Towards a Quantitative Risk Management Engine Implementation

COST ECON@Tel Workshop WG4

Ljubljana, May 21, 2010

Univerza v Ljubljani

Iztok Starc, Denis Trček

Outline

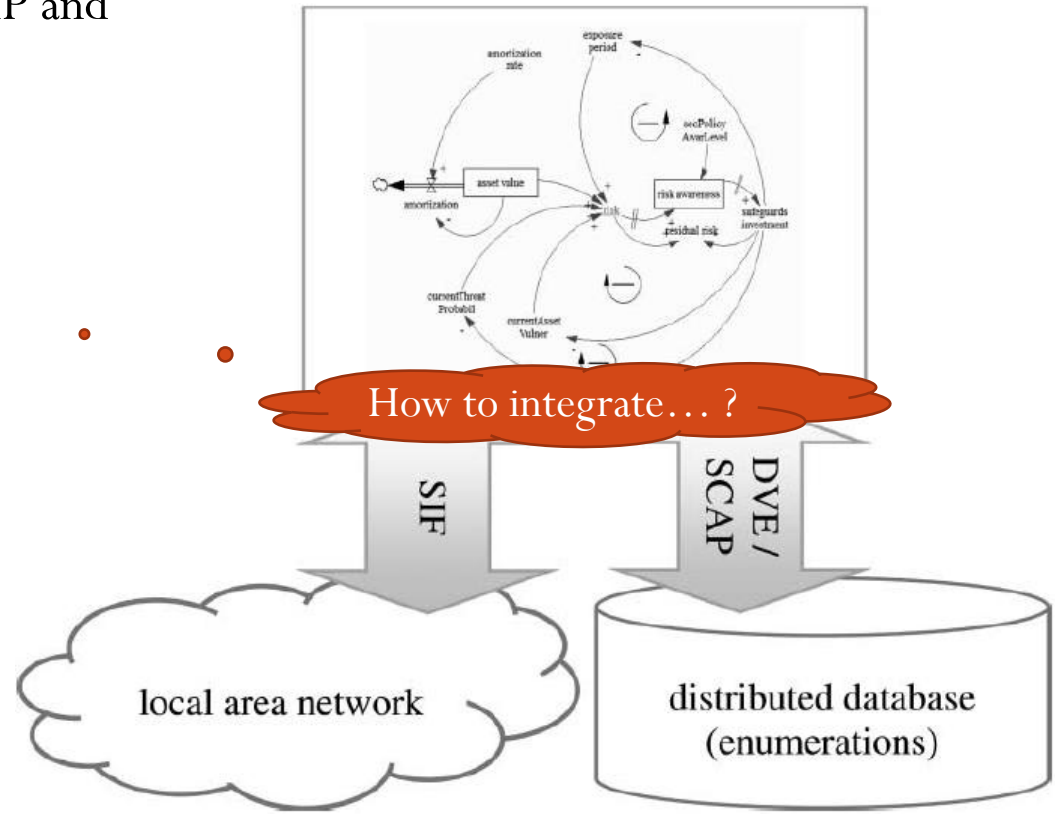
- Introduction
  - Past work
  - Open Questions
- The QnRME Domain Model Proposal
  - Requirements
  - Methodology
  - Proposal
- The QnRME Domain Model Analysis
- Conclusions
- Literature

Introduction

- Past work:
  - Risk management standards:
    - The ISO 27000 series of standards [1,2,3,4]
  - Vulnerability enumerations:
    - CVE [5]
    - and others [6]
  - Security Metrics:
    - DVE [7]
    - BAR [8]
    - Vulnerability Index (CIF, COS, SIF) [9]
    - and others [10]
  - The *Generic IT - Risk Management* (GIT-RM) [10]
    - System Dynamics model [11].

Introduction cont'd

- The open question of interest [10]:
  - How to *integrate* the GIT-RM model
    - with DVE/SCAP and
    - with SIF?



The GIT-RM engine integration model is courtesy of Prof. Dr. Denis Trček [10].

The Quantitative Risk Management Engine (QnRME) Domain Model Proposal

- Requirements:
  - *Compliance* with the ISO 27000 series of standards.
  - *Consistency* with the GIT-RM Model.
  - *Assistance* for
    - *specification*, *construction* and *documentation* of platform independent models that can be used further for
      - *refinement* and *construction* of platform specific models and
        - *construction* of proprietary application solutions.

The QnRME Domain Model Proposal cont'd

- Methodology:
  - A need for *software engineering modeling language* to facilitate effective implementation:
    - While *SD models* are good at capturing behavioral complexity at macro level of a system being modeled,
    - *UML models* [12, 13] are good at capturing structural complexity of a software system. Both models complement each other.
  - *Integration* of UML and SD models [14,15,16].
  - *To justify* the mapping between these two models:
    - Communication diagrams to show how objects of *the QnRME model* collaborate in a use case,
    - that should reflect system thinking [11] in *the GIT-RM model*.

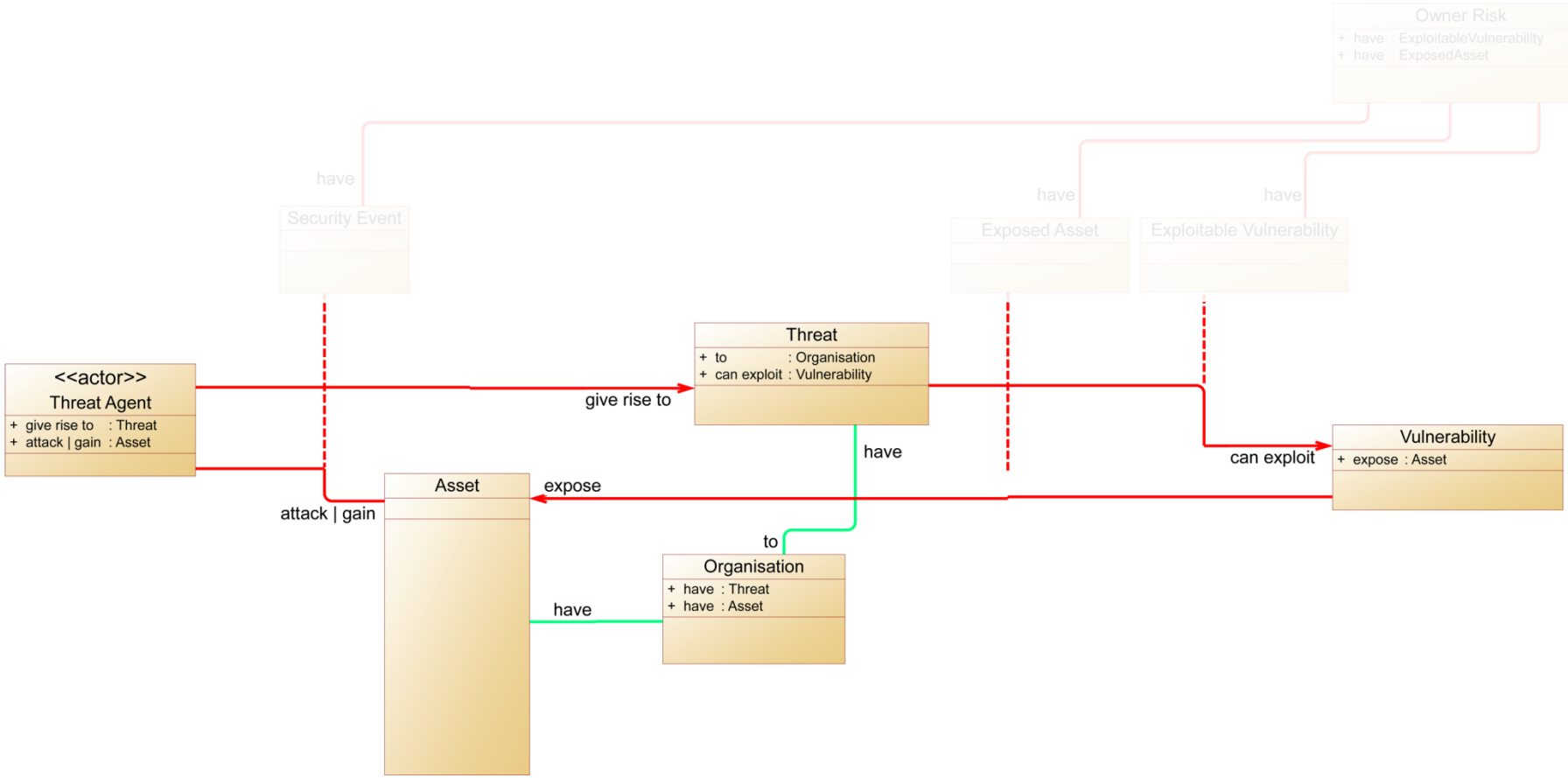


Figure 1: The QnRME model (part 1)

A threat agent's perspective on risk management.

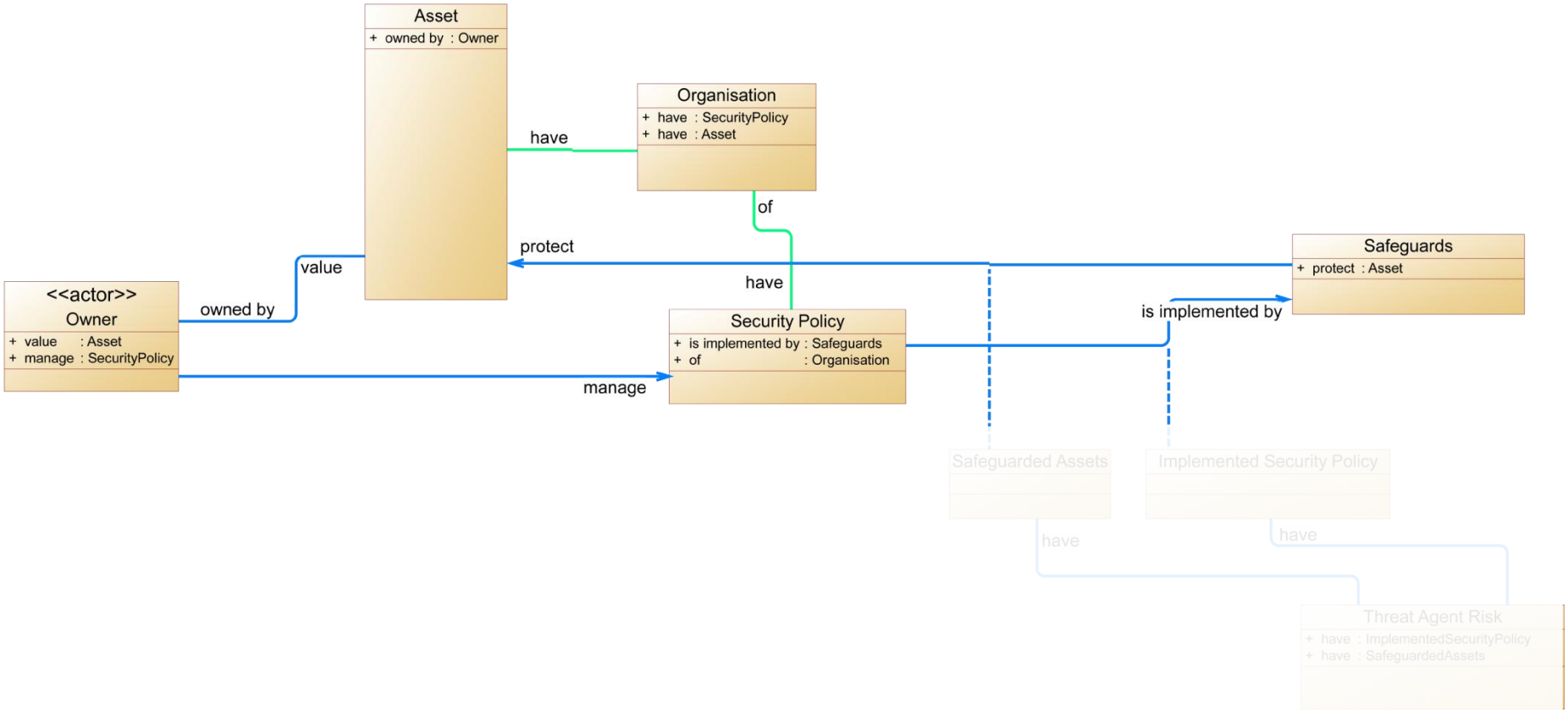


Figure 2: The QnRME model (part 2)

An owner's perspective on risk management.

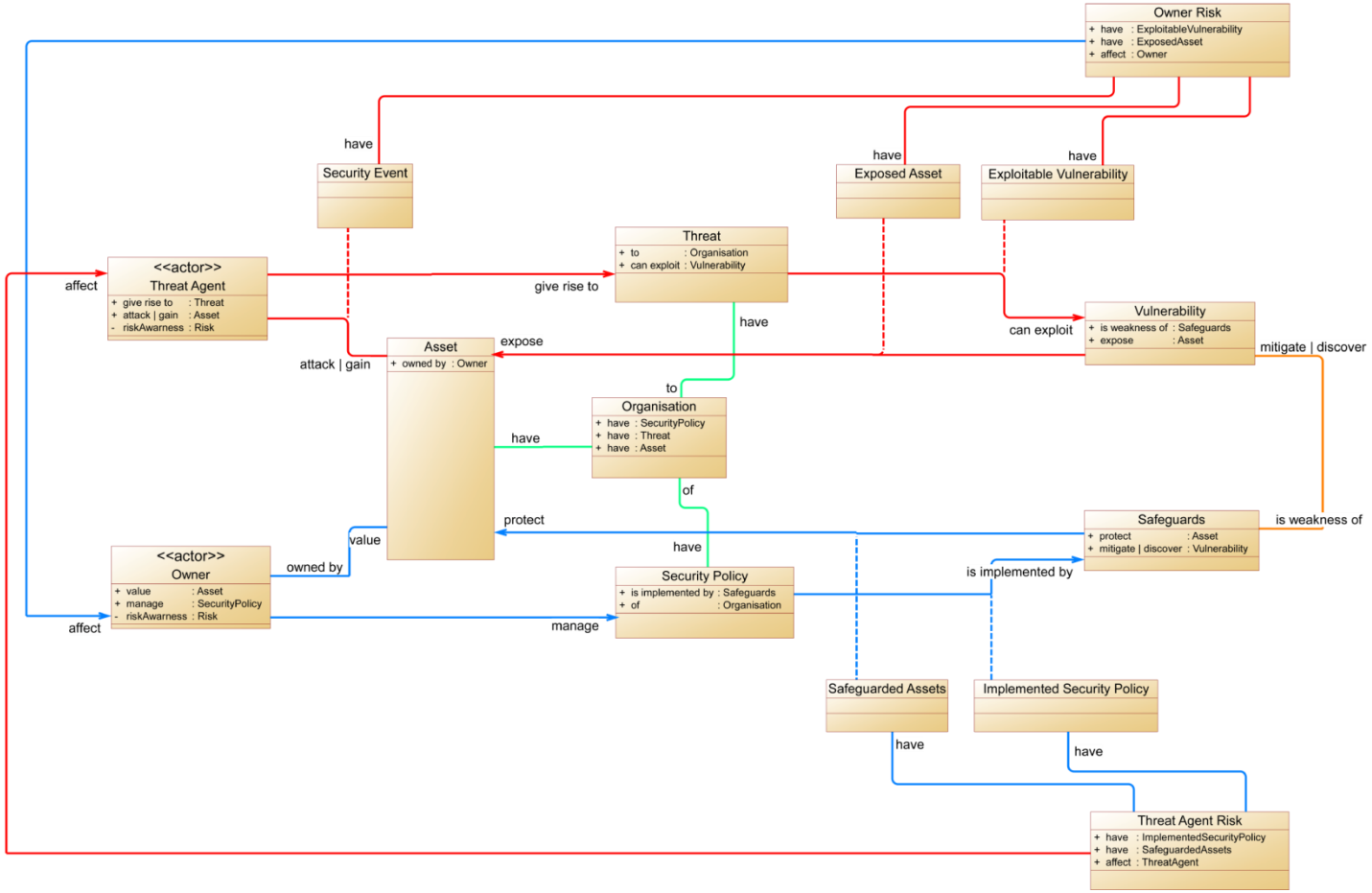
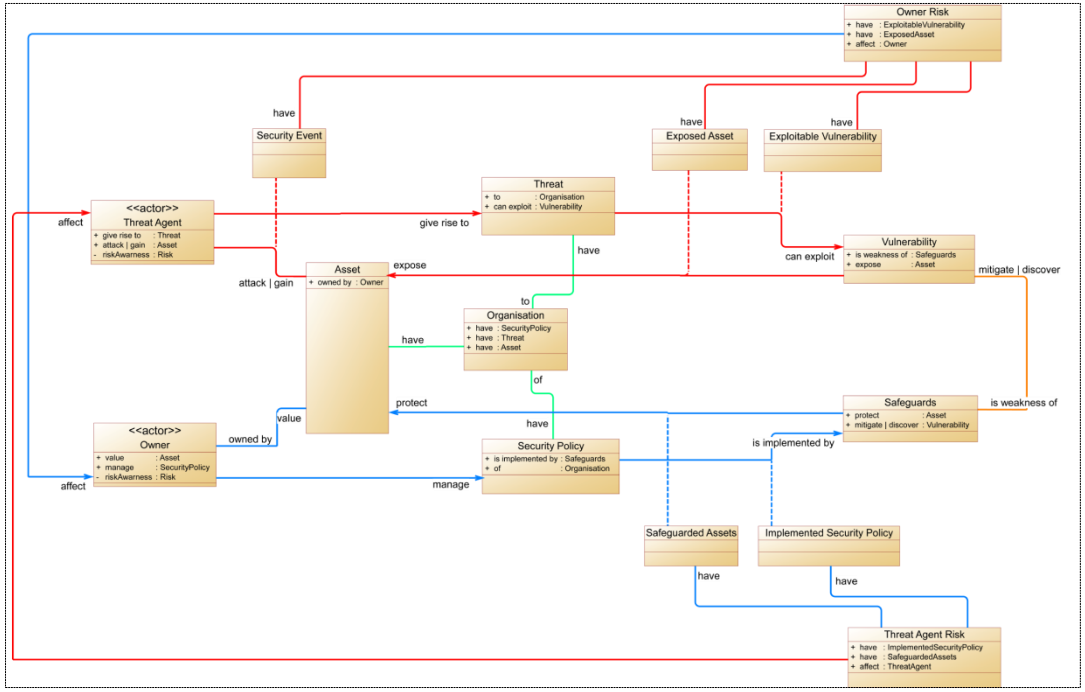


Figure 3: The QnRME model (full model)

A merged model with 4 additional relationships.

The QnRME Domain Model Analysis

- Is the mapping between the GIT-RM and the QnRME consistent?
- Do identified metrics of the GIT-RM apply to the QnRME as well?
  - How?



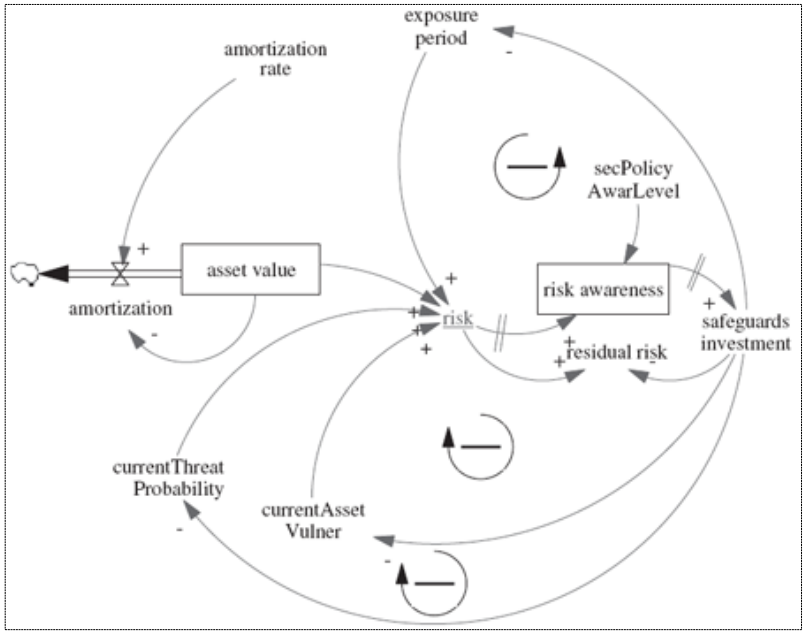


Figure 4: The mapping between the GIT-RM and the QnRME

The GIT-RM model subfigure on the right side is courtesy of Prof. Dr. Denis Trček [10].

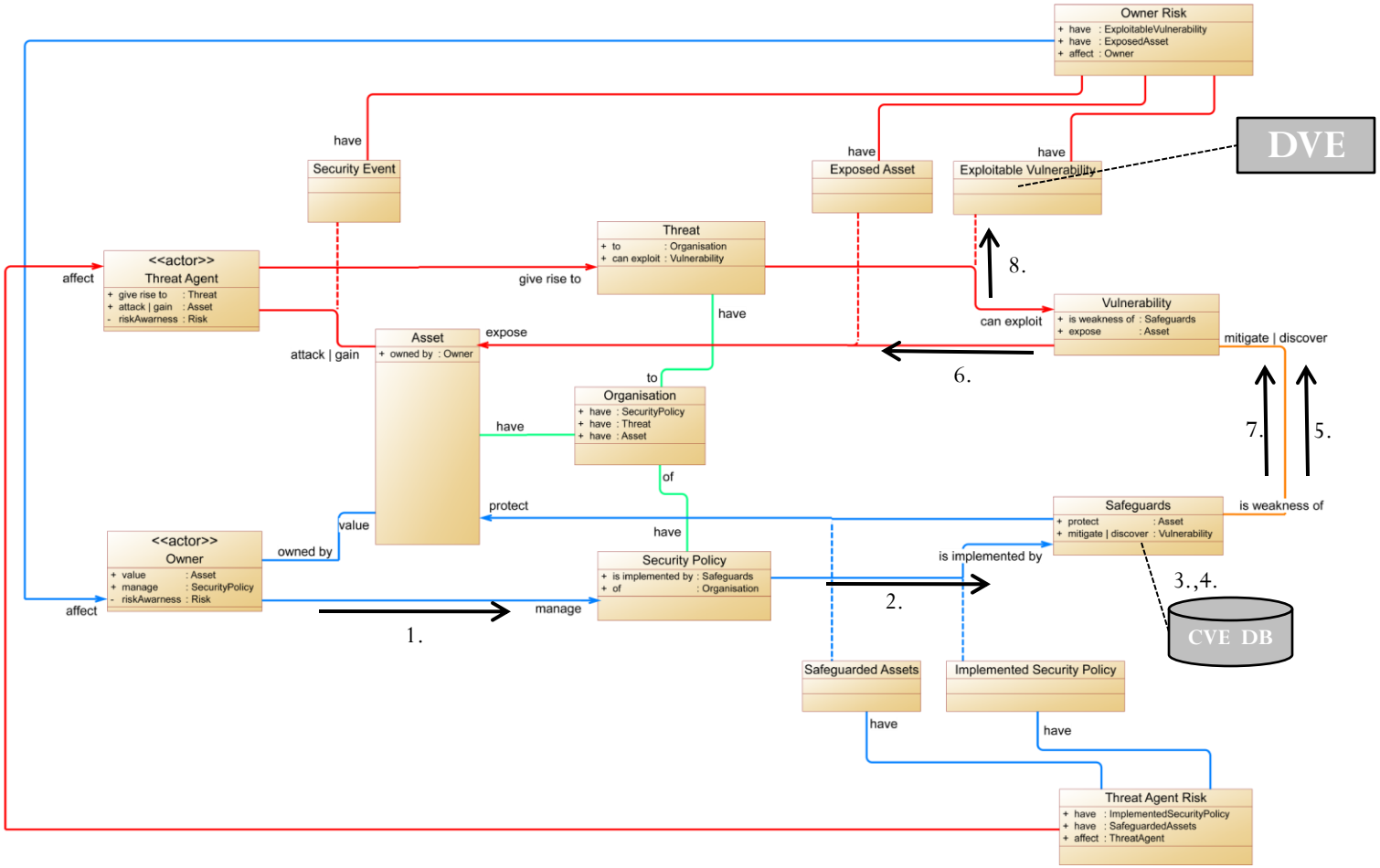


Figure 5: The DVE use case on the QnRME model

The DVE use case demonstration to justify the mapping of metrics between the GIT-RM and the QnRME model.

Conclusions

- Contribution:
  - We have *justified* the mapping between the GIT-RM and the QnRME model.
  - We have *demonstrated* that metrics suitable to the GIT-RM apply to the QnRME model as well.
  - The QnRME model *as a stepping stone* towards a Quantitative Risk Management Engine Implementation.

- Further research:
  - *Improvement* of the GIT-RM.
  - *Improvement* of the QnRME.
  - *Exploration*, *definition* and *integration* of new metrics.

References

[1] I.1. 27, *ISO/IEC 27000:2009, Information technology - Security techniques - Information security management systems - Overview and vocabulary*, Multiple. Distributed through American National Standards Institute (ANSI), 2009.

[2] I.1. 27, *ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements*, Multiple. Distributed through American National Standards Institute (ANSI), 2007.

[3] I.1. 27, *ISO/IEC 27002:2005, Information technology -- Security techniques -- Code of practice for information security management*, Multiple. Distributed through American National Standards Institute (ANSI), 2005.

[4] I.1. 27, *ISO/IEC 27005:2008, Information technology -- Security techniques -- Information security risk management*, Multiple. Distributed through American National Standards Institute (ANSI), 2008.

[5] R.A. Martin, "Managing Vulnerabilities in Networked Systems," *Computer*, vol. 34, 2001, pp. 32-38.

[6] MITRE, "Making Security Measurable: A Collection of Information Security Community Standardization Activities and Initiatives," 2010.

[7] J.R. Jones, "Estimating Software Vulnerabilities," *IEEE Security &Privacy Magazine*, vol. 5, 2007, pp. 28-32.

[8] D. Geer and A. Jaquith, "Information security: Why the future belongs to the quants," *IEEE Security &Privacy Magazine*, vol. 1, 2003, pp. 24-32.

[9] S. Hariri, T. Dharmagadda, M. Ramkishore, and C. Raghavendra, "Impact analysis of faults and attacks in large-scale networks," *IEEE Security & Privacy Magazine*, vol. 1, 2003, pp. 49-54.

[10] D. Trček, "Security Metrics Foundations for Computer Security," *The Computer Journal*, 2009.

[11] J.D. Sterman, *Business Dynamics: Systems Thinking and Modeling for a Complex World*, McGraw Hill Higher Education, 2000.

[12] O. Group, "OMG Unified Modeling Language (OMG UML), Infrastructure, V2.2," 2009.

[13] O. Group, "OMG Unified Modeling Language (OMG UML), Superstructure, V2.2," 2009.

[14] M. Myrtveit, "Object-oriented Extensions to System Dynamics," *Proceedings of the 17th International Conference of the System Dinamics Society*, 2000.

[15] W. Tignor and M. Myrtveit, "Object-oriented Design Patterns and System Dynamics Components," *Proceedings of the 17th International Conference of the System Dinamics Society*, 2000.

[16] A. Borshchev and A. Filippov, "From system dynamics and discrete event to practical agent based modeling: reasons, techniques, tools," *The 22nd International Conference of The System Dynamics Society*, 2004.