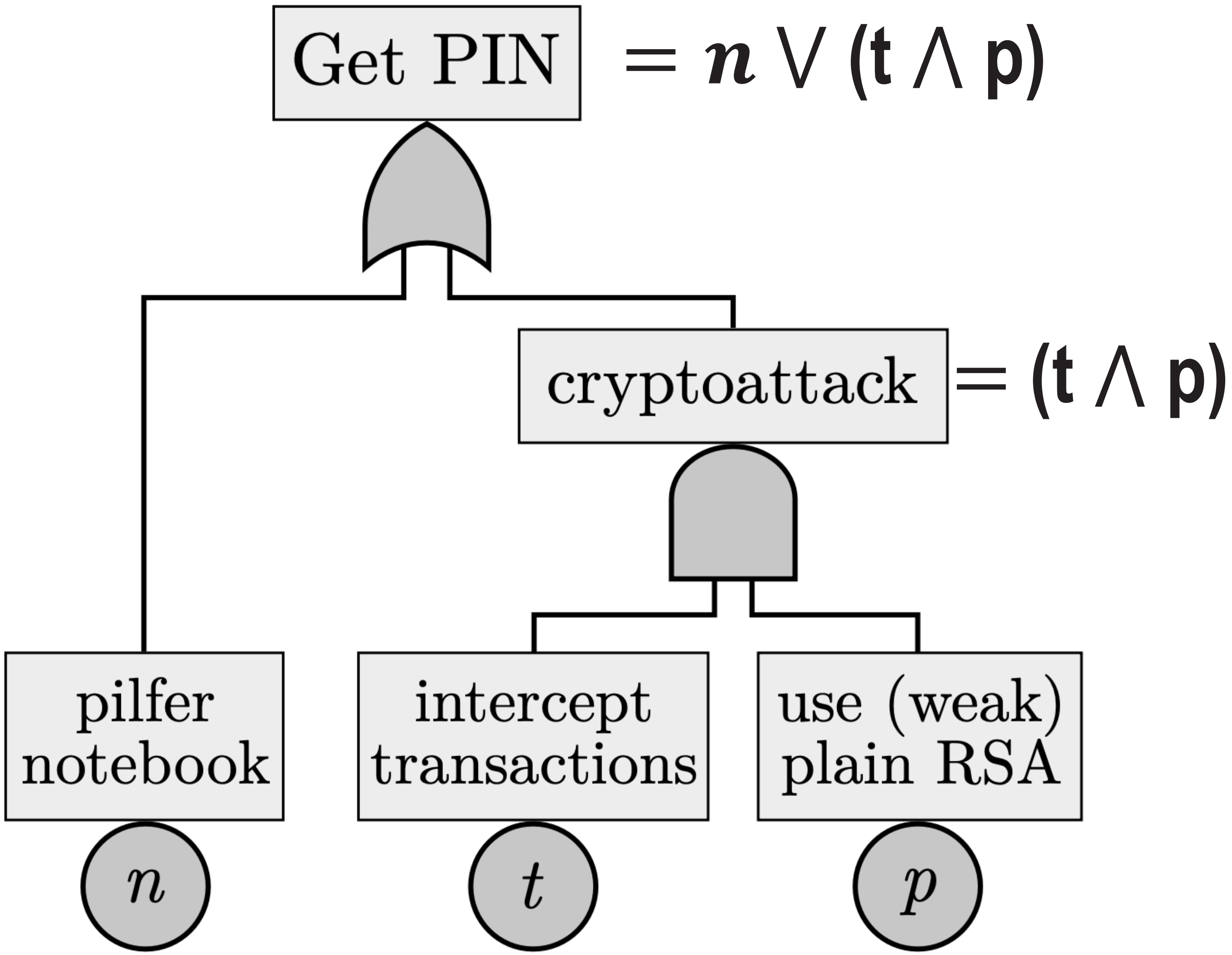
SITUATION?

Semantic Overload

The node description is highly overloaded because, without good descriptions, we do not know what we are talking about.

Consequently, the utility of calculating minimal conditions of successful attacks and security metrics depends entirely on naming nodes well enough.

Semantic Overload



$= \boldsymbol{n} \vee (\mathbf{t} \wedge \mathbf{p})$

$= (\mathbf{t} \wedge \mathbf{p})$

What is the relationship between “intercept transactions” and “use (weak) plain RSA”? And what is the relationship between them and “cryptoattack”?

- Mereological relation between events?
- Token Causation?
- Type Causation (regularities)?
- Parthood of Intention (Intrinsic Aspect)?
- Event Impact on Goals?

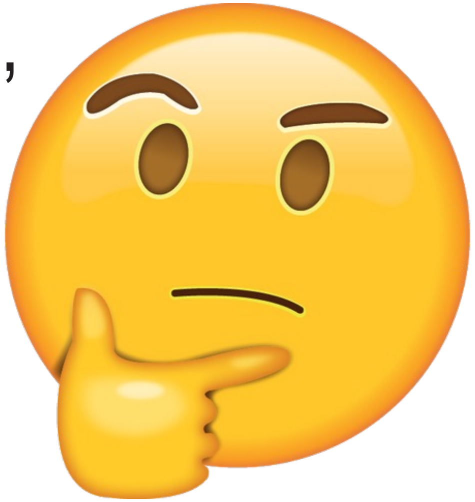
Ontological Incompleteness

A theory of risk should explain **why** a successful attack occurs, **who** is affected, and **how** they are affected, **which objects** participate in attacks, the role and features of **capabilities** and **vulnerabilities** in certain **situations**.

Ontological Incompleteness

A minimal successful attack out of 24 total nodes:

- “SCADA Compromised” (root),
  - “Incorrect estimates to customers” (intermediate node),
    - “Database” (leaf).



Limited Modeling Guidance

AT users have to:

(a) come up with the attacker’s final goal (root node) and start to

(b) branch it into intermediate nodes until

(c) they reach “basic attack steps”.

HOW?

HOW GOOD?

Semantic Interoperability Issues

1. Data Interoperability

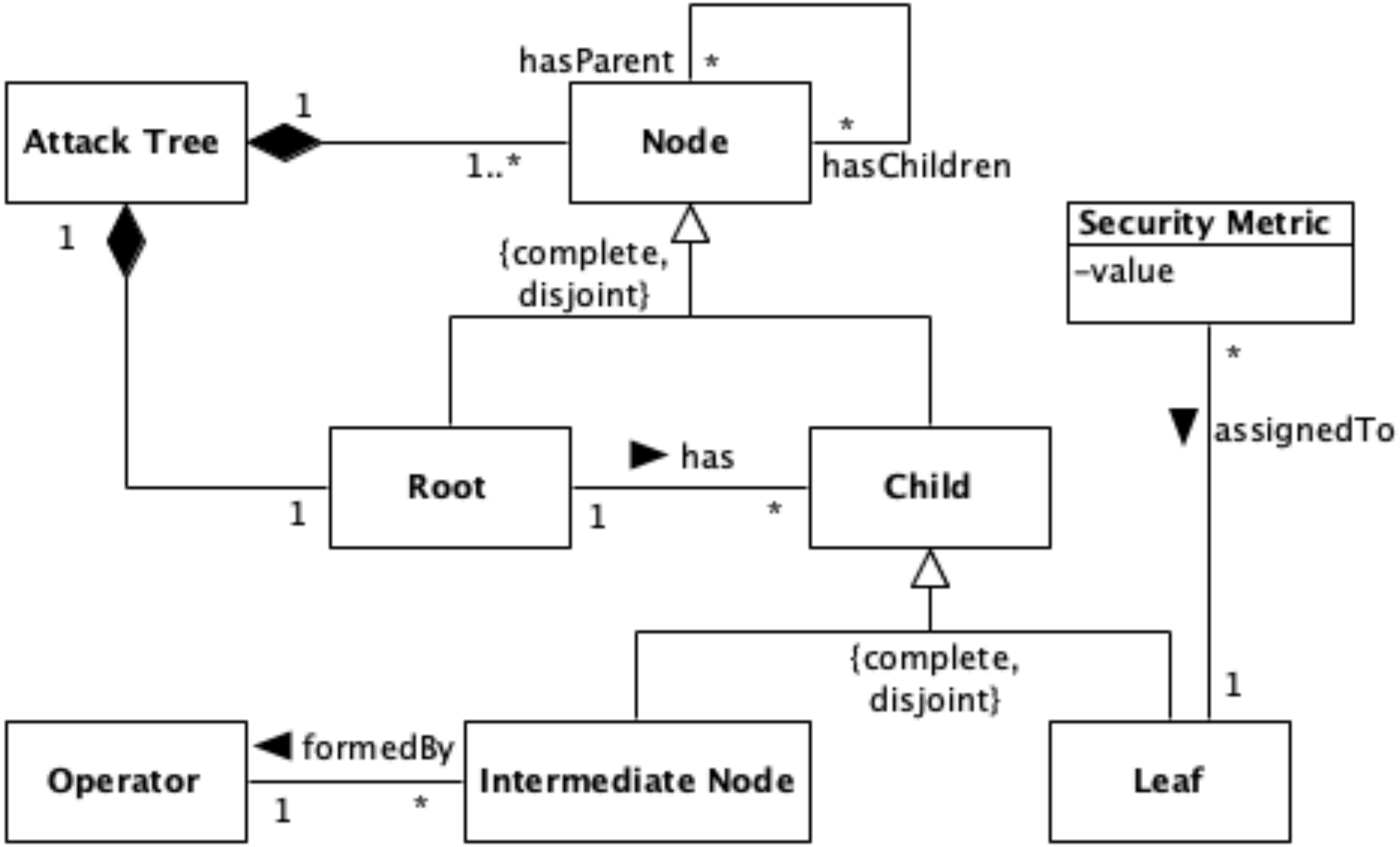
2. Technique Interoperability

3. Human Communication

AT Identity Crisis: When are two ATs the same?

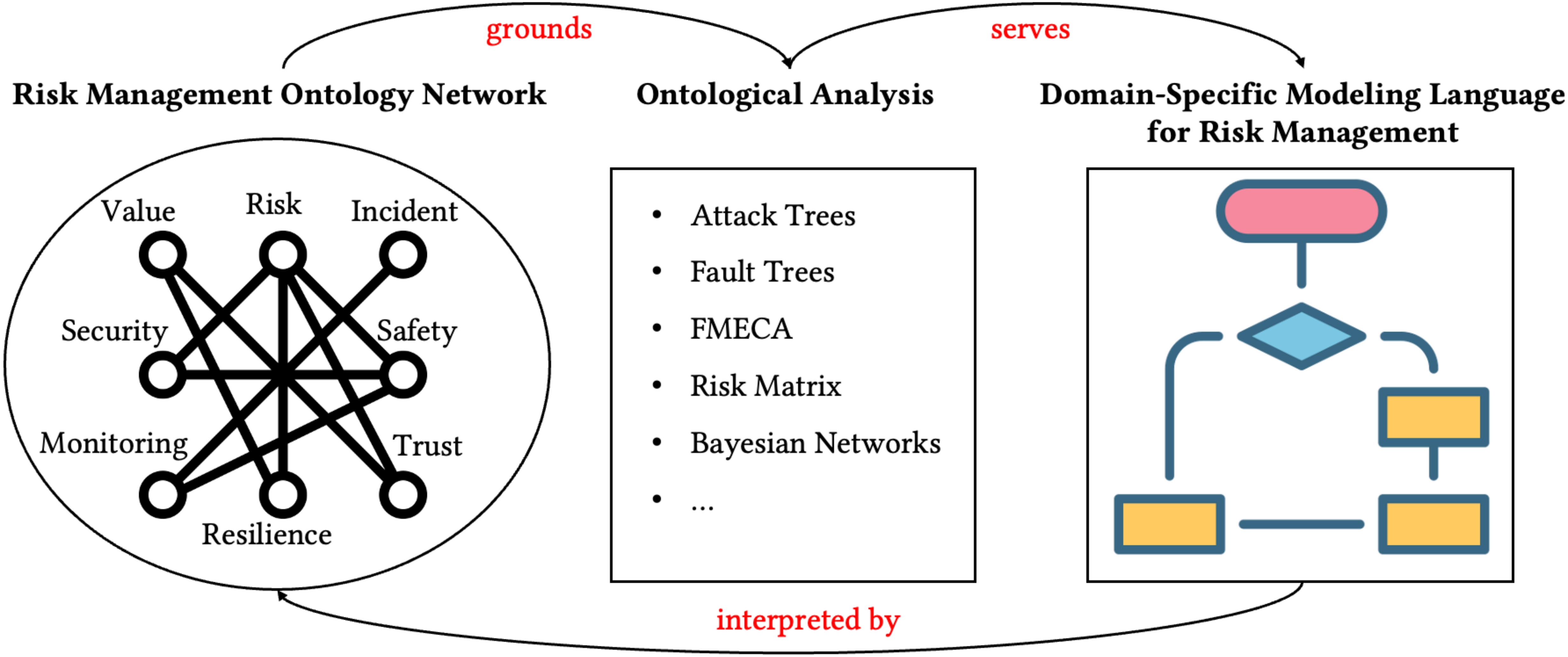
$\boldsymbol{n} \vee (\mathbf{t} \wedge \mathbf{p})$?

Incremental Solutions: Extending the Metamodel



- Dynamic Attack Trees
- Attack-defense Trees
- Agents

A Broad, Systematic Solution: Ontology-based Modeling for Risk Management



Risk Management Ontology Network

grounds

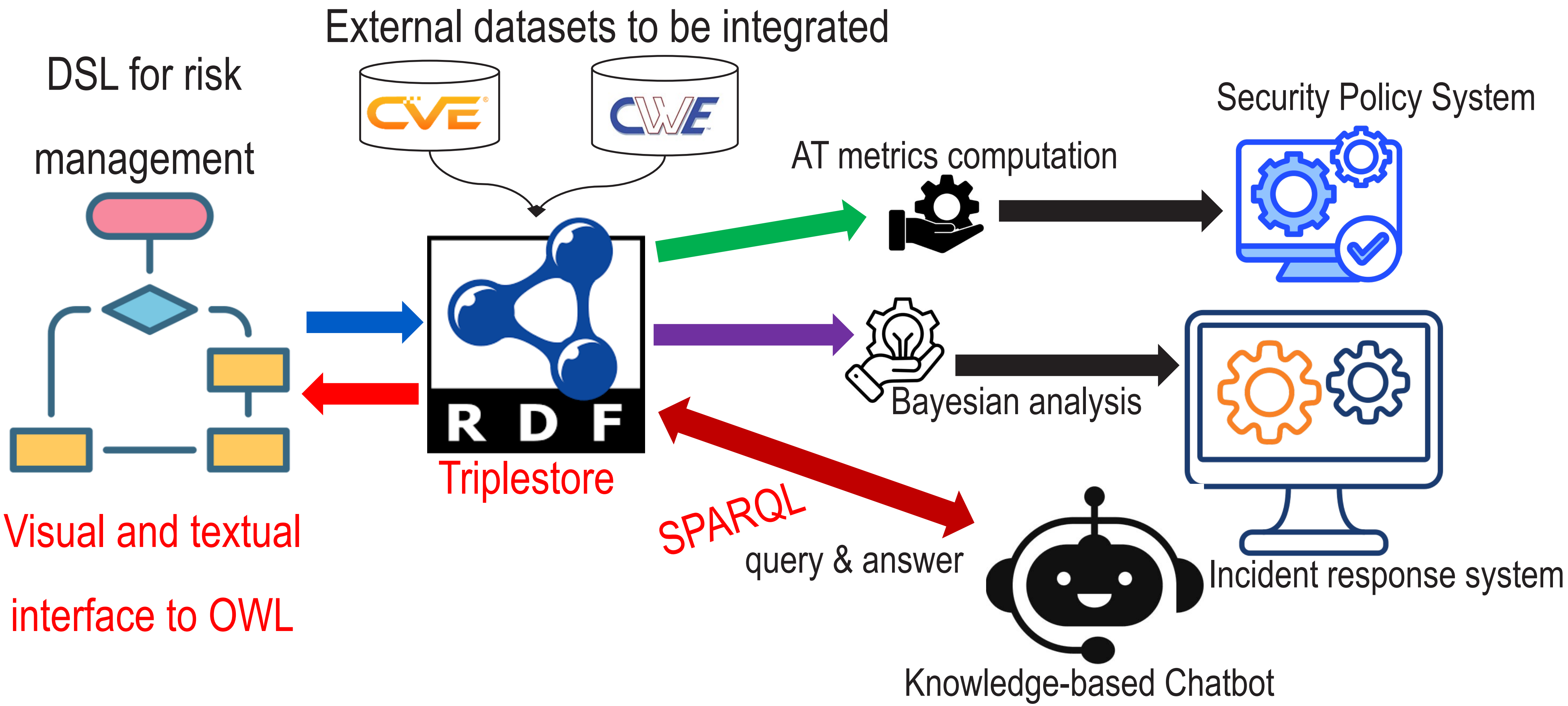
Ontological Analysis

serves

Domain-Specific Modeling Language for Risk Management

interpreted by

- Attack Trees
- Fault Trees
- FMECA
- Risk Matrix
- Bayesian Networks
- …



External datasets to be integrated

DSL for risk management

Visual and textual interface to OWL

Triplestore

AT metrics computation

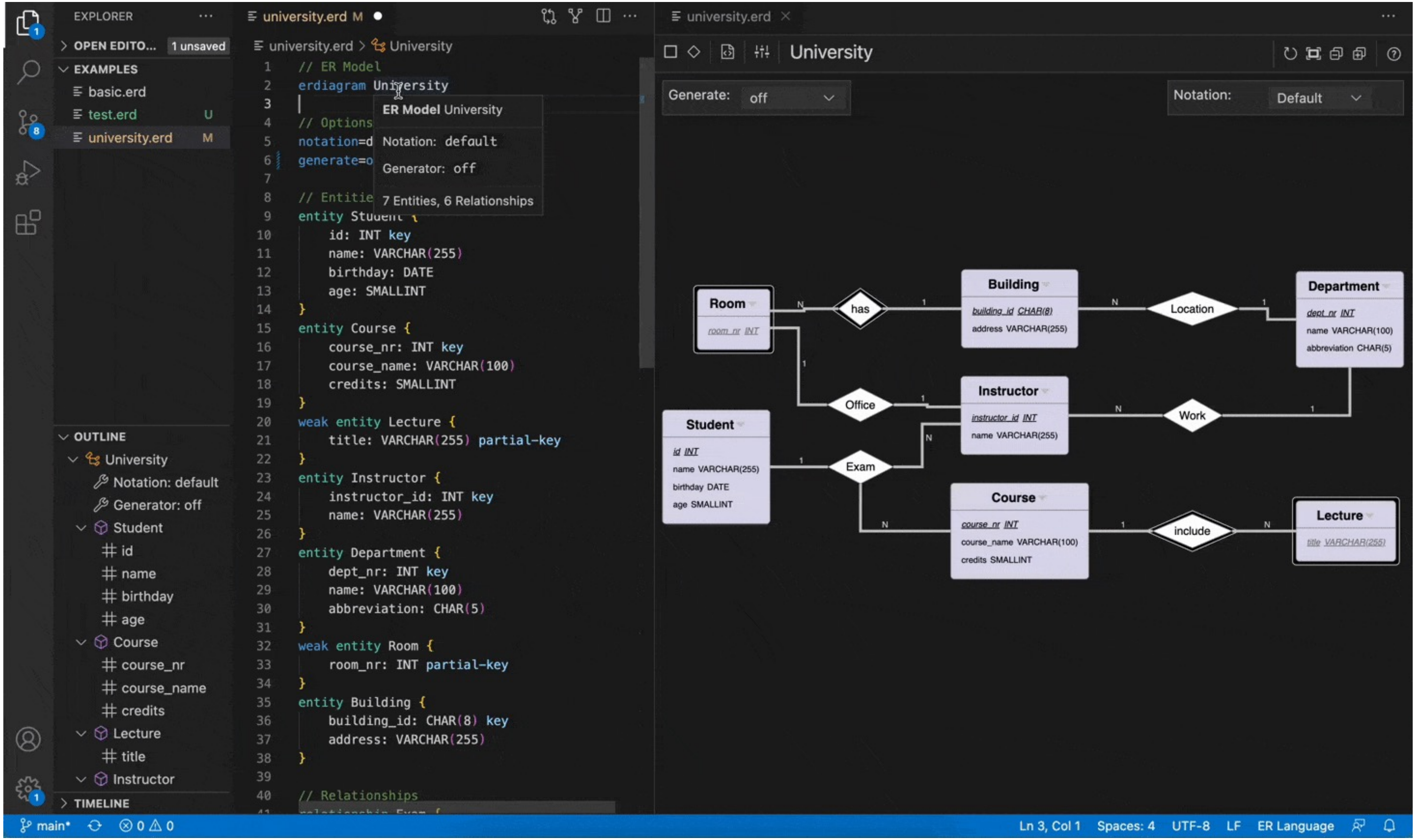
Security Policy System

Bayesian analysis

Incident response system

SPARQL query & answer

Knowledge-based Chatbot



```
// ER Model
erdiagram University

// Options
notation=d
generate=o

// Entitie
entity Student {
    id: INT key
    name: VARCHAR(255)
    birthday: DATE
    age: SMALLINT
}
entity Course {
    course_nr: INT key
    course_name: VARCHAR(100)
    credits: SMALLINT
}
weak entity Lecture {
    title: VARCHAR(255) partial-key
}
entity Instructor {
    instructor_id: INT key
    name: VARCHAR(255)
}
entity Department {
    dept_nr: INT key
    name: VARCHAR(100)
    abbreviation: CHAR(5)
}
weak entity Room {
    room_nr: INT partial-key
}
entity Building {
    building_id: CHAR(8) key
    address: VARCHAR(255)
}

// Relationships
relationship Exam {
```

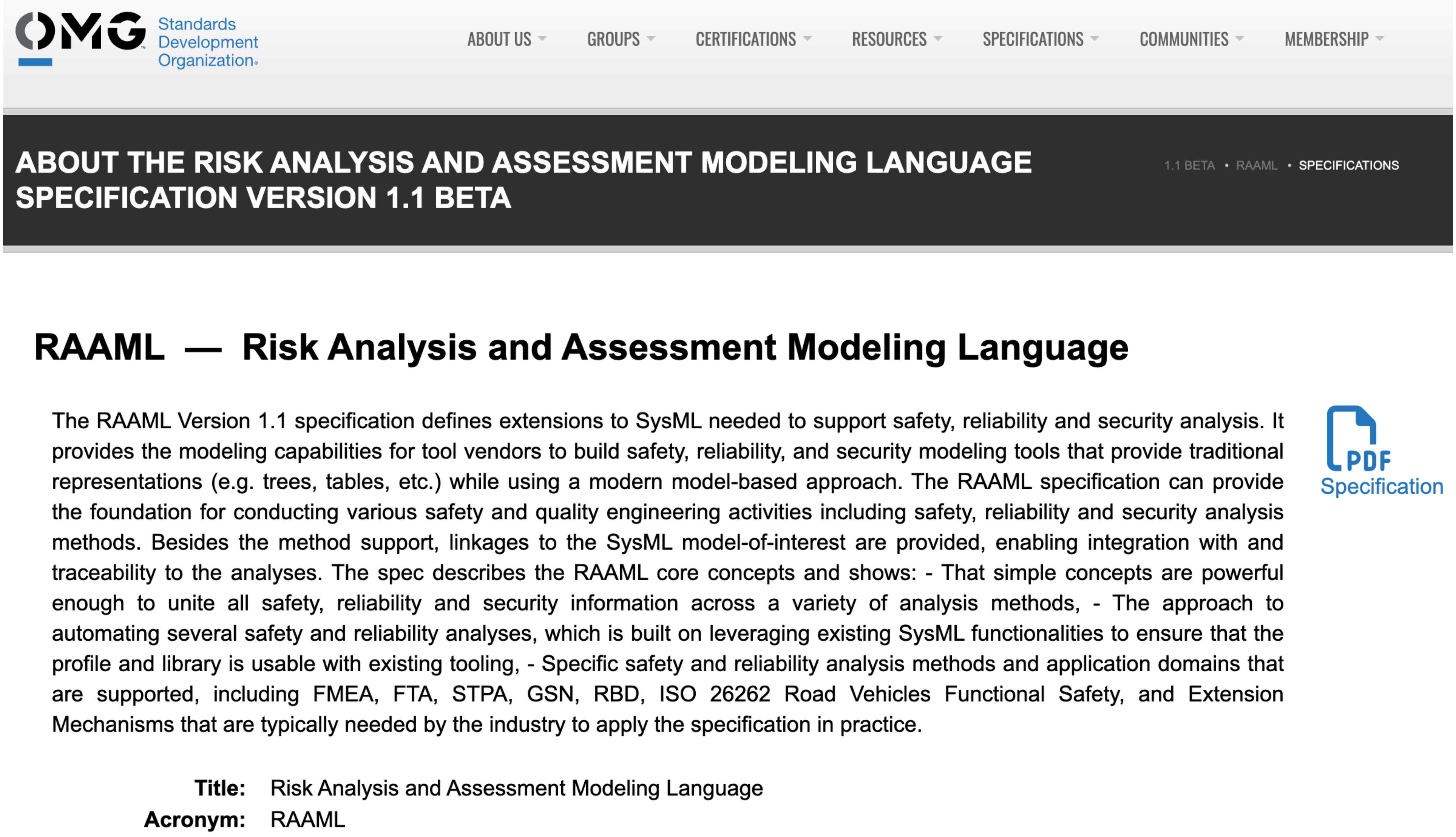
ER Model University

Notation: default

Generator: off

7 Entities, 6 Relationships

ER diagram modeling tool: https://github.com/borkdominik/bigER



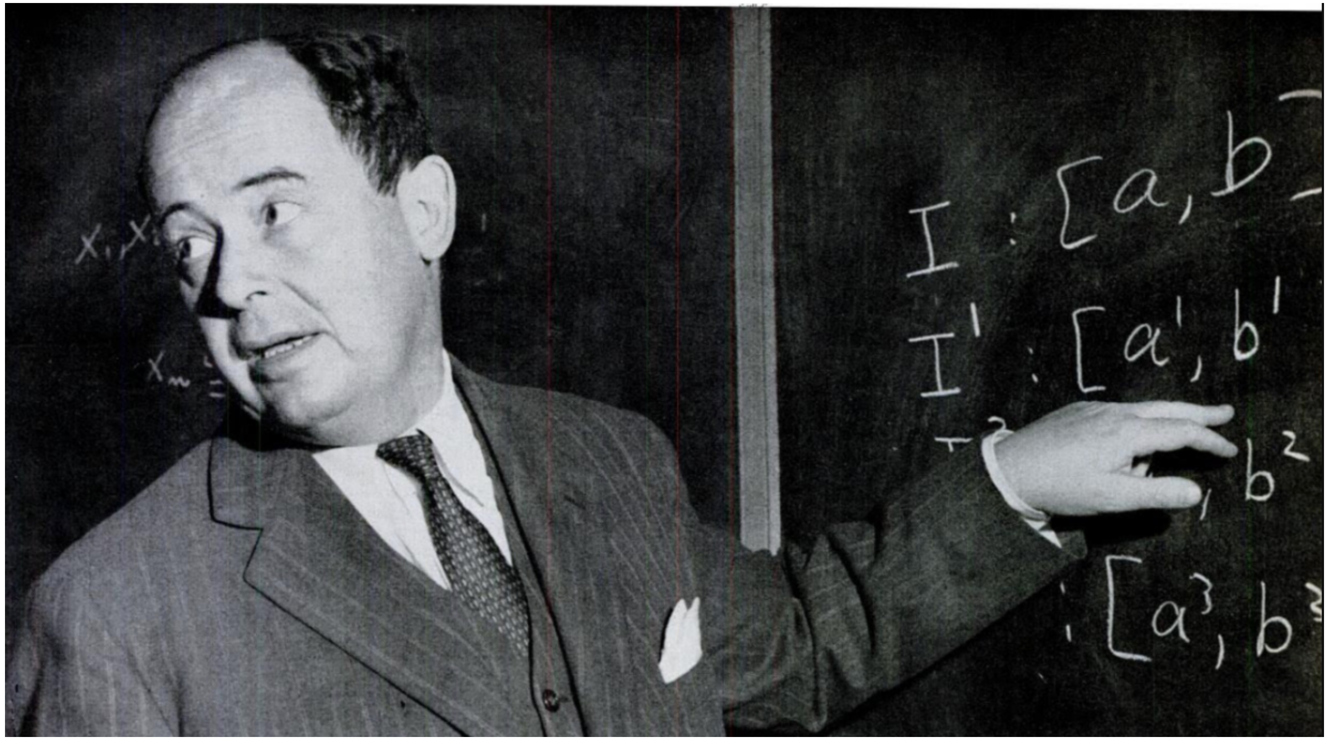
ABOUT THE RISK ANALYSIS AND ASSESSMENT MODELING LANGUAGE SPECIFICATION VERSION 1.1 BETA

RAAML — Risk Analysis and Assessment Modeling Language

The RAAML Version 1.1 specification defines extensions to SysML needed to support safety, reliability and security analysis. It provides the modeling capabilities for tool vendors to build safety, reliability, and security modeling tools that provide traditional representations (e.g. trees, tables, etc.) while using a modern model-based approach. The RAAML specification can provide the foundation for conducting various safety and quality engineering activities including safety, reliability and security analysis methods. Besides the method support, linkages to the SysML model-of-interest are provided, enabling integration with and traceability to the analyses. The spec describes the RAAML core concepts and shows: - That simple concepts are powerful enough to unite all safety, reliability and security information across a variety of analysis methods, - The approach to automating several safety and reliability analyses, which is built on leveraging existing SysML functionalities to ensure that the profile and library is usable with existing tooling, - Specific safety and reliability analysis methods and application domains that are supported, including FMEA, FTA, STPA, GSN, RBD, ISO 26262 Road Vehicles Functional Safety, and Extension Mechanisms that are typically needed by the industry to apply the specification in practice.

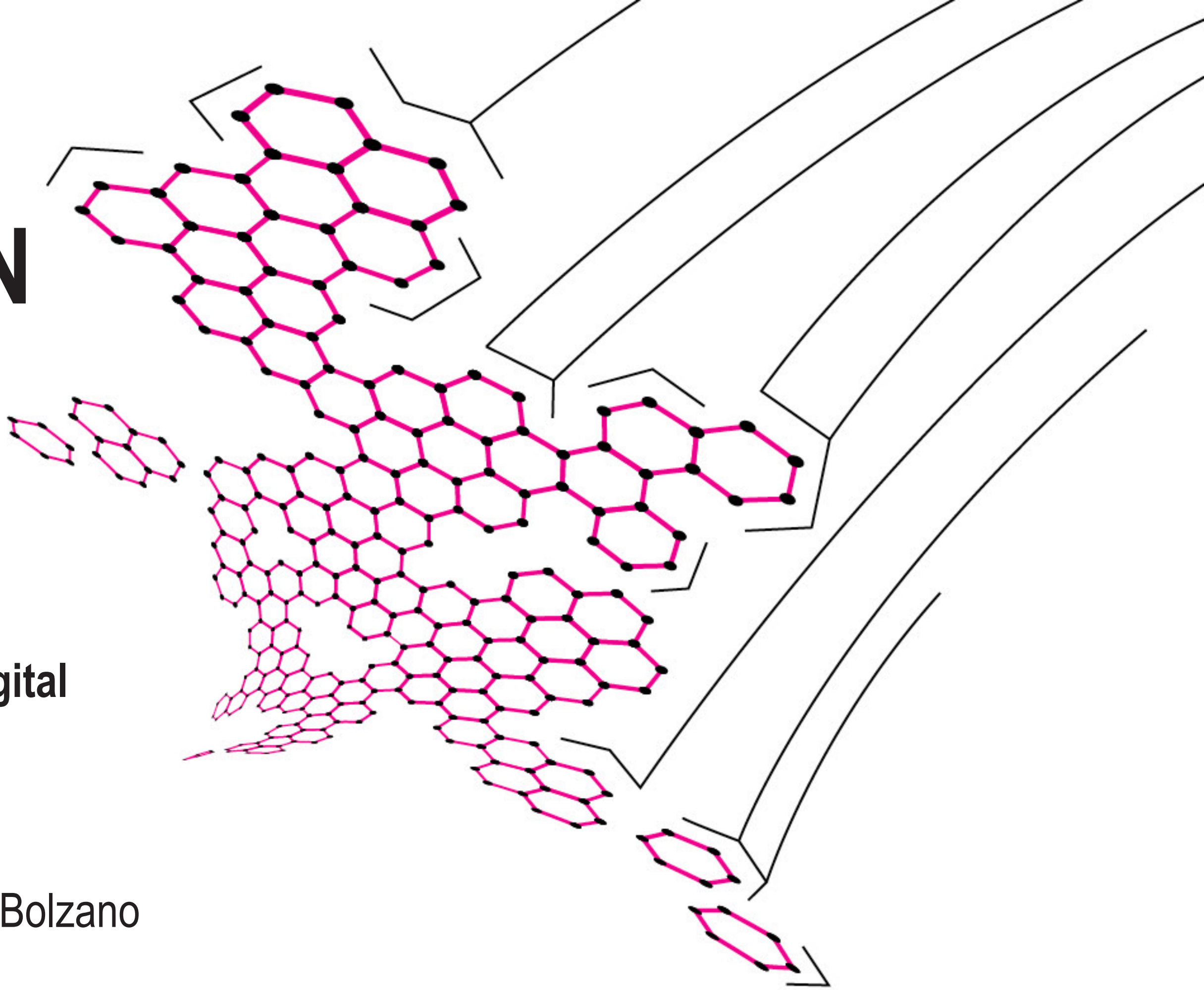
Title: Risk Analysis and Assessment Modeling Language
Acronym: RAAML

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



Semantics, Cybersecurity, and Services (SCS)

Faculty of Electrical Engineering, Mathematics, and Computer Science (EEMCS)



AN ONTOLOGICAL LENS ON ATTACK TREES:

TOWARD ADEQUACY AND INTEROPERABILITY

Ítalo Oliveira, University of Twente & Y.digital

Stefano Nicoletti, University of Twente

Mattia Fumagalli, Free University of Bozen-Bolzano

Gal Engelberg, University of Haifa

Dan Klein, Accenture EMEA

Giancarlo Guizzardi, University of Twente

https://italojsoliveira.github.io

digital
empowering humans

UNIVERSITY
OF TWENTE.