Model Management for Regulatory Compliance: *A Position Paper*

Sahar Kokaly, Rick Salay, Mehrdad Sabetzadeh,
Marsha Chechik and Tom Maibaum

MiSE 2016, Austin, Texas
May 16, 2016
kokalys@mcmaster.ca

Technology

Airbus A400M plane crash linked to software fault

By Leo Kelion
Technology desk editor

20 May 2015 | Technology

The A400M cargo plane crashed near Seville airport on 9 May

Tec

US aviation authority: Boeing 787 bug could cause 'loss of control'

More trouble for Dreamliner as Federal Aviation Administration warns glitch in control unit causes generators to shut down if left powered on for 248 days

The Boeing 787 has four generator-control units that, if powered on at the same, could fail simultaneously and cause a complete electrical shutdown. Photograph: Elaine Thompson/AP

Tec US

Ai co

sc

By Le
Techr

More
contr

20

The
cause a

threatpost

FDA: SOFTWARE FAILURES RESPONSIBLE FOR 24% OF ALL MEDICAL DEVICE RECALLS

by **Paul Roberts**

June 20, 2012 , 9:05

Software failures were behind 24 percent of all the medical device recalls in 2011, according to data from the U.S. Food and Drug Administration, which said it is gearing up its labs to spend more time analyzing the quality and security of software-based medical instruments and equipment.

Volvo recalls 59,000 cars over software fault

20 February 2016 | Europe

Sweden, Britain and Germany are the main markets affected

Swedish carmaker Volvo is recalling 59,000 cars across 40 markets over a fault that can temporarily shut down the engine.

"Standards are documented agreements containing technical **specifications** or other precise criteria to be used consistently as **rules**, **guidelines**, or **definitions** of characteristics, to ensure that materials, products, processes and services are fit for their purpose."

[ISO 1997]

DO-178B - Software Considerations in Airborne Systems and Equipment Certification.

IEC62304 – Medical device software – software life cycle processes.

ISO26262 - Functional Safety of Road Vehicles

Compliance

What is it?

The extent to which software developers have acted in accordance with practices set down in the standard.

Why it is done?

Establish **consistency** between actual development process and normative models embedded in the standards.

Standards are great, but they are also…

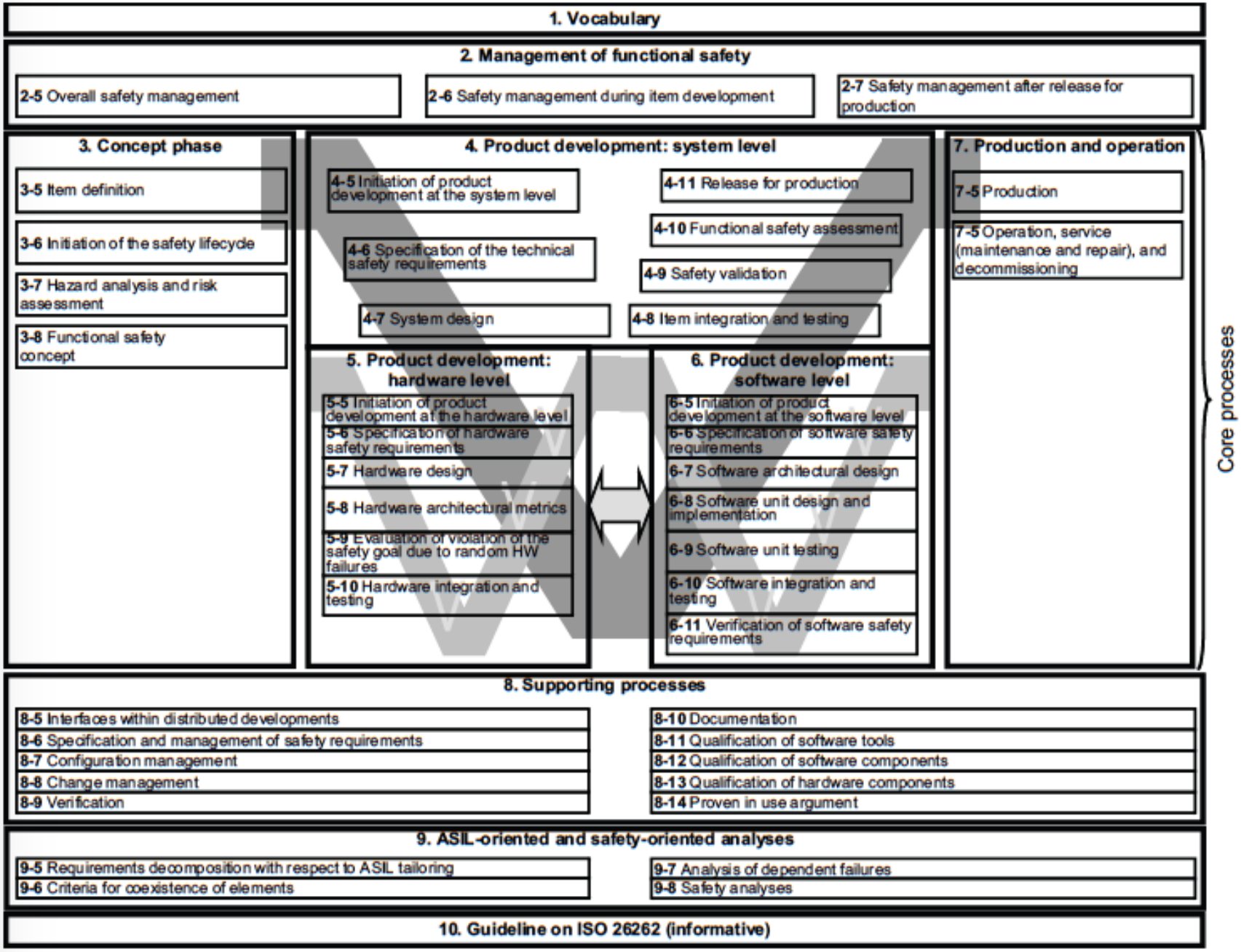
Standards are great, but they are also…

BIG

Standards are great, but they are also…

BIG

complex


1. Vocabulary
2. Management of functional safety
2-5 Overall safety management
2-6 Safety management during item development
2-7 Safety management after release for production
3. Concept phase
3-5 Item definition
3-6 Initiation of the safety lifecycle
3-7 Hazard analysis and risk assessment
3-8 Functional safety concept
4. Product development: system level
4-5 Initiation of product development at the system level
4-6 Specification of the technical safety requirements
4-7 System design
4-8 Item integration and testing
4-9 Safety validation
4-10 Functional safety assessment
4-11 Release for production
5. Product development: hardware level
5-5 Initiation of product development at the hardware level
5-6 Specification of hardware safety requirements
5-7 Hardware design
5-8 Hardware architectural metrics
5-9 Evaluation of violation of the safety goal due to random HW failures
5-10 Hardware integration and testing
6. Product development: software level
6-5 Initiation of product development at the software level
6-6 Specification of software safety requirements
6-7 Software architectural design
6-8 Software unit design and implementation
6-9 Software unit testing
6-10 Software integration and testing
6-11 Verification of software safety requirements
7. Production and operation
7-5 Production
7-5 Operation, service (maintenance and repair), and decommissioning
Core processes
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and management of safety requirements
8-7 Configuration management
8-8 Change management
8-9 Verification
8-10 Documentation
8-11 Qualification of software tools
8-12 Qualification of software components
8-13 Qualification of hardware components
8-14 Proven in use argument
9. ASIL-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses
10. Guideline on ISO 26262 (informative)

…this makes compliance

…this makes compliance

Co$tly

…this makes compliance

Co$tly

What is needed?

…this makes compliance

Co$tly

What is needed?

A way to (semi-)automate compliance assessment activity to reduce its cost.

Model Management for Regulatory Compliance
Outline

- Introduction
- Getting started:
  - Modeling for Compliance
  - Model Management as a toolbox
- Adapting Model Management for Regulatory Compliance
  - Why adapt?
  - Example: Assurance Case Reuse due to System Evolution
  - Model Management for other compliance problems
- Next Steps

Related Work:
Modeling for Compliance

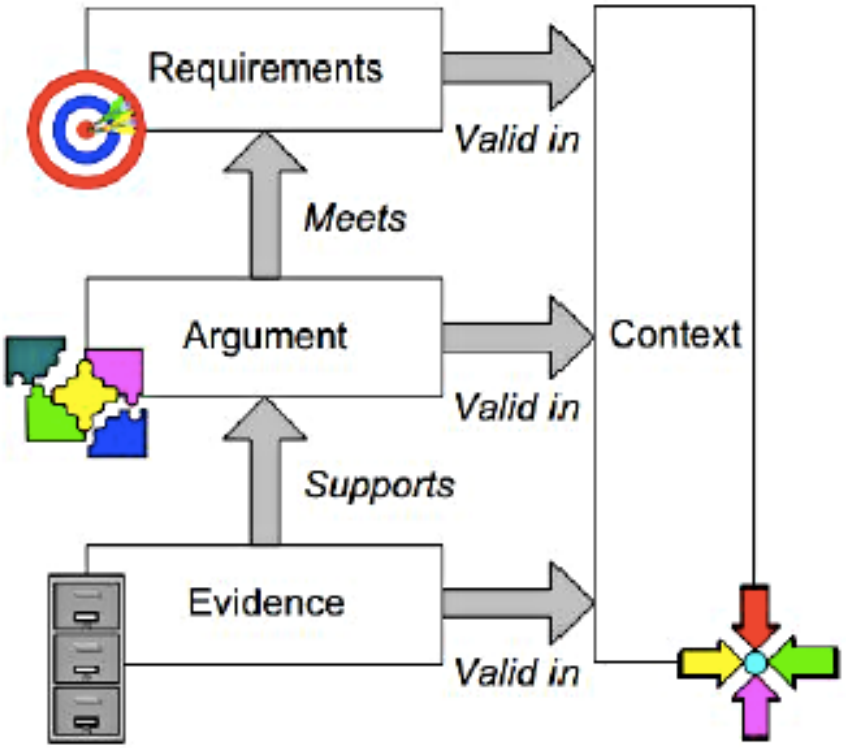
- standards as models
- compliance checking as a model conformance problem
- model based assurance cases

What is an Assurance Case?

- An artifact that shows how important **claims** about the system (e.g., requirement satisfaction) can be **argued** for, ultimately from **evidence** obtained about the system such as model checking, test results, expert opinion, etc.

- Approaches for modeling assurances cases:
  - GSN
  - CAE
  - KAOS-based
  - OMG SACM

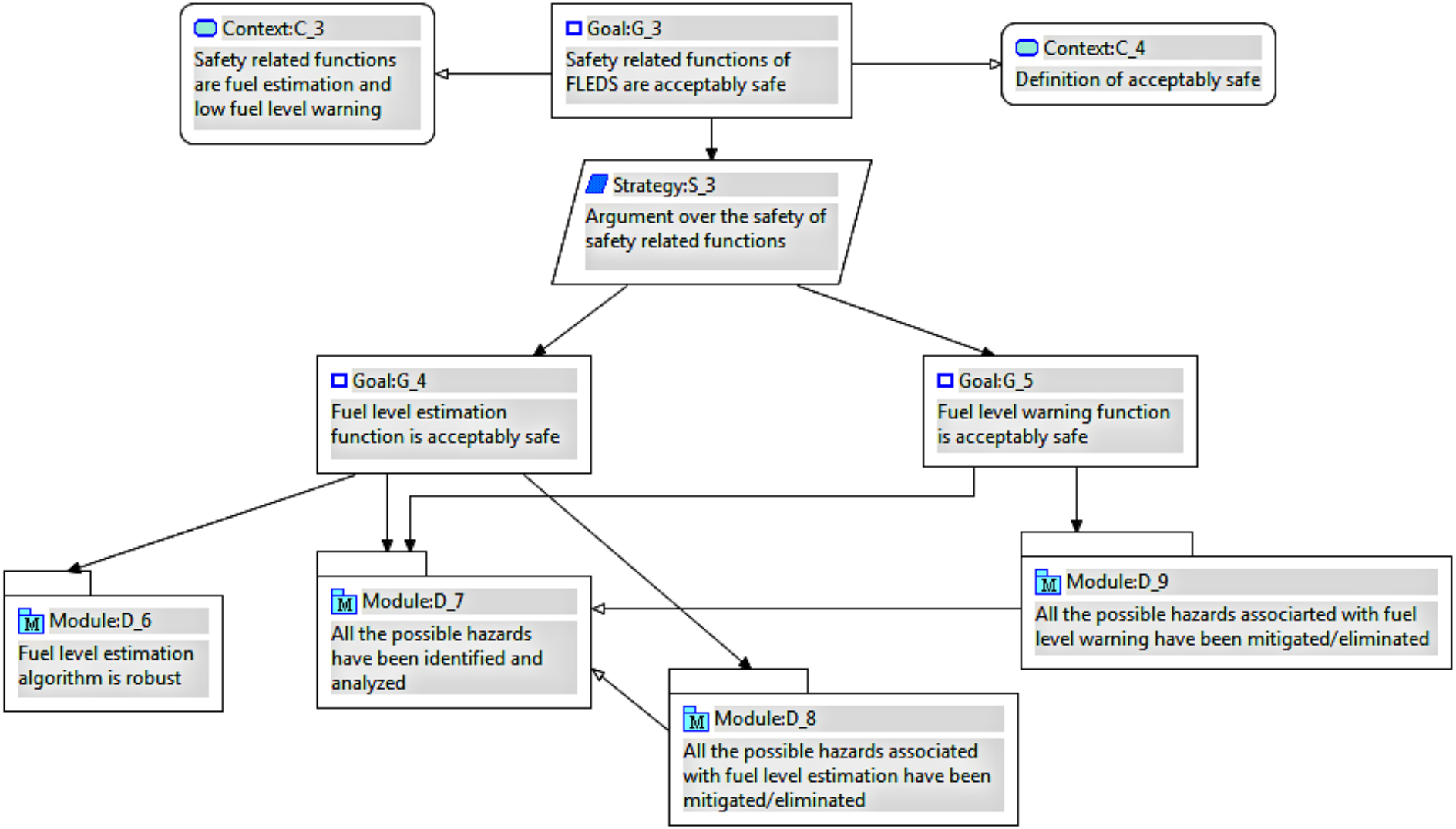
Model-Based Assurance Cases*



* Illustration borrowed from [Dardar'13] “Building a Safety Case in Compliance with ISO 26262 for Fuel Level Estimation and Display System “ Raghad Dardar. Master Thesis. M¨alardalen University, Sweden. 2013

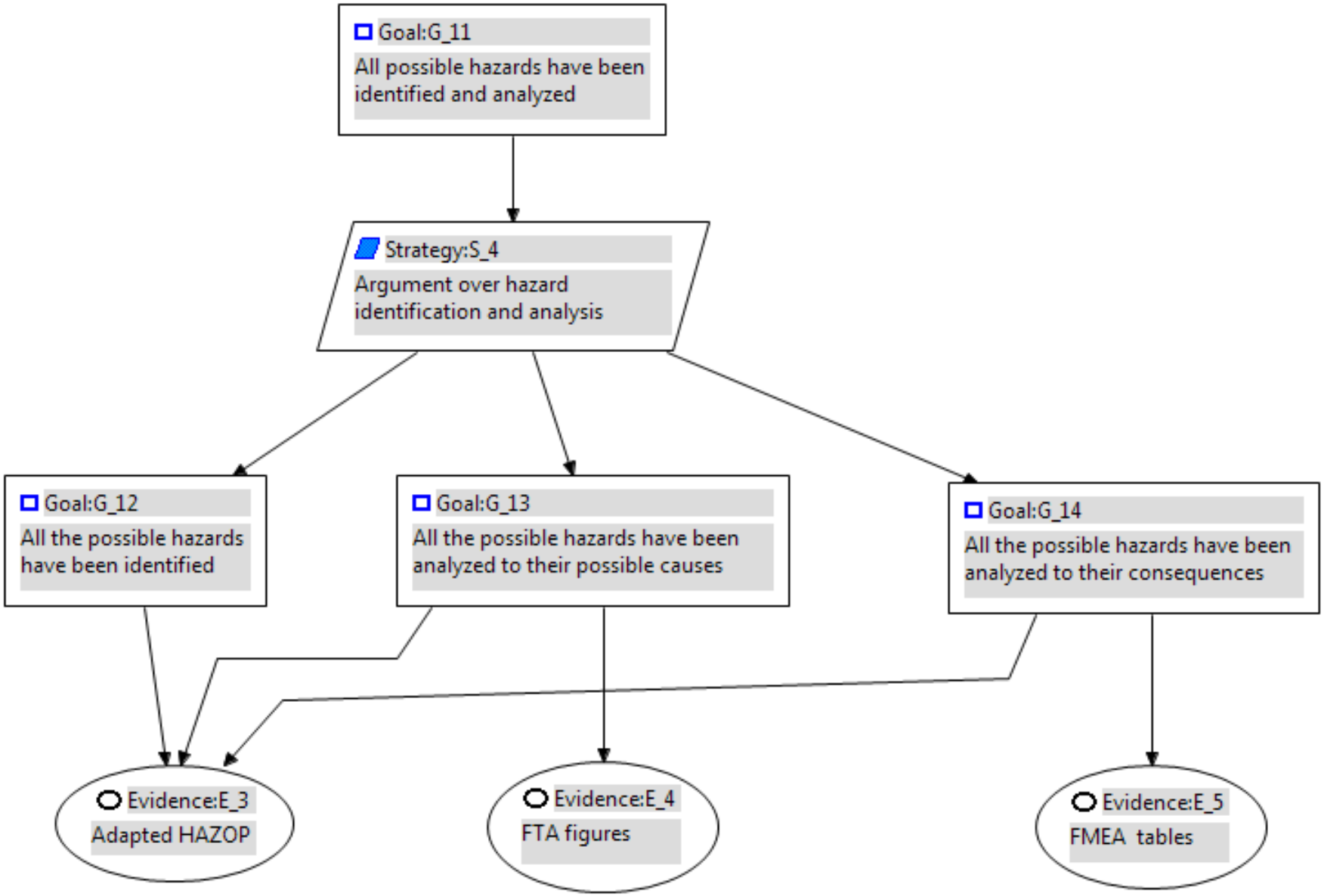
Example: FLEDS*

(Fuel Level Estimation and Display) System)



* Example borrowed from [Dardar'13]

Example: FLEDS* *ctd.*



* Example borrowed from [Dardar'13]

Modeling for Compliance: What's Missing?

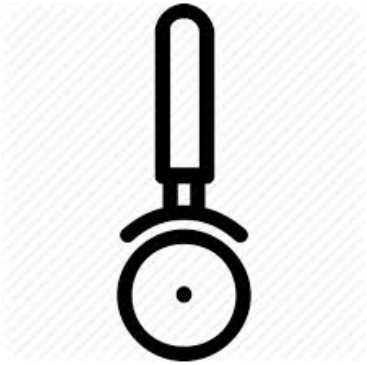
- More holistic view of compliance
- Workflows to address interesting compliance-related problems:
  - E.g.,
    - assessing compliance due to evolution
    - compliance to multiple standards
    - compliance of product lines

The Toolbox: Model Management (MM)

- high-level view in which entire **models** and their **relationships** can be manipulated using **operators** to achieve useful outcomes.
- **megamodel:** a special type of model in which the elements represent models and the links between the elements represent relationships between the models.

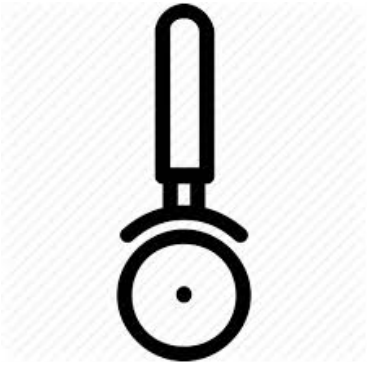
Model Management Operators

Model Management Operators

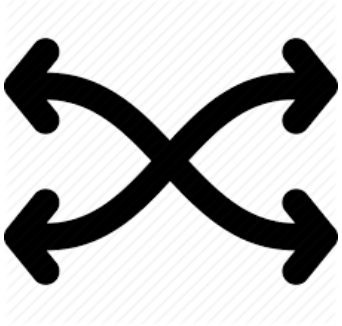


slice

Model Management Operators

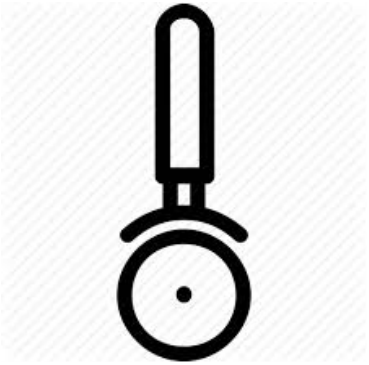


slice

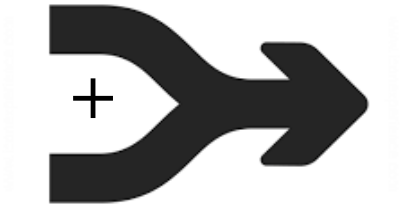


match

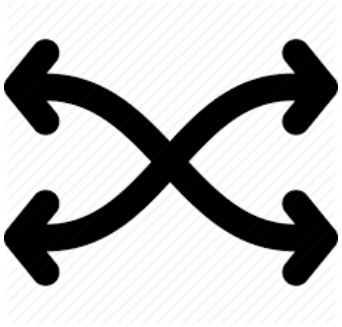
Model Management Operators



slice

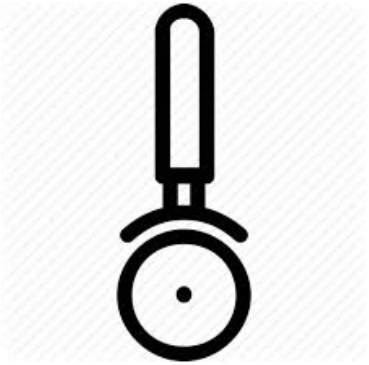


merge

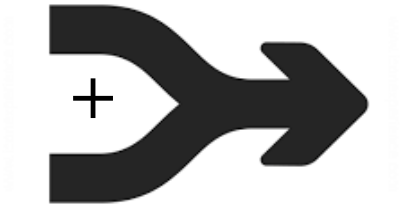


match

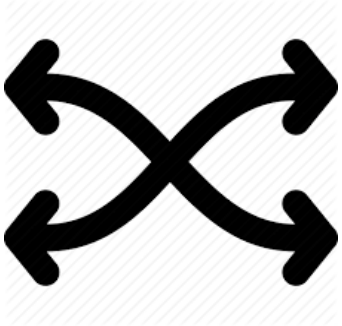
Model Management Operators



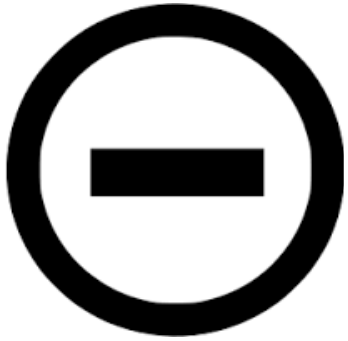
slice



merge

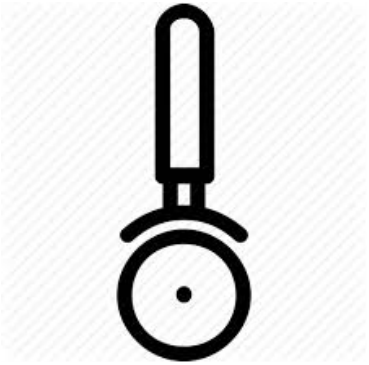


match

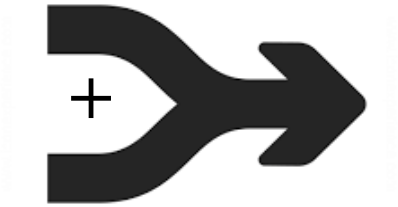


diff

Model Management Operators

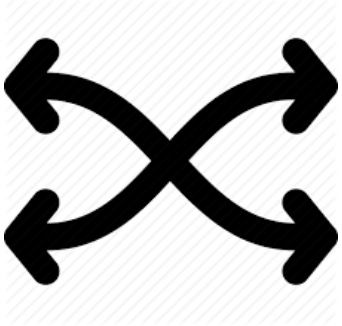


slice

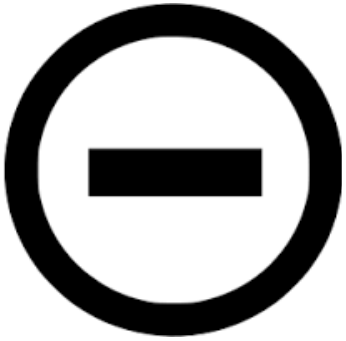


merge

lift

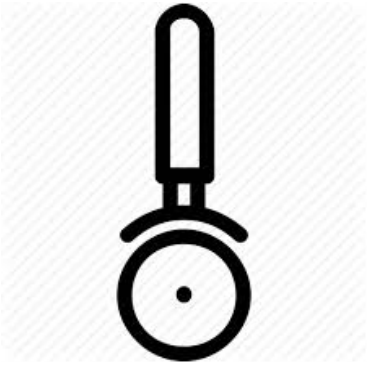


match

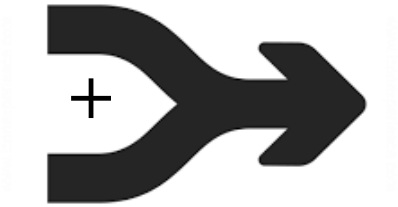


diff

Model Management Operators

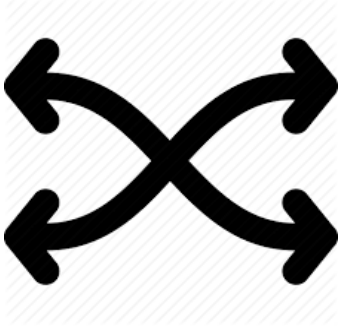


slice

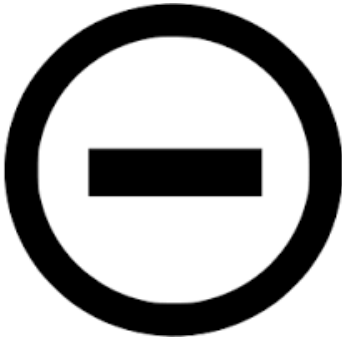


merge

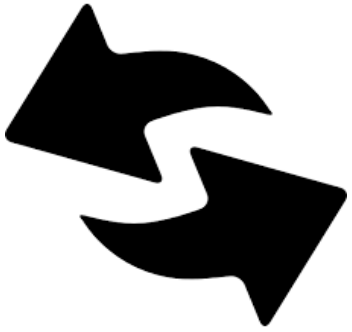
lift



match

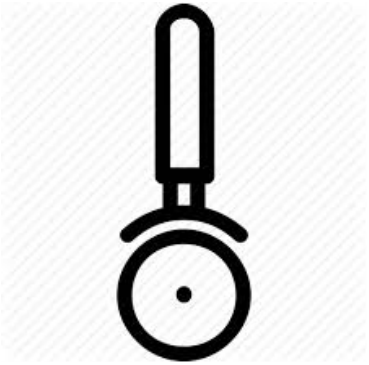


diff

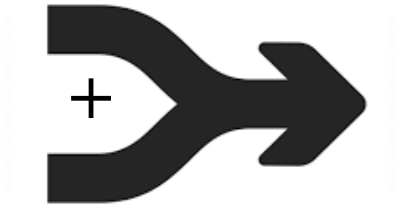


bidirectional MT

Model Management Operators



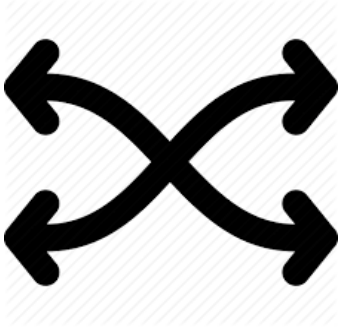
slice



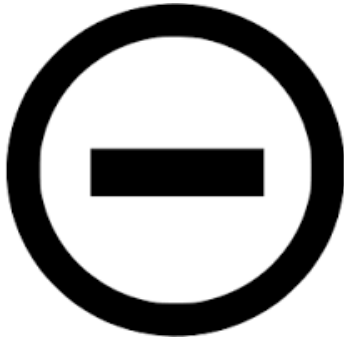
merge

lift

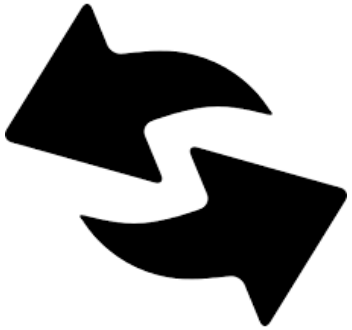
\+ Megamodel Operators (Map, Filter, Reduce) [*MODELS'15*]



match



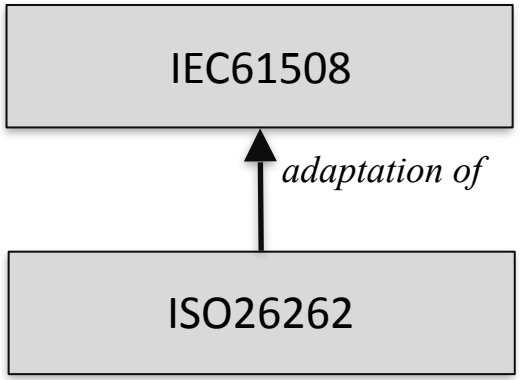
diff

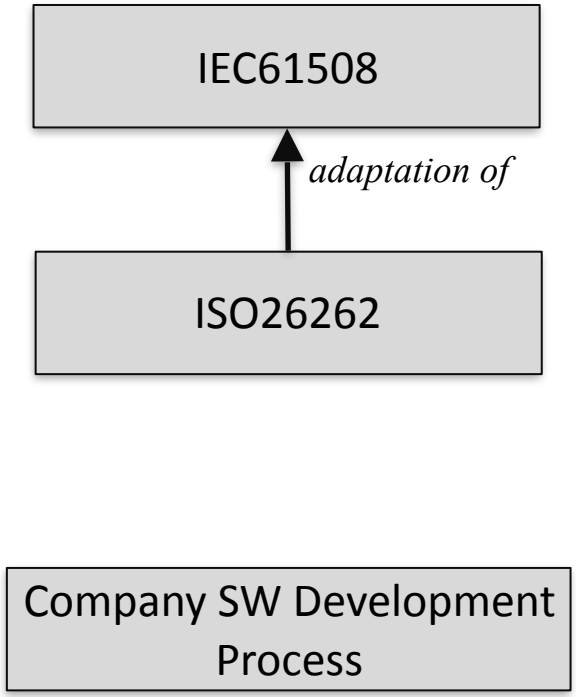


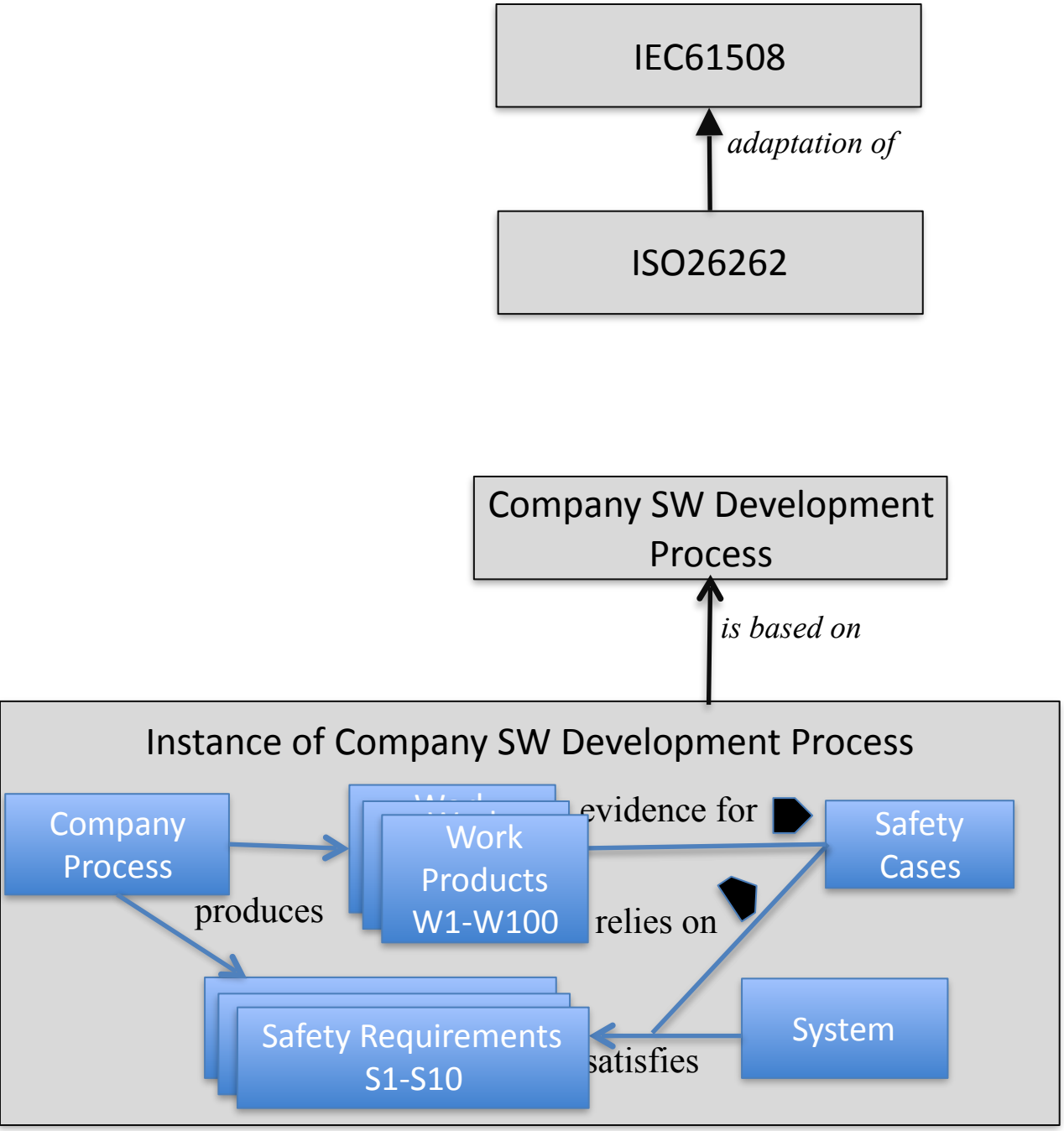
bidirectional MT

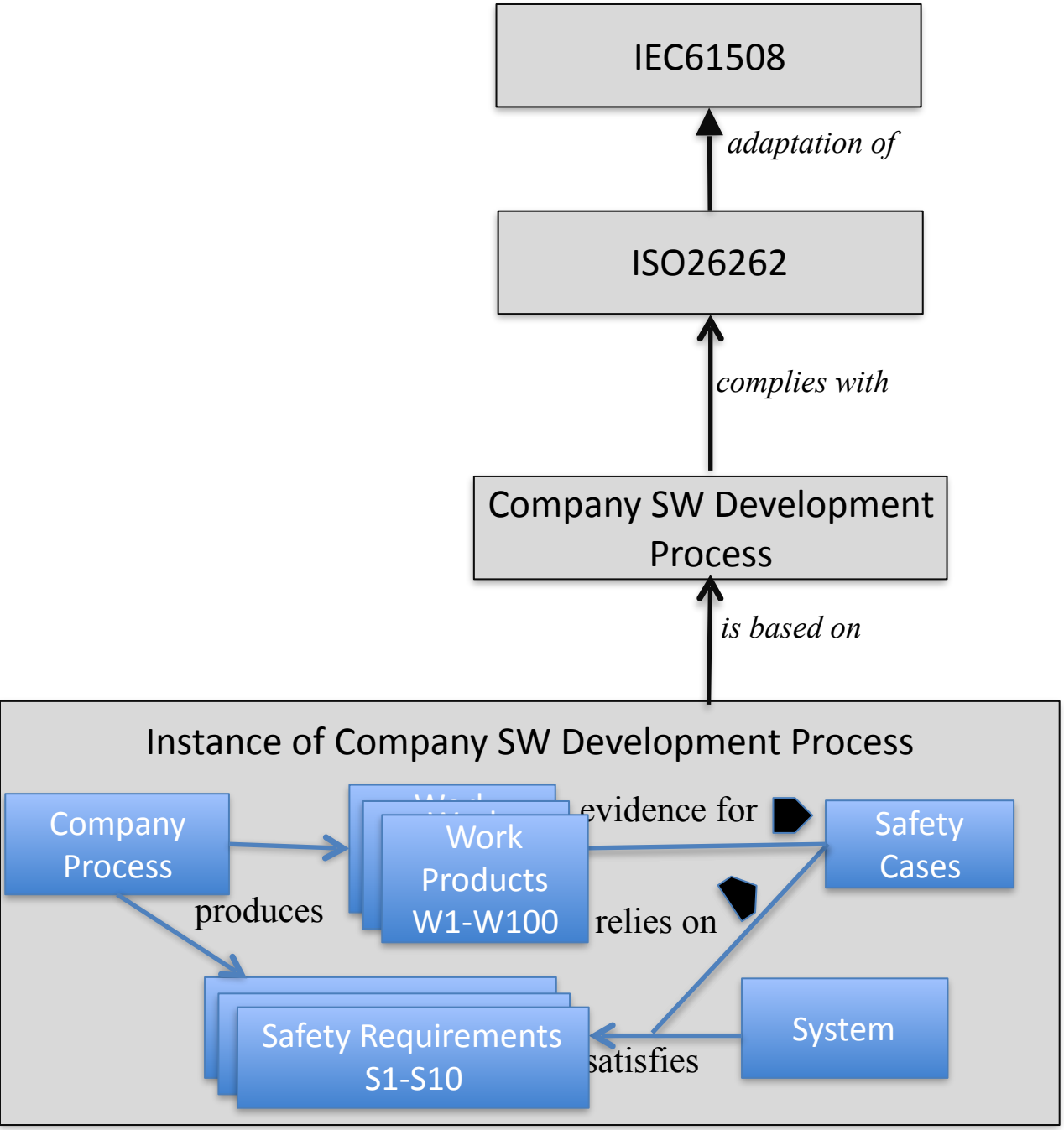
Model Management for Regulatory Compliance
Outline

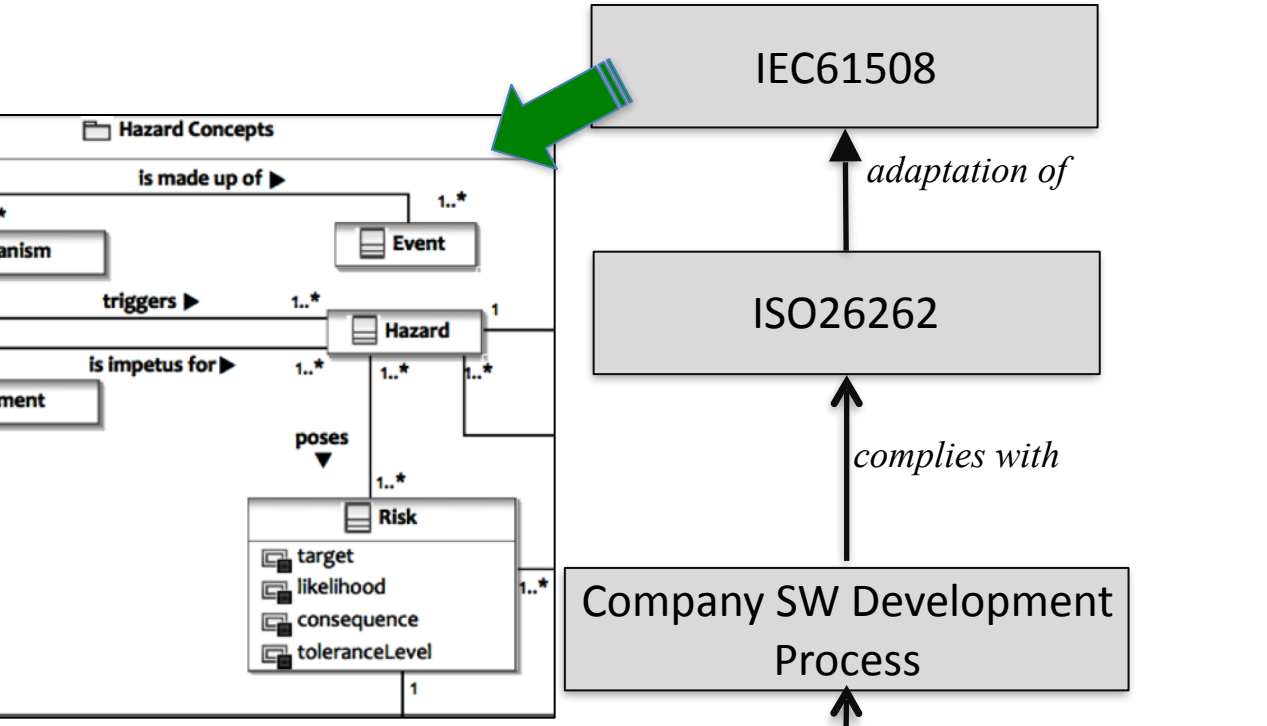
- Introduction
- Getting started:
  - Modeling for Compliance
  - Model Management as a toolbox
- Adapting Model Management for Regulatory Compliance
  - Why adapt?
  - Example: Assurance Case Reuse due to System Evolution
  - Model Management for other compliance problems
- Next Steps


IEC61508
adaptation of
ISO26262


IEC61508
adaptation of
ISO26262
Company SW Development Process


IEC61508
adaptation of
ISO26262
Company SW Development Process
is based on
Instance of Company SW Development Process
Company Process
Work Products W1-W100
evidence for
Safety Cases
produces
relies on
Safety Requirements S1-S10
System
satisfies


IEC61508
adaptation of
ISO26262
complies with
Company SW Development Process
is based on
Instance of Company SW Development Process
Company Process
Work Products W1-W100
evidence for
Safety Cases
produces
relies on
Safety Requirements S1-S10
satisfies
System



IEC61508

adaptation of

ISO26262

complies with

Company SW Development Process

is based on

Instance of Company SW Development Process

Company Process

produces

Work Products W1-W100

evidence for

Safety Cases

relies on

Safety Requirements S1-S10

satisfies

System

IEC61508

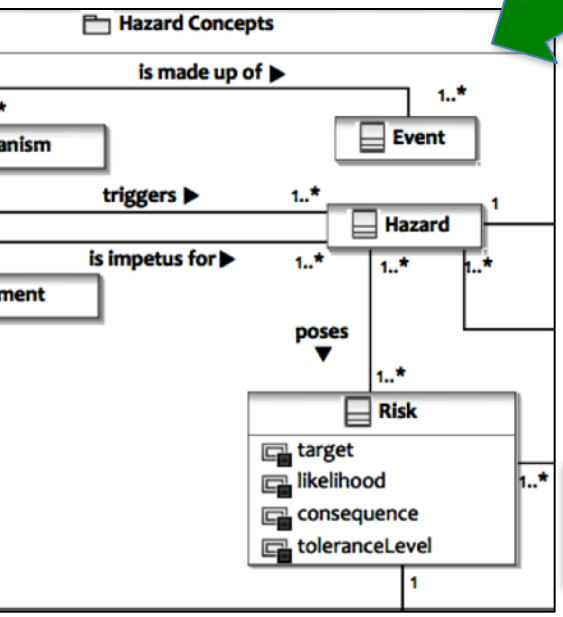
adaptation of

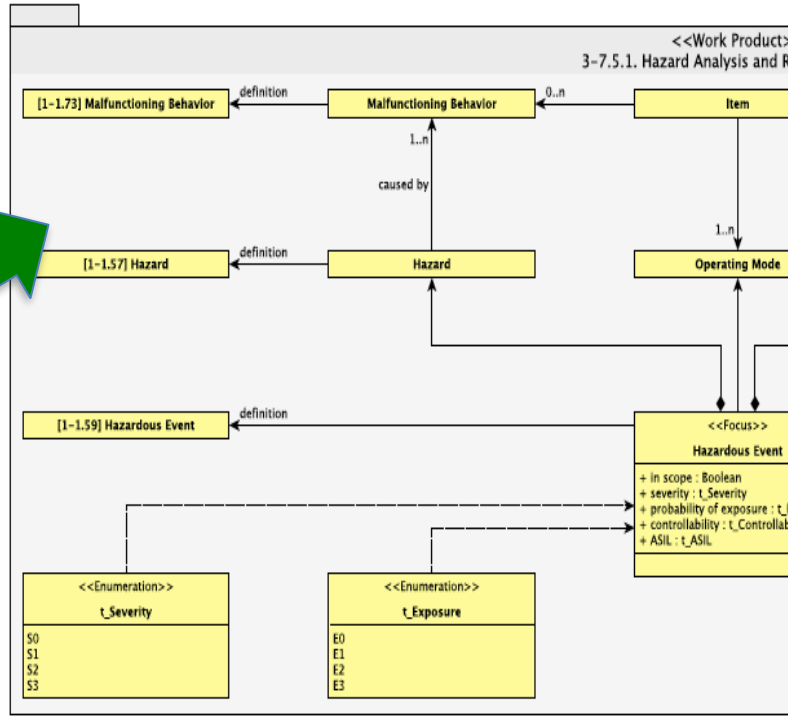
ISO26262

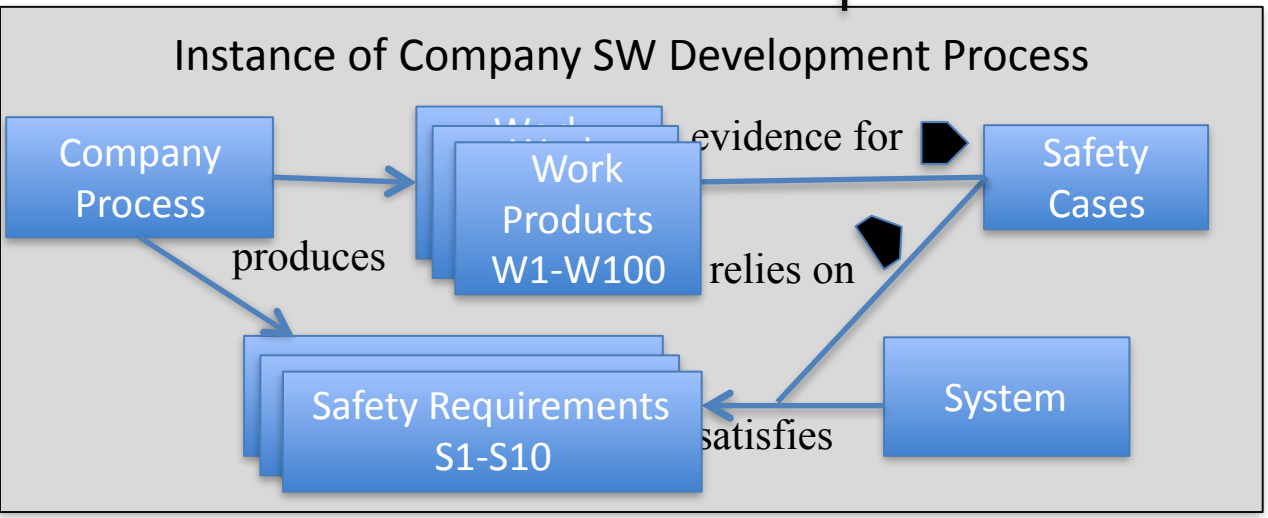
complies with

Company SW Development Process

is based on







IEC61508

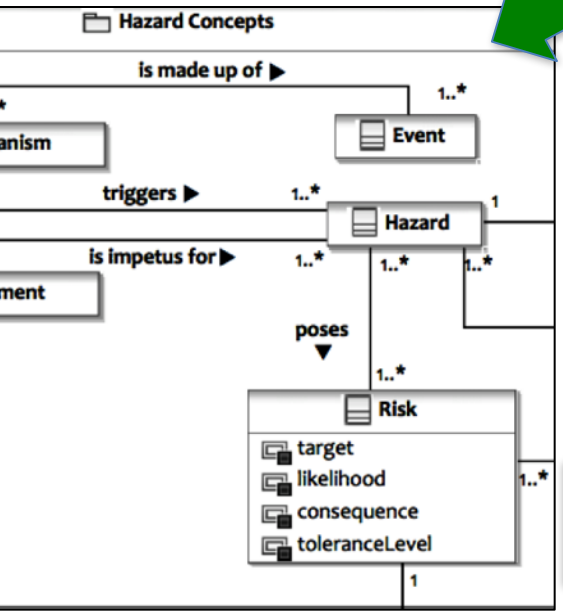
adaptation of

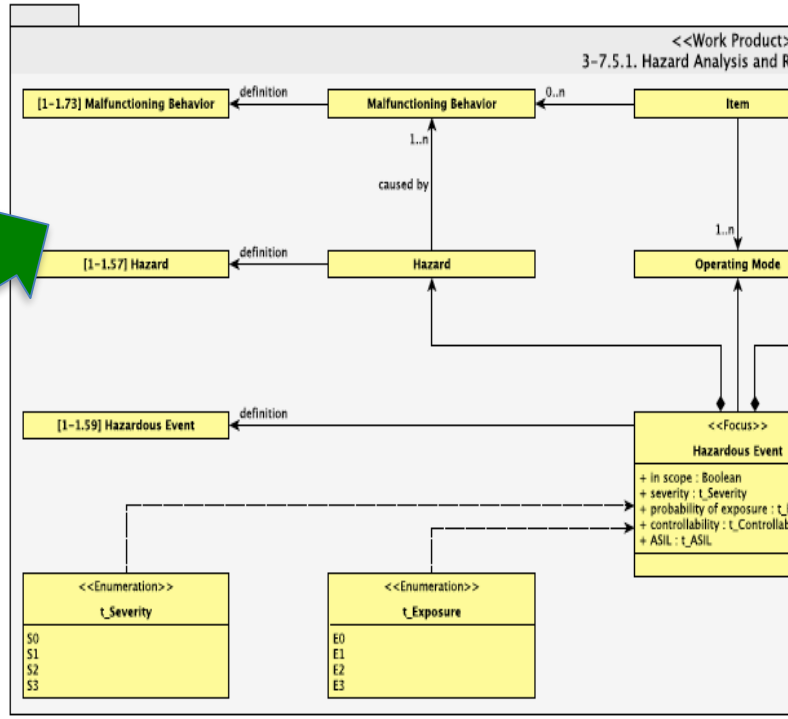
ISO26262

complies with

Company SW Development Process

is based on





Instance of Company SW Development Process

Company Process

produces

Work Products W1-W100

evidence for

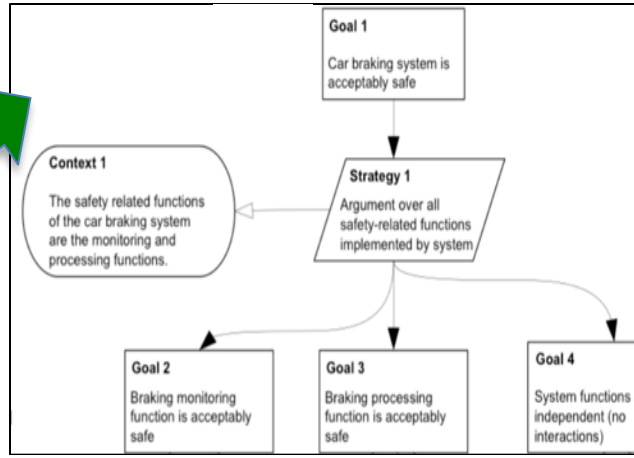
Safety Cases

relies on

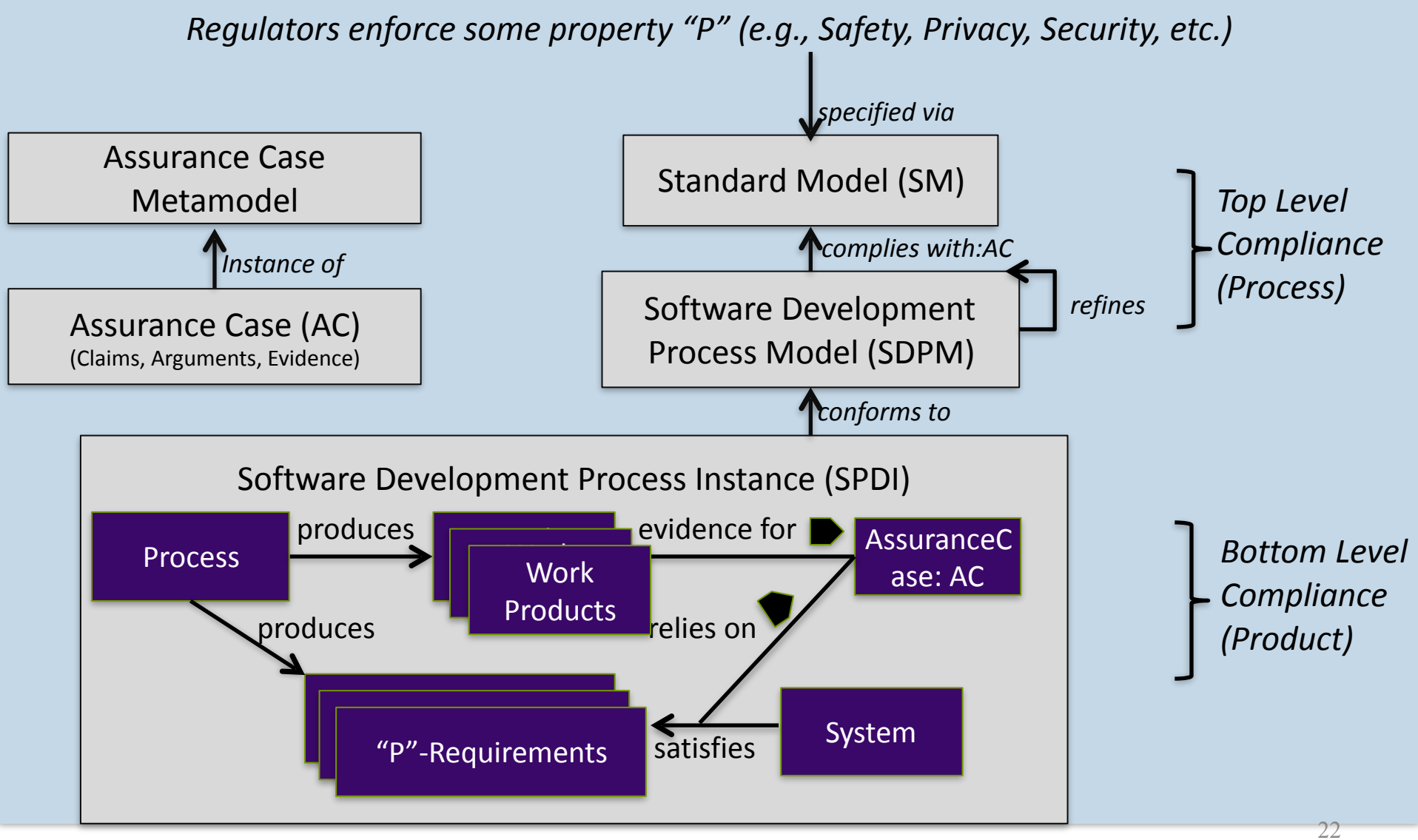
Safety Requirements S1-S10

satisfies

System



A General Model of Compliance



Why Adapt?

- Challenges introduced when applying MM for compliance:
  1. Amount of **natural language** used in expressing the standards and the claims/arguments in the assurance cases.
  2. The **human-in-the-loop** factor and reliance on expert opinion.
  3. The **assurance artifacts** that need to be carefully managed when applying the various model management operators.

Why Adapt?

- Challenges introduced when applying MM for compliance:
  1. Amount of **natural language** used in expressing the standards and the claims/arguments in the assurance cases.
  2. The **human-in-the-loop** factor and reliance on expert opinion.
  3. The **assurance artifacts** that need to be carefully managed when applying the various model management operators.

- What is needed:
  - Adapted MM operators to work with Assurance Cases
  - MM workflows to address interesting scenarios

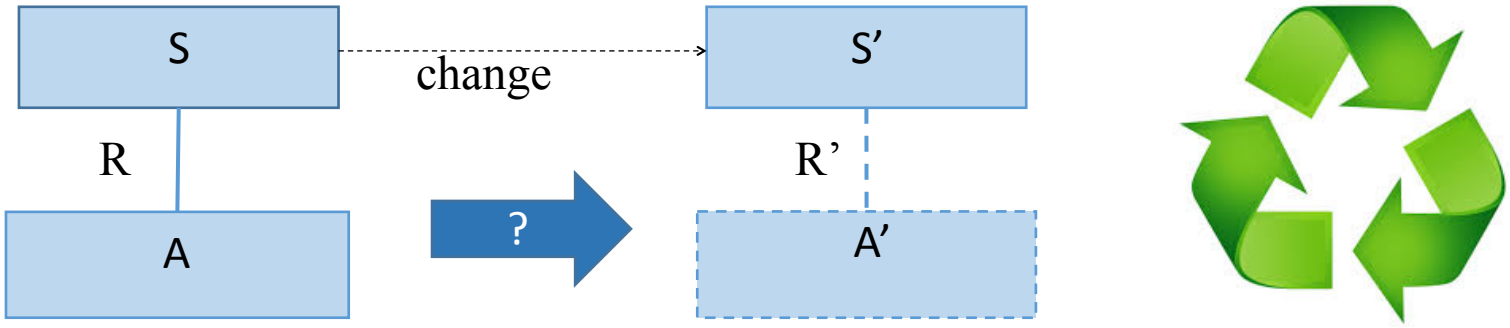
Adapted Model Management Toolbox

Hypothesis: Model Management Operators and Tools can be *adapted* to help structure, manage and reason about regulatory compliance.

Model Management for Regulatory Compliance
Outline

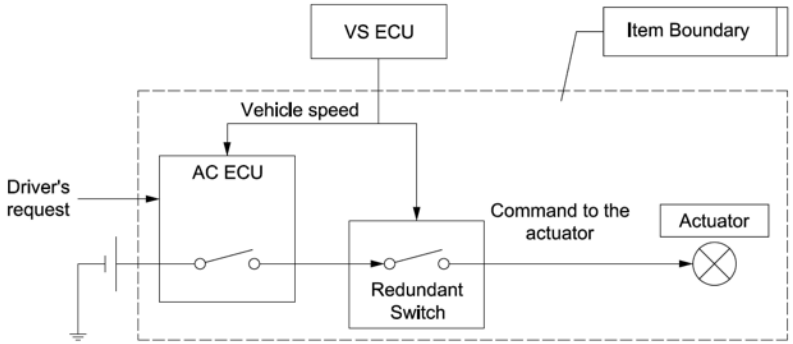
- Introduction
- Getting started:
  - Modeling for Compliance
  - Model Management as a toolbox
- Adapting Model Management for Regulatory Compliance
  - Why adapt?
  - Example: Assurance Case Reuse due to System Evolution
  - Model Management for other compliance problems
- Next Steps

Assurance Case reuse due to system evolution [submitted to MODELS'16]

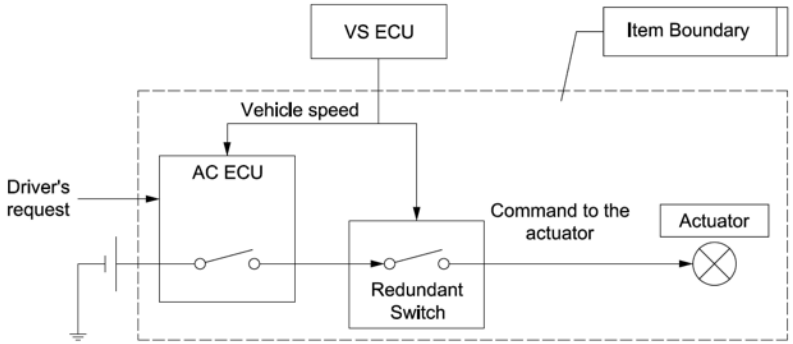


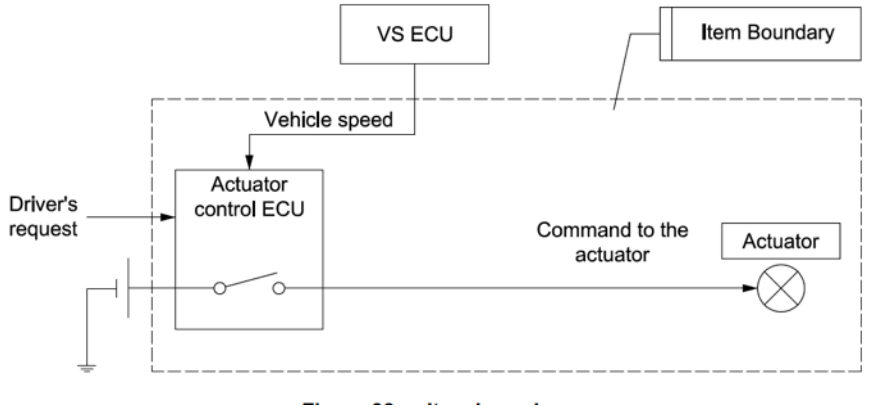
- Addressed in model management using **co-evolution/bidirectional transformations.**
- **Challenge:** carefully managing the assurance case (claims, arguments, evidence) that is attached to the compliance relationship.
- **Goal**: Reuse as much of the original assurance case components as possible.

Example: Power Sliding Door

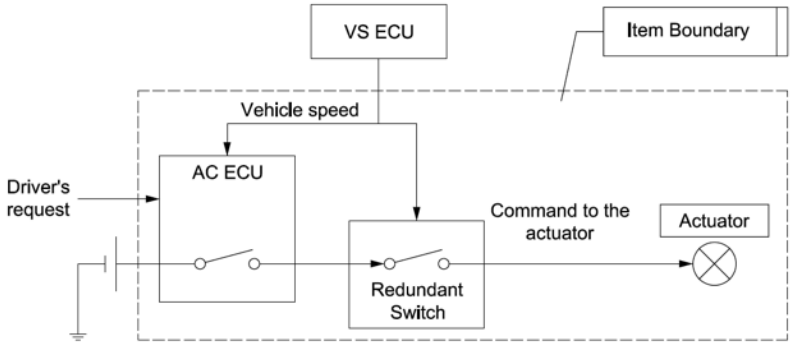


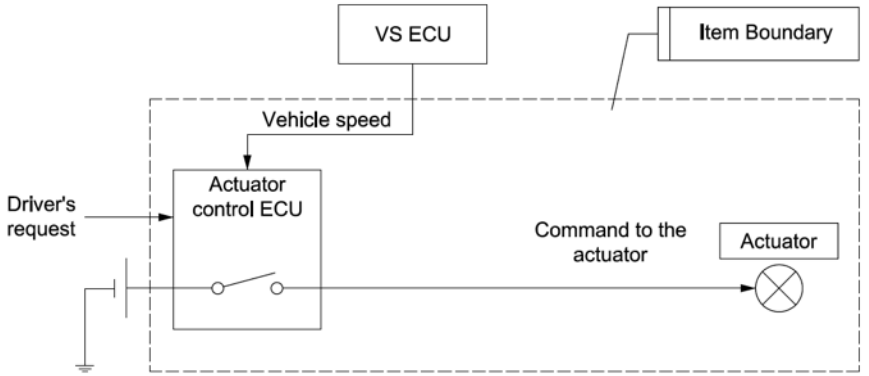
Example: Power Sliding Door

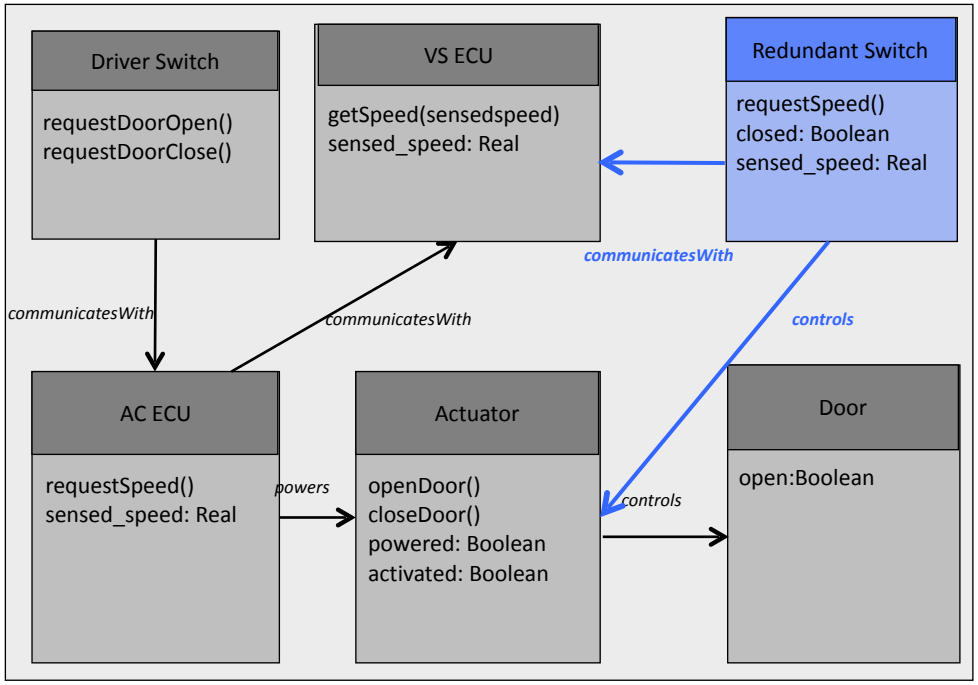


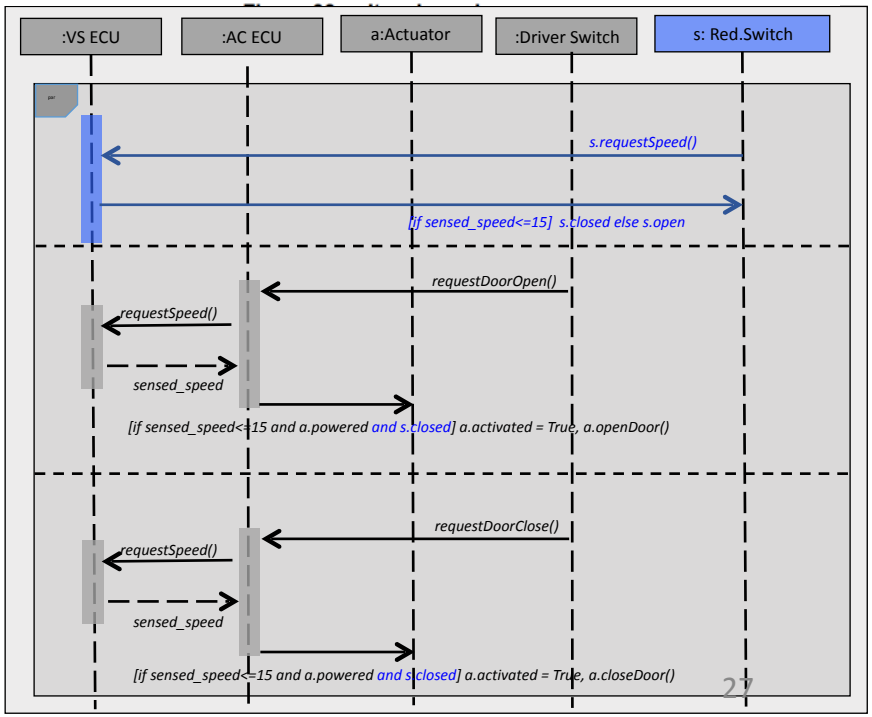


Example: Power Sliding Door

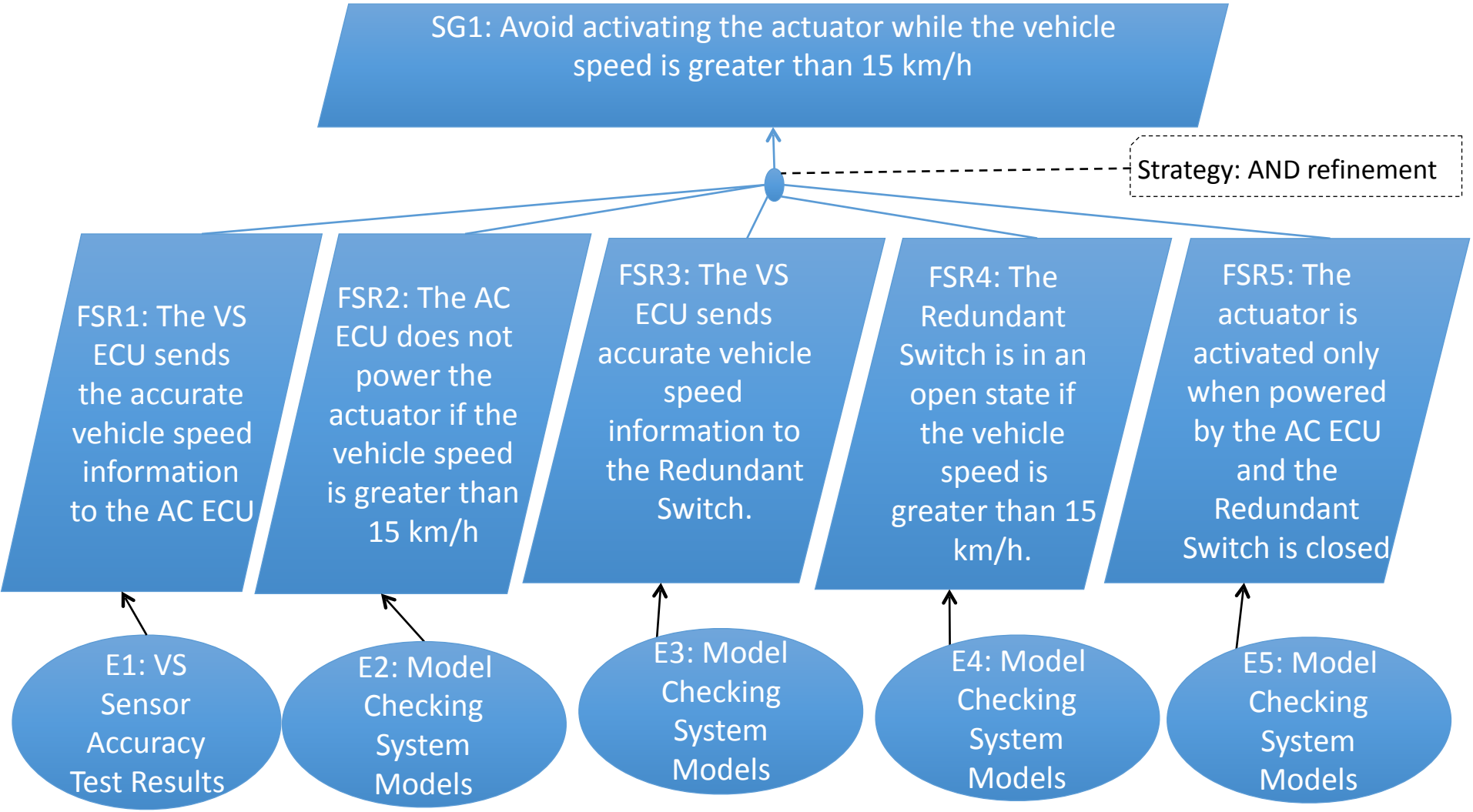








Original Assurance Case



Model Management AC Reuse
Impact Assessment Algorithm

Params: <$Slice_T$; $Merge_T$>

Input: initial spec S : T, assurance case A : AC, traceability map R, changed spec S' : T, delta D = <C0a;C0d;C0c>

Output: Impact set estimate A_{RMM}, impact kind annotation k_{RMM}

1: $R'_A \leftarrow Restrict(R, D)$

2: $dc \leftarrow Slice_T (S, Merge_T (d,c))$

3: $ac \leftarrow Slice_T (S', Merge_T (a,c))$

4: $C2_{recheck} \leftarrow Merge_{AC}(Trace(R, dc), Trace(R'_A , ac))$

5: $C2_{revise} \leftarrow Trace(R, d)$

6: $C3_{revise} \leftarrow Slice_{AC}(M, C2_{revise})$

7: $C3_{recheck} \leftarrow Slice_{AC}(M, C2_{recheck})$

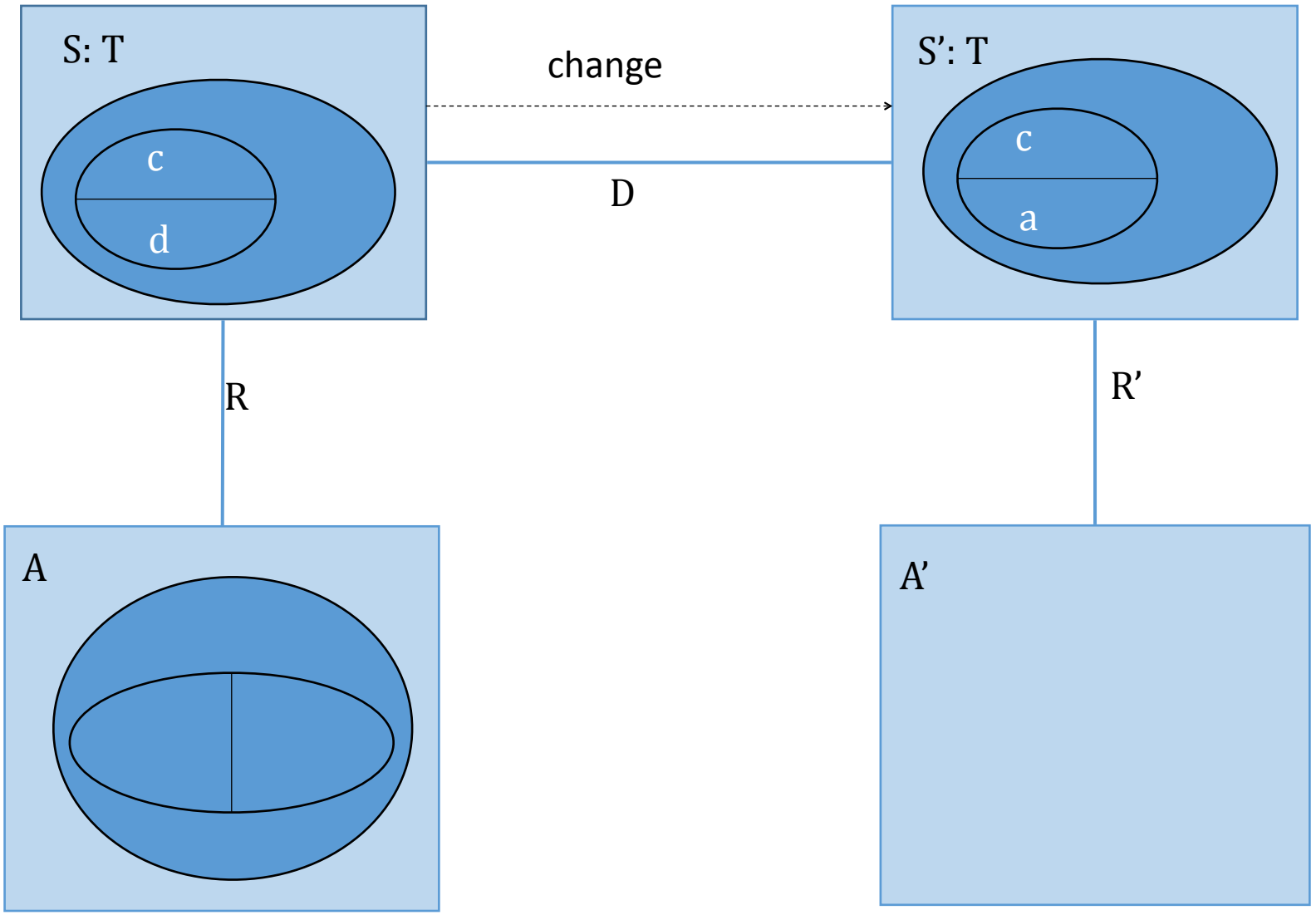
8: $A_{RMM} \leftarrow Merge_{AC}(C3_{revise}, C3_{recheck})$

9: $k_{RMM} (C3_{recheck}) \leftarrow$ 'recheck'

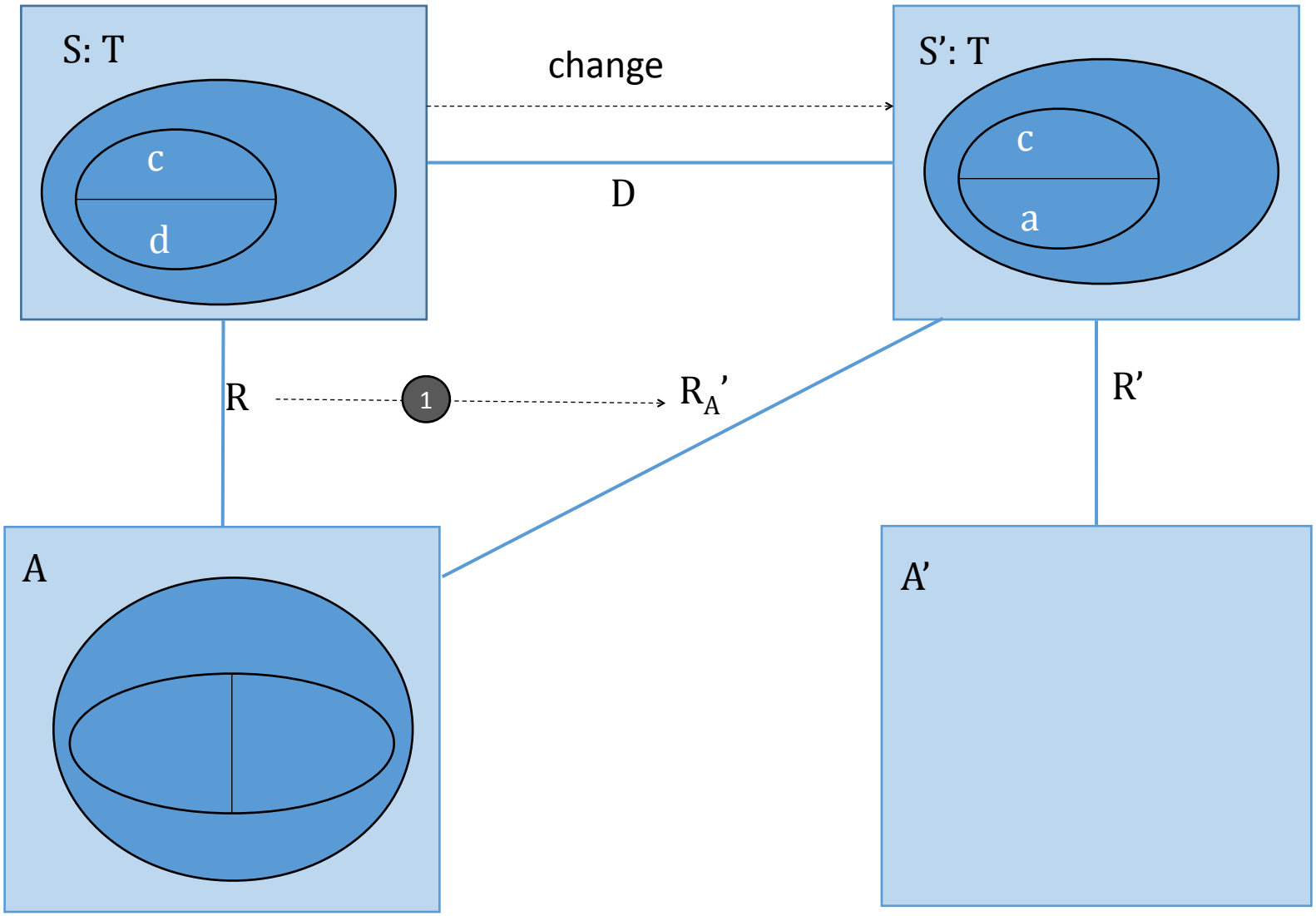
10: $k_{RMM}(C3_{revise}) \leftarrow$ 'revise'

11: return A_{RMM}, k_{RMM}

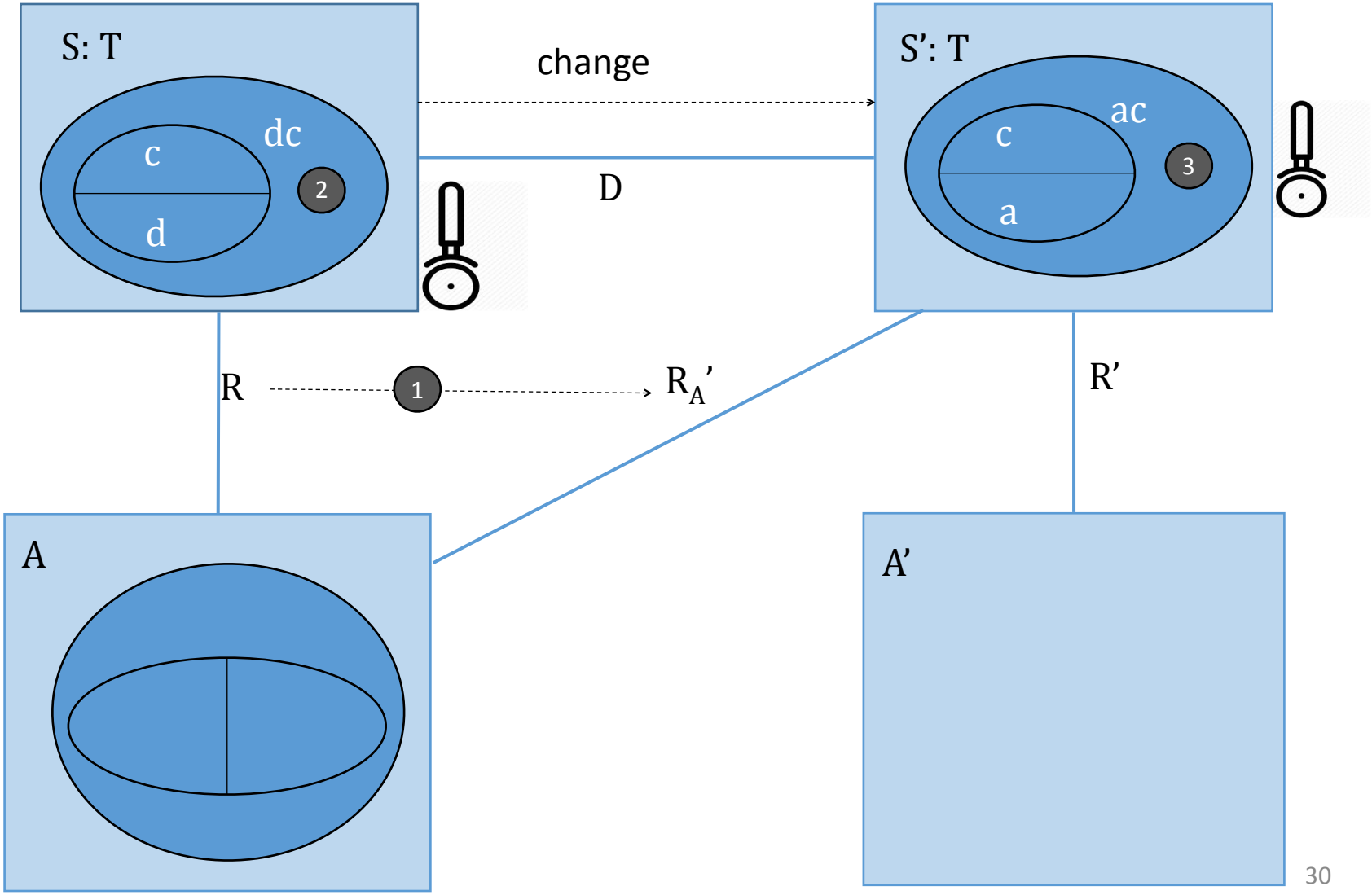
MMt algorithm for AC reuse due to System Evolution



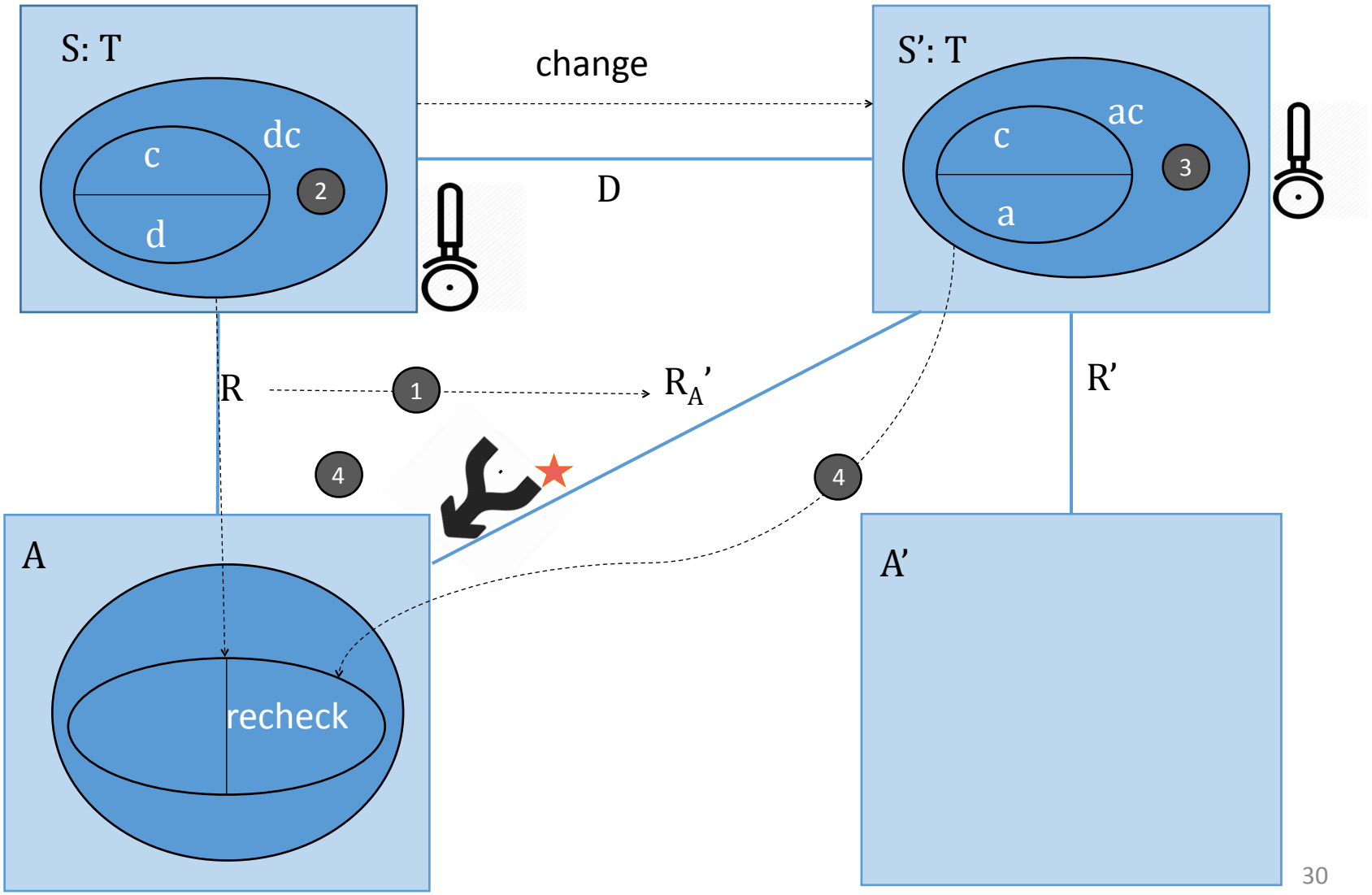
MMt algorithm for AC reuse due to System Evolution



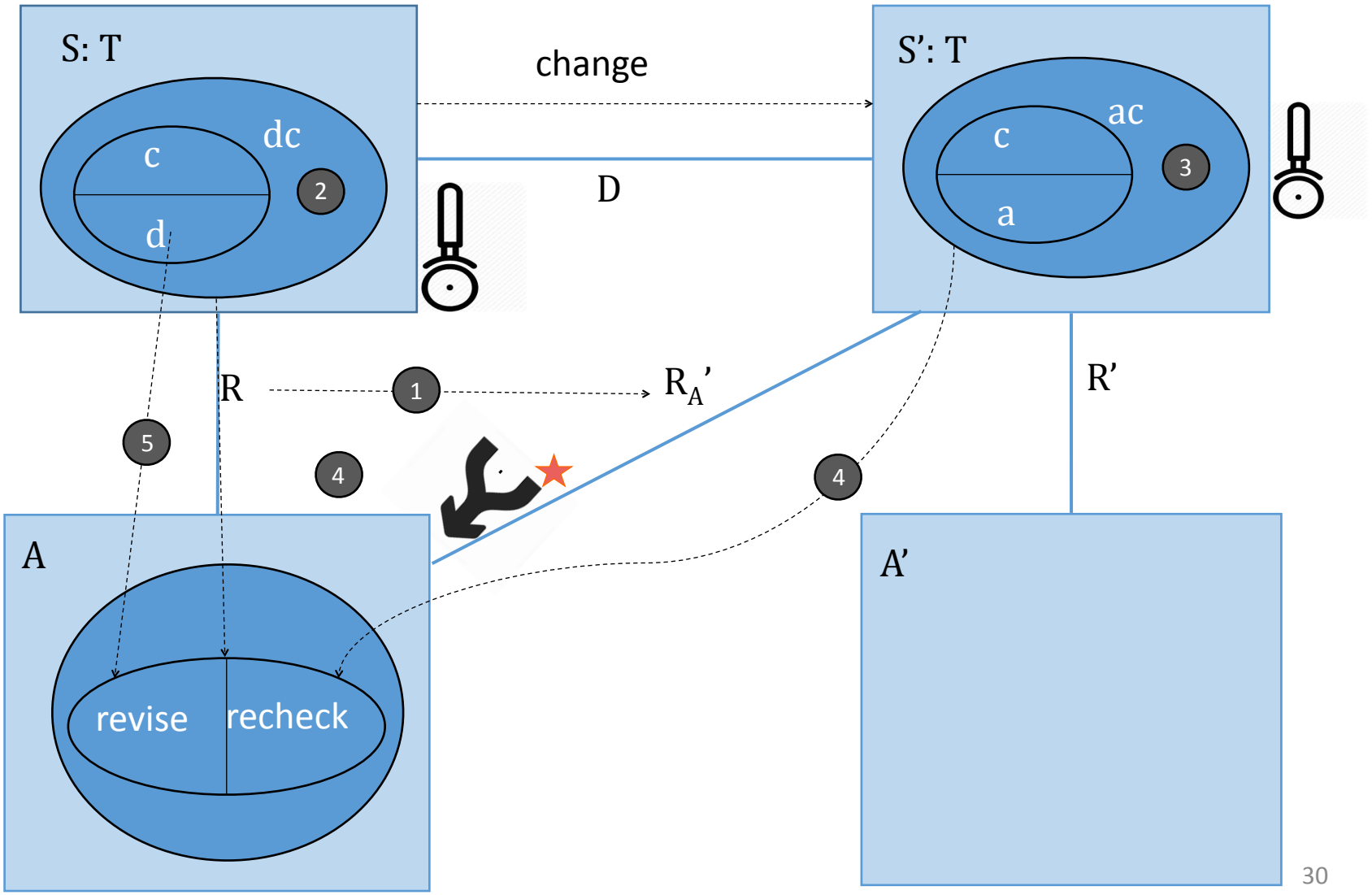
MMt algorithm for AC reuse due to System Evolution



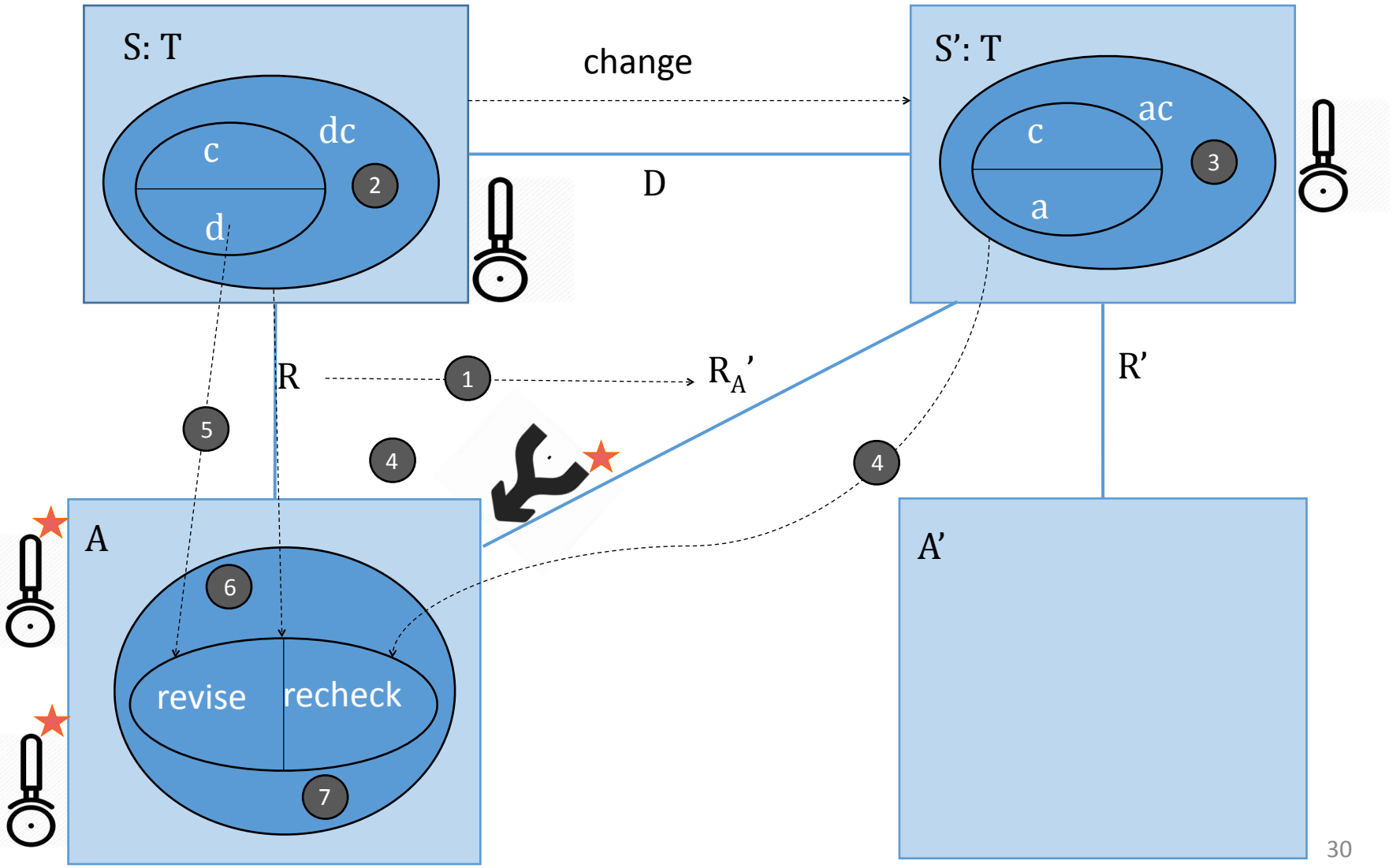
MMt algorithm for AC reuse due to System Evolution



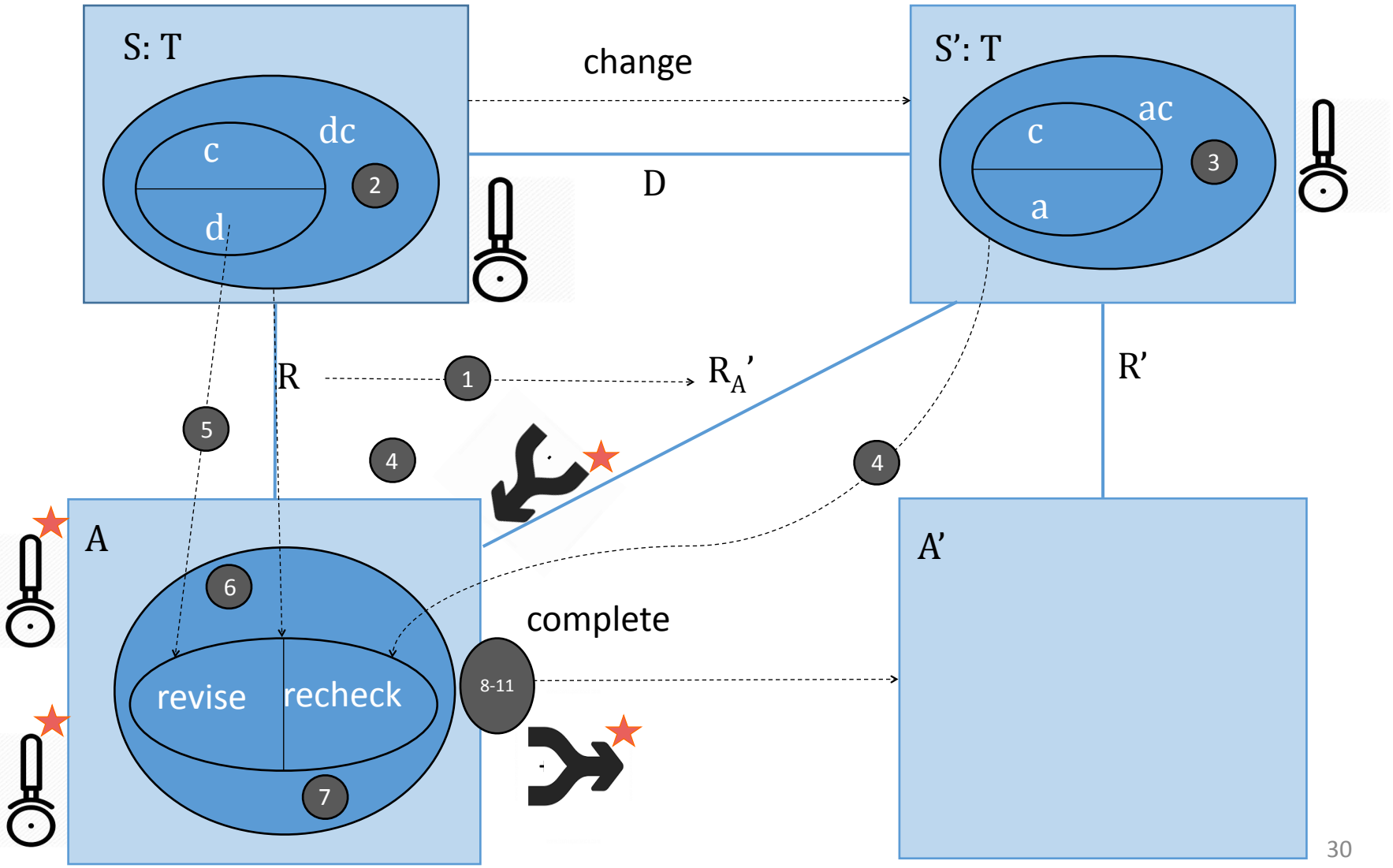
MMt algorithm for AC reuse due to System Evolution



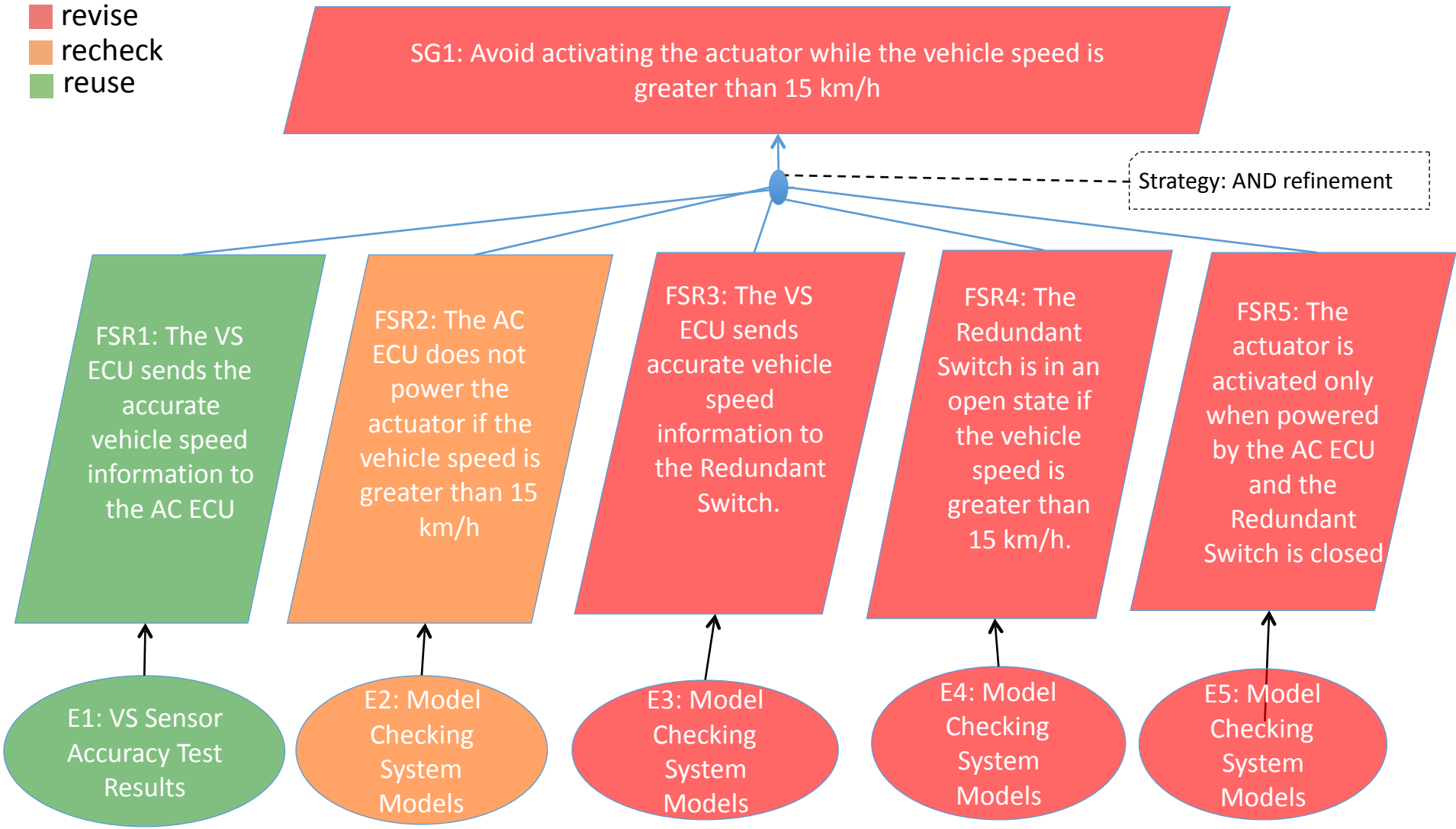
MMt algorithm for AC reuse due to System Evolution



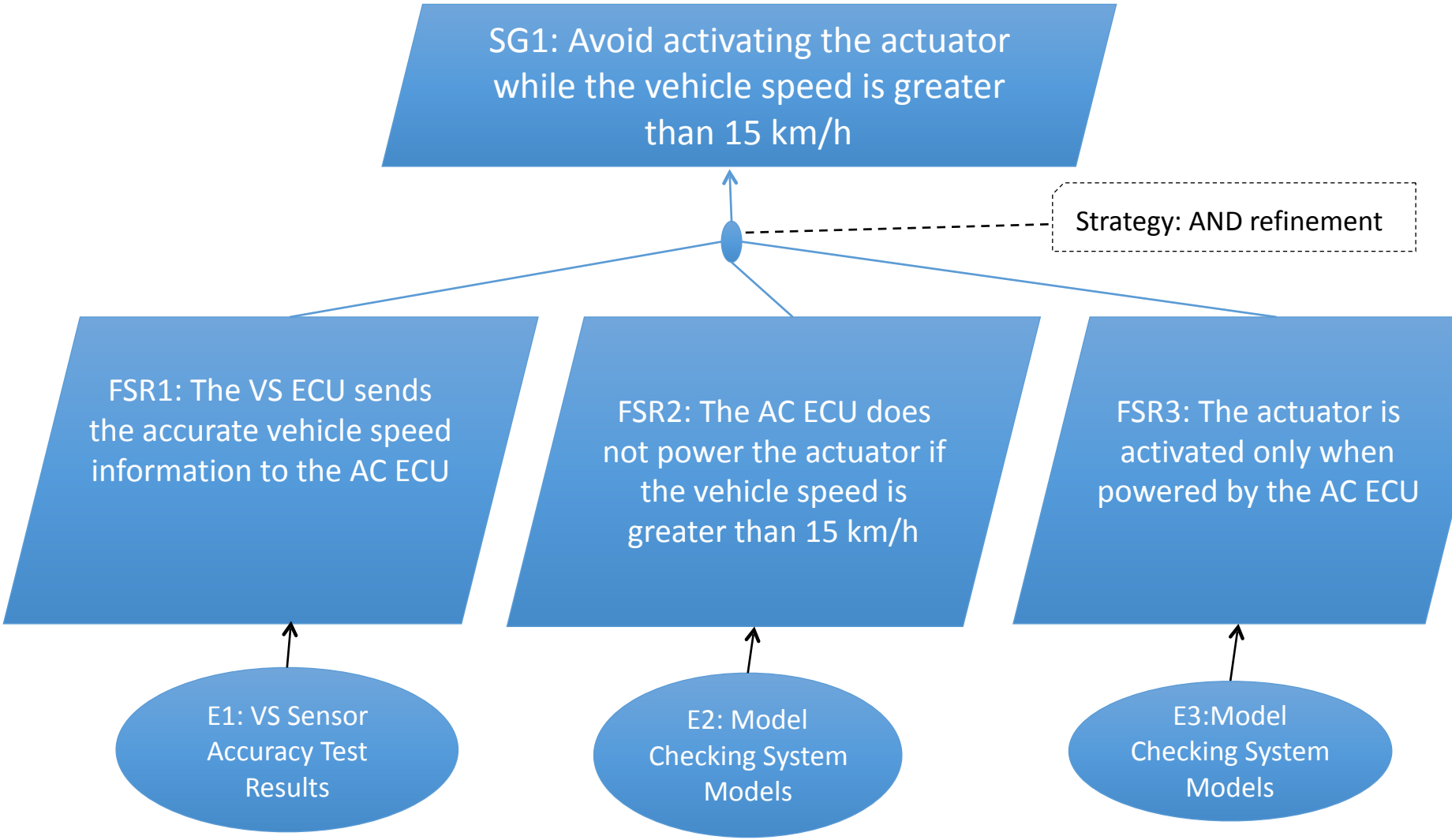
MMt algorithm for AC reuse due to System Evolution



“Partial” Assurance Case
(after impact assessment)



Evolved Assurance Case
(after completion by Assurance Engineer)



Model Management for Regulatory Compliance
Outline

- Introduction
- Getting started:
  - Modeling for Compliance
  - Model Management as a toolbox
- Adapting Model Management for Regulatory Compliance
  - Why adapt?
  - Example: Assurance Case Reuse due to System Evolution
  - Model Management for other compliance problems
- Next Steps

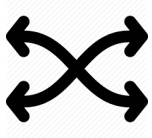
Model Management for other Compliance Problems

Model Management for other Compliance Problems

Compliance with multiple standards.

Model Management for other Compliance Problems

Compliance with multiple standards.



Model Management for other Compliance Problems

Compliance with multiple standards.

Model Management for other Compliance Problems

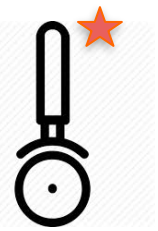
Compliance with multiple standards.

Standard or system slicing for partial compliance checking.

Model Management for other Compliance Problems

Compliance with multiple standards.

Standard or system slicing for partial compliance checking.



Model Management for other Compliance Problems

Compliance with multiple standards.

Lifting compliance assessment from products to product lines.

Standard or system slicing for partial compliance checking.

Model Management for other Compliance Problems

Compliance with multiple standards.

Lifting compliance assessment from products to product lines.

Standard or system slicing for partial compliance checking.

Model Management for other Compliance Problems

Compliance with multiple standards.

Lifting compliance assessment from products to product lines.

Standard or system slicing for partial compliance checking.

Identifying relationships between standards.

Model Management for other Compliance Problems

Compliance with multiple standards.

Lifting compliance assessment from products to product lines.

Standard or system slicing for partial compliance checking.

Identifying relationships between standards.

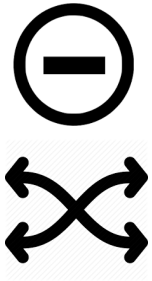
Model Management for other Compliance Problems

Compliance with multiple standards.

Lifting compliance assessment from products to product lines.

Standard or system slicing for partial compliance checking.

Identifying relationships between standards.



Next Steps

- Addressing the research questions outlined in the paper
  - Focus on demonstrating **reuse** and support for **multiplicities.**

- **MMINT*** + Compliance
  - Incorporate assurance case metamodel
  - Library of templates/patterns for assurance cases
  - Adapt MM operators to work with assurance cases
  - MM workflows for compliance problems

- Case study with industrial partner to assess cost savings.

**https://github.com/adisandro/MMINT/*

Summary

- Regulatory Compliance is a key challenge for many domains including automotive.
- Model management is a mature area that helps manage complexity of modeling artifacts.
- Identified some interesting compliance management scenarios.
- Showed how model management techniques could be *adapted* and used to address these scenarios.

Summary

- Regulatory Compliance is a key challenge for many domains including automotive.
- Model management is a mature area that helps manage complexity of modeling artifacts.
- Identified some interesting compliance management scenarios.
- Showed how model management techniques could be *adapted* and used to address these scenarios.

Thank You! Questions?

kokalys@mcmaster.ca

References

[Dardar'13] “Building a Safety Case in Compliance with ISO 26262 for Fuel Level Estimation and Display System “ Raghad Dardar. Master Thesis. M¨alardalen University, Sweden. 2013