29th Annual INCOSE international symposium
Orlando, FL, USA
July 20 - 25, 2019

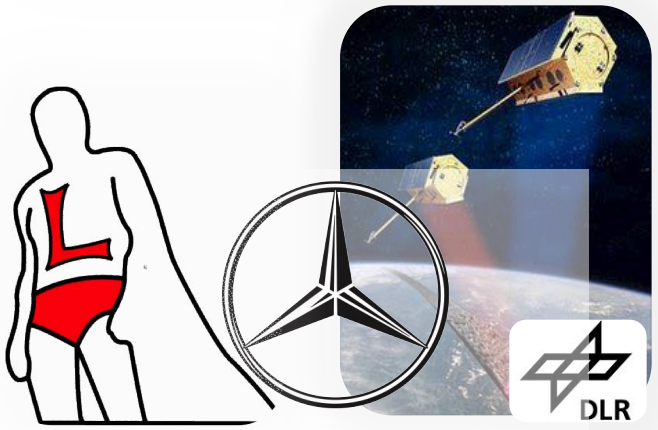
An Evaluation Ontology Applied to Connected Vehicle Security Assurance

Stephen Powley MEng MIET MINCOSE
Institute for Future Transport and Cities
Coventry University
powleys@uni.coventry.ac.uk

Thanks to:

Co-authors:
Simon Perry, Scarecrow Consultants
Jeremy Bryans, Coventry University
Jon Holt, Scarecrow Consultants

Reviewer:
James Towers, Object Flow



Mercedes-Benz

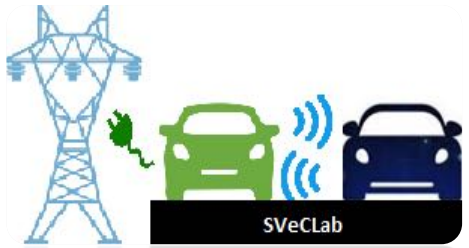
Stephen Powley MEng MIET MINCOSE

Research Institute
Future Transport and Cities

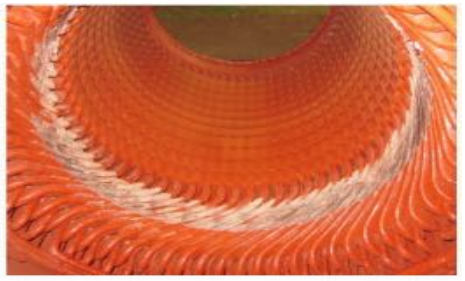
Coventry University

Systems Group

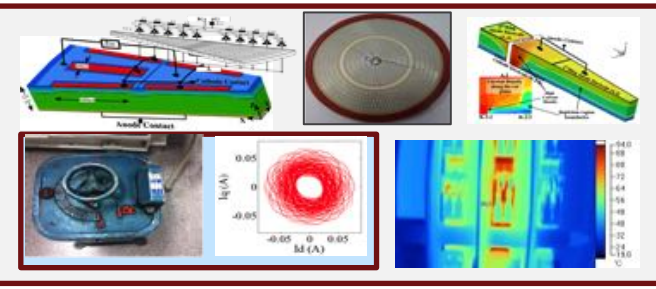
Threat Analysis
Security Validation
Penetration Testing
Software Assurance
Functional Safety (X/VDS)



Hybrid Electric/Electric Vehicles
Autonomous Vehicles
Connected Vehicles



Electrical Machines
Semi-Conductors
Battery Management
Power Drives and Controls



ASK

How can the organisations responsible for a connected vehicle ensure that it remains secure throughout its lifecycle?

ENABLING SYSTEMS ENGINEERING

Enabling **systems engineering**
by
engineering **enabling systems**

enabling system

A system that provides some or all of conditions necessary for the creation, existence, and/or destruction of one or more other whole or part systems of interest

Typically represents a set of organisations, individuals, tools, processes, and activities involved in conceiving, developing, maintaining, retiring, and destroying a purposeful system (or systems) or part thereof

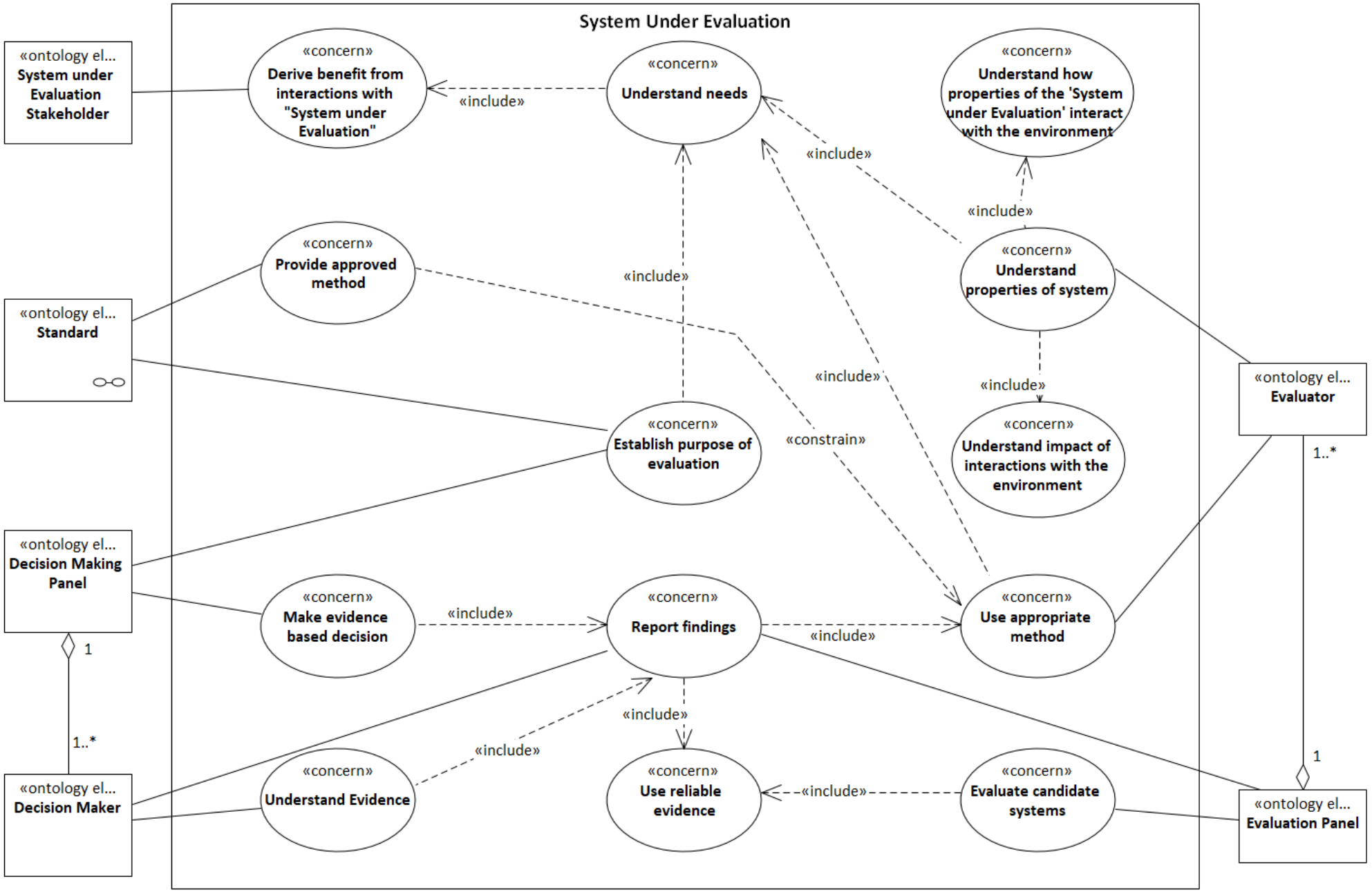
29th Annual INCOSE international symposium

Orlando, FL, USA

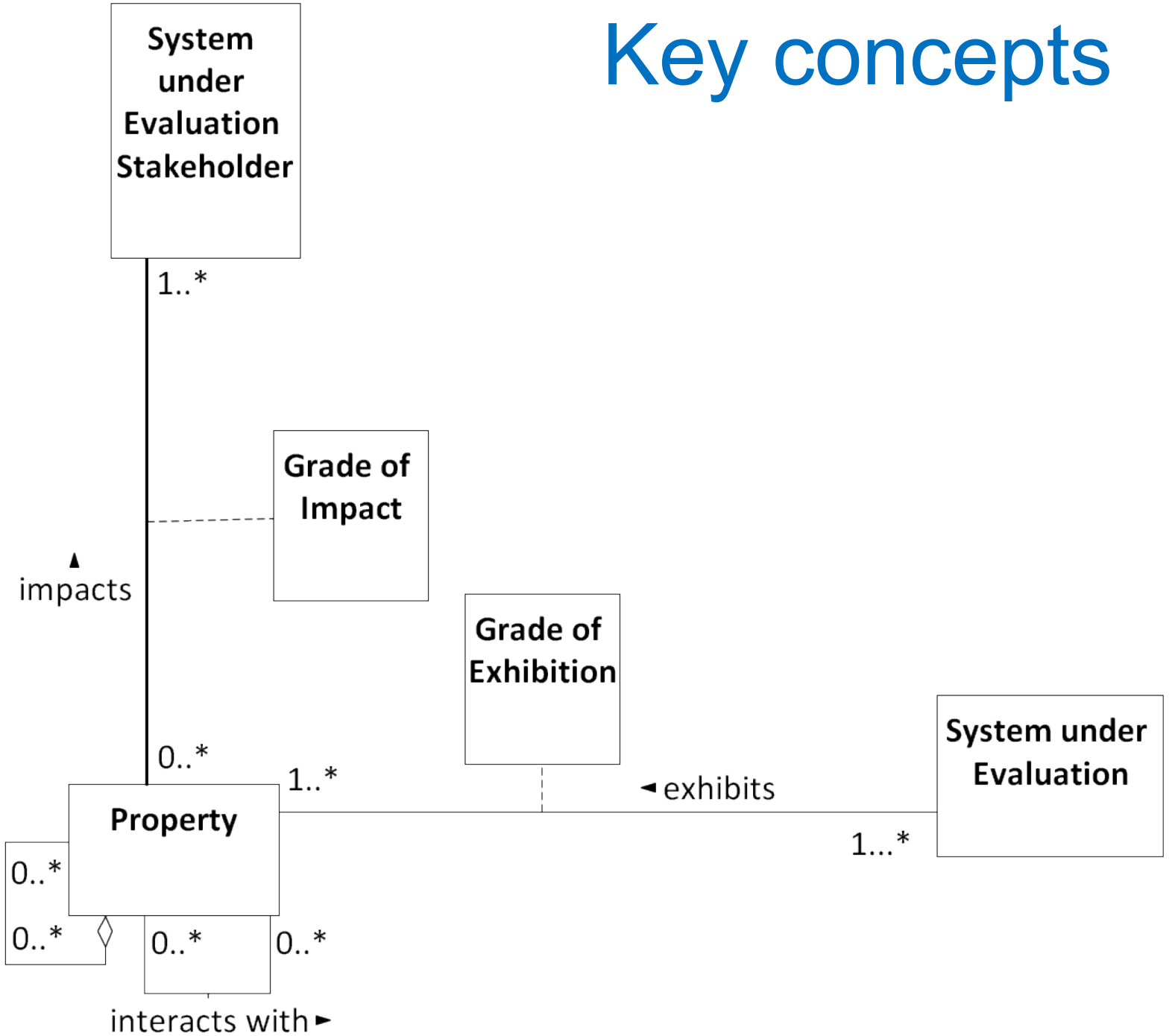
July 20 - 25, 2019

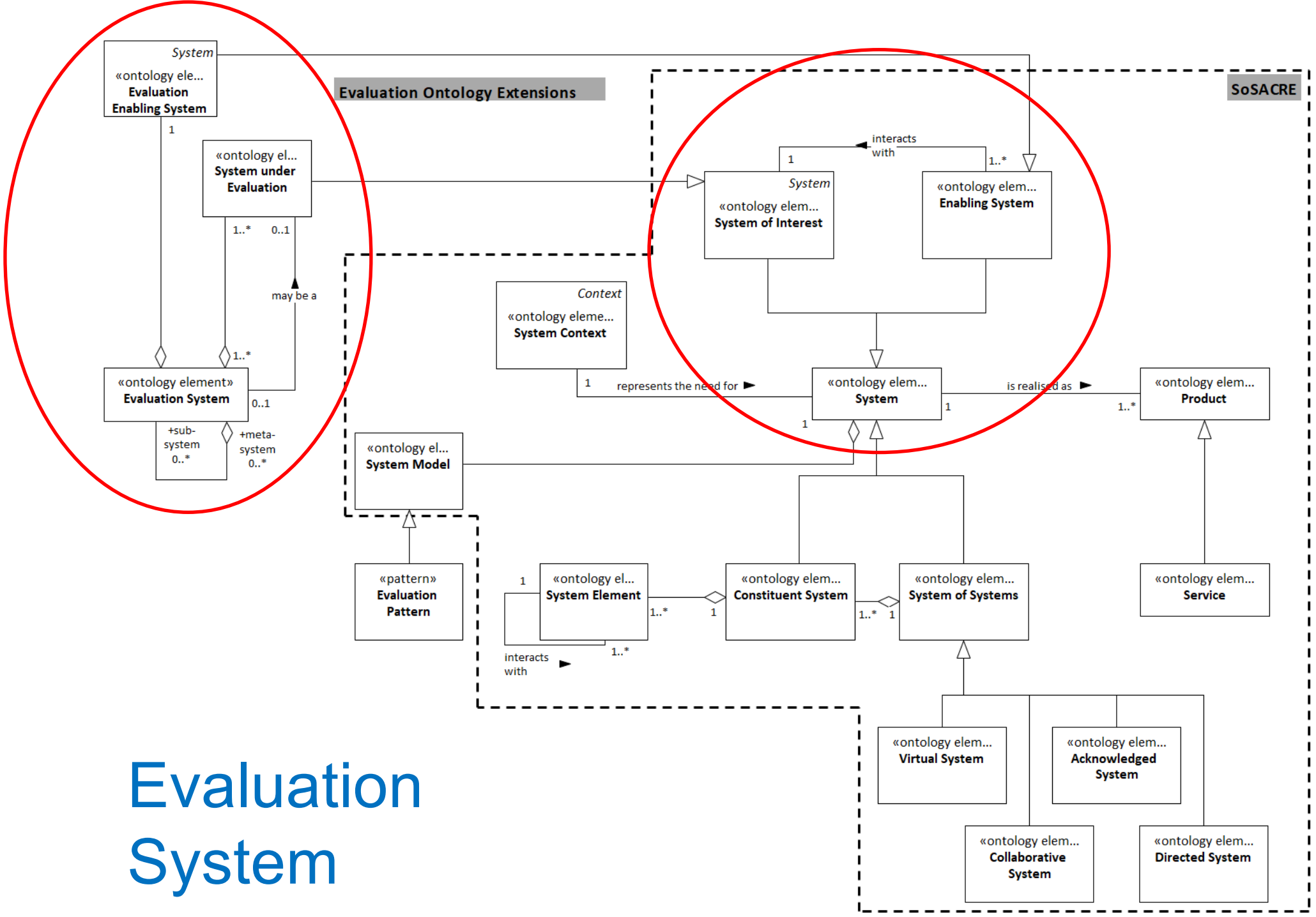
An Evaluation Ontology

Evaluation Pattern Context



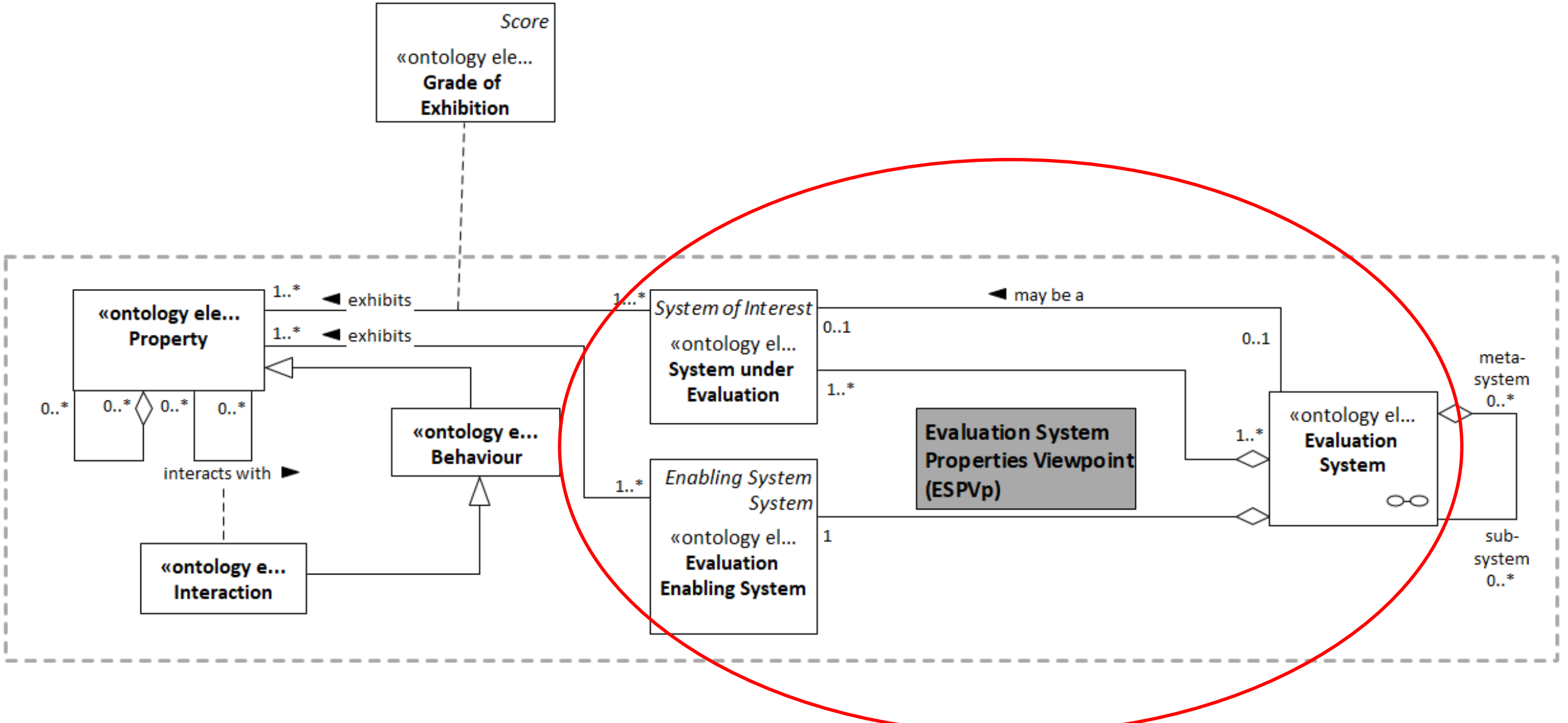
Key concepts

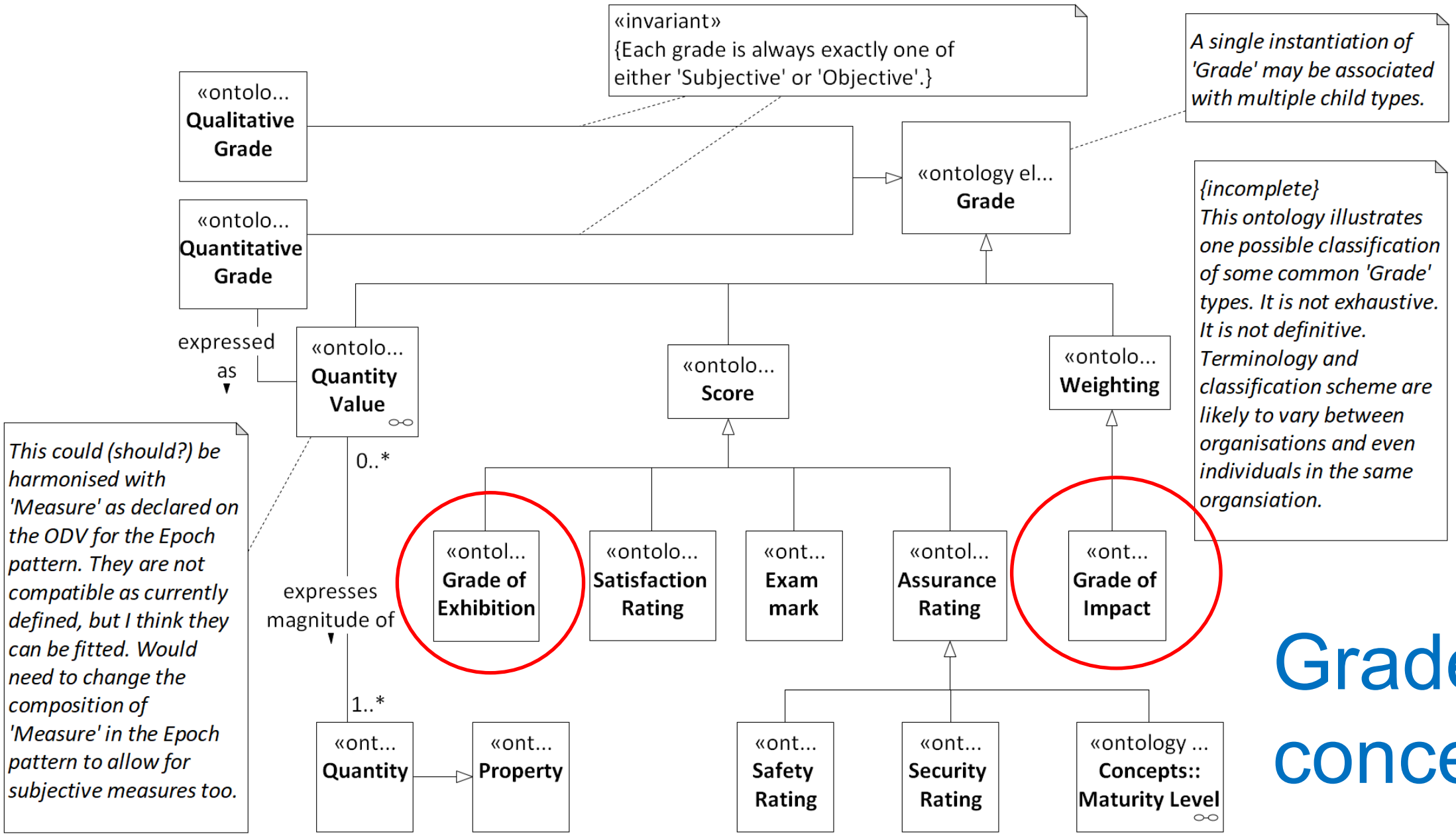




Evaluation System

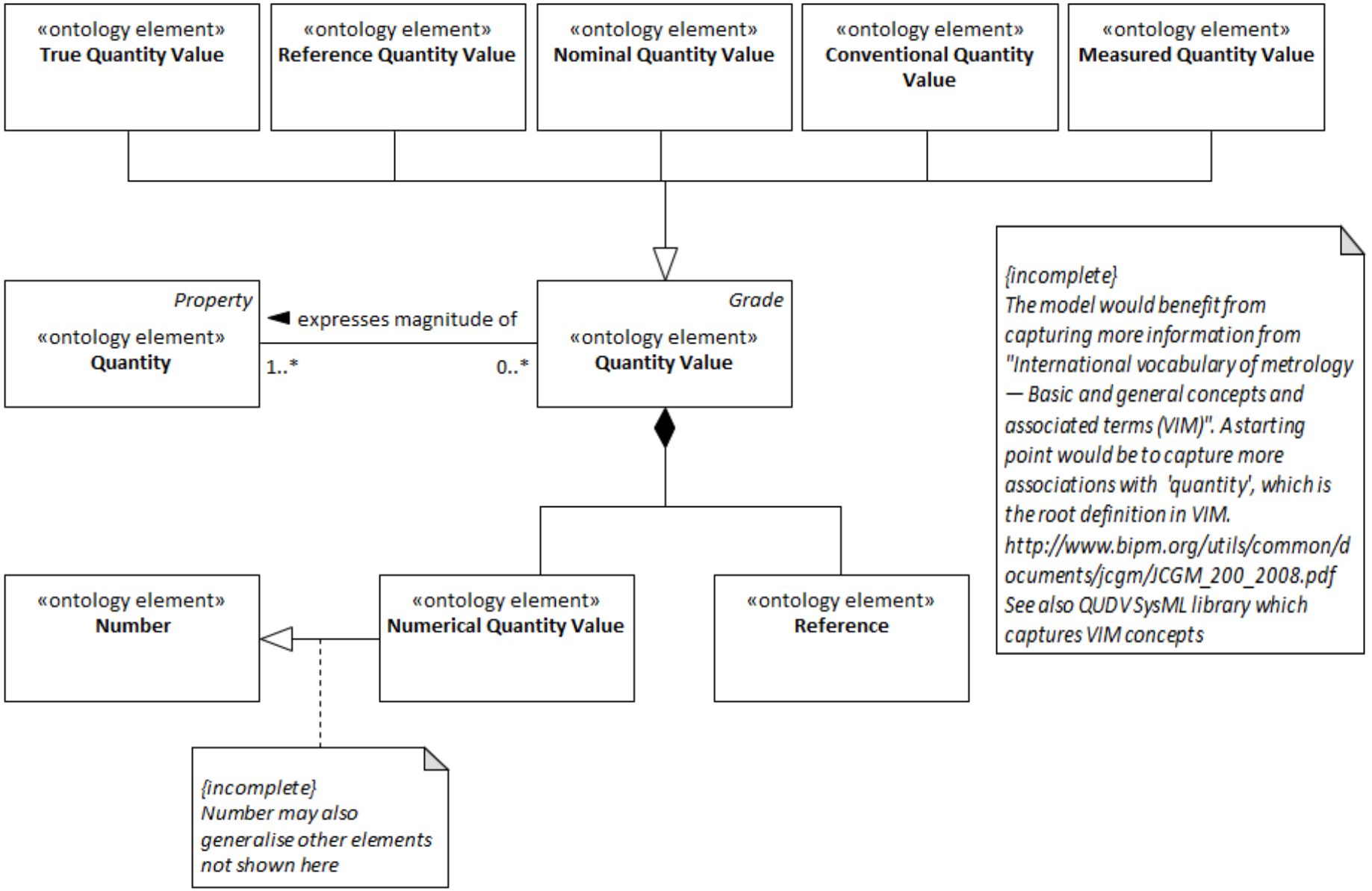
Evaluation System Properties Viewpoint

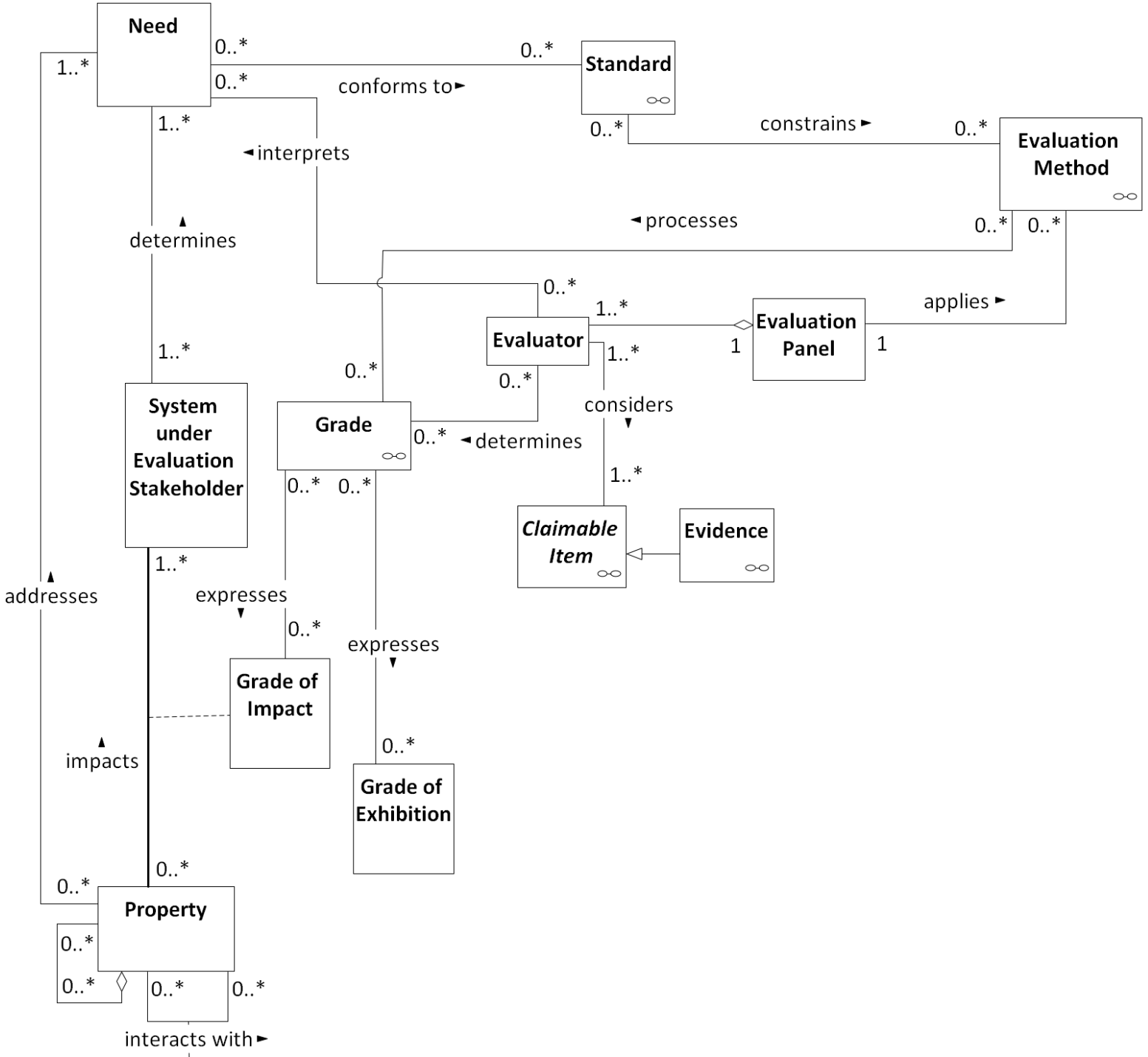




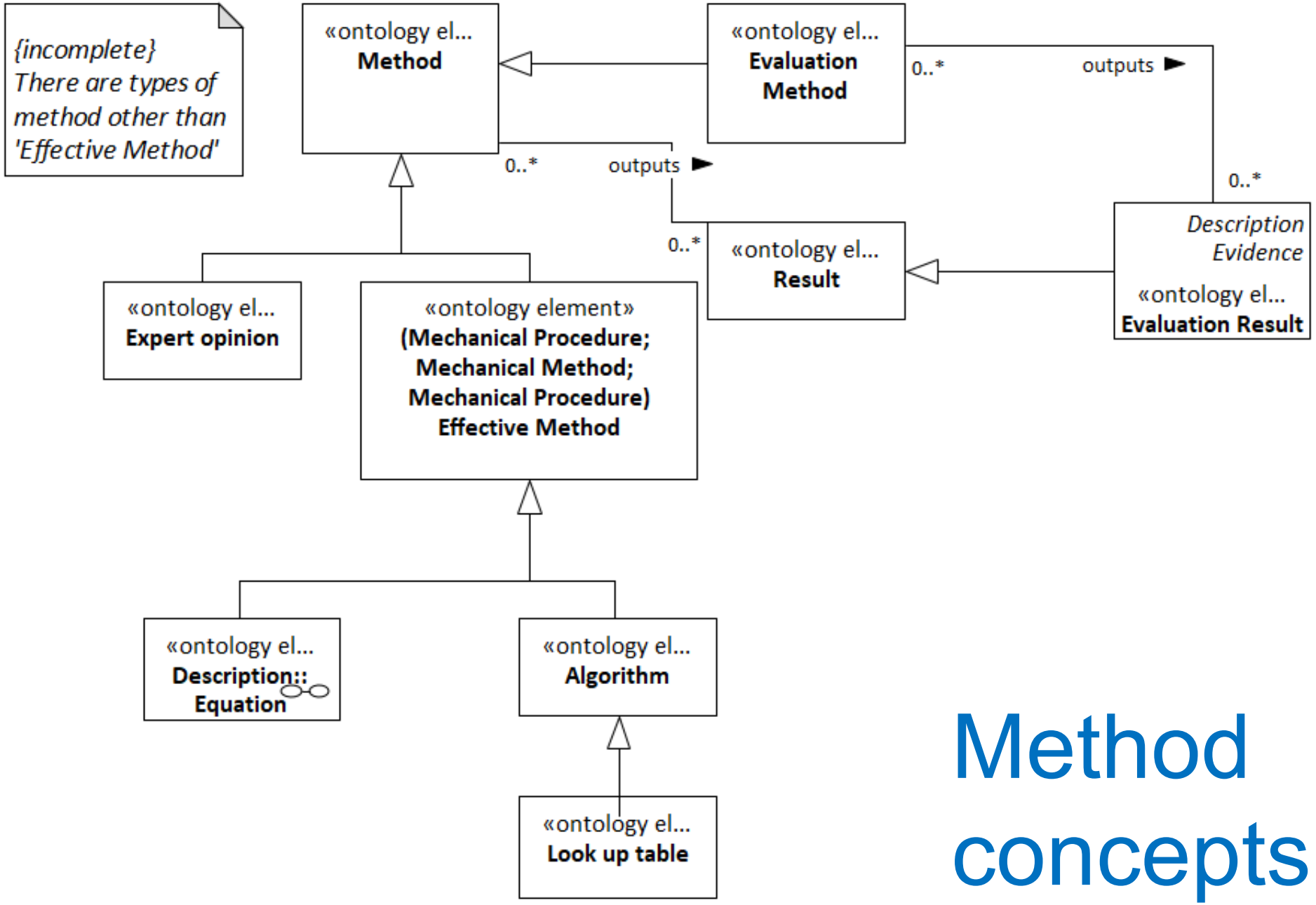
Grade concepts

Quantity Concepts



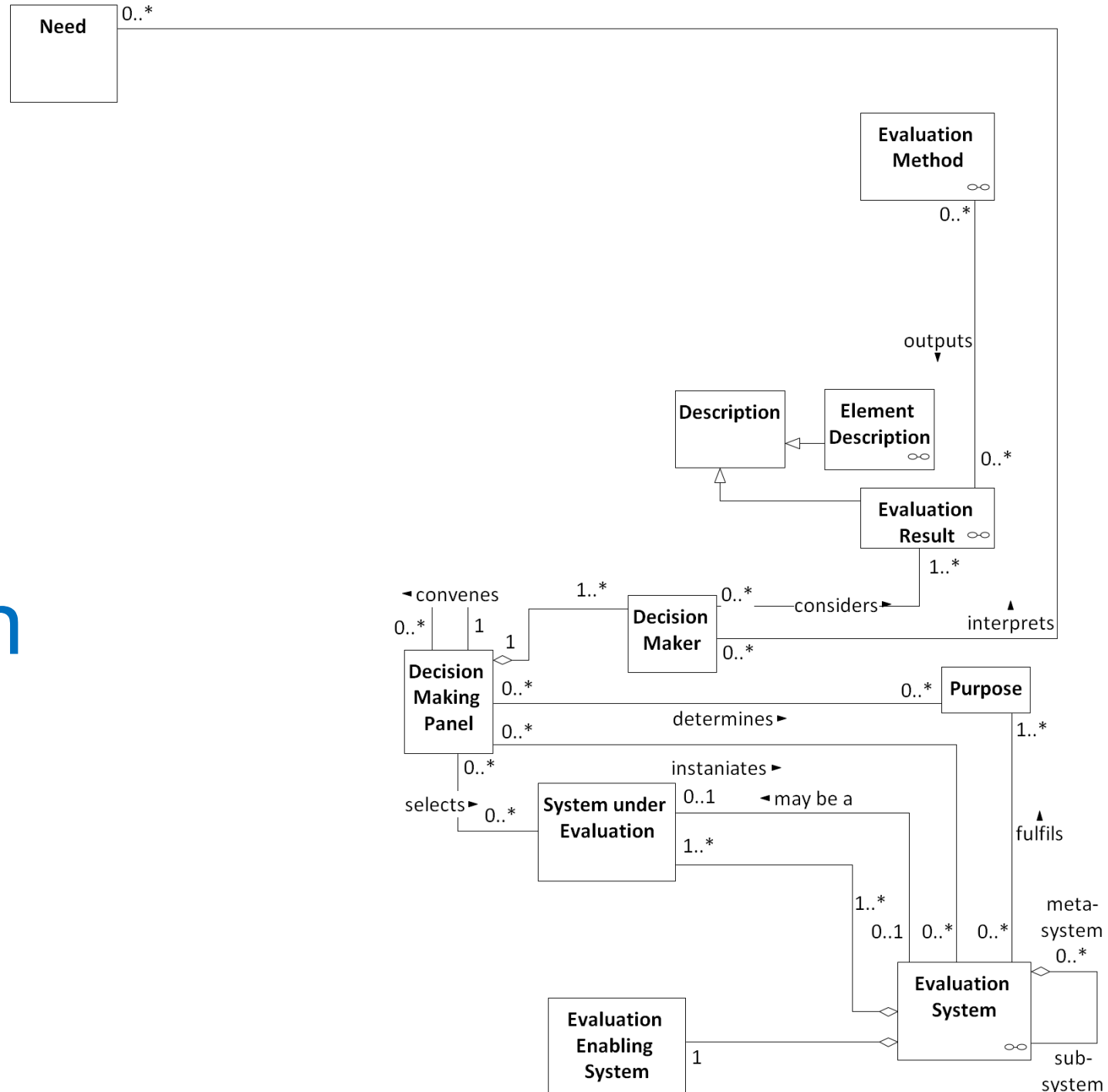


Evaluation Panel Viewpoint

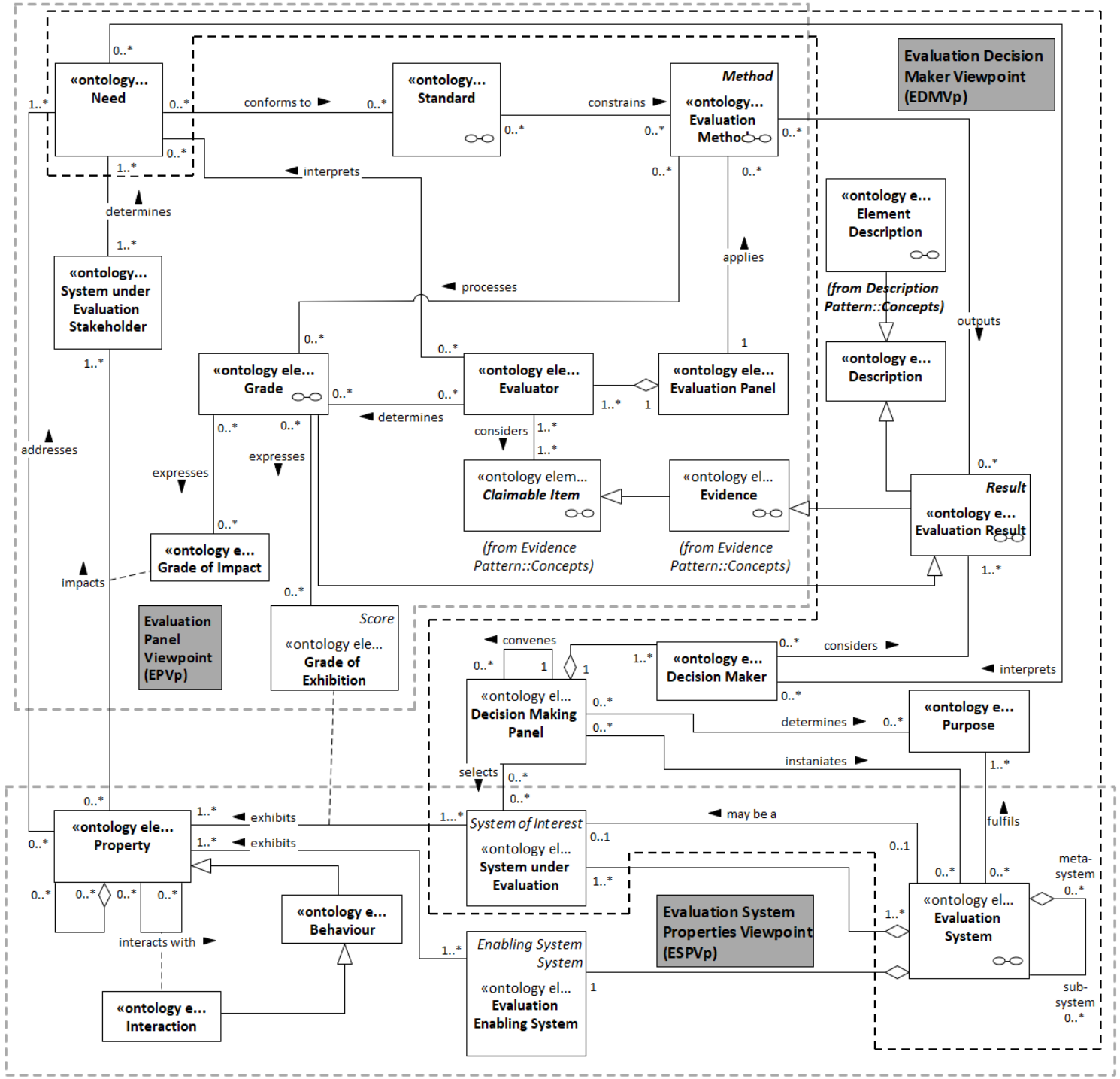


Method concepts

Evaluation Decision Maker Viewpoint



Ontology Definition View showing Evaluation Ontology concepts

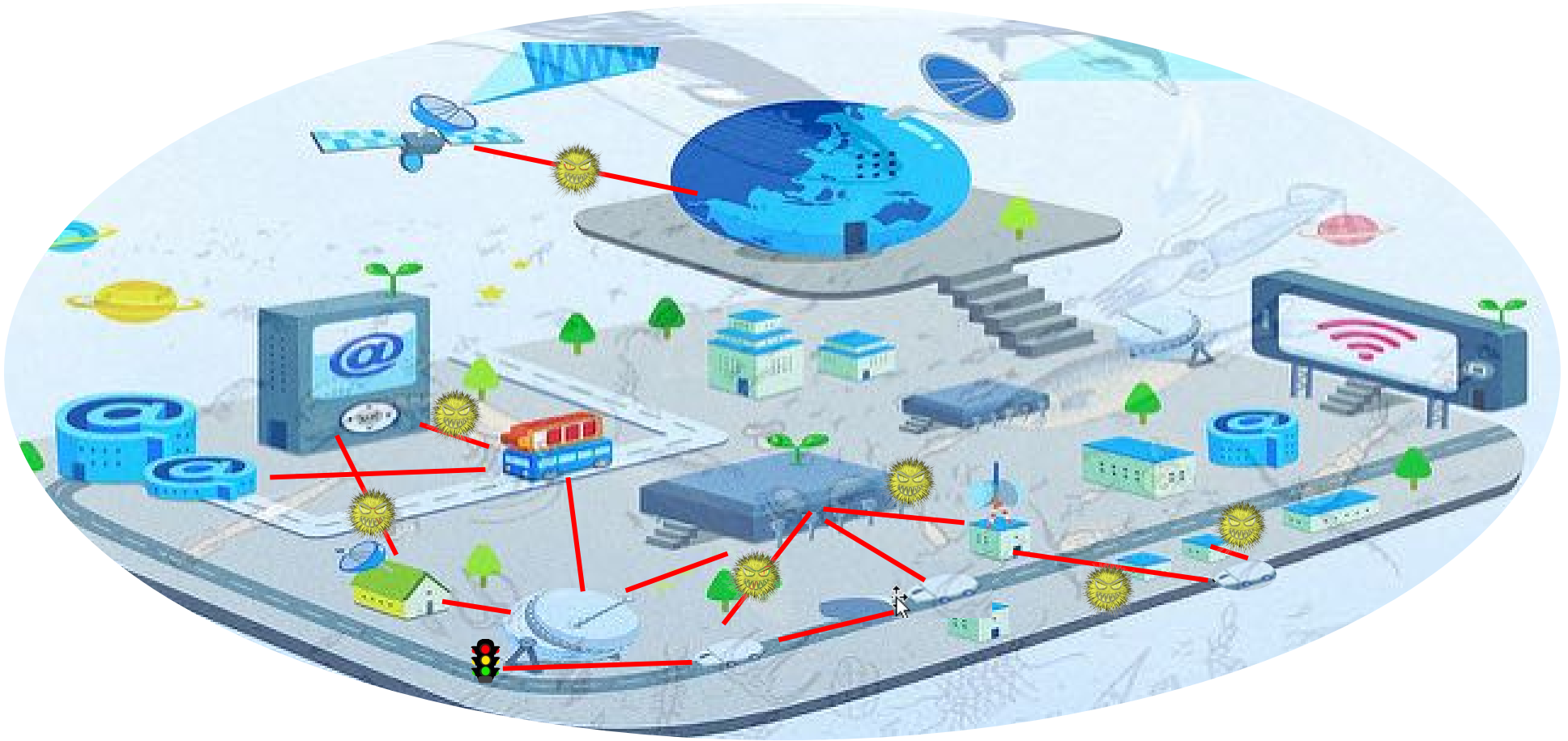


29th Annual INCOSE international symposium

Orlando, FL, USA

July 20 - 25, 2019

Application to Connected Vehicle Security Assurance



Connected Vehicle Security - What's the problem?

Connected systems

- Communication between vehicles
- Communication with infrastructure
- In future, an even greater number of devices sharing even more data
- Risk to life, risk to privacy

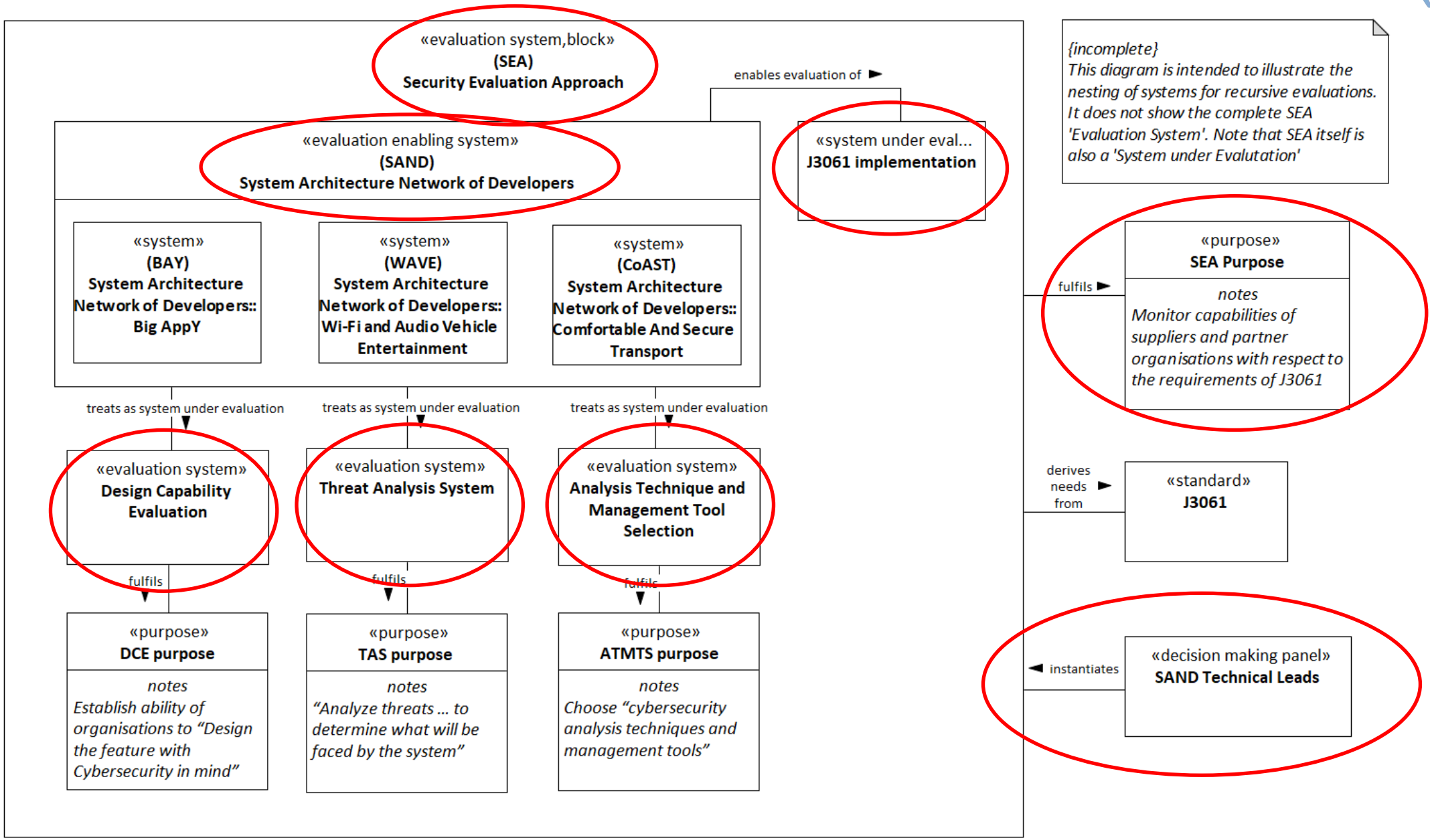
Complex, nested systems of systems (SoSs)

- Unprecedented complexity (uncertain relationships between cause and effect)
- Products and services (things, infrastructure, data storage, analytics, apps, …)
- Enabling system(s) (people, processes & tools in the responsible enterprise)

Lack of standard best-practice

- Disparate stakeholders have to agree what achieving acceptable security means and how to determine success (end users, employees, manufacturers, regulators, shareholders, road users, infrastructure systems, connected vehicles, emergency services, app developers, governments, malicious actors

Security assurance example



Benefits

- Describe evaluations and their dependencies across organisations
- Combine disparate evaluation types to roll-up evaluation results
- Identify areas of good/poor practice by querying aggregated evaluations
- Control granularity to match level of rigour expected
- Conduct gap analysis between existing and required capabilities
- Improve decision making through better business intelligence
- Quantify the impact of decision making processes on the quality of upstream/downstream evaluations
- Generate automated compliance evidence for security audits

Stephen Powley MEng MIET MINCOSE Research Centre Future Transport and Cities powleys@uni.coventry.ac.uk

29th Annual INCOSE international symposium

Orlando, FL, USA

July 20 - 25, 2019

www.incose.org/symp2019