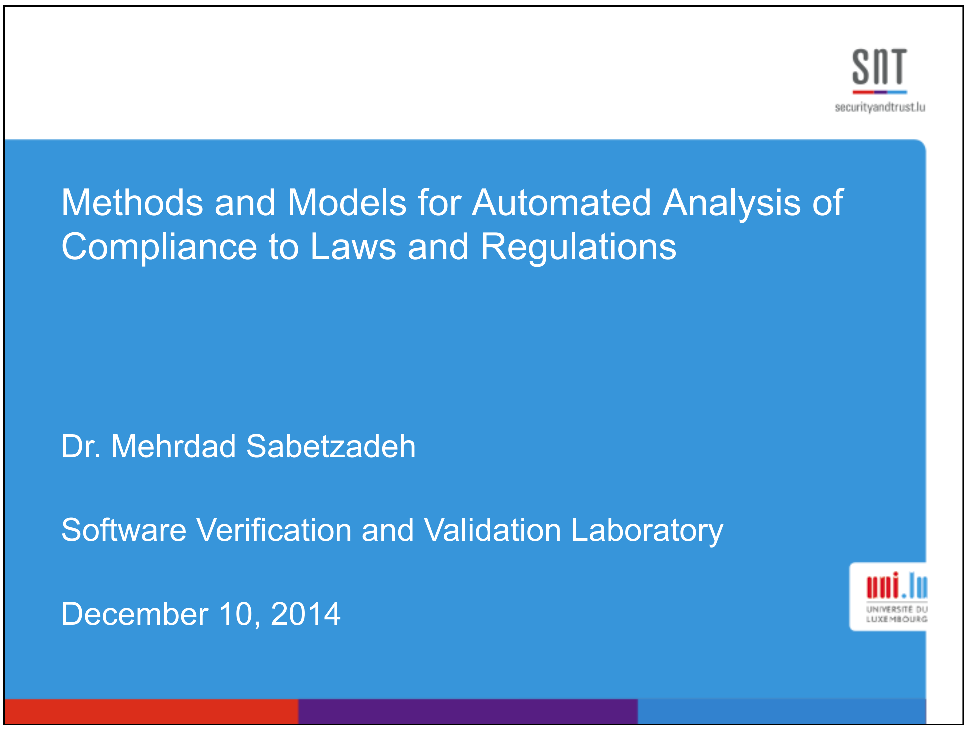
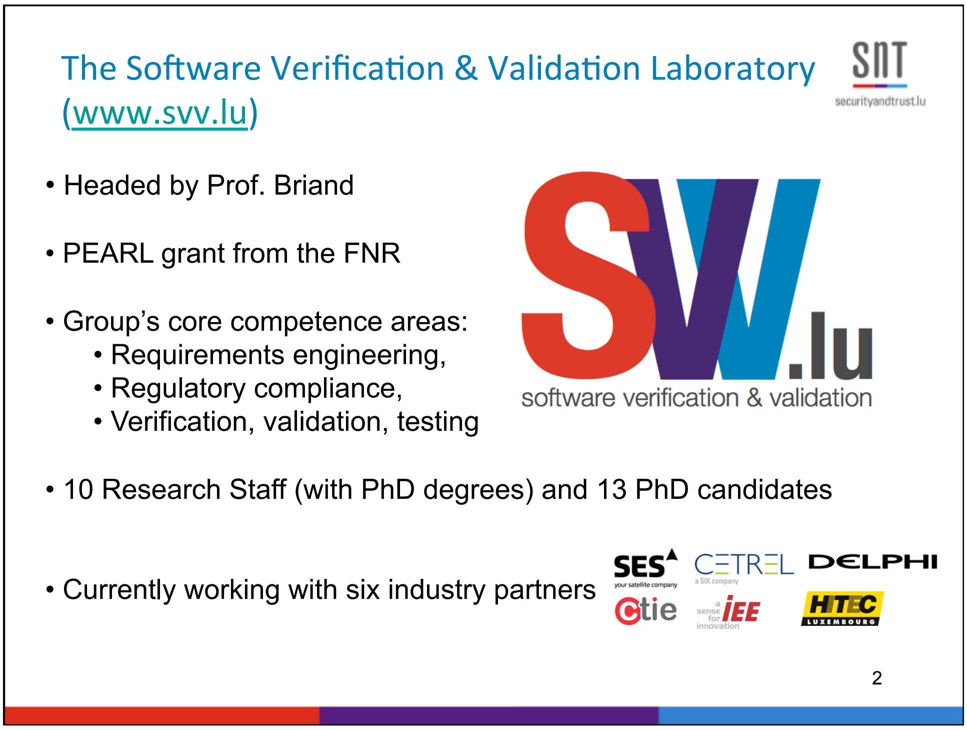


Methods and Models for Automated Analysis of Compliance to Laws and Regulations

Dr. Mehrdad Sabetzadeh

Software Verification and Validation Laboratory

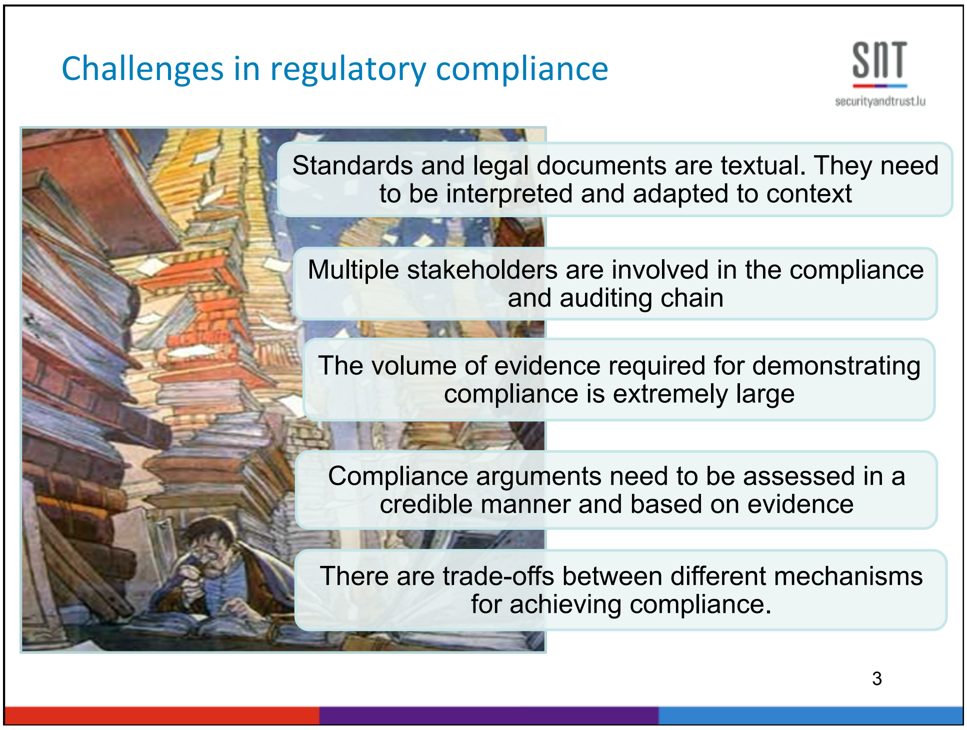
December 10, 2014



The Software Verification & Validation Laboratory (www.svv.lu)

- Headed by Prof. Briand
- PEARL grant from the FNR
- Group's core competence areas:
  - Requirements engineering,
  - Regulatory compliance,
  - Verification, validation, testing
- 10 Research Staff (with PhD degrees) and 13 PhD candidates
- Currently working with six industry partners

SVV.lu
software verification & validation



Challenges in regulatory compliance

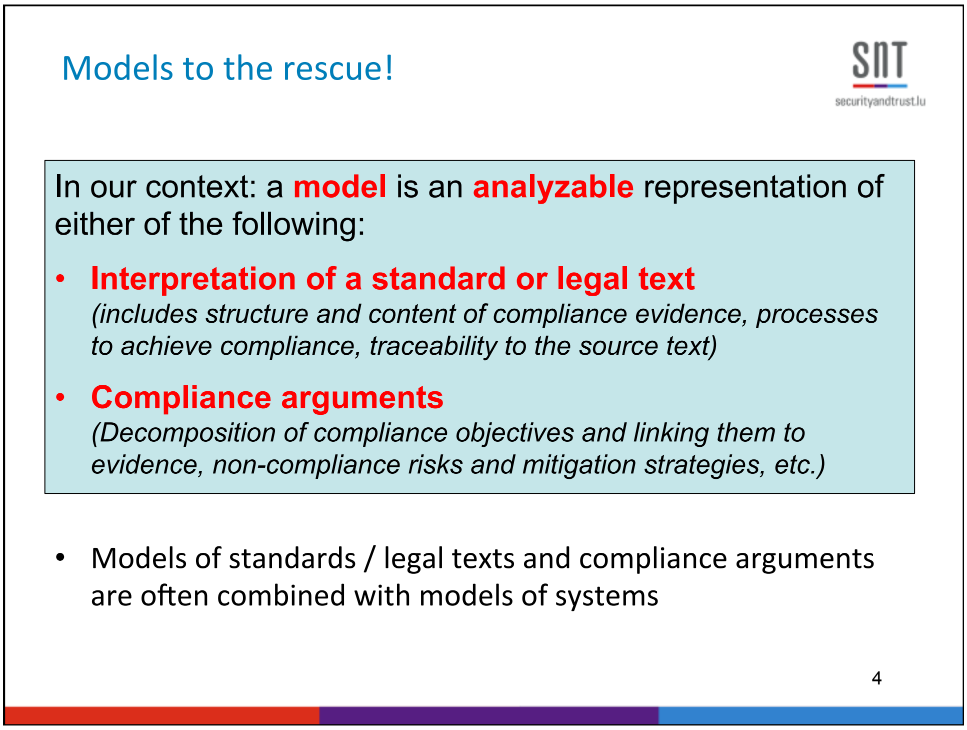
Standards and legal documents are textual. They need to be interpreted and adapted to context

Multiple stakeholders are involved in the compliance and auditing chain

The volume of evidence required for demonstrating compliance is extremely large

Compliance arguments need to be assessed in a credible manner and based on evidence

There are trade-offs between different mechanisms for achieving compliance.

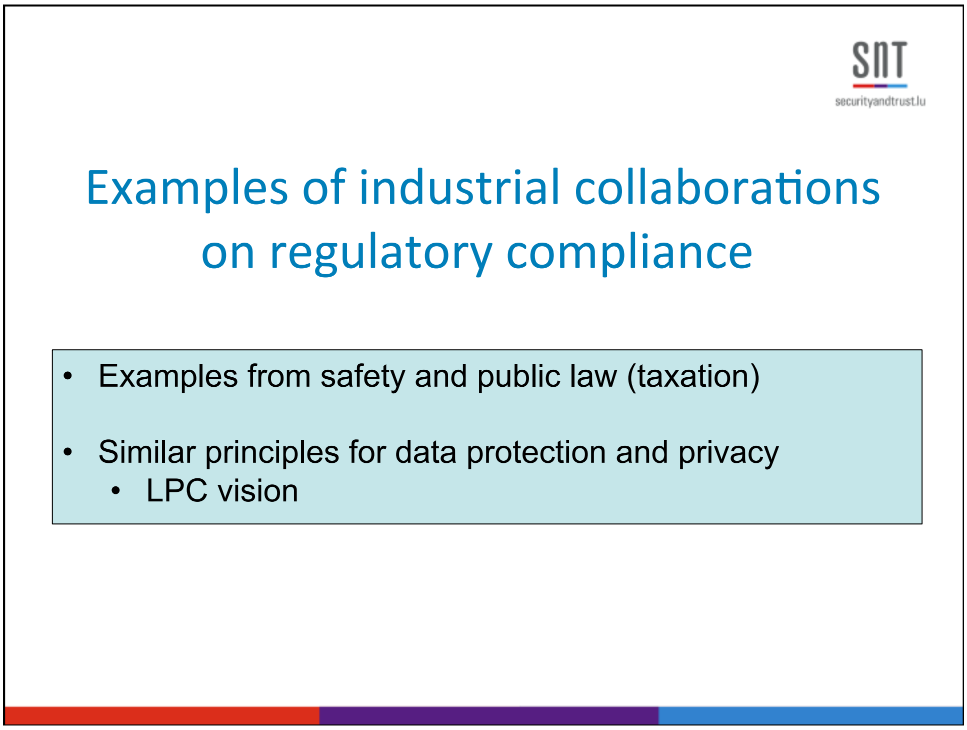


Models to the rescue!

In our context: a **model** is an **analyzable** representation of either of the following:

- **Interpretation of a standard or legal text**
  (includes structure and content of compliance evidence, processes to achieve compliance, traceability to the source text)
- **Compliance arguments**
  (Decomposition of compliance objectives and linking them to evidence, non-compliance risks and mitigation strategies, etc.)

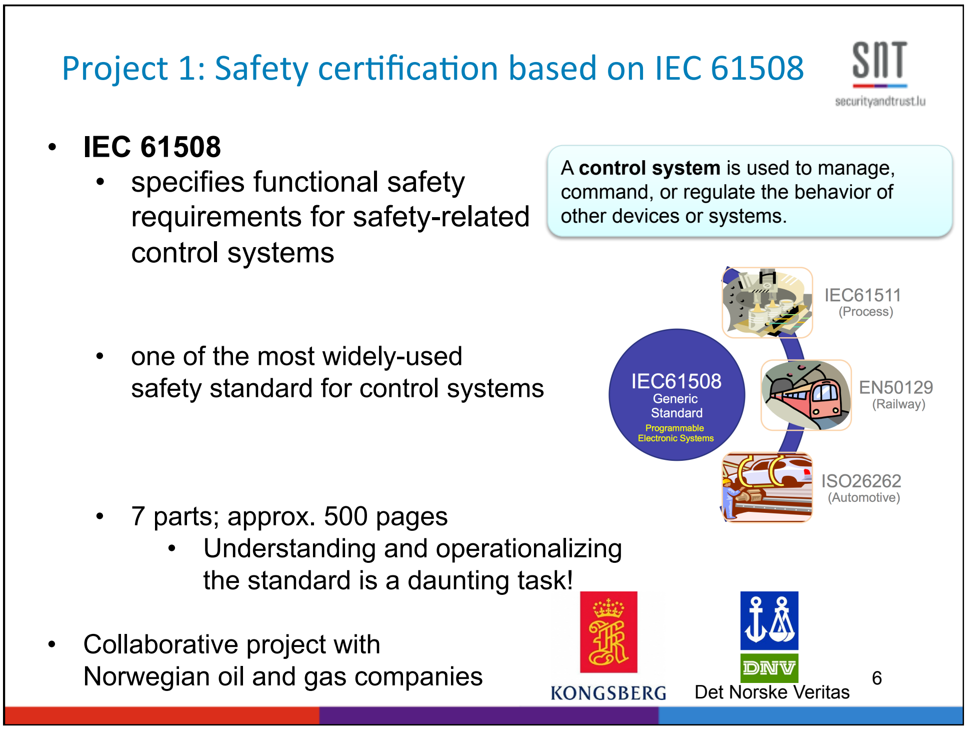
- Models of standards / legal texts and compliance arguments are often combined with models of systems



SnT securityandtrust.lu

Examples of industrial collaborations on regulatory compliance

- Examples from safety and public law (taxation)
- Similar principles for data protection and privacy
  - LPC vision



Project 1: Safety certification based on IEC 61508

SnT securityandtrust.lu

- **IEC 61508**
  - specifies functional safety requirements for safety-related control systems
  - one of the most widely-used safety standard for control systems
  - 7 parts; approx. 500 pages
    - Understanding and operationalizing the standard is a daunting task!
- Collaborative project with Norwegian oil and gas companies

A **control system** is used to manage, command, or regulate the behavior of other devices or systems.

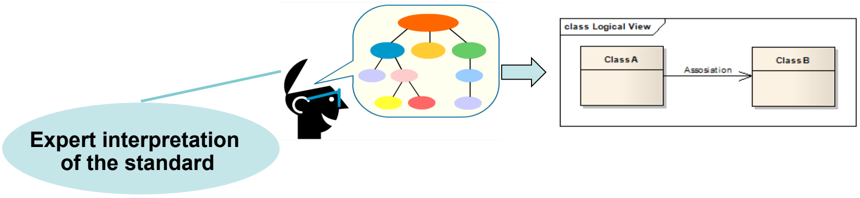
KONGSBERG

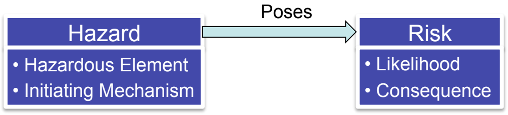
DNV Det Norske Veritas

6

Expressing the interpretation of IEC 61508 as a conceptual model

- A conceptual model is a map of important concepts, their attributes and relationships





7 Software safety lifecycle requirements

7.1 General

7.1.1 Objective

The objective of the requirements of this subclause is to structure the development of the software into defined phases and activities (see table 1 and figures 2 to 5).

1 Concepts: Phase, Activity.

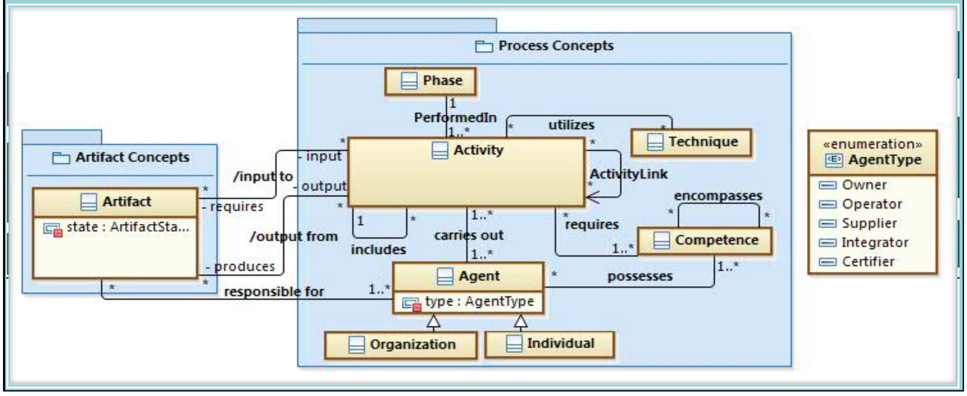
7.1.2 Requirements

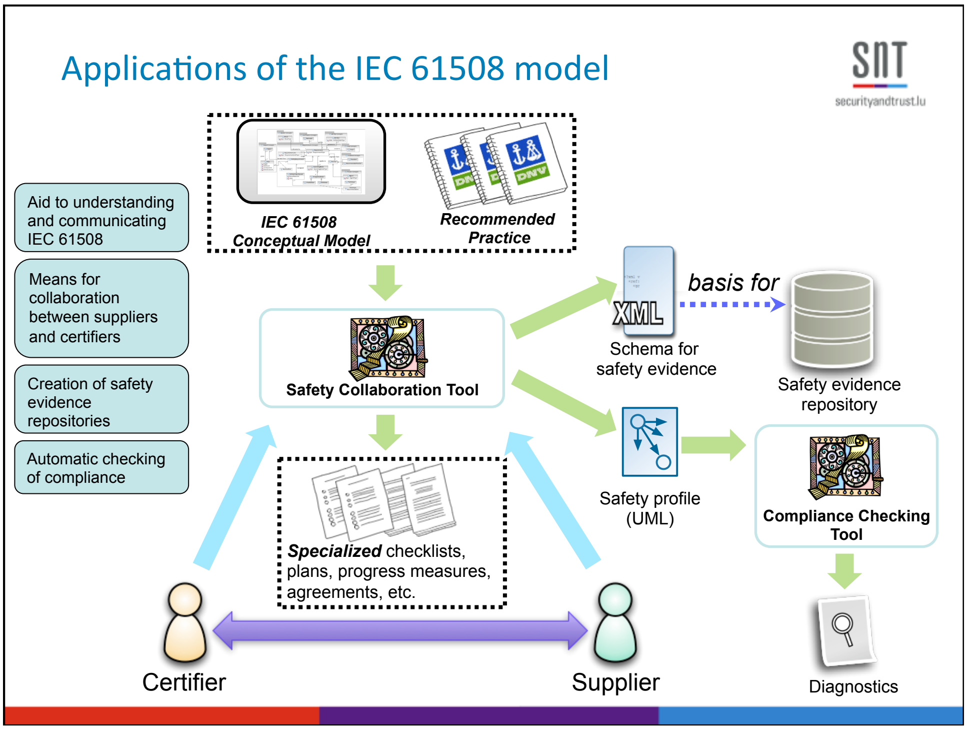
7.1.2.1 A safety lifecycle for the development of software shall be selected and specified during safety planning in accordance with clause 6 of IEC 61508-1.

7.1.2.2 Quality and safety assurance procedures shall be integrated into safety lifecycle activities.

2 Concept: Artifact.
Relationship: PerformedIn, InputTo and OuputFrom

7.1.2.3 Each phase of the software safety lifecycle shall be divided into elementary activities with the scope, inputs and outputs specified for each phase.





Applications of the IEC 61508 model

SnT securityandtrust.lu

Aid to understanding and communicating IEC 61508

Means for collaboration between suppliers and certifiers

Creation of safety evidence repositories

Automatic checking of compliance

IEC 61508 Conceptual Model

Recommended Practice

Safety Collaboration Tool

Specialized checklists, plans, progress measures, agreements, etc.

Certifier

Supplier

Schema for safety evidence

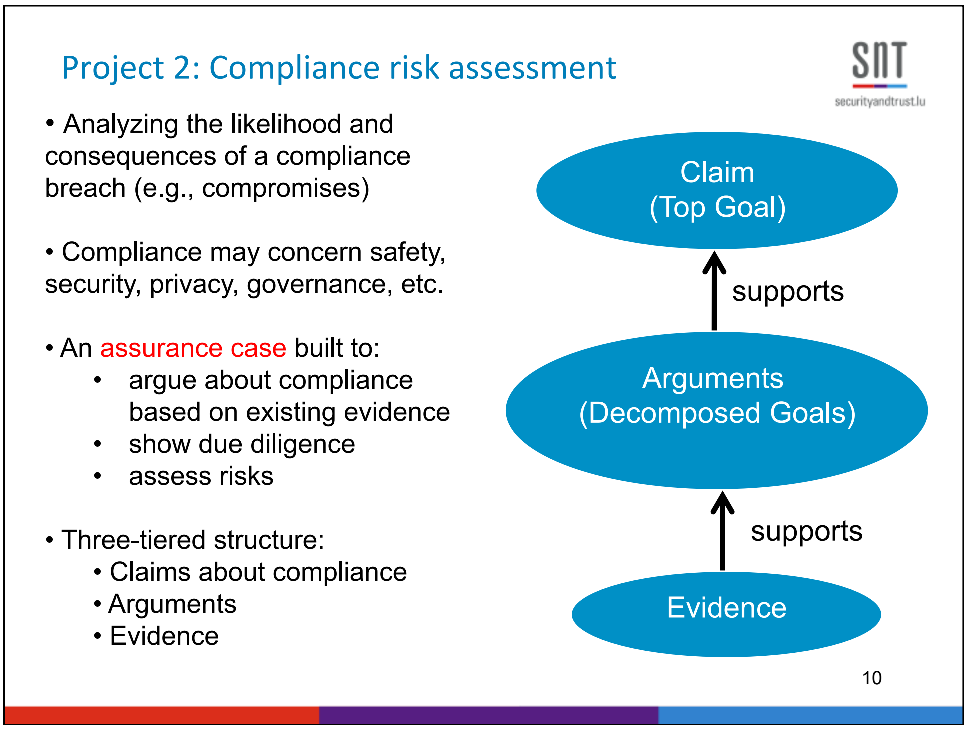
basis for

Safety evidence repository

Safety profile (UML)

Compliance Checking Tool

Diagnostics



Project 2: Compliance risk assessment

SnT securityandtrust.lu

- Analyzing the likelihood and consequences of a compliance breach (e.g., compromises)
- Compliance may concern safety, security, privacy, governance, etc.
- An assurance case built to:
  - argue about compliance based on existing evidence
  - show due diligence
  - assess risks
- Three-tiered structure:
  - Claims about compliance
  - Arguments
  - Evidence

Claim (Top Goal)

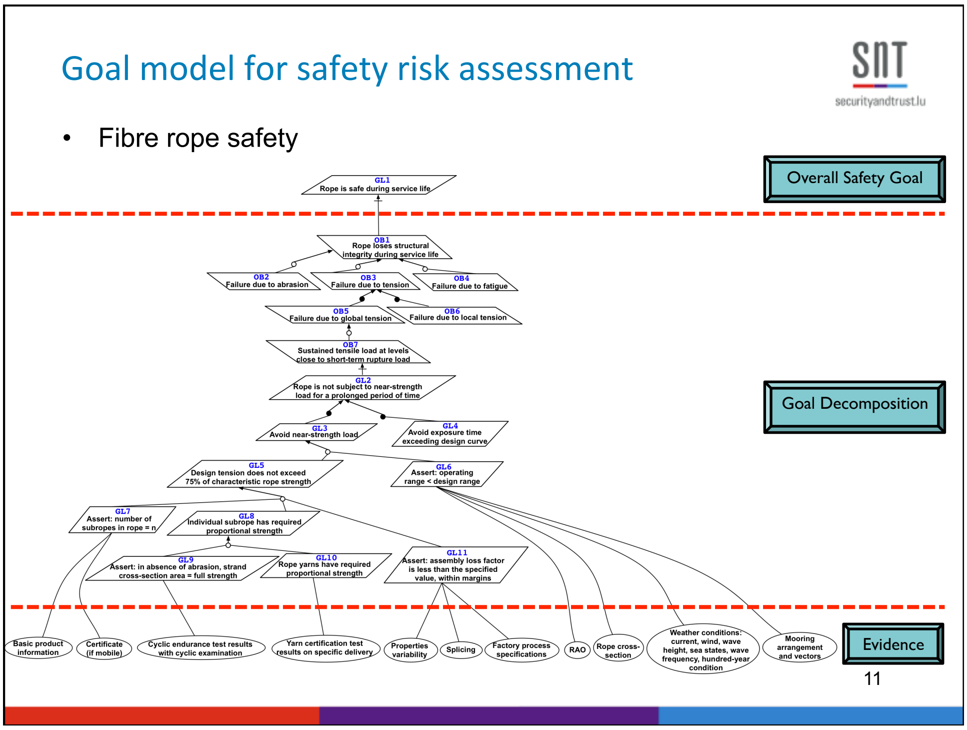
supports

Arguments (Decomposed Goals)

supports

Evidence

10



Goal model for safety risk assessment

- Fibre rope safety

Overall Safety Goal

GL1
Rope is safe during service life

Goal Decomposition

OB1
Rope loses structural integrity during service life

OB2
Failure due to abrasion

OB3
Failure due to tension

OB4
Failure due to fatigue

OB5
Failure due to global tension

OB6
Failure due to local tension

OB7
Sustained tensile load at levels close to short-term rupture load

GL2
Rope is not subject to near-strength load for a prolonged period of time

GL3
Avoid near-strength load

GL4
Avoid exposure time exceeding design curve

GL5
Design tension does not exceed 75% of characteristic rope strength

GL6
Assert: operating range < design range

GL7
Assert: number of subropes in rope = n

GL8
Individual subrope has required proportional strength

GL9
Assert: in absence of abrasion, strand cross-section area = full strength

GL10
Rope yarns have required proportional strength

GL11
Assert: assembly loss factor is less than the specified value, within margins

Evidence

Basic product information

Certificate (if mobile)

Cyclic endurance test results with cyclic examination

Yarn certification test results on specific delivery

Properties variability

Splicing

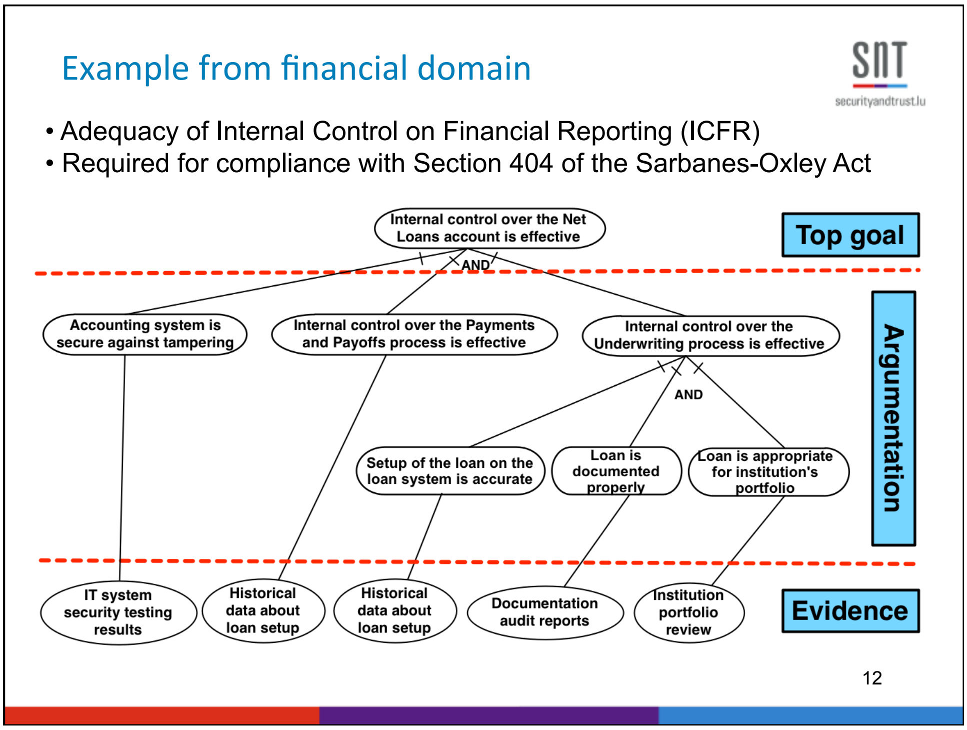
Factory process specifications

RAO

Rope cross-section

Weather conditions: current, wind, wave height, sea states, wave frequency, hundred-year condition

Mooring arrangement and vectors



Example from financial domain

- Adequacy of Internal Control on Financial Reporting (ICFR)
- Required for compliance with Section 404 of the Sarbanes-Oxley Act

Top goal

Internal control over the Net Loans account is effective

AND

Argumentation

Accounting system is secure against tampering

Internal control over the Payments and Payoffs process is effective

Internal control over the Underwriting process is effective

AND

Setup of the loan on the loan system is accurate

Loan is documented properly

Loan is appropriate for institution's portfolio

Evidence

IT system security testing results

Historical data about loan setup

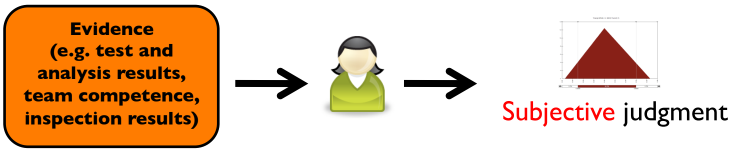
Historical data about loan setup

Documentation audit reports

Institution portfolio review

Expert elicitation

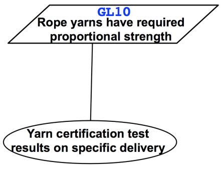
- Why expert elicitation?
- Evidence always has to be interpreted



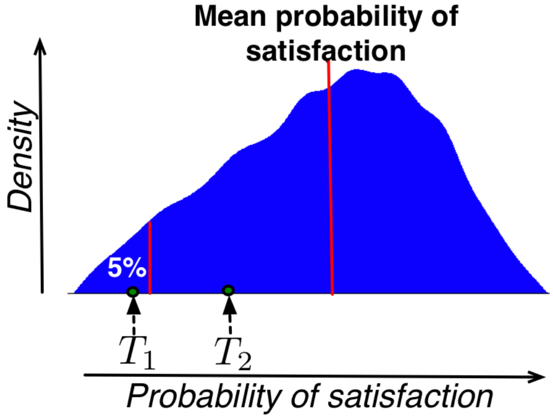
Evidence (e.g. test and analysis results, team competence, inspection results)

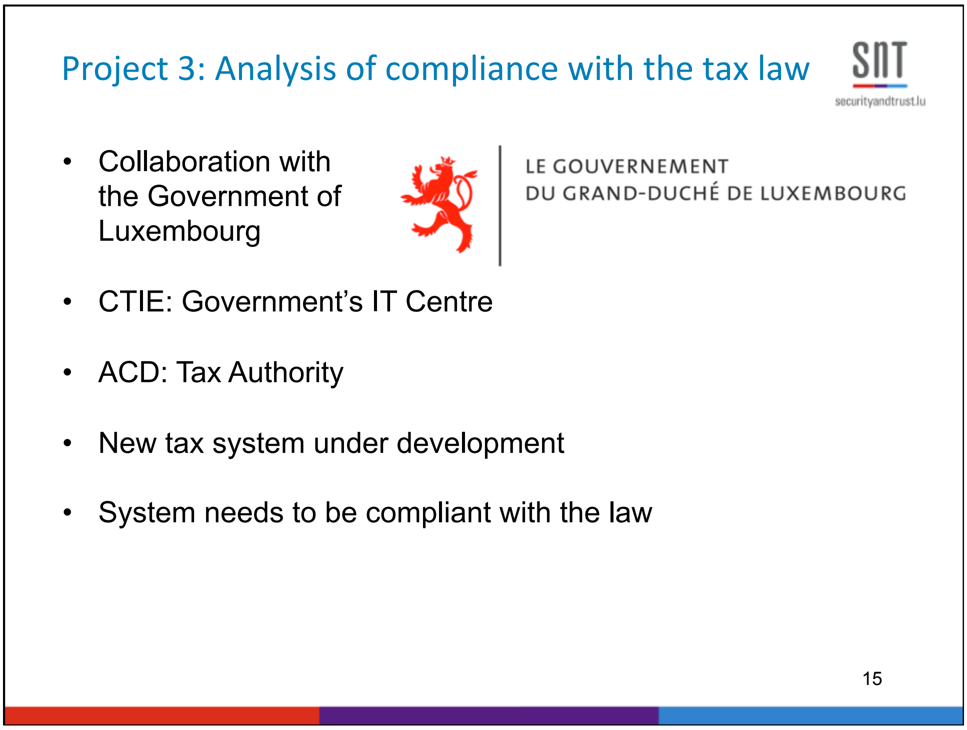
Subjective judgment

- Essence of the question asked from expert:
  - How likely is a leaf goal to be satisfied based on the evidence linked to it?


GL10
Rope yarns have required proportional strength
Yarn certification test results on specific delivery

Monte Carlo simulation





Project 3: Analysis of compliance with the tax law

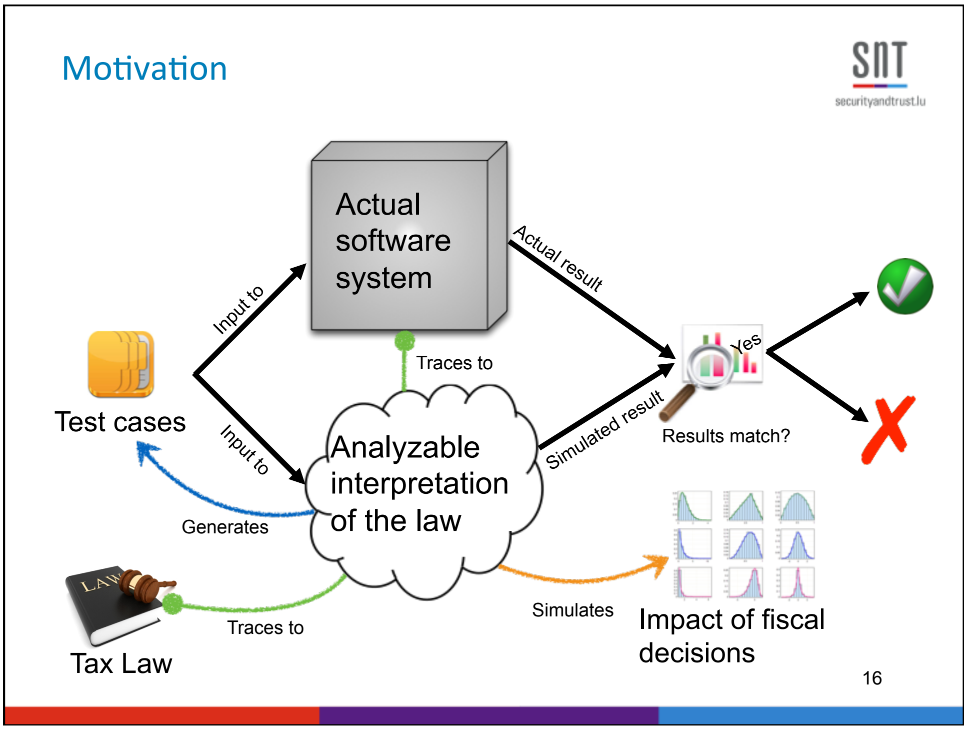
SnT
securityandtrust.lu

- Collaboration with the Government of Luxembourg

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- CTIE: Government's IT Centre
- ACD: Tax Authority
- New tax system under development
- System needs to be compliant with the law

15



Motivation

SnT
securityandtrust.lu

Actual software system

Input to

Actual result

Test cases

Traces to

Yes

Input to

Analyzable interpretation of the law

Simulated result

Results match?

Generates

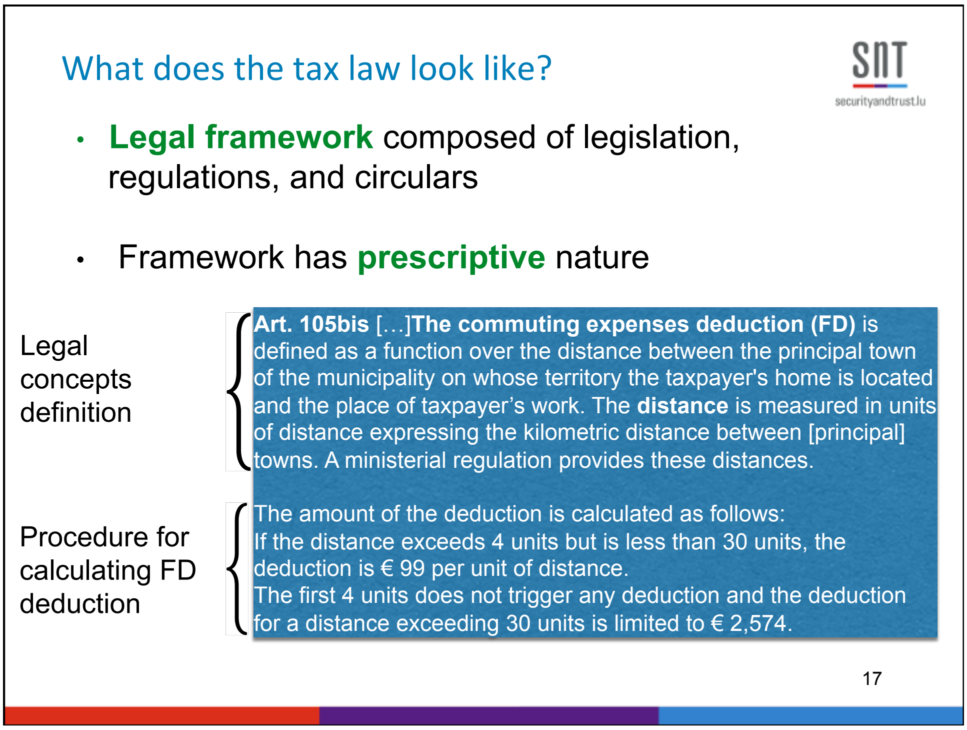
Tax Law

Traces to

Simulates

Impact of fiscal decisions

16



What does the tax law look like?

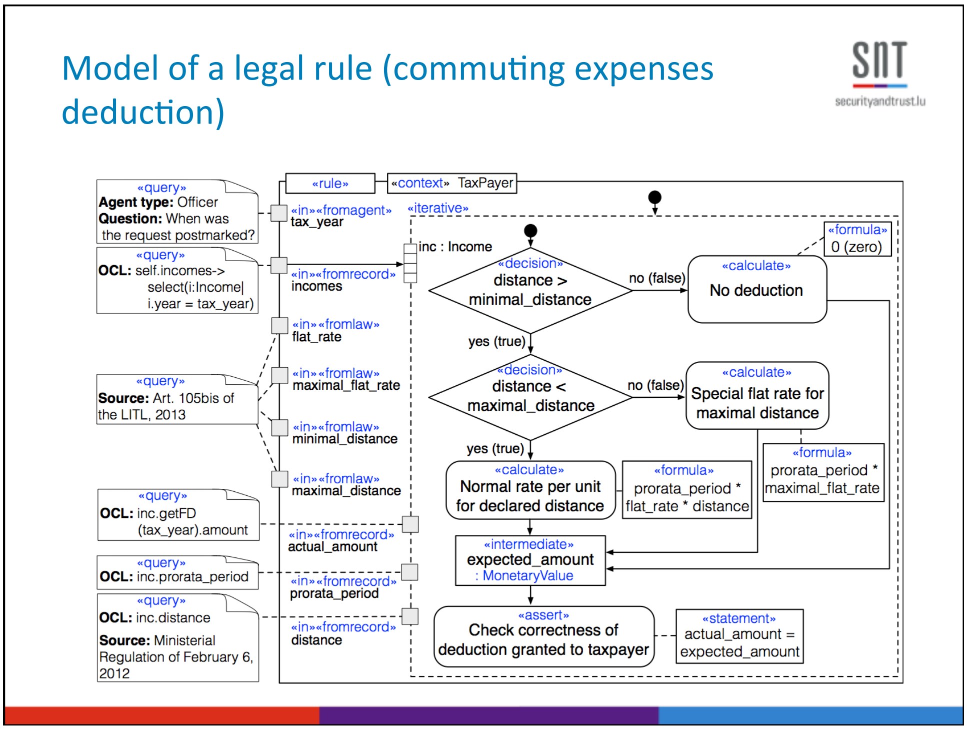
- **Legal framework** composed of legislation, regulations, and circulars
- Framework has **prescriptive** nature

Legal concepts definition

Art. 105bis […]**The commuting expenses deduction (FD)** is defined as a function over the distance between the principal town of the municipality on whose territory the taxpayer's home is located and the place of taxpayer's work. The **distance** is measured in units of distance expressing the kilometric distance between [principal] towns. A ministerial regulation provides these distances.

Procedure for calculating FD deduction

The amount of the deduction is calculated as follows:
If the distance exceeds 4 units but is less than 30 units, the deduction is € 99 per unit of distance.
The first 4 units does not trigger any deduction and the deduction for a distance exceeding 30 units is limited to € 2,574.



Model of a legal rule (commuting expenses deduction)

«query»
Agent type: Officer
Question: When was the request postmarked?

«query»
OCL: self.incomes->
select(i:Income|
i.year = tax_year)

«query»
Source: Art. 105bis of the LITL, 2013

«query»
OCL: inc.getFD
(tax_year).amount

«query»
OCL: inc.prorata_period

«query»
OCL: inc.distance
Source: Ministerial Regulation of February 6, 2012

«rule»

«context» TaxPayer

«in»«fromagent»
tax_year

«in»«fromrecord»
incomes

«in»«fromlaw»
flat_rate

«in»«fromlaw»
maximal_flat_rate

«in»«fromlaw»
minimal_distance

«in»«fromlaw»
maximal_distance

«in»«fromrecord»
actual_amount

«in»«fromrecord»
prorata_period

«in»«fromrecord»
distance

«iterative»

inc : Income

«decision»
distance >
minimal_distance

no (false)

«calculate»
No deduction

«formula»
0 (zero)

yes (true)

«decision»
distance <
maximal_distance

no (false)

«calculate»
Special flat rate for maximal distance

«formula»
prorata_period *
maximal_flat_rate

yes (true)

«calculate»
Normal rate per unit for declared distance

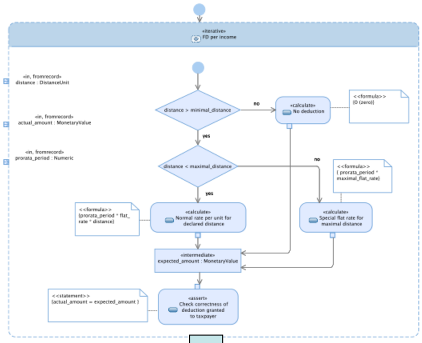
«formula»
prorata_period *
flat_rate * distance

«intermediate»
expected_amount
: MonetaryValue

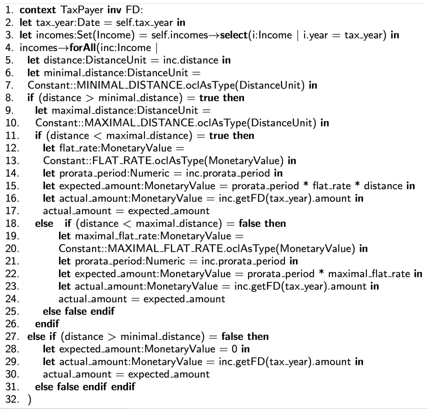
«assert»
Check correctness of deduction granted to taxpayer

«statement»
actual_amount =
expected_amount

Transformation to logical formulas and simulation code


«iterative»
FD per income
«in, fromrecord»
distance : DistanceUnit
«in, fromrecord»
actual_amount : MonetaryValue
«in, fromrecord»
prorata_period : Numeric
distance > minimal_distance
no
«calculate»
No deduction
<<formula>>
(0 (zero))
yes
distance < maximal_distance
no
<<formula>>
(prorata_period * maximal_flat_rate)
yes
<<formula>>
(prorata_period * flat_rate * distance)
«calculate»
Normal rate per unit for declared distance
«calculate»
Special flat rate for maximal distance
«intermediate»
expected_amount : MonetaryValue
<<statement>>
(actual_amount = expected_amount)
«assert»
Check correctness of deduction granted to taxpayer

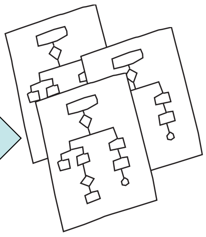
Automated model transformer



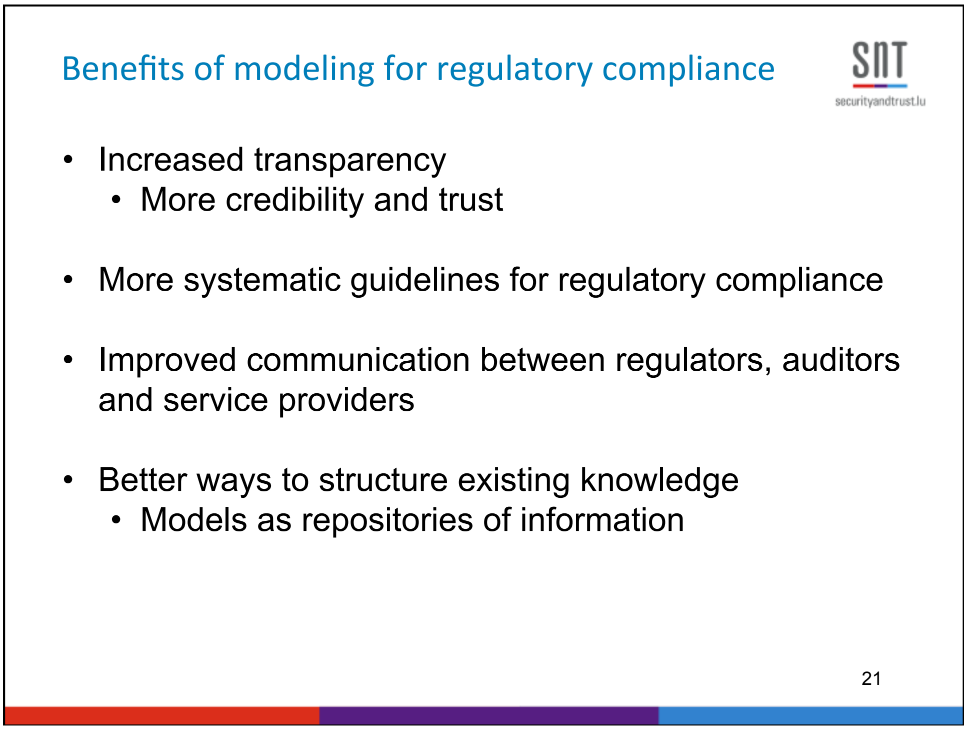
```
context TaxPayer inv FD:
let tax_year:Date = self.tax_year in
let incomes:Set(Income) = self.incomes→select(i:Income | i.year = tax_year) in
incomes→forAll(inc:Income |
  let distance:DistanceUnit = inc.distance in
  let minimal_distance:DistanceUnit =
  Constant::MINIMAL_DISTANCE.oclAsType(DistanceUnit) in
  if (distance > minimal_distance) = true then
    let maximal_distance:DistanceUnit =
    Constant::MAXIMAL_DISTANCE.oclAsType(DistanceUnit) in
    if (distance < maximal_distance) = true then
      let flat_rate:MonetaryValue =
      Constant::FLAT_RATE.oclAsType(MonetaryValue) in
      let prorata_period:Numeric = inc.prorata_period in
      let expected_amount:MonetaryValue = prorata_period * flat_rate * distance in
      let actual_amount:MonetaryValue = inc.getFD(tax_year).amount in
      actual_amount = expected_amount
    else   if (distance < maximal_distance) = false then
          let maximal_flat_rate:MonetaryValue =
          Constant::MAXIMAL_FLAT_RATE.oclAsType(MonetaryValue) in
          let prorata_period:Numeric = inc.prorata_period in
          let expected_amount:MonetaryValue = prorata_period * maximal_flat_rate in
          let actual_amount:MonetaryValue = inc.getFD(tax_year).amount in
          actual_amount = expected_amount
      else false endif
    endif
  else if (distance > minimal_distance) = false then
      let expected_amount:MonetaryValue = 0 in
      let actual_amount:MonetaryValue = inc.getFD(tax_year).amount in
      actual_amount = expected_amount
    else false endif endif
)
```

Coping with the large scale of standards and legal texts

automated extraction of trace links, concepts, processes

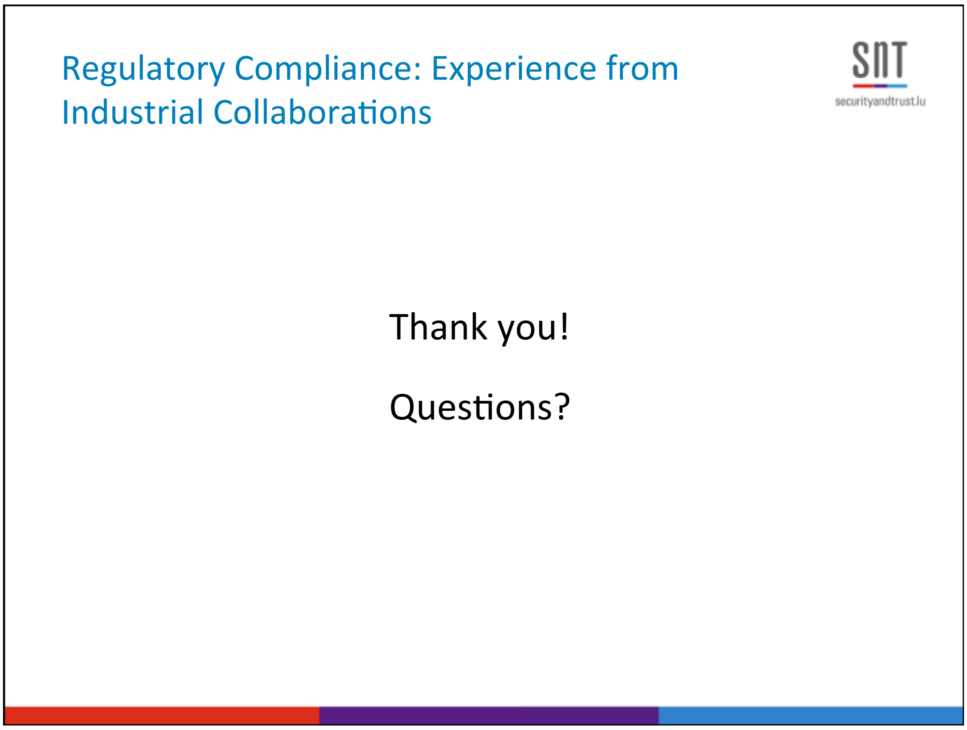


- Several projects on-going at SVV on Natural Language Processing of requirements documents and legal texts
- Cross reference analysis, keyword identification, model extraction, vocabulary correlation analysis, change analysis



Benefits of modeling for regulatory compliance

- Increased transparency
  - More credibility and trust
- More systematic guidelines for regulatory compliance
- Improved communication between regulators, auditors and service providers
- Better ways to structure existing knowledge
  - Models as repositories of information



Regulatory Compliance: Experience from Industrial Collaborations

Thank you!

Questions?