SAFETY CASE IMPACT ASSESSMENT IN AUTOMOTIVE SOFTWARE SYSTEMS: AN IMPROVED MODEL-BASED APPROACH

SAHAR KOKALY, *MCMASTER UNIVERSITY*

RICK SALAY, UNIVERSITY OF TORONTO

MARSHA CHECHIK, *UNIVERSITY OF TORONTO*

MARK LAWFORD, *MCMASTER UNIVERSITY*

TOM MAIBAUM, *MCMASTER UNIVERSITY*

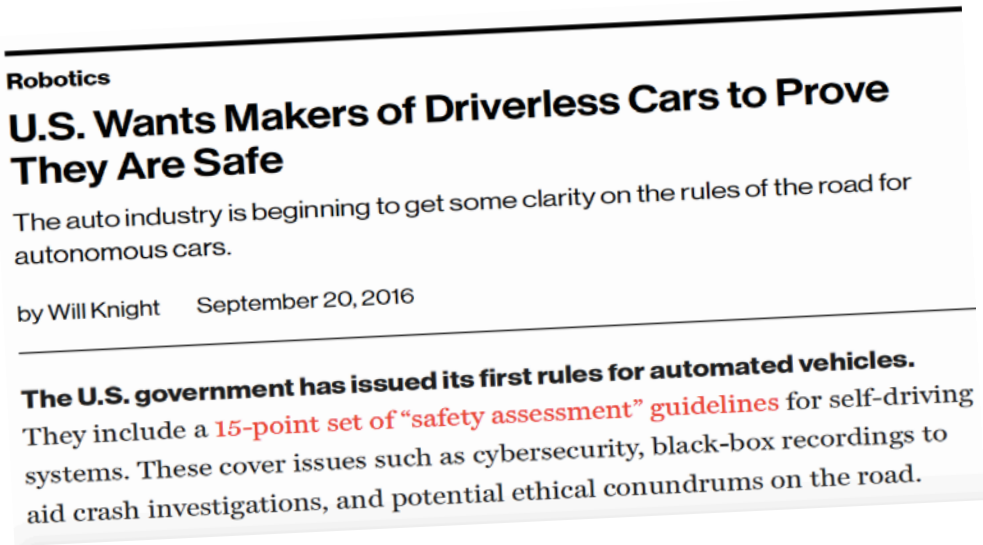
SAFECOMP'17

TRENTO, ITALY

SEP 12-15, 2017

CONTEXT

Pervasiveness of software has created special concerns regarding issues such as *safety*, *security* and *privacy*.



Robotics

U.S. Wants Makers of Driverless Cars to Prove They Are Safe

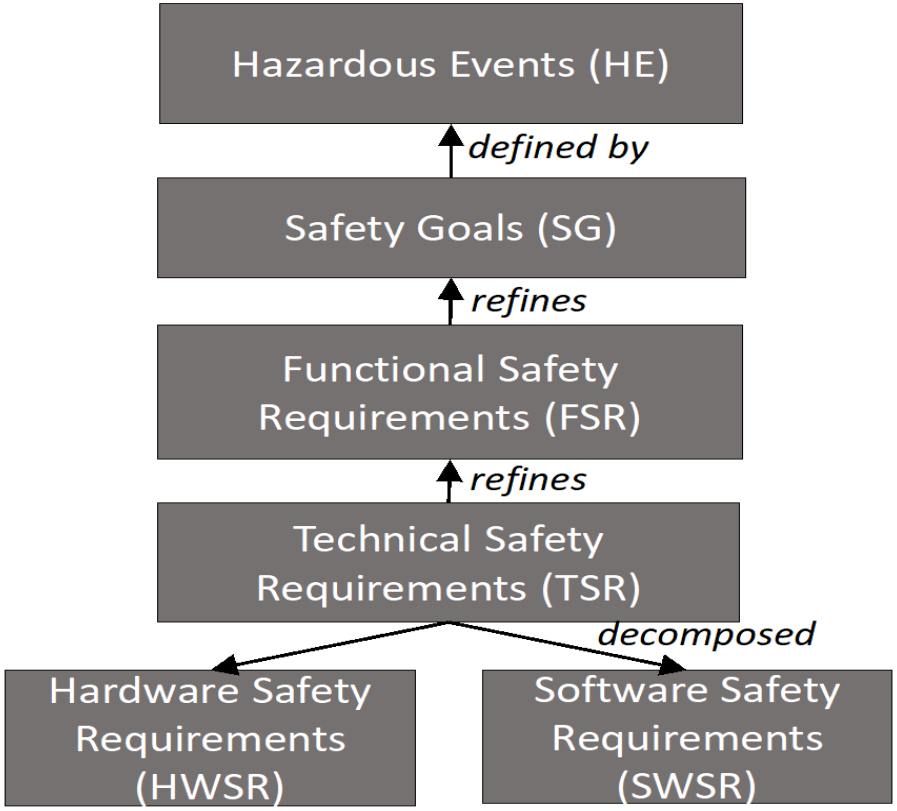
The auto industry is beginning to get some clarity on the rules of the road for autonomous cars.

by Will Knight September 20, 2016

The U.S. government has issued its first rules for automated vehicles. They include a 15-point set of "safety assessment" guidelines for self-driving systems. These cover issues such as cybersecurity, black-box recordings to aid crash investigations, and potential ethical conundrums on the road.

Regulations and standards, e.g., ISO 26262 (Functional Safety in Road Vehicles) to demonstrate compliance.

ISO 26262 RECOMMENDATION



SAFETY CASES

A *Safety Case* is an argument which demonstrates that each of the safety goals has been met, by eventually linking them to *evidence (solution)* in the system.

Evidence can come in many forms: e.g., test results, analyses, model checking results, expert opinion, etc.

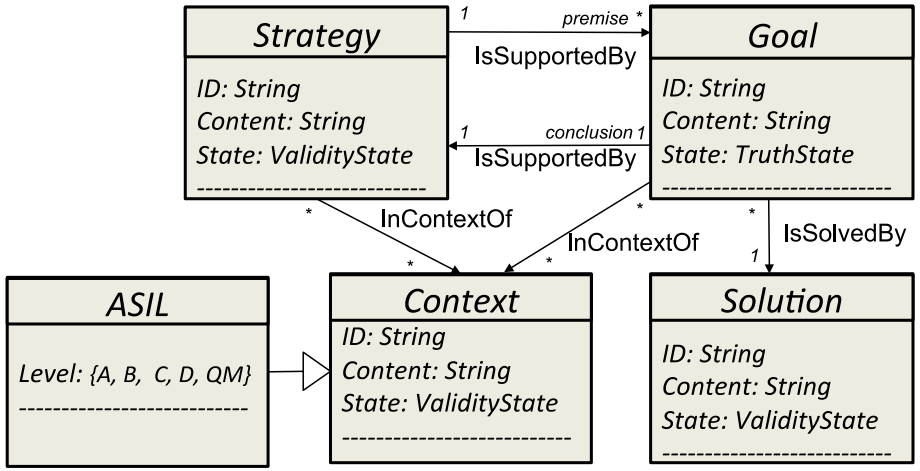
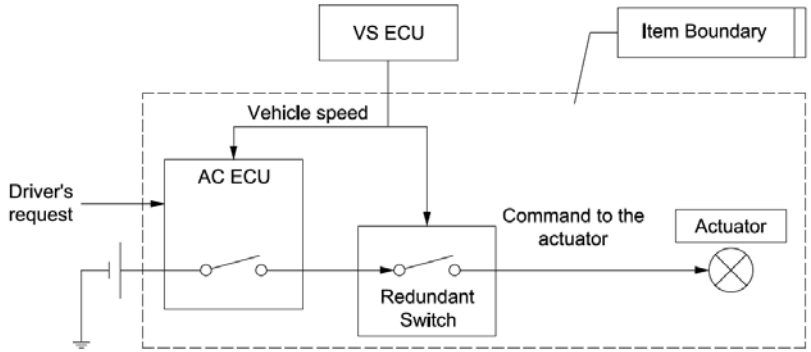
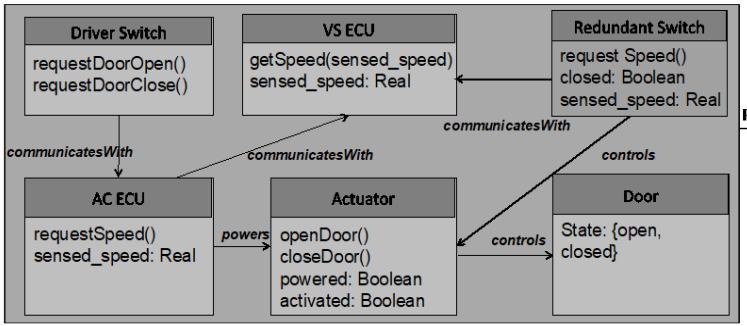


Figure: Goal Structured Notation (GSN) Metamodel

EXAMPLE: POWER SLIDING DOOR (PSD)

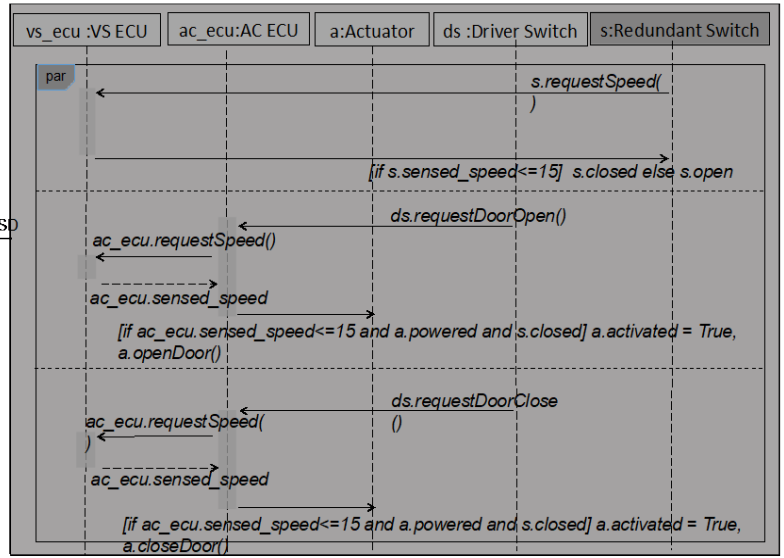


PSD: CD

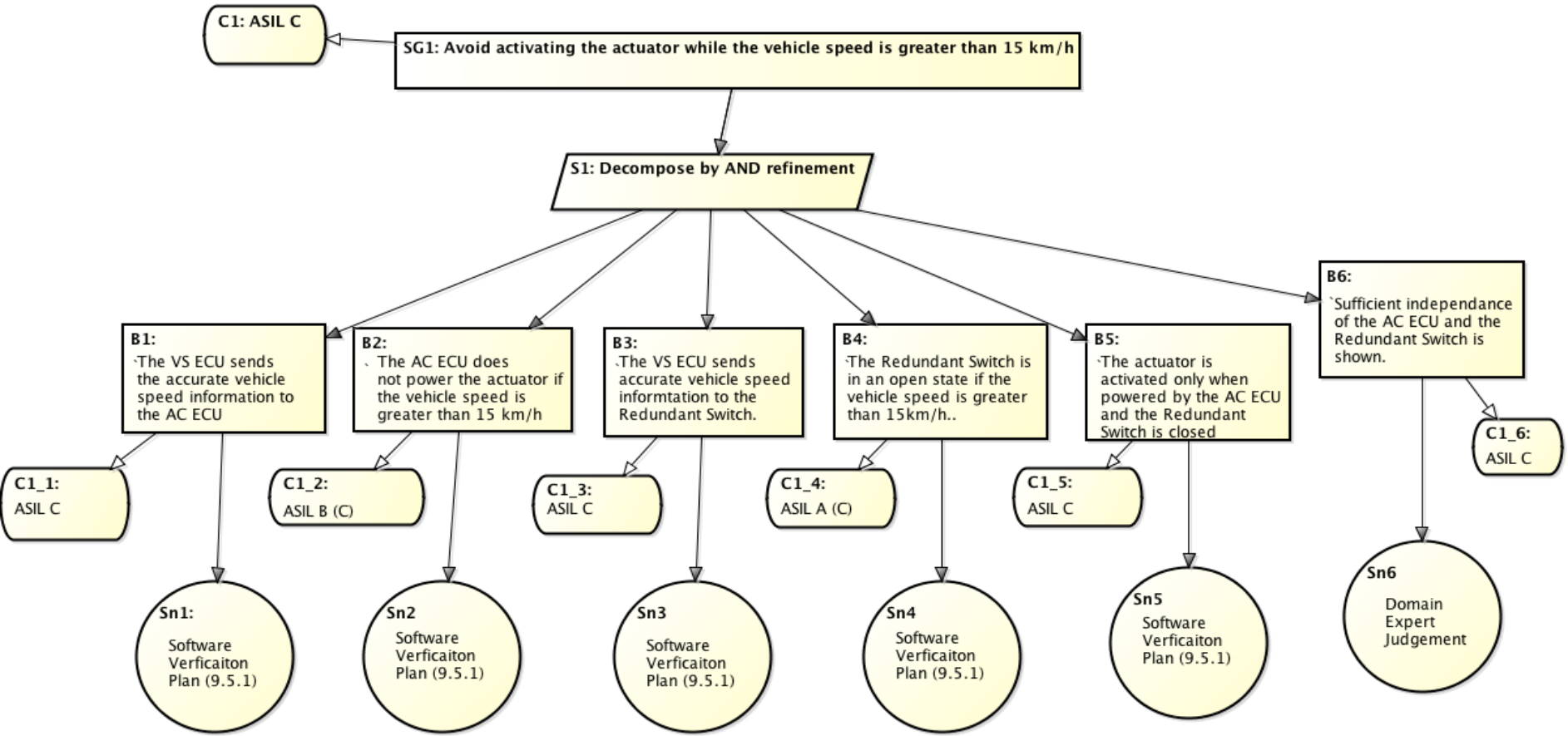


R: CD-SD

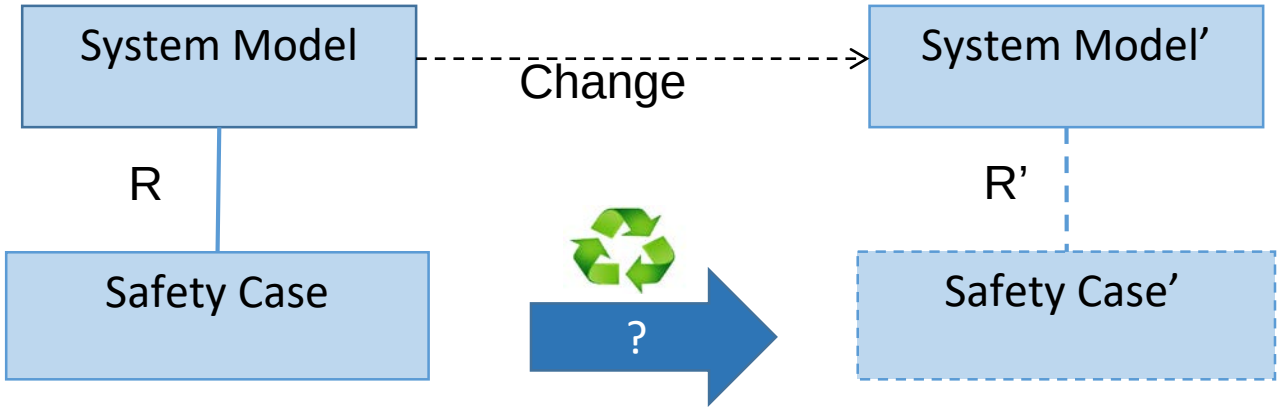
PSD: SD



PSD ORIGINAL SAFETY CASE



PROBLEM: SAFETY CASE AND SYSTEM CO-EVOLUTION



Problem: Can we aid the safety engineer in constructing a safety case for an evolved system by reusing the components of the original safety case as *much* and as *soundly* as possible, thus reducing the overall revision cost incurred?

Necessary step: Impact assessment to identify how changes in the system affect the safety case.

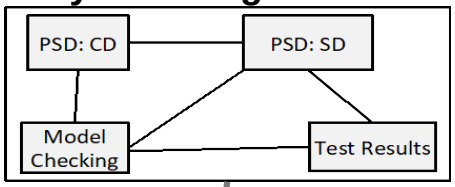
MAIN CONTRIBUTIONS

1. **Presented a model-based approach for impact assessment on GSN safety cases used with ISO 26262.**

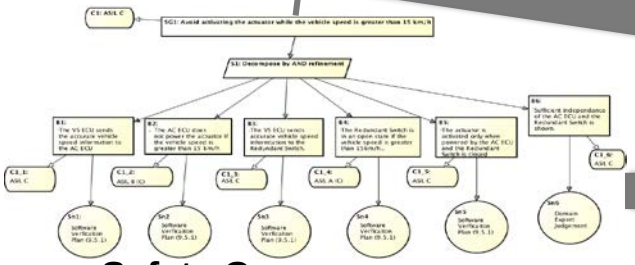
2. **Identified *six* techniques for improving the precision of the impact assessment approach.**

MODEL BASED SAFETY CASE IMPACT ASSESSMENT

System Megamodel



Traceability

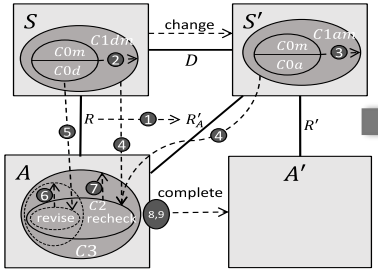


Safety Case

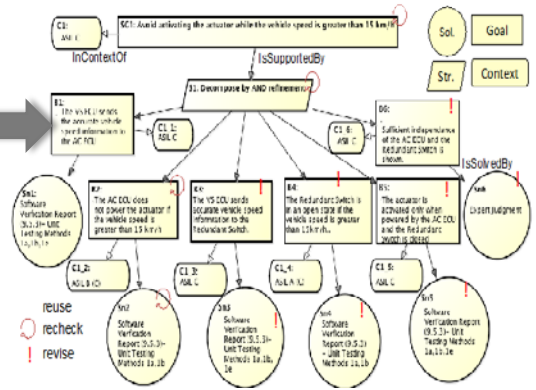
Delta (change)

Model Slicers

Model-Based Impact Assessment Algorithm

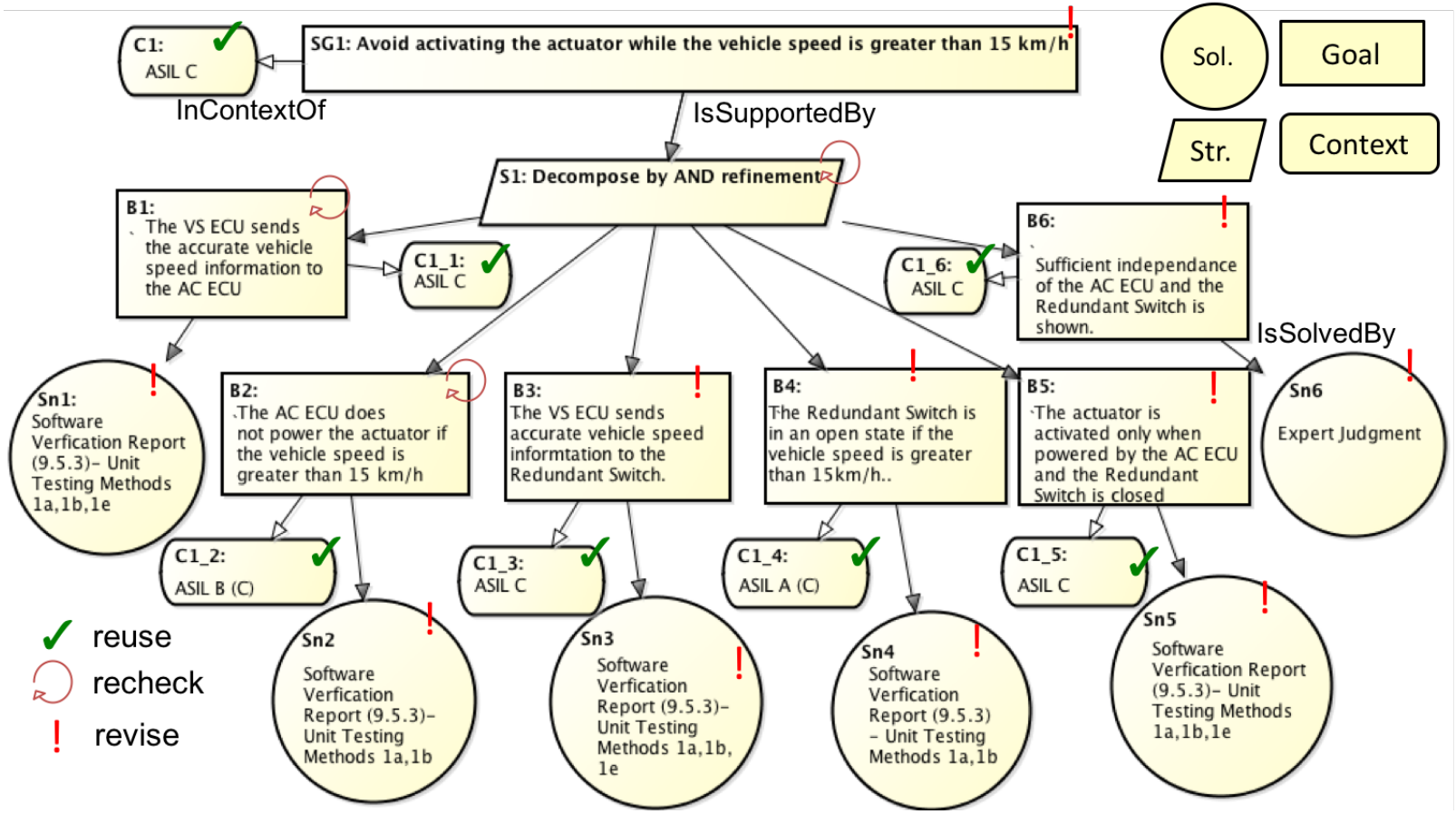


Annotated Safety Case



✓ reuse recheck ! revise

REMOVAL OF REDUNDANT SWITCH IN PSD – RESULTING ANNOTATED SAFETY CASE



IMPROVING THE PRECISION OF IMPACT ASSESSMENT

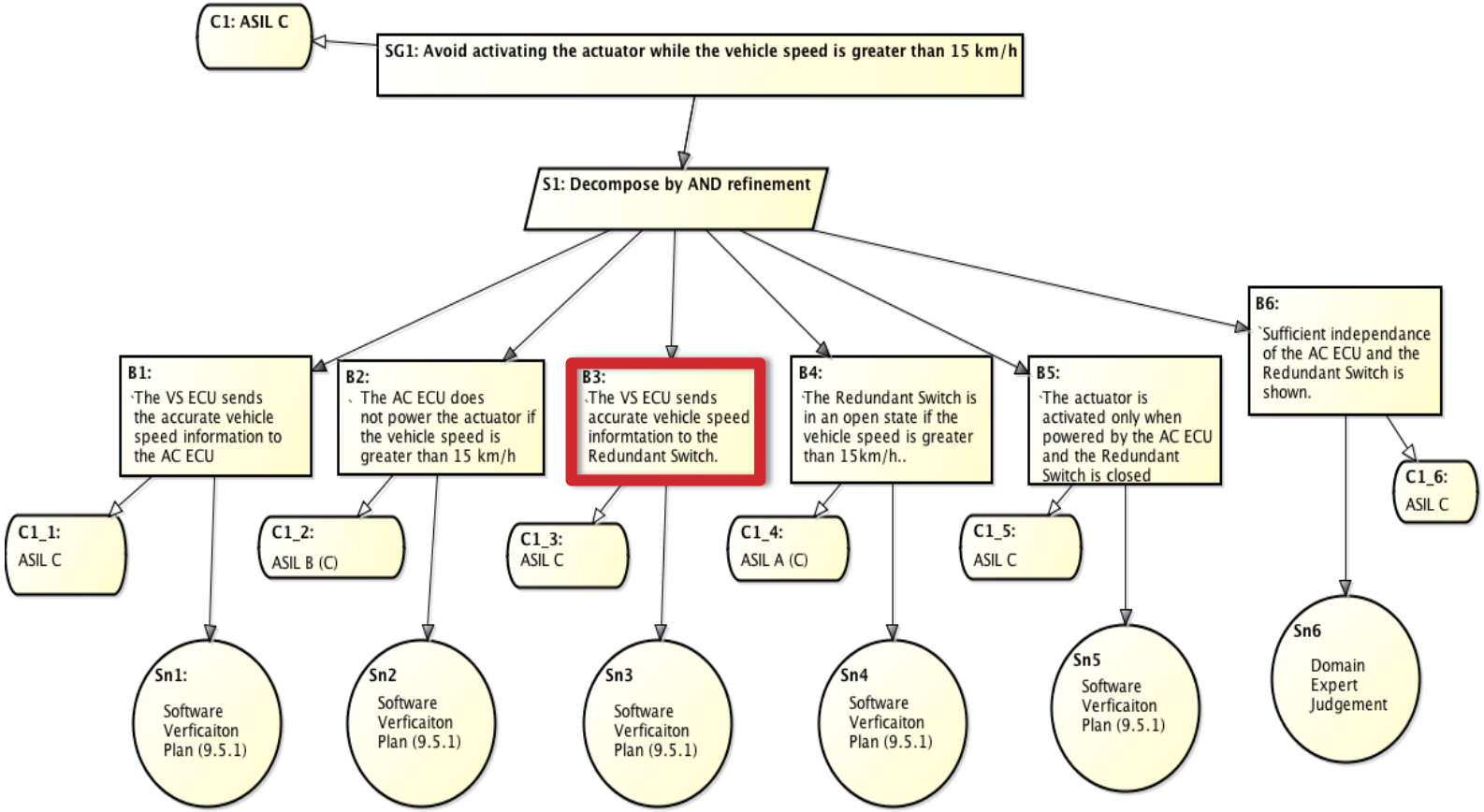
Identified six techniques:

1. Increasing the granularity of traceability between the system and the safety case.
2. Identifying sensitivity of safety case to system changes.
3. Understanding semantics of strategies
4. Decoupling revision from rechecking
5. Strengthened solutions do not impact associated goals
6. Understanding standard-system and standard-safety case traceability.

Outcome:

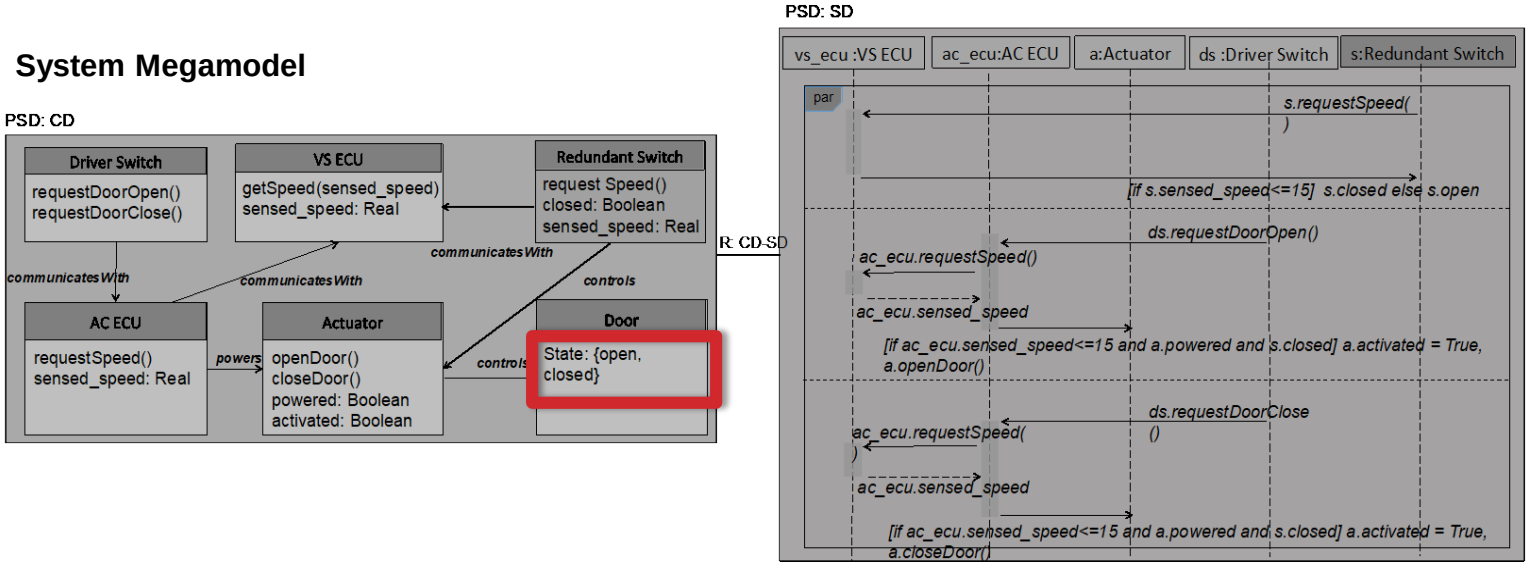
less “false positives” in “revise” and “recheck” annotations

1: INCREASING THE GRANULARITY OF TRACEABILITY BETWEEN THE SYSTEM AND THE SAFETY CASE



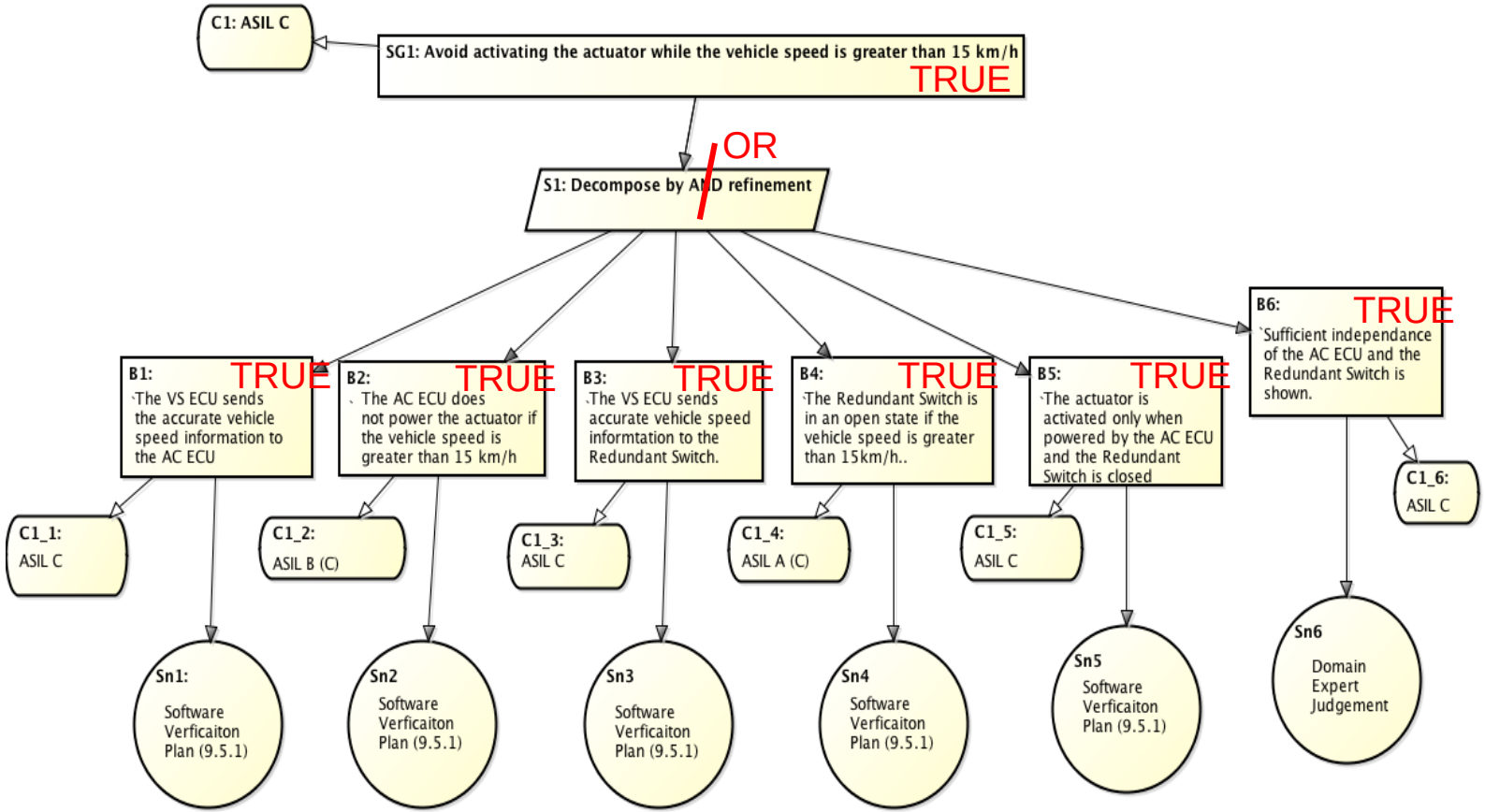
2: IDENTIFYING SENSITIVITY OF SAFETY CASE TO SYSTEM CHANGES

System Megamodel

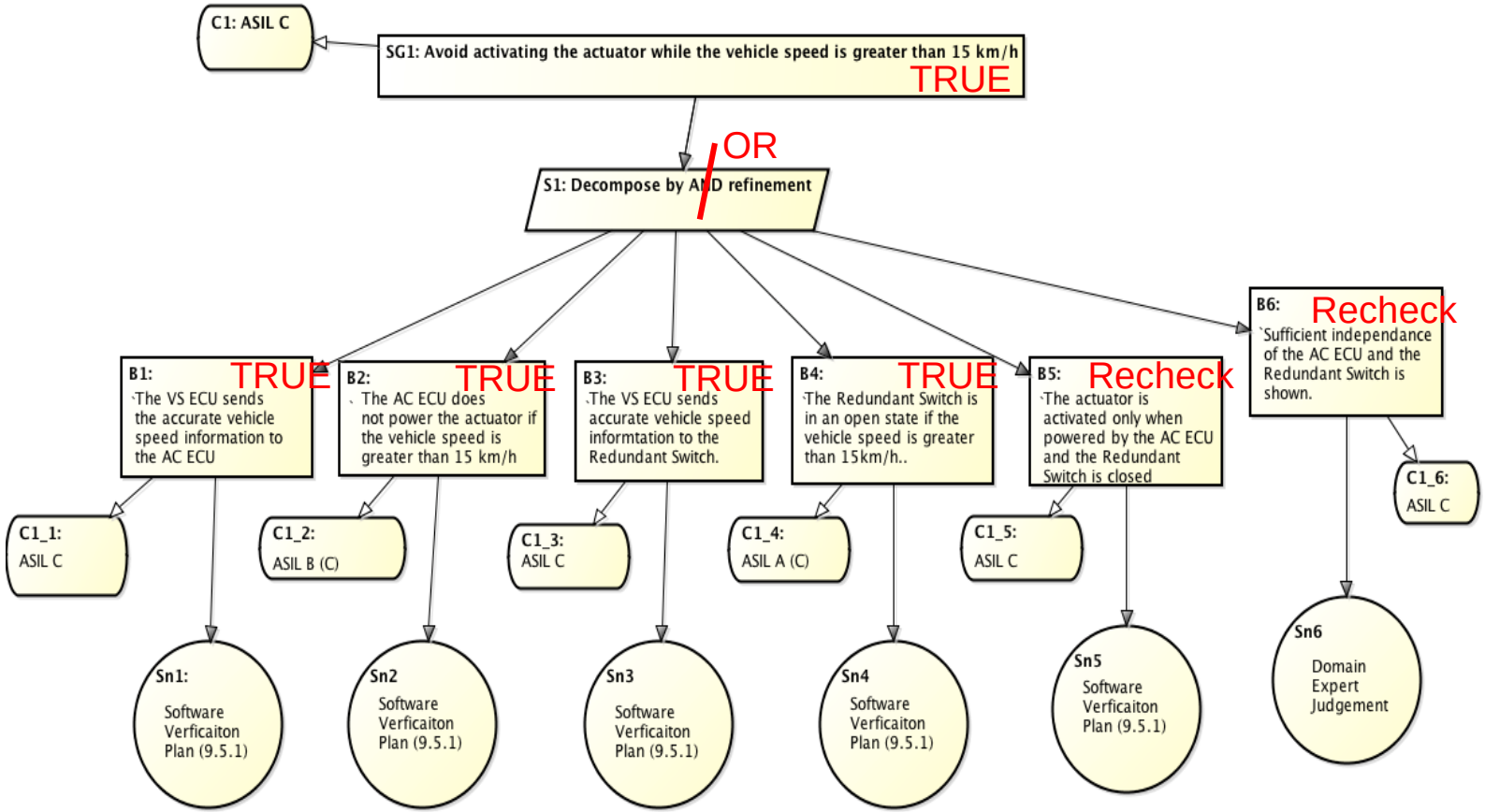


Consider the goal:
"If the **door state** is open and the speed is greater than 15km/h, the driver is notified."

3: UNDERSTANDING SEMANTICS OF STRATEGIES



3: UNDERSTANDING SEMANTICS OF STRATEGIES



4: DECOUPLING REVISION FROM RECHECKING

***Idea:* By knowing circumstances under which revising a goal will not impact its truth value, we require a recheck after a revision only when necessary.**

***Example*: changing the name of a system element (e.g., Redundant Switch is renamed to Extra Switch) will cause the goals referring to it to be marked for revision.**

- However, since changing the name does not impact the truth state of the goal, rechecking can be skipped.
- *Other examples:* capitalization of names, spelling corrections or language translations, such that the renaming is done consistently in both system and safety case.

5: STRENGTHENED SOLUTIONS DO NOT IMPACT ASSOCIATED GOALS

***Idea:* A change to a solution that strengthens it should not affect its support for associated goals.**

***Example*:**

- Assume that B1 was **"The VS ECU sends accurate vehicle speed information to the AC ECU *90% of the time*"** and that it was linked to a solution with test cases which showed accuracy 90% of the time.
- If the system changes so that the test cases can now demonstrate accuracy *100% of the time*, this does not affect goal B1 (meaning it should not be marked for rechecking).

6: UNDERSTANDING STANDARD-SYSTEM AND STANDARD-SAFETY CASE TRACEABILITY

ISO 26262 includes additional information about how ASILs (Automotive Software Integrity Levels), assigned to safety case goals, are related to ISO 26262 Work Products, which refer to system models used as evidence to support the safety case.

Methods		ASIL			
		A	B	C	D
1a	Requirements-based test[a]	++	++	++	++
1b	Interface test	++	++	++	++
1c	Fault injection test[b]	+	+	+	++
1d	Resource usage test[c]	+	+	+	++
1e	Back-to-back comparison test between model and code, if applicable[d]	+	+	++	++

Knowing (and using) this traceability could significantly enhance the impact assessment and produce more precise results.

RESULTS

Derived a formula which computes the cost incurred revising a safety case after a change in the system.

Demonstrated that cost is reduced with the improved impact assessment techniques.

TOOL SUPPORT

We are actively working on extending the model management framework MMINT* to include:

- safety cases as a model type
- model management operators for safety cases (e.g., safety case slice)
- explicit trace links between the safety case and the standard/system.
- Heterogeneous megamodeling operators (e.g., megamodel slice) as model management workflows.

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

FUTURE DIRECTIONS

- **Consider the use of approach in *design space exploration* to enable answering what-if questions about the impact of changes on safety cases.**
  - Constructing a “change assurance case”
- **Study the effect of changes, other than system changes, on the safety case and understand what types of *trace links* are required to support them.**
- **Consider changes involving the *addition* of elements.**
  - Do not currently handle this since we are unable to automatically “discover” links to the safety case.

SAFETY CASE IMPACT ASSESSMENT IN AUTOMOTIVE SOFTWARE SYSTEMS: AN IMPROVED MODEL-BASED APPROACH

SAHAR KOKALY, *MCMASTER UNIVERSITY*

RICK SALAY, UNIVERSITY OF TORONTO

MARSHA CHECHIK, *UNIVERSITY OF TORONTO*

MARK LAWFORD, *MCMASTER UNIVERSITY*

TOM MAIBAUM, *MCMASTER UNIVERSITY*

SAFECOMP'17

TRENTO, ITALY

SEP 12-15, 2017

QUESTIONS?