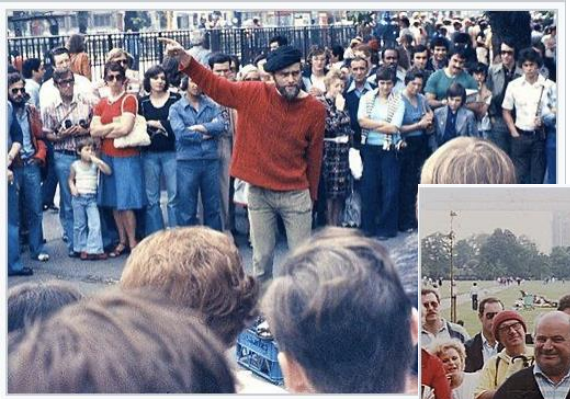
Good morning and Welcome!



Orator at Speakers' Corner in London, 1974

Speakers' Corner, April 1987

Standards (nowadays) are bad…e.g., X, Y, Z

AI is more than LLMs and ML..

AI standards are popping up.. ..influenced by a bad agenda..

Safety is not

Safety is..

Not explainable yet..

Not explainable ..

SCC-Speaker's Corner

Sources:

https://commons.wikimedia.org/wiki/File:Orator_at_Speakers_Corner_London_with_crowd_1974.jpg
https://upload.wikimedia.org/wikipedia/commons/5/5d/Hydeparkapril87.jpg

Unstructured expert opinions..counterclaims/defeaters?

AI is more than LLMs and ML.. Knowledge representation and reasoning (inference..)..

Barbara Gallina

Mälardalens universitet

Grateful to be here today!

Disclaimer: I'm not a knowledge engineer

SCC-Speaker's Corner

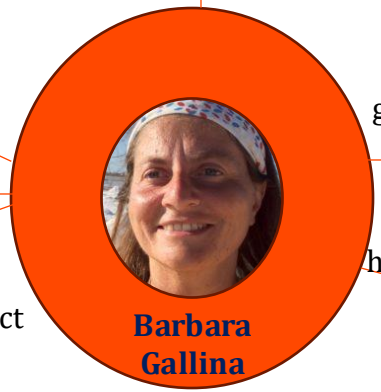
conducts research aligned with

Associate professor of dependable software systems

plays role

employed at

Mälardalens universitet



Barbara Gallina

gives presentation on

Ontology-based representation for assurance and compliance

has e-mail address

barbara.gallina@mdu.se

DVA437 Safety Critical Systems Engineering-H25
OAI400 Functional Safety of Battery Management Systems (BMS)-H25

manages & teaches

runs research project

Collaborates within

#49-∞COMPASS – Continuous Regulatory Compliance and Assurance of Socio-technical Systems – focus on variability/traceability management

has partner

Collaborates within

Software Center

BOSCH DEIF GRUNDFOS

A graph-based knowledge representation!

Assuming the underlying existence of:
an ontological underpinning
and reasoning engine

it is Knowledge Graph!

Outline

- **What is a knowledge graph?**
- **What is an ontology?**
- **How can an ontology be developed?**
- **How can an ontology be represented?**

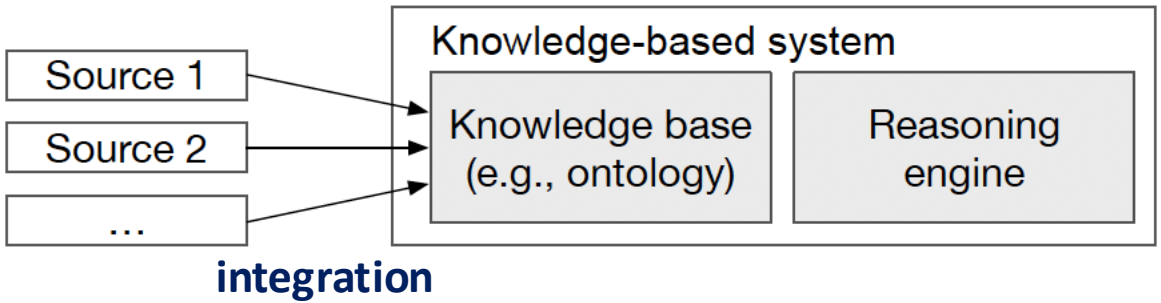
- **Why does all this matter for assurance and compliance?**

- **What is assurance?**
- **What is compliance?**

- **Pieces of solution towards the ontology-based representation for assurance and compliance**

What? Knowledge Graph

“A knowledge graph acquires and integrates information into an ontology and applies a reasoner to derive new knowledge.”



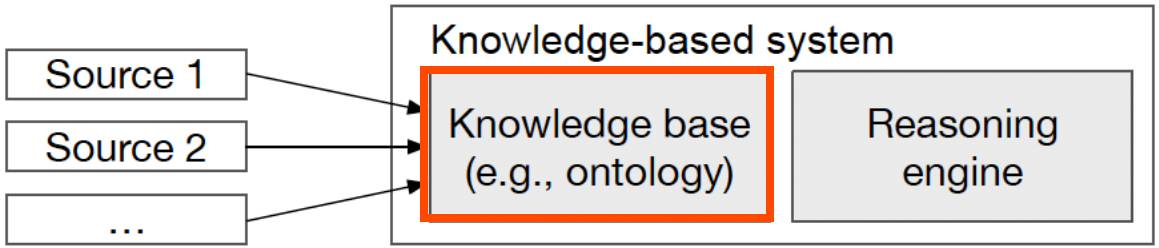
Lisa Ehrlinger and Wolfram Wöß. *Towards a Definition of Knowledge Graphs.*
Joint Proceedings of the Posters and Demos Track of the 12th International Conference on Semantic Systems- SEMANTiCS2016 and the 1st International Workshop on Semantic Change & Evolving Semantics (SuCCESS'16)
co-located with the 12th International Conference on Semantic Systems (SEMANTiCS 2016)
Leipzig, Germany, September 12-15, **2016**.

Do you know any knowledge graph?

The Semantic Web!

What? Ontology

An ontology is a formal description providing human users a shared understanding of a given domain



What? Ontology engineering

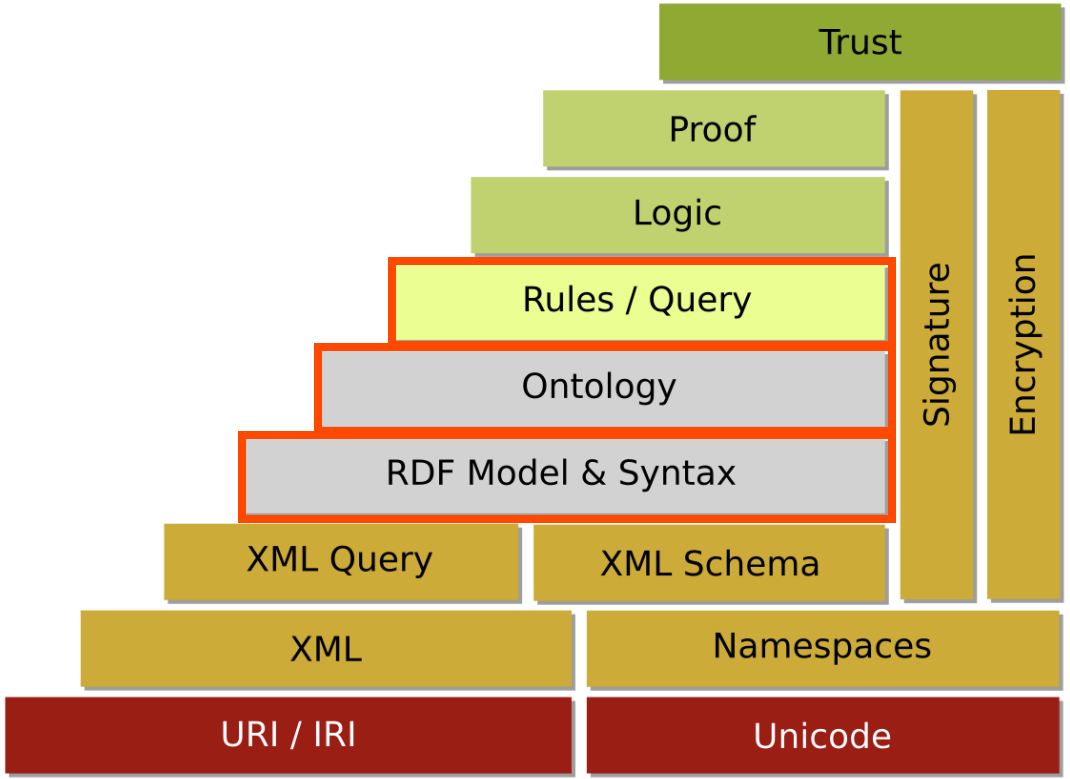
METHONTOLOGY:
From Ontological Art Towards Ontological Engineering

Mariano Fernández, Asunción Gómez-Pérez, Natalia Juristo

Specification – purpose specification, *competency questions (*)*
Conceptualisation – terms distinguished from verbs
Formalisation – transform the conceptual model of the ontology into a formal model
Integration
Implementation
Maintenance

(*) questions that the ontology must be able to answer
Competency questions capture the functional requirements of the ontology

What? Ontology representation



Source: https://it.wikipedia.org/wiki/File:W3c-semantic-web-layers.svg

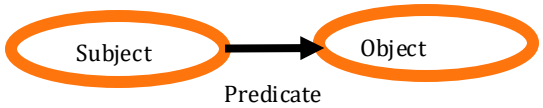
What? RDF –Resource Description Framework

A standard for capturing triples

a simple language for writing statements about Web resources identified by URIs.

An RDF document is a set of RDF statements

An RDF statement expresses a relationship between two resources.
The **subject** and the **object** represent the two resources being related
The **predicate** represents the nature of their relationship
The relationship is phrased in a **directional way** (from subject to object) and is called in RDF a **property**.
We can visualize triples as a connected **graph**. Graphs consists of nodes and arcs.



Informal textual representation of the previous graph-based representation

Barbara Gallina	**plays role**	**Associate Professor of Dependable Software Systems**
Barbara Gallina	**gives presentation on**	**Ontology-based representation for assurance and compliance**
Barbara Gallina	**runs project**	**#49-4DASafeOps**
#49-4DASafeOps	**has partner**	**Bosch**

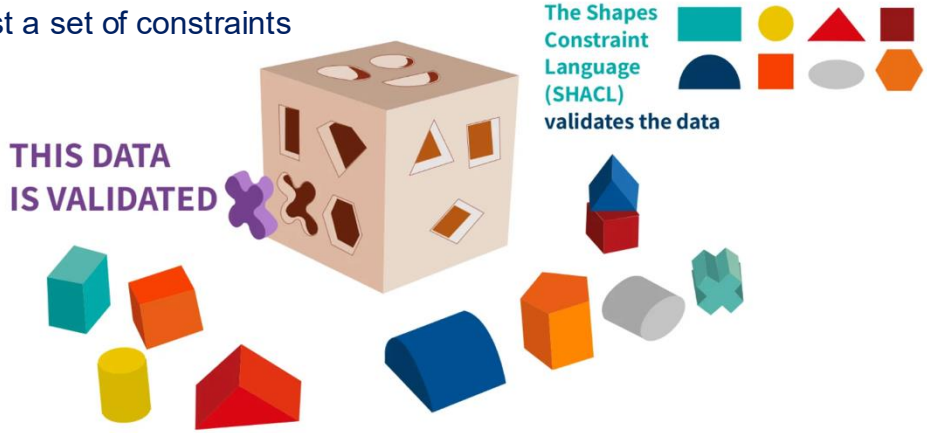
Source: https://www.w3.org/TR/rdf11-primer/#section-data-model

What? OWL

OWL-Web Ontology Language
Allows for the definition of the semantics of RDF statements.
The main building blocks of an OWL ontology are classes.

What? SHACL

A standard for a language for validating RDF graphs against a set of constraints



[source: https://www.ontotext.com/knowledgehub/fundamentals/what-is-shacl/]

What? SPARQL

SPARQL-SPARQL Protocol and RDF Query Language
A standard for querying the knowledge graphs, as well as constructing them

Query forms:

-SELECT - Returns all, or a subset of, the variables bound in a query pattern match

-CONSTRUCT -Returns an **RDF graph** constructed by substituting variables in a set of triple **templates**

-ASK - Returns a boolean indicating whether a query pattern matches or not

-DESCRIBE -Returns an **RDF graph** that describes the resources found

Why does all of this matter for assurance and compliance?

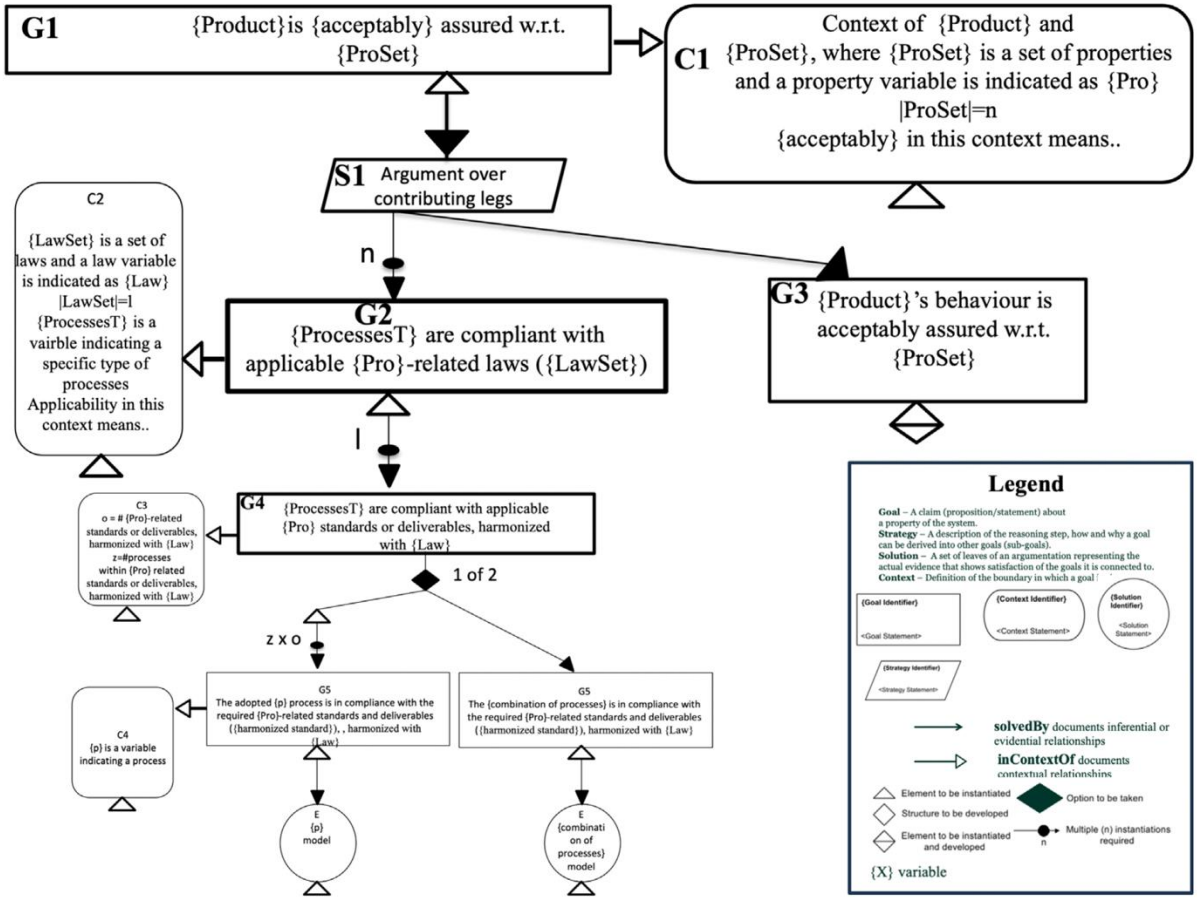
What? Assurance

Assurance **“grounds for justified confidence that a claim has been or will be achieved”**
[ISO/IEC JTC 1/SC 7, ISO/IEC 15026: Systems and software engineering — Systems and software assurance, Part 1: Concepts and vocabulary (2019)]

Multiconcern assurance means grounds for justified confidence that:
multi-concern claims have been or will be achieved, as well as
arguments that those claims about multi-concerns are justified by the evidence about the system

Concern: **safety**, security, **sustainability**, explainability..

What? Assurance

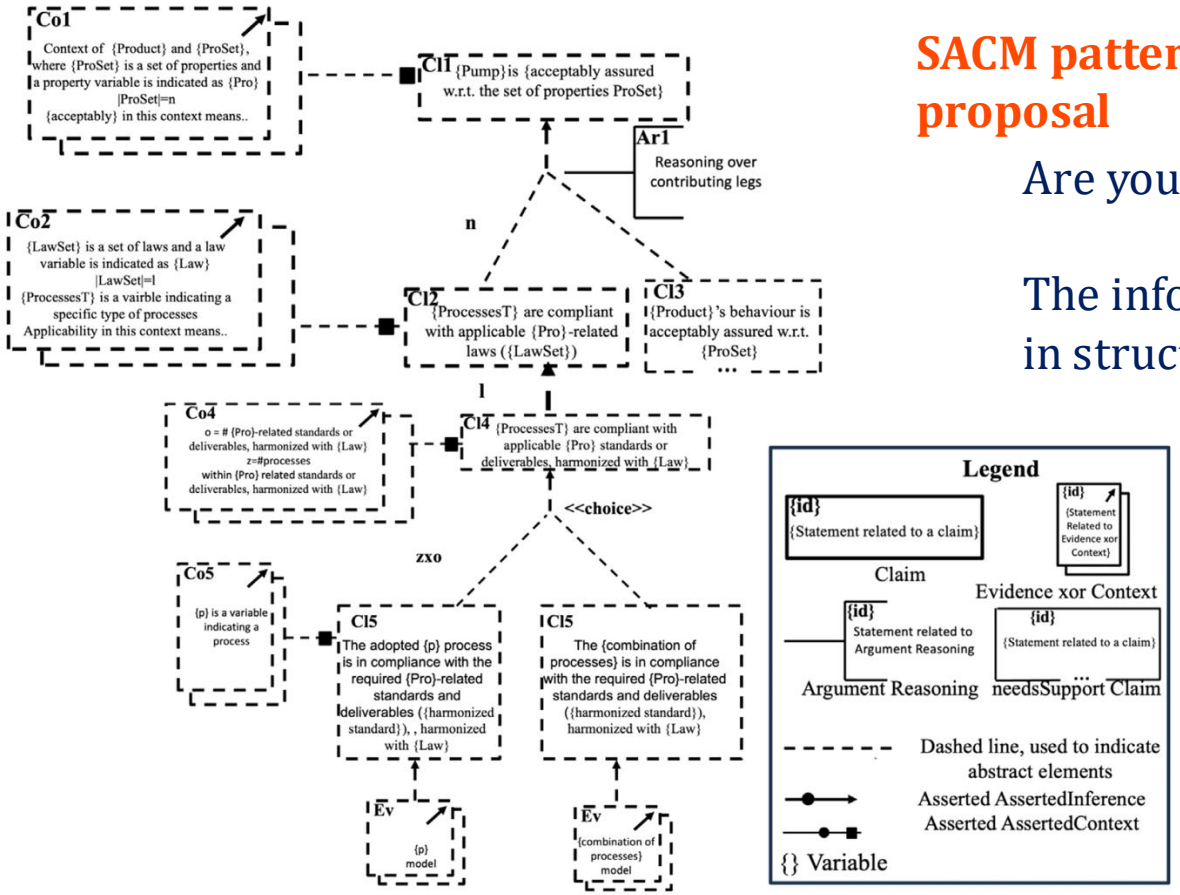


GSN pattern proposal

By the way, would a GSN co-pilot be useful here?

In my opinion, no (too many faulty examples)

What? Assurance



SACM pattern proposal

Are you instead **text-inclined**?

The information could be rendered in structured prose!

By the way, would a SACM co-pilot be useful here?

In my opinion, no (too few examples)

What? Compliance

Compliance **“meeting all the organization’s compliance obligations”**

[ISO 37301:2021 Compliance management systems — Requirements with guidance for use]

Compliance obligations - **“ requirements that an organization mandatorily has to comply with as well as those that an organization voluntarily chooses to comply with. ”**

[ISO 37301:2021 Compliance management systems — Requirements with guidance for use]

Compliance Obligations: example

29.6.2023 EN Official Journal of the European Union L 165/1

I

(Legislative acts)

Machinery Regulation

REGULATIONS

REGULATION (EU) 2023/1230 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 June 2023

on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC

(Text with EEA relevance)

Directives provides:

Essential health and safety requirements relating to the the design and construction of machinery

→process of risk assessment and risk reduction

Compliance Obligations: examples

- **On 17 October 2024, the Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 entered into force.**
- **On 25 July 2024, the Directive on corporate sustainability due diligence (Directive 2024/1760) entered into force.**
- **On 17 August, 2023, Regulation (EU) 2023/1542 of the European Parliament and of the Council of 12 July 2023 concerning batteries and waste batteries has entered into force.**
- **On 1 August, 2024, The AI Act - Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence has entered into force.**
- **Product Liability Act ...**

Interplay including synergies, potential conflicts, redudancy

When is it necessary to care about assurance and compliance?

…continuously…

Typical *Kaizen* PDCA cycle

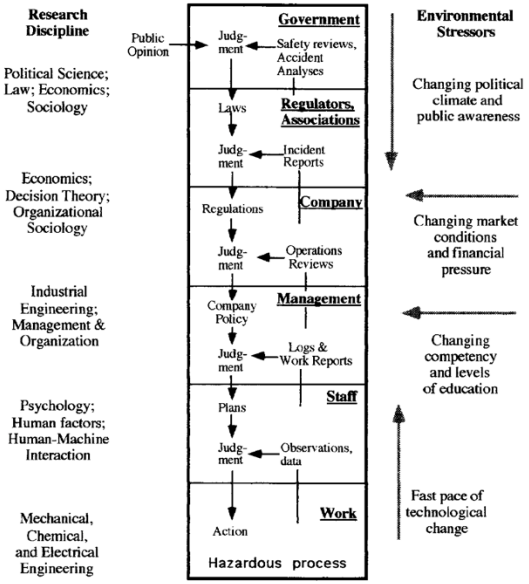
Change for the better
Continuous improvement

Claims + Evidence
Claims + Argument + Evidence

[ISO 37301:2021 Compliance management systems — Requirements with guidance for use]

Vision: Knowledge graph capturing the socio-technical system – en evolving system

[Gallina et al.2024a]



J. Rasmussen, "Risk management in a dynamic society: a modelling problem," *Safety Science*, vol. 27, no. 2, pp. 183–213, 1997.

J. Rasmussen and I. Svedung, *Proactive Risk Management in a Dynamic Society*. Swedish Rescue Services Agency, 2000.

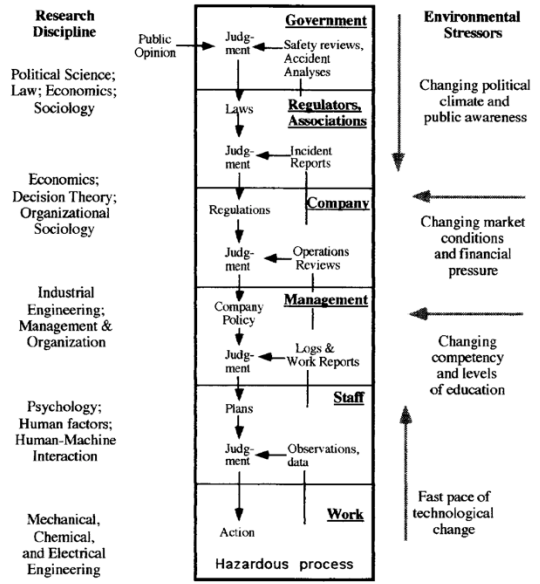
• A very fast pace of change of technology is found at the operative level of society within many domains, such as transport, shipping, manufacturing and process industry. This pace of change is much faster than the pace of change presently in management structures — Savage and Appleton (1988) talk of ''second generation management applied to fifth generation technology'' in manufacturing. An even longer lag in response to change is found in legislation and regulation. The different time lags found at the different levels thus present a problem, and the dynamic interaction among levels during a period of change becomes an important modelling issue.

In this situation we need more studies of the vertical interaction among the levels of socio-technical systems with reference to the nature of the technological hazard they are assumed to control.

Calls for closed loop feeback control..

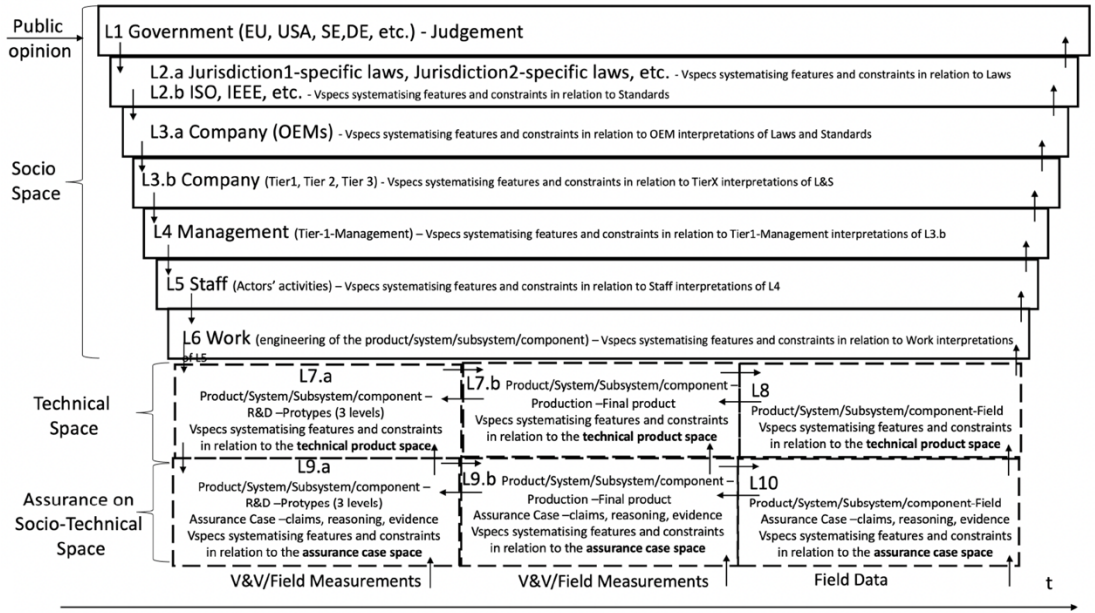
Vision: Knowledge graph capturing the socio-technical system – en evolving system

[Gallina et al.2024a]



J. Rasmussen, "Risk management in a dynamic society: a modelling problem," *Safety Science*, vol. 27, no. 2, pp. 183–213, 1997.

J. Rasmussen and I. Svedung, *Proactive Risk Management in a Dynamic Society*. Swedish Rescue Services Agency, 2000.



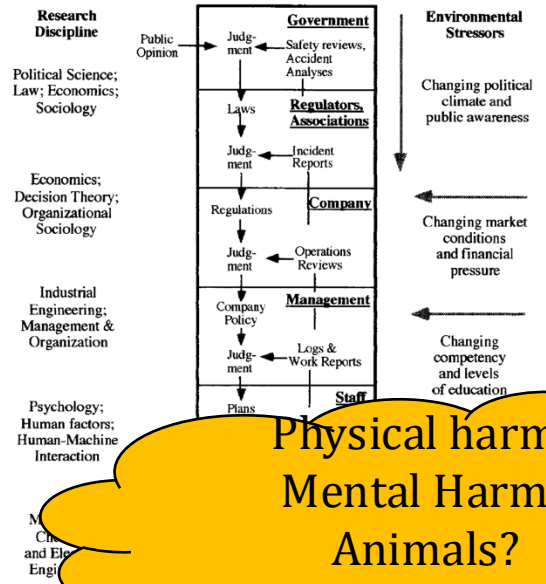
B. Gallina, Peter Munk, Markus Schweizer.
An Extension of the Rasmussen Socio-technical System for Continuous Safety Assurance.
Proceedings of 8th International Workshop on Critical Automotive Applications: Robustness & Safety (C[illegible]
Leuven, Belgium, April 8th, 2024. Soon available at HAL archives ouvertes.fr

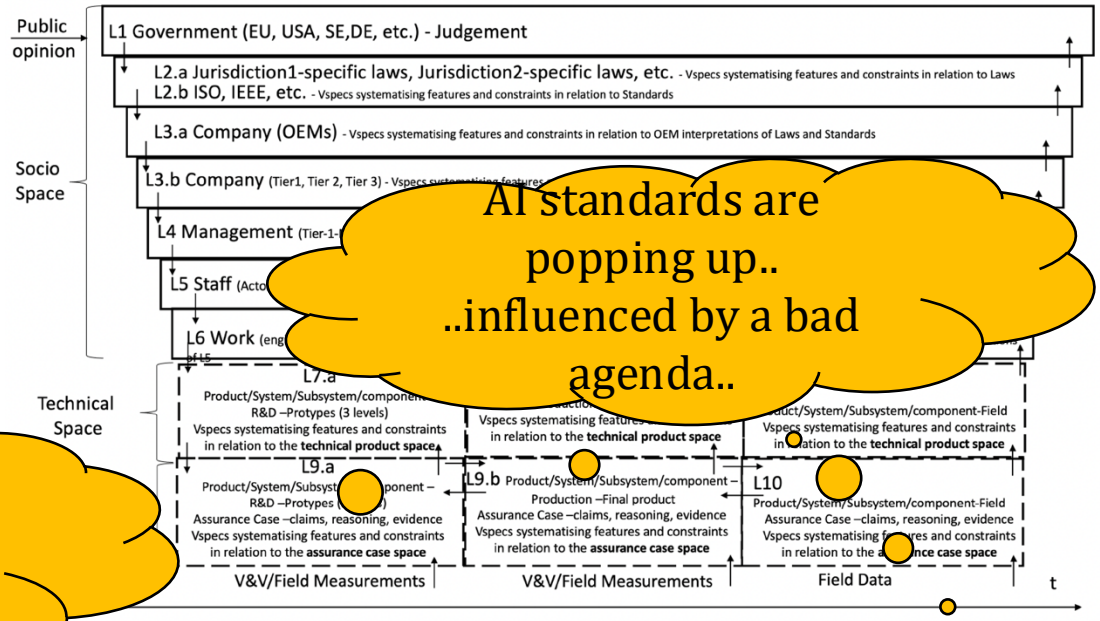
B. Gallina, T. Young Olesen, E. Parajdi, and M. Aarup.
A Knowledge Management Strategy for Seamless Compliance with the Machinery Regulation.
30th European & Asian Systems, Software & Service Process Improvement & Innovation (EuroSPI), Communications in Computer and Information Science (CCIS), vol. 1890, Springer Cham, pp. 220-234, DOI: 10.1007/978-3-031-42307-9_17, Grenoble, France, August 30.-September 1. 2023.

Variability in space and time..

Vision: Knowledge graph capturing the socio-technical system – en evolving system

[Gallina et al.2024a]





AI standards are popping up..
..influenced by a bad agenda..

Physical harm?
Mental Harm?
Animals?
etc.

J. Rasmussen, "Risk management in a dyna modelling problem," *Safety Science*, vol. 27, no. 2, pp. 183–213, 1997.

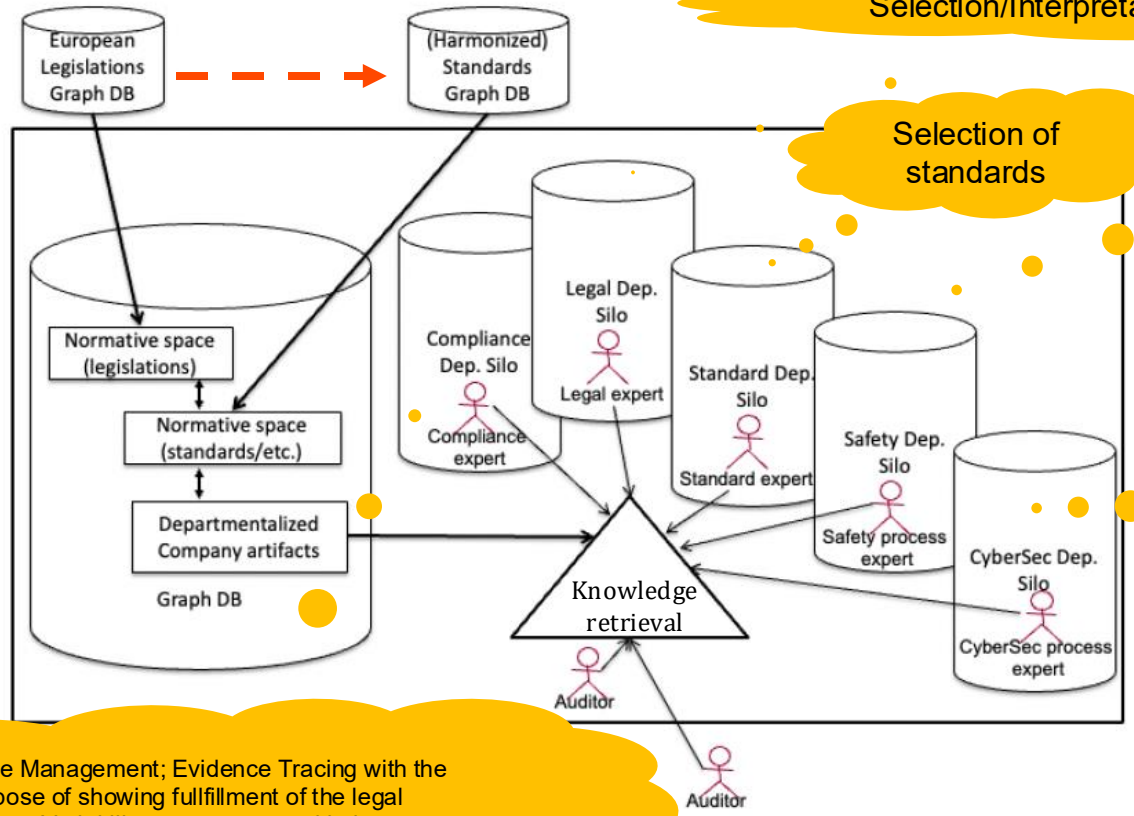
J. Rasmussen and I. Svedung, *Proactive Risk Management in a Dynamic Society*. Swedish Rescue Services Agency, 2000.

B. Gallina, Peter Munk, Markus Schweizer.
An Extension of the Rasmussen Socio-technical System for Continuous Safety Assurance.
Proceedings of 8th International Workshop on Critical Automotive Applications: Robustness & Safety (C
Leuven, Belgium, April 8th, 2024. Soon available at HAL archives ouvertes.fr

B. Gallina, T. Young Olesen, E. Parajdi, and M. Aarup.
A Knowledge Management Strategy for Seamless Compliance with the Machinery Regulation.
30th European & Asian Systems, Software & Service Process Improvement & Innovation (EuroSPI), Communications in Computer and Information Science (CCIS), vol. 1890, Springer Cham, pp. 220-234, DOI: 10.1007/978-3-031-42307-9_17, Grenoble, France, August 30.-September 1. 2023.

Variability in space and time..

Vision: Knowledge Engineering within Highly Regulated Companies



Selection/Interpretation of laws

Selection of standards

Safety Risk Assessment and control

Security Risk Assessment and control

Sustainability Risk Assessment and control

Evidence Management; Evidence Tracing with the purpose of showing fullfillment of the legal requirements; Variability management with the purpose of reusing as well as managing the impact of changes

Vision: Goals

- Capturing conceptually connected heterogeneous information in order to:
  - guarantee seamless traceability,
  - enable semi-automated multi-concern assurance argumentation
  - streamline auditing / regulatory compliance demonstration
- Braking the silos by connecting people with heteterogeneous background or competence
- On demand-Knowledge Retrieval
- Flexible evolution

IEC Open systems dependability IEC 62853

Edition 1.0 2018-06

Frame of reference

Pieces of solution towards the ontology-based representation
Yet another glass cage (?)

Pumps product line and corresponding regulations

The physical world meets the digital world

- Transforming the pump to a digital pump using IoT connectivity, AI and sensing capabilities

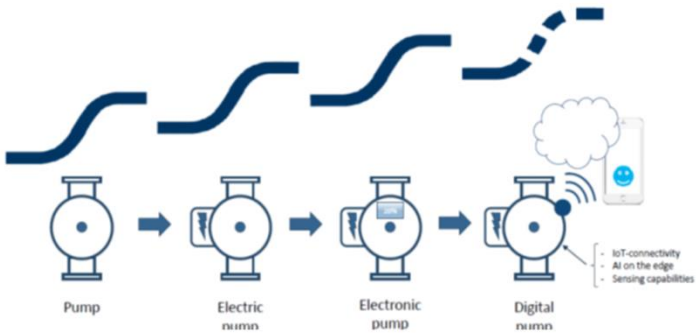


Image source: Grundfos

[https://iot.telenor.com/iot-case/grundfos/]

EN 809:1998 + A1:2009
Pumps and pump units for liquids – Common safety requirements

ISO 12100: 2010 -Safety of machinery- General principles for design — Risk assessment and risk reduction

Machine Directive
2006/42/EC

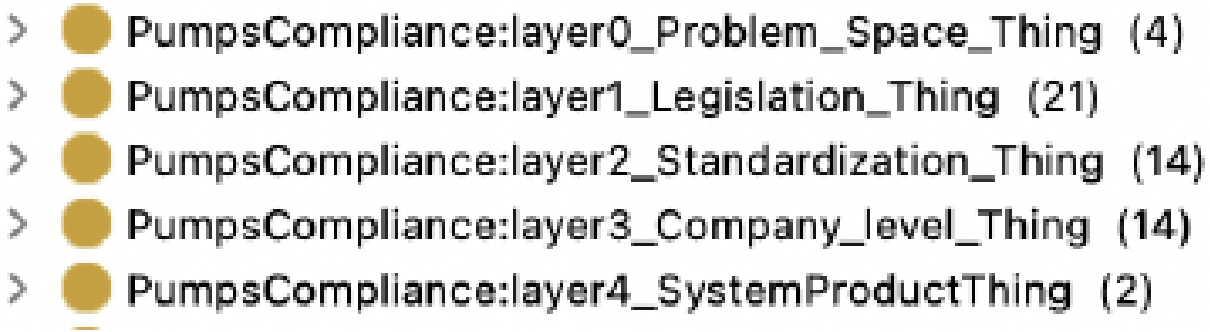
Machine Regulation

Cybersecurity Act
Cyber Resilience Act

Artificial Intelligence Act
Trustworthy AI Guidelines

A layered ontology-based representation of the socio-technical system

[Gallina et al.2024c]

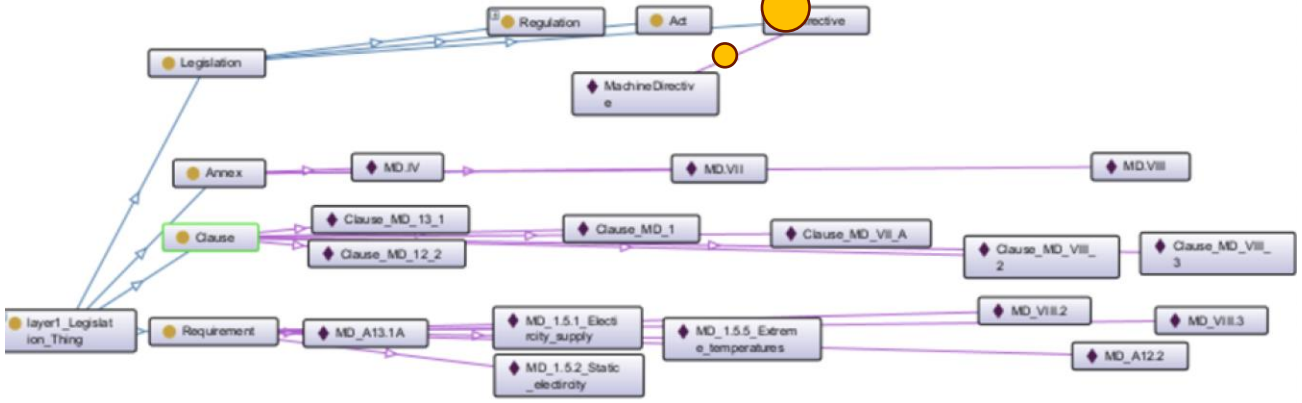


A layered ontology-based representation of the socio-technical system –Legislation layer

[Gallina et al.2024c]

- PumpsCompliance:layer0_Problem_Space_Thing (4)
- PumpsCompliance:layer1_Legislation_Thing (21)
- PumpsCompliance:layer2_Standardization_Thing (14)
- PumpsCompliance:layer3_Company_level_Thing (14)
- PumpsCompliance:layer4_SystemProductThing (2)

Formalisation after specification, conceptualisation
A legislation has a preamble, which in turns is constituted by
a set of citations
a set of recitals
- a set of articles
- a set of annexes

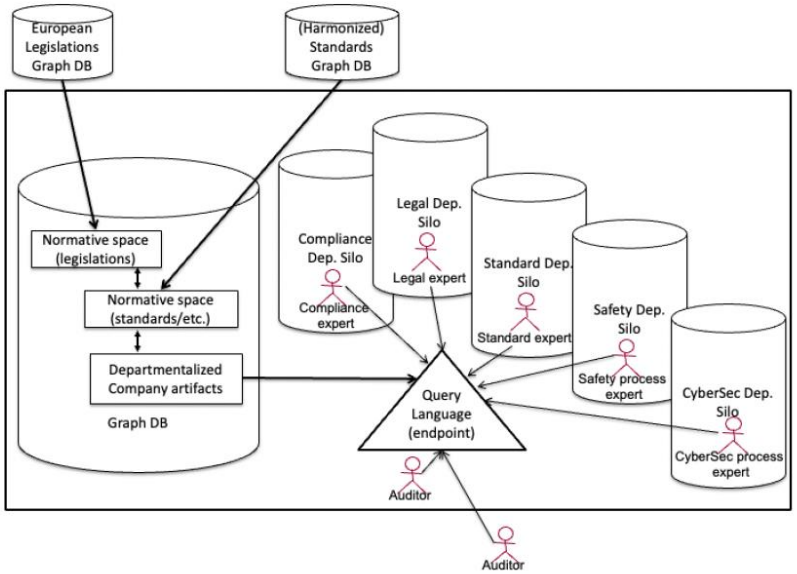


A layered ontology-based representation of the socio-technical system –Legislation layer

[Gallina et al.2024c]

Which are the safety-related legislations?

- PumpsCompliance:layer0_Problem_Space_Thing (4)
- PumpsCompliance:layer1_Legislation_Thing (21)
- PumpsCompliance:layer2_Standardization_Thing (14)
- PumpsCompliance:layer3_Company_level_Thing (14)
- PumpsCompliance:layer4_SystemProductThing (2)



Imports | Instances | Inheritance | Domain | Relevant Properties | Error Log | SPARQL | SPARQL | Text Search

Query Editor | Query Library

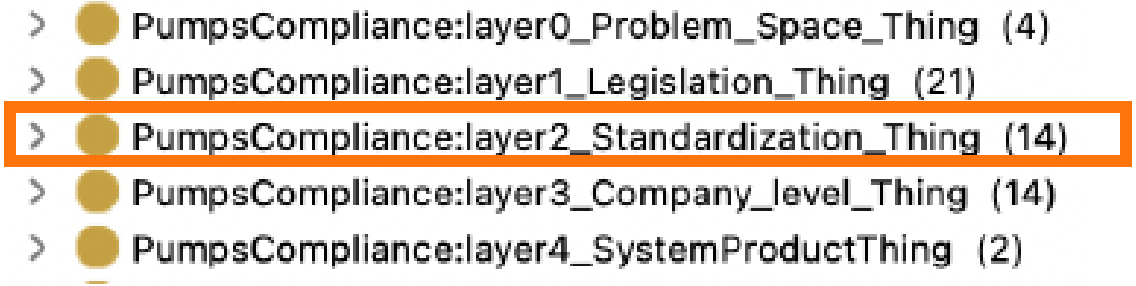
```
SELECT ?Legislation
WHERE {
  ?Legislation PumpsCompliance:SubjectsOfApproval ?Subject .
  ?Legislation a ?L .
  ?L rdfs:subClassOf* PumpsCompliance:Legislation .
  Filter (?Subject = PumpsCompliance:FunctionalSafety)

}
```

[Legislation]

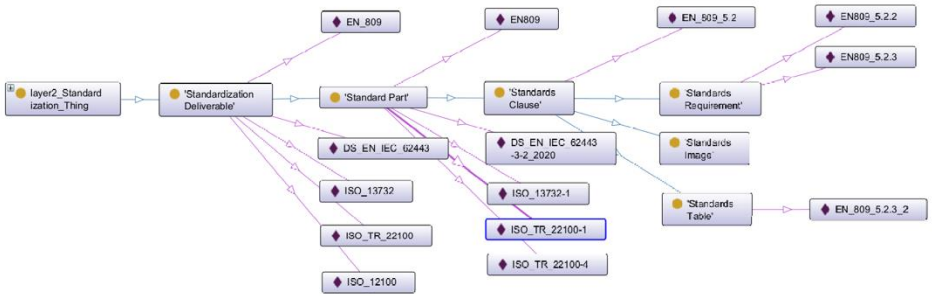
- PumpsCompliance:MachineDirective
- PumpsCompliance:MachinearyRegulation

A layered ontology-based representation of the socio-technical system –Standardization layer

[Gallina et al.2024c]



- a set of parts. Each part in turns is constituted by:
  - set of clauses, Each clause in turns is constituted by:
    - set of requirements
    - set of images
    - set of tables
- a set of associated standards
- a set of associated legislations

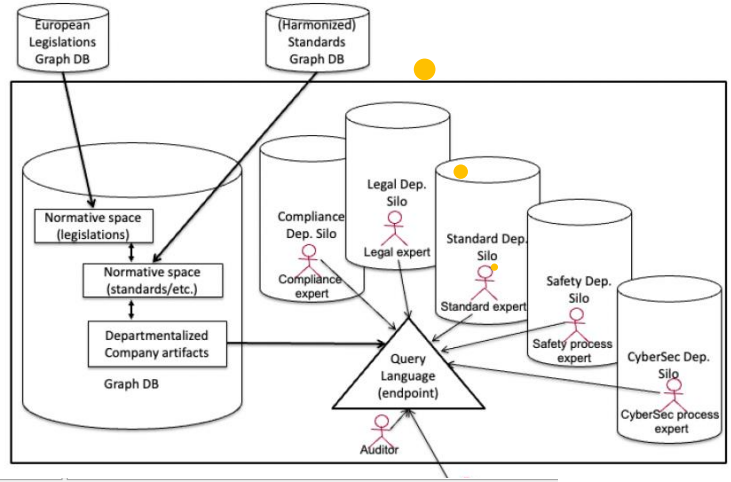


A layered ontology-based representation of the socio-technical system –Standardization layer

[Gallina et al.2024c]

Which are the safety-related standards?

- PumpsCompliance:layer0_Problem_Space_Thing (4)
- PumpsCompliance:layer1_Legislation_Thing (21)
- PumpsCompliance:layer2_Standardization_Thing (14)
- PumpsCompliance:layer3_Company_level_Thing (14)
- PumpsCompliance:layer4_SystemProductThing (2)



Imports | Instances | Inheritance | Domain | Relevant Properties | Error Log | SPARQL | SPARQL | Text Search | Targets | SHACL Validation

Query Editor | Query Library

```
SELECT ?Standard
WHERE {
  ?Standard PumpsCompliance:SubjectsOfApproval ?Subject .
  ?Standard a PumpsCompliance:StandardizationDeliverable .
  Filter (?Subject = PumpsCompliance:FunctionalSafety)

}
```

[Standard]

- PumpsCompliance:EN_809
- PumpsCompliance:ISO_12100
- PumpsCompliance:ISO_TR_22100

A layered ontology-based representation of the socio-technical system –Company layer

[Gallina et al.2024c]

- PumpsCompliance:layer0_Problem_Space_Thing (4)
- PumpsCompliance:layer1_Legislation_Thing (21)
- PumpsCompliance:layer2_Standardization_Thing (14)
- PumpsCompliance:layer3_Company_level_Thing (14)
- PumpsCompliance:layer4_SystemProductThing (2)

- a set of phases, where each phase in turn is constituted by:
  - a set of activities, where each activity in turn is constituted by:
    - a set of tasks, where each task in turn is constituted by:
      - a set of steps, where each step in turn is constituted by:

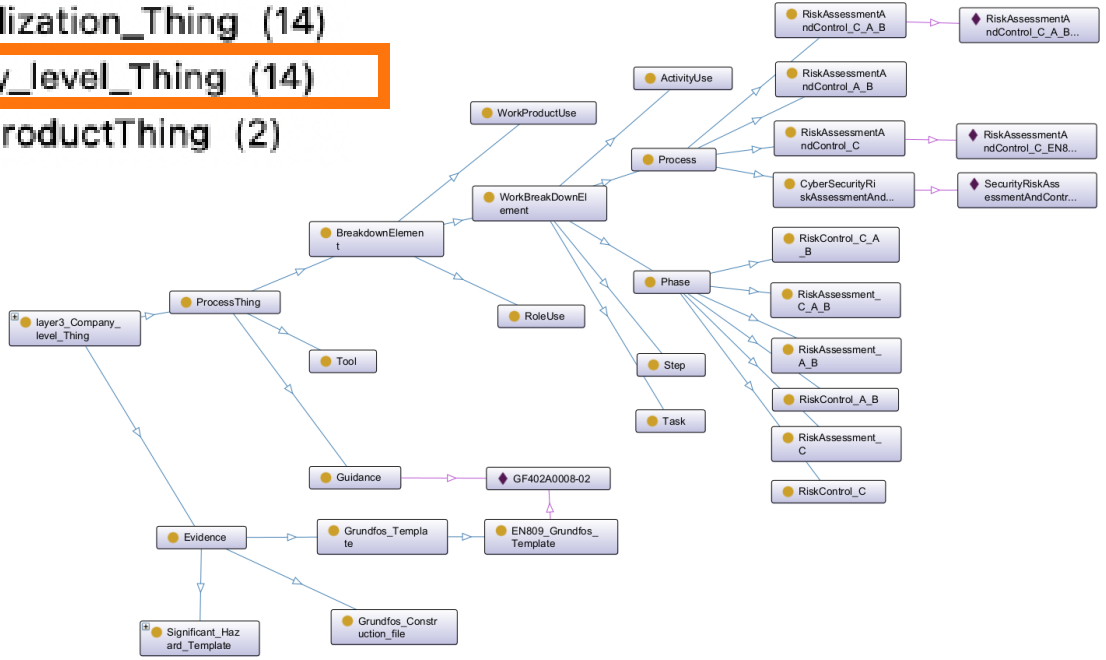
  a set of roles

  a set of tools

  a set of work products in input

  a set of work products in output

  a set of guidelines/templates

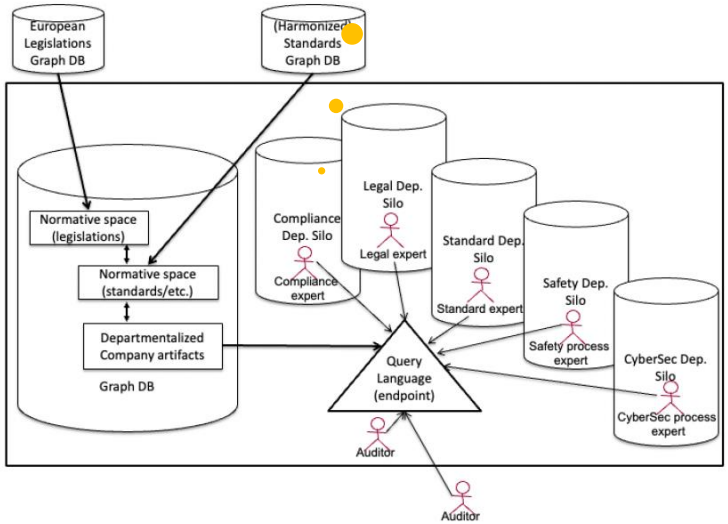


A layered ontology-based representation of the socio-technical system –Company layer

[Gallina et al.2024c]

Which is the process model overview adopted for developing pump CR-1?

- PumpsCompliance:layer0_Problem_Space_Thing (4)
- PumpsCompliance:layer1_Legislation_Thing (21)
- PumpsCompliance:layer2_Standardization_Thing (14)
- PumpsCompliance:layer3_Company_level_Thing (14)
- PumpsCompliance:layer4_SystemProductThing (2)



Imports | Instances | Inheritance | Domain | Relevant Properties | Error Log | SPARQL | SPARQL | SPARQL | SPARQL | Text Search | Targets | SHACL Validation

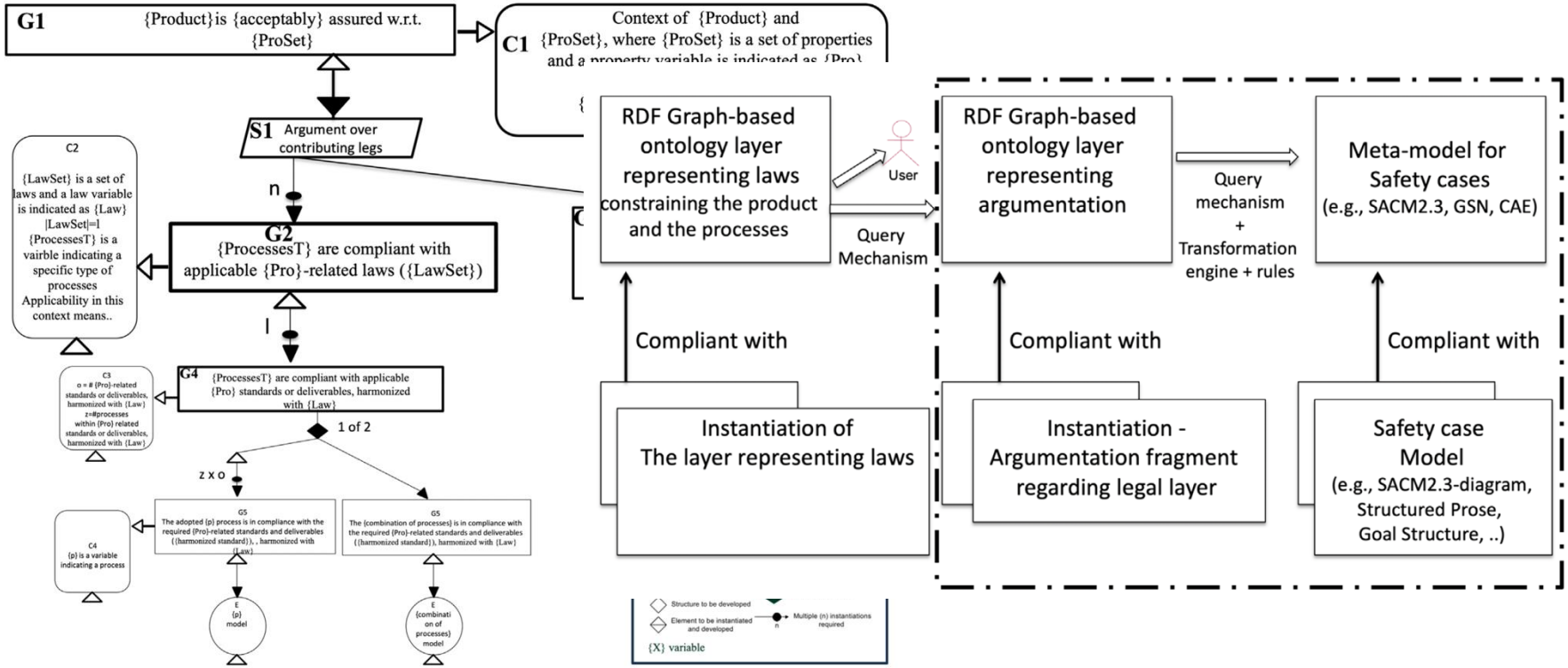
Query Editor | Query Library

```
SELECT ?pump ?PMO
WHERE {
  ?pumpclass rdfs:subClassOf* PumpsCompliance:PumpDriveSystem .
  ?pump a ?pumpclass .
  ?pump PumpsCompliance:AssociatedSetOfProcesses ?process .
  ?process PumpsCompliance:ProcessModelOverview ?PMO
}
```

[pump]	PMO
PumpsCompliance:Pump_CR_1	https://grundfos.sharepoint.com/:i:/r/sites/Project50-ET4CQPPAJ/Shared%20Documents/General/ProcessModelOverview.p...

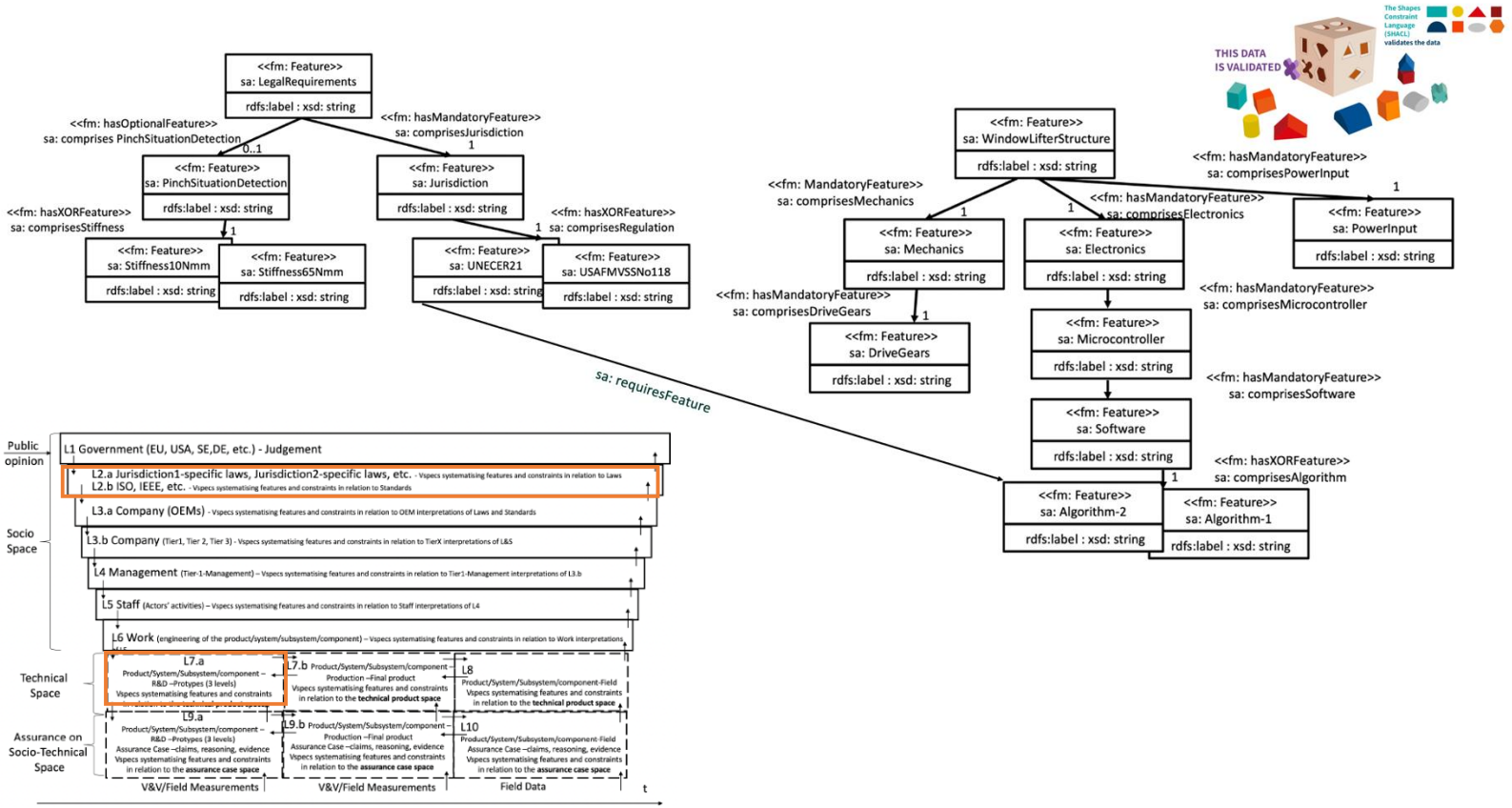
Automated generation of multi-concern assurance argumentation

[Gallina et al.2024c]



Variability management – cross jurisdiction UNECE -

[Gallina et al.2024b]



OntoGSN – ontology to manage GSN assurance cases

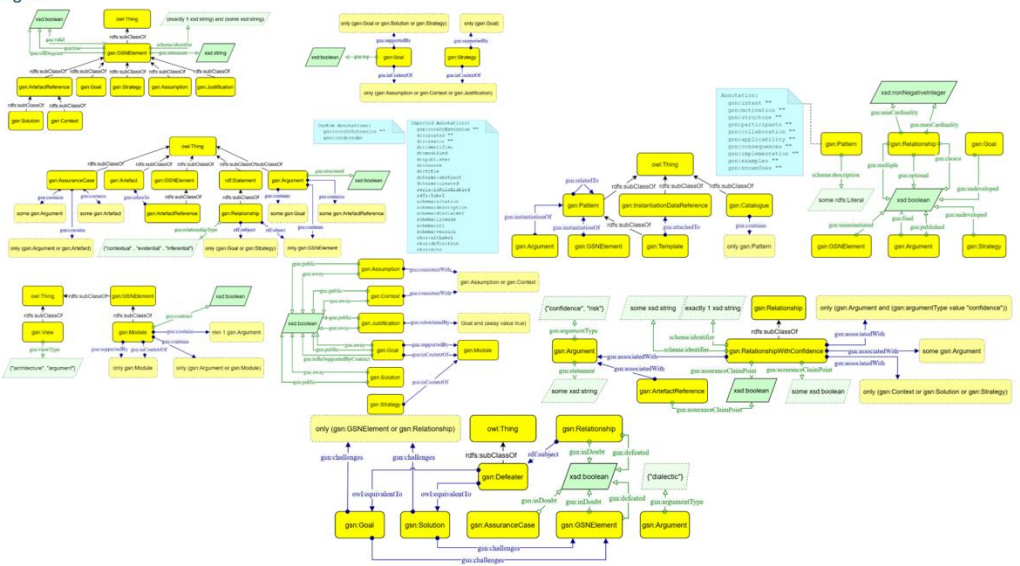
[Bueno Momcilovic et al.2025]

OntoGSN / OntoGSN Design Document.pdf

2.16 MB

[1] The assertion box (ABox) is to be created by the user; currently, only example individuals are provided in a separate file for tutorial purposes.
[2] https://protege.stanford.edu/
[3] https://www.w3.org/TR/owl2-overview
[4] https://www.w3.org/TR/rdf-schema/
[5] https://www.w3.org/TR/xmlschema11-1/
[6] http://purl.org/dc/elements/1.1/
[7] https://www.schema.org
[8] https://www.w3.org/2004/02/skos/
[9] https://www.w3.org/submissions/SWRL/
[10] https://www.w3.org/2001/sw/wiki/Pellet
[11] https://www.drools.org/
[12] https://www.w3.org/TR/sparql11-query/
[13] https://www.w3.org/TR/shacl/
[14] In v2.1.2 and below, it is known as SWRLTab.

Diagram



https://fortiss.github.io/OntoGSN/

Next?

- More complex case study in cooperation with stakeholders
  - Competency questions/stakeholder
- Criteria for assessment of *performative linking* among the different layers and domains
- Criteria for ontology engineering in relation to human/AI users
  - Exploration of SOTA practices
  - Integration with existing ontologies
- Tooling
- Exploitation of LLMs? Defeaters? Still skeptical..

References

[Gallina et al.2024a] B. Gallina, P. Munk, M. Schweizer. An Extension of the Rasmussen Socio-technical System for Continuous Safety Assurance. Proceedings of 8th International Workshop on Critical Automotive Applications: Robustness & Safety (CARS), Leuven, Belgium, April 8th, 2024. HAL archives ouvertes.fr, <hal-04558510>

[Gallina et al.2024b] B. Gallina, H. Dibowski, M. Schweizer. An Ontology-based Representation for Shaping Product Evolution in Regulated Industries. 21st International Conference on Software and Systems Reuse (ICSR-2024), Lecture Notes in Computer Science, vol 14614. Springer, Cham. DOI: 10.1007/978-3-031-66459-5_6, Limassol, Cyprus, June 19-20, 2024.

[Gallina et al.2024c] B. Gallina, G. L. Steierhoffer, T. Young Olesen, E. Parajdi, M. Aarup. Towards an ontology for process compliance with the (machinery) legislations. Journal of Software Evolution and Process (JSEP). 2024; e2728. DOI; 10.1002/smr.2728

- B. Gallina and M. Nyberg. Pioneering the Creation of ISO 26262-compliant OSLC-based Safety Cases. Proceedings of the 7th IEEE WoSoCER, IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), IEEE Computer Society, pp. 325-330, DOI: 10.1109/ISSREW.2017.41, Toulouse, France, 23rd of October 2017.
- B. Gallina and M. Nyberg. Reconciling the ISO 26262-compliant and the Agile Documentation Management in the Swedish Context. In *Critical Automotive applications: Robustness & Safety (CARS), Matthieu Roy, Paris, France, HAL*, September 2015.
- B. Gallina, J. P. Castellanos Ardila, and M. Nyberg. Towards Shaping ISO 26262-compliant Resources for OSLC-based Safety Case Creation. In *Critical Automotive applications: Robustness & Safety (CARS), Göteborg, Sweden, HAL*, September 2016.
- B. Gallina, K. Padira, M. Nyberg. Towards an ISO 26262-compliant OSLC-based Tool Chain Enabling Continuous Self-assessment. 10th International Conference on the Quality of Information and Communications Technology- Track: Quality Aspects in Safety Critical Systems (QUATIC), Lisbon, Portugal, 6-9 September 2016

Hope it was interesting!
Thank you very much for your attention!

#49-∞COMPASS – Continuous Regulatory Compliance and Assurance of Socio-technical Systems
– focus on variability/traceability management –

Software Center

barbara.gallina@mdu.se