F2014-AST-086

DOMAIN ANALYSIS FOR STANDARDISED FUNCTIONAL SAFETY: A CASE STUDY ON DESIGN-TIME VERIFICATION OF AUTOMATIC EMERGENCY BRAKING

[1]Masood, Jawad[*]; [1]Philippsen, Roland; [1]Duracz, Jan; [1,2]Taha, Walid; [3]Eriksson, Henrik; [4]Grante, Christian
[1]Halmstad University, Sweden; [2]Rice University, USA; [3]SP Technical Research Institute, Sweden; [4]Volvo Group Trucks Technology, Sweden

KEYWORDS – Functional Safety, Testing, Engineering Methodology, Advanced Driver Assistance Systems, ISO 26262

ABSTRACT –

Simulation traditionally computes individual trajectories, which severely limits the assessment of overall system behaviour. To address this fundamental shortcoming, we rely on computing enclosures to determine bounds on system behaviour instead of individual traces. In the present case study, we investigate the enclosures of a generic Automatic Emergency Braking (AEB) system and demonstrate how this creates a direct link between requirement specification and standardized safety criteria as put forward by ISO 26262. The case study strongly supports that a methodology based on enclosures can provide a missing link across the engineering process, from design to compliance testing. This result is highly relevant for ongoing efforts to virtualize testing and create a unified tool-chain for the development of next generation Advanced Driver Assistance Systems.

TECHNICAL PAPER –

INTRODUCTION

Background

Recently, active safety systems have started to appear in production automobiles, and they will be a significant factor in eliminating road accidents with serious or fatal outcome. As opposed to passive safety systems such as seat belts and ABS, which protect mainly the occupants of vehicles, significant improvements for protecting vulnerable road users are most likely best achieved using active safety systems such as collision mitigation by automatic emergency braking. Currently, one of the major bottlenecks for widespread deployment of active safety systems is the challenge of validating and verifying them.

Given this context, the Swedish innovation agency Vinnova is funding a three-year project called NG-Test under their Strategic Vehicle Research Partnership (FFI Project #2011-01819). The project involves Volvo Group Trucks Technology, SP Technical Research Institute, Volvo Car Corporation, Autoliv, the Swedish National Road and Transport Research Institute VTI, as well as Chalmers and Halmstad Universities. In this paper, we focus on the intimate link between certification according to international safety standards and the use of model-based engineering at the early design stages of automotive safety functions. This work was done in close collaboration with our research on the link between robotics and Cyber-Physical Systems supported by US NSF Award #1136099, and research on a CPS modeling language

supported by the Swedish Knowledge Foundation through the CERES+ centre and under the Acumen+ project."

Research and Engineering Objectives

The viability of future Advanced Driver Assistance Systems (ADAS) will depend on the virtualization of tests and formal verification of system performance. Simulation traditionally computes individual trajectories, which limits the assessment of overall behaviour. We address this fundamental shortcoming using enclosures which allow computing bounds on system behaviour instead of individual traces. This refers to representing the state of a simulated system as a set of intervals which are guaranteed to contain the true state in spite of numerical inaccuracies or other uncertainties. Recent work allows us to compute enclosures for an important class of hybrid systems [9]. Major benefits are expected from leveraging these results for verification and validation of automotive systems, in particular by linking early stage engineering to empirically validated standards compliance.

Methodology

The formal computation of general bounds on hybrid system behaviour is a formidable challenge studied intensively by a large research community. To develop a methodology for virtualized testing based on enclosures, we propose a generic ADAS component model along with a set of component characteristics (measures of complexity) to guide the engineering process from initial sketches to more intricate models. This architecture aids with scoping particular system models in terms of completeness and complexity. Additionally, during early stage engineering, having a clear generic system architecture supports the task of establishing a series of increasingly complex models to streamline the process.

The case study detailed in Sec. AEBS Use Cases investigates the enclosures of a generic Automatic Emergency Braking System (AEBS) and demonstrates how this creates a direct link between requirement specification and standardized safety criteria as put forward by ISO 26262.

The concrete models we develop (see Sec. Use Cases) are implemented in Acumen, a small domain-specific language for modelling of Cyber-Physical Systems [1, 11, 12] that supports enclosures. We illustrate the significance of the work with the example of determining rear-end collision severity according to Automotive Safety Integration levels (ASIL).

Contributions

To our knowledge, the enclosure-based approach to guide risk analysis according to ISO 26262 is novel. Acumen enclosures have been used to study other types of cyber-physical systems, but the automotive domain has not been addressed before.

ACUMEN ENCLOSURES

Models of Hybrid Systems

Intuitively, a hybrid system model expresses an abstract view of a system exhibiting continuous as well as discrete dynamics. An Acumen model of a hybrid system specifies:
- The initial state of the system

- A set of differential equations describing the possible ways of evolving in time
- Switching conditions that determine the dynamics of the system at a given point in time

Such a specification describes the evolution of a hybrid system as a trace that is the piece-wise solution of a set of differential equations. In other words, the system trace is a function of time that at each instance gives the system state as a set of values satisfying some differential equation.

Traces for Acumen models can be approximated by simulation using numerical schemes similar to those found in traditional simulation tools, but also by enclosures for the system that come with so-called soundness guarantees. Soundness guarantees state that an enclosure produced for a system gives, at each point in time, a set of intervals that contain the true system state.

Enclosures with Soundness Guarantees

To produce enclosures with soundness guarantees the Acumen enclosure simulator computes:
- Solutions to differential equations that come with soundness guarantees
- Mathematically correct valuations of switching conditions

Sound solutions to differential equations are simply enclosures that contain the true solution to the differential equation. In the case when the initial conditions are intervals, the enclosure is required to contain all solutions starting from any point within the intervals. For a theoretical treatment of the approach on which the implementation is based we refer to [6, 7].

To judge with certainty whether a switching condition may be true, Acumen employs techniques pioneered by the constraint satisfaction community based on interval arithmetic [3]. In essence, relations between the variables that occur in a switching condition are used to obtain a set of intervals that contain all true states for which the condition is true. When one of these intervals is empty there is no state for which the condition holds, and therefore the corresponding switch in dynamics cannot occur.

It is not possible in general to produce infinitely precise enclosures for arbitrary models. Approximation of the true state of the system leads to over-approximation in the valuation algorithm for switching conditions. Thus, more states than the true one are taken into account when determining the possible switching conditions. Consequently, multiple dynamics may simultaneously be judged possible. In such cases all possible evolutions are taken into account and included in the reported enclosure for the system, to guarantee that simulations are sound.

SAFETY STANDARDISATION

The lifecycle of ISO 26262 [8] consists of three main phases: Concept, Product development, and After SOP. The Hazard analysis and risk assessment (HARA) activity is part of the Concept phase. It is based on the Item definition, which specifies the item and its expected behaviour and interaction with other items and the environment. Additionally, elements of the item are described as well as functionality required by/from other items, elements or the environment.

An elucidative item definition in an AEBS example could be:
- Measures headway using a sensor(s)

- Control unit (ECU) determines braking based on: ego speed, target speed, and headway
- Decelerates using the conventional service brake system (includes brake lights)
- Requires vehicle speed from ABS (anti-lock braking system) system
- Provides headway to ACC (adaptive cruise control) system
- Sensor performance is allowed to be affected by weather and lighting conditions
- The functionality shall be disabled when the vehicle is reversing

A hazardous event is formed by combining a hazard due to a malfunctioning item with an operational situation. An operational situation is defined by the driving conditions, such as: country road driving at 70 km/h in a curve during night time and rain. The risk of the hazardous event is classified by three properties: severity, exposure, and controllability. Severity concerns the level of injury that might happen: ranging from bruises to fatalities. Exposure expresses the probability of a specific situation, e.g. highway driving is more probable than driving on snow. The level to which the driver or surrounding actors can mitigate the hazardous event is defined by the controllability parameter.

A hazard is usually related to some source of energy, either potential or kinetic. In the AEBS case the hazard comes from the movement of the own vehicle or neighbouring ones. A typical malfunctioning behaviour of the AEBS item is commission or omission of service brakes and/or brake lights. Commission means that the system outputs (brakes or lights) are activated when they should not be, whereas omission means that the system outputs are not activated although they should. At this level, it is not important whether it is the sensor(s), ECU, bus system, or actuators that are malfunctioning. Omission failures pose large risks at higher speeds with vehicles in front, whereas commission failures pose high risks at higher speeds with vehicles in rear. By attributing different operational situations to these failures, classifying their risks according to severity, exposure, and controllability, the result becomes a number of safety goals and their safety integrity levels.

If the availability of the system is simultaneously considered, a high safety integrity level does in most cases imply a large cost. The cost stems from more reliable and possibly redundant components as well as a more rigorous development process. Since sound early decisions reduce cost for later reiterations and redesigns, it is important to have tool support already during the concept phase. This allows simulating the risk consequences of the design decisions as early as possible.

AEBS CASE STUDY

This section presents the studied Automatic Emergency Braking System (AEBS) in terms of functional requirements, use cases, the Acumen models that implements those parts of the system which are relevant for determining severity levels according to ISO 26262, and simulation results that highlight the power of our enclosure method.

The main goal of the AEBS is to avert, or minimize the effects, of potential collisions. We have modelled functional requirements in a state-flow diagram, as proposed by [5]. A full description is beyond the scope of this paper, the relevant aspects are summarized as follows.

AEBS is enabled, if the driver chooses so, when vehicle speed exceeds some threshold (e.g. 30 km/h). When enabled, a sensor-based algorithm continuously estimates the critical time to collision (TTC) for example using data from cameras, lidar, radar, or some combination thereof. Road conditions (i.e. current coefficient of friction) may also be taken into account.

Depending on the TTC, the AEBS will warn the driver of the danger, and ultimately intervene with an emergency braking manoeuvre at maximum available deceleration (unless overridden by driver intervention e.g. on the brake pedals). Figure 1(A) illustrates this with some concrete numerical values for different warning and intervention thresholds.

As explained in the figure caption, the Acumen models directly use the distance between subject and target vehicle to keep the expressions as simple and direct as possible. As we are interested in the kinds of formal guarantees that can be achieved with respect to severity levels, what matters is the range of relative velocities between subject and target at the moment of impact, as well as the relative mass of the vehicles. The relative velocity does not directly depend on whether we trigger AEBS based on TTC or distance, given that the trigger thresholds are open to discussion and can be adapted as needed.

Notice that a full ISO 26262 Item definition, as outlined in Section 3, can be derived from a description such as the one above with relative ease [10, 4]. Furthermore, regulations such as [2] govern AEBS performance in detail. For example, the specific numerical values for the severity level thresholds in Table 1(A) are inspired by such regulation.

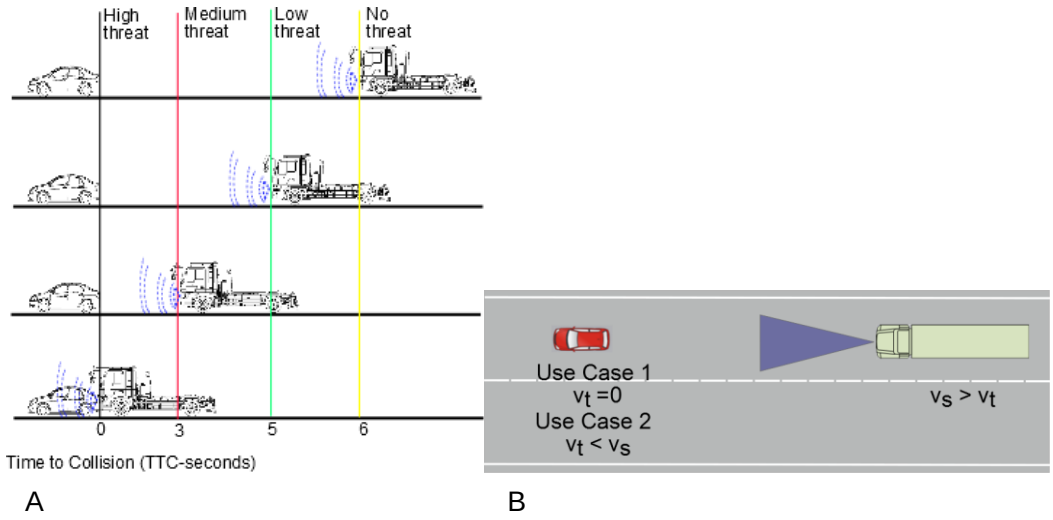


Figure 1: (A) Example threat levels for AEBS based on sensor-based time to collision estimates. Suggested severity level definitions are inspired by [2]; (B) Use cases for AEBS functional testing.

Use Cases

The case study focuses on the model-driven virtual verification of the initial conditions under which an AEBS such as described above conforms to specific standard severity classes. This is illustrated in Figure 1(B). In order to keep the computational burden as low as possible, the simulations start at the moment where the emergency braking intervention has been triggered. To simplify setup as well as the interpretation of results, we assume without loss of generality that the vehicle starts at position 0 with some initial speed and decelerates at a constant rate until standstill. We then determine if it would collide, as well as at what distance and with what speed this would occur. This is based on the assumption that the other vehicle, termed the target in this paper, is initially at some given distance in front.

Notice that all the initial conditions can be affected by uncertainty represented as intervals, as opposed to exact values. Acumen enclosures simulate the bounds of all system traces arising from any combination and evolution of individual values within their bounds.

To illustrate the tremendous gain in soundness provided by enclosures, consider Figure 2, which shows 6 traditional simulation runs undertaken in a naive effort to assess AEBS behaviour under uncertainty in initial velocity or deceleration. The top row shows the position over time, and the bottom row the velocity. On the left, the initial velocities are the same but three different deceleration levels are used to explore the range of system behaviour. On the right, it is the initial velocity that is sampled from the range of possible values while the deceleration is always the same. This example neglects the combination of different values for velocity and deceleration (this would require 9 runs). Consider that for every parameter or variable that is uncertain, we would need to multiply the number of runs by the number of samples taken for that particular parameter. This would result in an exponential growth of the number of required simulations. And that would still not be sufficient, because the deceleration level might fluctuate over time. Thus, uncertainties cannot be tractably handled by traditional simulation.

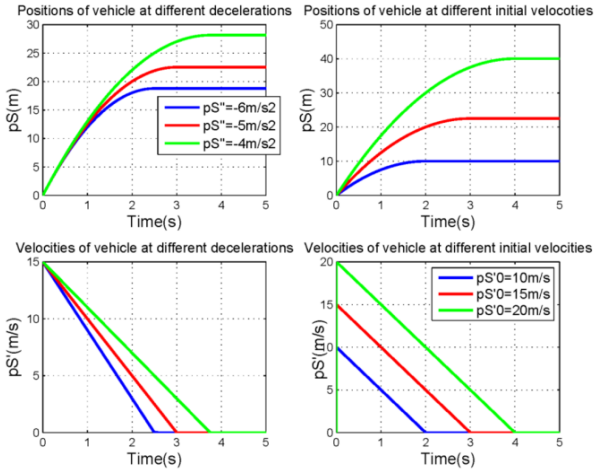


Figure 2: Instead of individual simulation traces to cover ranges of possible system behavior, enclosures allow us to automatically compute the upper and lower bound of any possible combination of the individual traces.

Our enclosure-based simulation method eliminates the exponentially growth in the number of runs. A single simulation captures all the bounds. However, determining sound enclosures at each simulation step incurs a high computational burden, so this benefit is currently tractable only for relatively small system models. For this reason as well as for the sake of keeping the presentation manageable in this paper, the number of interval-valued conditions is limited to three. We consider two variations of this case: the target may be at standstill, or it may be moving at constant velocity. For the sake of explaining the methodology, we focus first on impact velocity in the stationary case. Then we consider the change of velocity due to inelastic shock, which is of particular relevance for collisions between trucks and passenger vehicles. The use cases, along with concrete numerical values for the mentioned initial conditions, are summarized in Table 1(B).

$\mathbf{S_0}$	$\boldsymbol{\Delta v < 5km/h = 1.39m/s}$
$\mathbf{S_1}$	$5km/h \leq \Delta v < 10km/h = 2.78m/s$
$\mathbf{S_2}$	$10km/h \leq \Delta v < 20km/h = 5.56m/s$
$\mathbf{S_3}$	$20km/h \leq \Delta v < 40km/h = 2.78m/s$
$\mathbf{S_4}$	$\Delta v > 40km/h = 2.78m/s$

A

Subject Vehicle: mass 10,000 kg		
Case	Speed	Acceleration
1	$22.5 \pm 2.5 m/s$	$-4.5 \pm 0.5 m/s^2$
2	$25 \pm 1 m/s$	$-4.5 \pm 0.5 m/s^2$
Target Vehicle: mass 2,000 kg		
Case	Position	Speed
1	$\{10 \pm 0.5, 41 \pm 1\} m$	0
2	$35 m$	-2,2±0.2m/s

B

Table1: (A) Suggested severity level definitions, inspired by [2]; (B) Initial conditions for the two used cases

Acumen Models and Simulations

The mathematical models used in this study represent the vehicles as point mass traveling along a straight road. As mentioned, we assume braking to start at time $t = 0$ and to continue until standstill. This is capture in the following (semi-formal) hybrid system model:

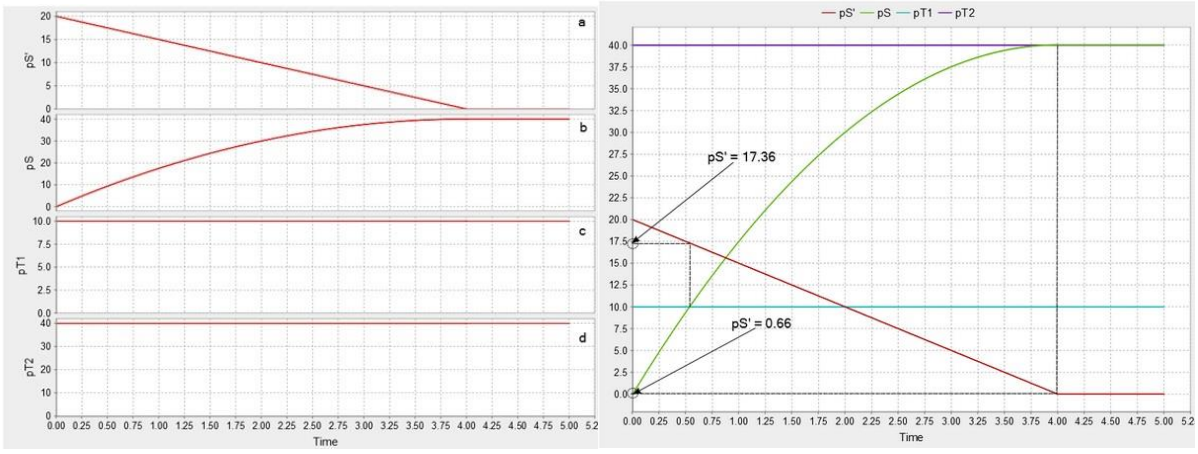
$$\ddot{p}_S = \begin{cases} a_S, & \Leftarrow m = \textbf{\textit{Braking}} \\ 0, & Otherwise \end{cases}$$
$$when \;\; \dot{p}_S = 0 \;\; then \;\; m \leftarrow \textbf{\textit{Stopped}}$$
$$\dot{p}_T = v_T$$

Where $\dot{p}_S$ is the position of the subject vehicle (initialized to zero), $\dot{p}_T$ is the position of the target vehicle (initialized according to the use case), a_S is the acceleration parameter of the subject vehicle according to the use case, m is a mode variable which is initialized to Braking, and v_T is the velocity parameter of the target vehicle. Notice that $\dot{p}_S$ is initialized according to the use case, and that all use cases have a positive $\dot{p}_S$ and a negative a_S such that the system as guaranteed to come to standstill.

To illustrate the methodology, we begin by presenting a simulation trace without enclosures of the above system with a stationary target vehicle. This is followed by the enclosures induced by the interval-valued first use case, in order to introduce the method for determining the enclosure of resulting potential collision velocities. Then we introduce the vehicle masses to determine the bounds on the change of velocity due to impact, assuming inelastic collision. Finally, we run the enclosure simulation on the second use case, and hint at the more complete system model employed for that use case.

Design-time verification without enclosures

Figure 3(A) shows the AEBS simulation with exact values. We use the lower bounds on the first use case's initial conditions for this example. Before simulation starts, the subject vehicle moves with constant speed ($\dot{p}_S = 20m/s$ in this case), and at $t = 0$ a constant braking force is applied (in this example $\ddot{p}_S = a_S = -5m/s^2$). Notice that $\dot{p}_S$ becomes zero at $t = 4s$, and that the subject vehicle comes to standstill at $\dot{p}_S \approx 40m$. The target vehicle is at standstill throughout.



A B

Figure 3: (A) Simulation trace produced by Acumen with exact (non-enclosure) values; (B) Merged plots of the subject position and velocity as well as two target positions (horizontal lines).

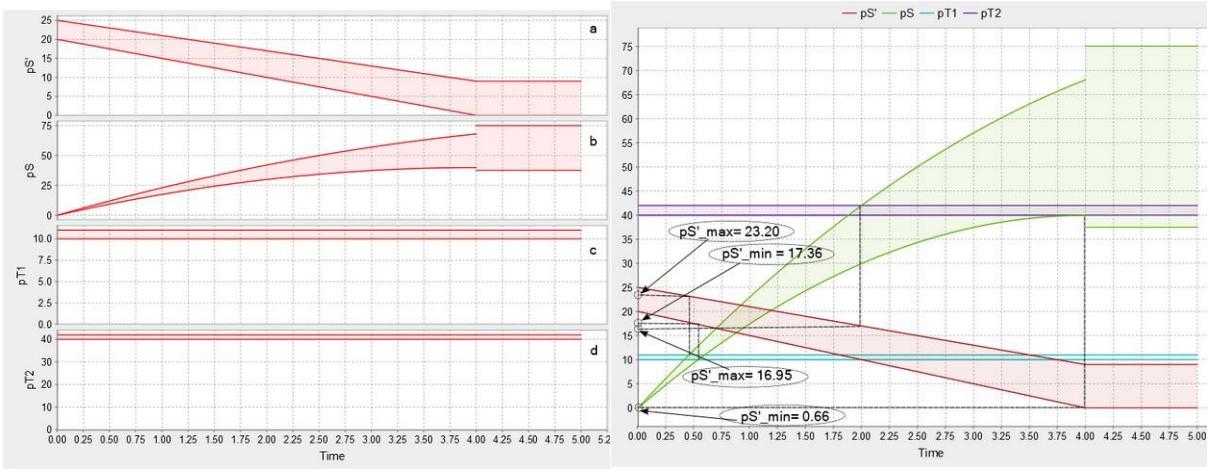
Figure 3(B) merges the relevant graphs and overlays two target vehicle positions given by the first use case: $\dot{p}_{T1} = 10m$ and $\dot{p}_{T2} = 40m$. Intersecting these horizontal position lines with the trace of the subject vehicle position allows to determine that $\dot{p}_{T1}$ is encountered by the subject when it is moving with $\dot{p}_S = 17.36m/s$. Similarly, it encounters $\dot{p}_{T2}$ with $\dot{p}_S = 0.66m/s$. These impact velocities are an important parameter during design-time verification of the active safety function. However, the change of velocity due to impact is more pertinent for describing the accident severity class. It can be estimated using the well-known equations for inelastic shock based on the vehicle masses M_S and M_T combined with the velocities $\dot{p}_S$ and $\dot{p}_T$ at the instant before impact:

$$\Delta\dot{p}_S = \frac{M_T(\dot{p}_T - \dot{p}_S)}{M_T + M_S}, \Delta\dot{p}_T = \frac{M_S(\dot{p}_S - \dot{p}_T)}{M_T + M_S}$$

With the masses given in Table 1(B) and the velocities determined by simulation, it is straightforward to arrive at the following numerical values in this example. Note that $\dot{p}_T = 0$ in this use case. $p_{T1} = 10m$ leads to $\Delta\dot{p}_{s1} = -2.89m/s$ and $\Delta\dot{p}_{T1} = 14.47m/s$, whereas $p_{T2} = 40m$ leads to $\Delta\dot{p}_{s2} = -0.11$ and $\Delta\dot{p}_{T2} = 0.55m/s$. Comparison with the Δv for the different severity classes indicates that with an initial distance of $10m$, the severity class would be s_2 for the subject and s_4 for the target. For an initial distance of $40m$ it would be s_0 for both.

Design-time verification with enclosures

Figure 4(A) and 4(B) repeat the above procedure, but this time on simulation traces produced with Acumen's enclosure semantics. The velocities immediately before potential impact are now intervals instead of exact values. We take advantage of the fact that the given system exhibits monotonic behaviour in the domain of interest. It is thus sufficient to consider only the upper bound of velocity at the lower bound of collision time, and the lower bound on velocity at the upper bound of collision time.

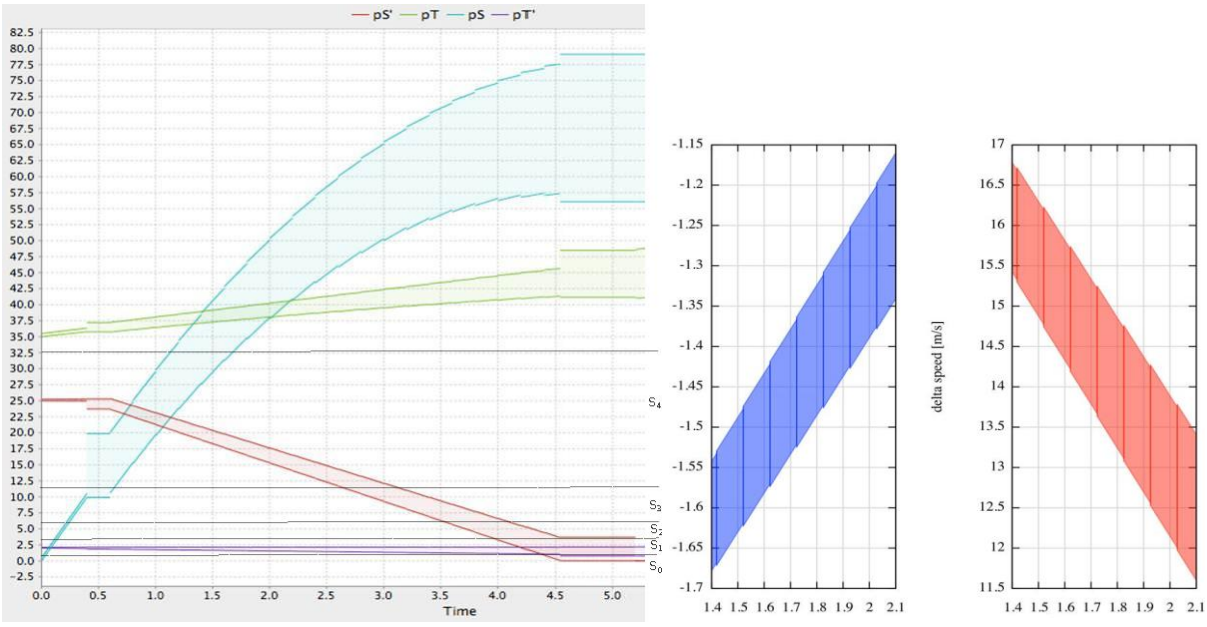


A B

Figure 4: (A) Re-running the simulation shown in Figure 3(A) with enclosures, enables the automatic computation of the bounds of system behaviour; (B) Similarly to the method employed in Figure 3(B), we can determine the velocities at impact.

Thus, the subject vehicle reaches the target vehicle 1 (initially at $10m$ distance) with a collision velocity in the range of $\dot{p}_s \in [17.36,23.2]m/s$; and target vehicle 2 (initially at $40m$) with $\dot{p}_s \in [0.0,0.66]m/s$. Using the inelastic shock equations, this can again be converted into Δv values for the subject and target. Severity levels can then be determined.

We emphasize that the severity levels computed with enclosures thus also become interval-valued. In particular, if a given use case yields certain severity levels, then we have a formal guarantee that those levels bound any combination of the uncertainties explicitly fed into the model via interval valued parameters. For example, this makes it possible to compare two sensor setups with differing noise characteristics in terms of their impact on the severity levels that can be guaranteed. A less precise sensor may be cheaper, but its greater uncertainty on the measured distance may lead to the AEBS being triggered too late to reach the targeted severity level. A counter-measure could be to reduce the distance threshold of course, in which case the likelihood of unnecessary intervention grows. This trade-off can be better understood with the help of the employed enclosure method. To streamline the process of determining enclosures for $\Delta\dot{p}_s$ and $\Delta\dot{p}_T$, we have developed a combination of a more complete Acumen model and a plot script to analyze the resulting simulation traces. This is illustrated in Figure 5(A) and 5(B). The principle again is the same: find the earliest and latest possible moment of collision and determine the corresponding upper and lower bounds for the subject and target vehicles. However, in this case we directly convert the resulting $(\dot{p}_s; \dot{p}_T)$ into $\Delta\dot{p}_s; \Delta\dot{p}_T$using the vehicle masses. Notice that this Acumen model supports three modes for the subject vehicle (coasting, braking, and stopped) as well as two modes for the target vehicle (coasting and stopped). For the sake of brevity, the details of this model are not included here.



A B

Figure 5: (A) Enclosure value plots for moving target; (B) Enclosure plots of $\Delta\dot{p}_S$ and $\Delta\dot{p}_T$, which can be directly mapped to severity levels.

CONCLUSION

We discuss our generic ADAS component model and a set of complexity measures that can easily be extracted from hybrid system models thereof. We describe how the hybrid systems modelling approach fits the engineering process using an AEBS as concrete example. We sketch its implementation in Acumen, a domain-specific modelling language for cyber-physical systems with direct support for enclosures. A set of concrete simulations round off the study by showing the use of Acumen for severity level analysis according to ISO 26262. The computation of hybrid system enclosures is generally intractable, and this remains an unresolved challenge. The studied AEBS models thus had to be kept fairly simple. Note,

however, that the proposed methodology is intended as a guidance for risk analysis during early stage engineering. At this stage, relatively simple models are meaningful, and our work clearly demonstrates the relevance of enclosure-based methods in simulation. In particular, appropriately chosen enclosures will produce over-approximations of system behaviour. This means that simulation traces which remain within bounds specified by a given criterion can provide a strong formal guarantee that the same criterion is fulfilled by the modelled system. Simple models are thus a very effective tool for early stage decision making.

Our case study thus strongly supports that a methodology based on enclosures can provide a missing link across the engineering process, from design to compliance testing. This result is highly relevant for ongoing efforts to virtualize testing and create a unified tool-chain for the development of next generation Advanced Driver Assistance Systems.

REFERENCES

[1] Acumen web-site. www.acumen-language.org.
[2] Commission Regulation (EU) No 347/2012 as of 16 April 2012 implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council with respect to type-approval requirements for certain categories of motor vehicles with regard to advanced emergency braking systems. Official Journal of the European Union 21.4.2012.
[3] Frederic Benhamou, Frederic Goualard, Laurent Granvilliers, Jean-Francois Puget. Revising hull and box consistency. International conference on logic programming. MIT press 1999: 230-244.
[4] Torsten Dittel, Hans-Jörg Aryus. How to "survive" a safety case according to ISO 26262. Computer Safety, Reliability, and Security. Springer, 2010: 97-111.
[5] Alma L Juarez Dominguez. Detection of Feature Interactions in Automotive Active Safety Features. PhD thesis, University of Waterloo, 2012.
[6] Abbas Edalat, Dirk Pattinson. A domain theoretic account of Picard's theorem. Proceedings of ICALP 2004, 3142 (Lecture Notes in Computer Science):494-505.
[7] Amin Farjudian, Michal Konecny. Time complexity and convergence analysis of domain theoretic Picard method. Logic, Language, Information and Computation. Springer Berlin Heidelberg, 2008, 5110 (Lecture Notes in Computer Science):149-163.
[8] International Organization for Standards ISO. Final draft international standard 26262, road vehicles- functional safety, 2011.
[9] Michal Konecny, Walid Taha, Jan Duracz, Adam Duracz, Aaron Ames. Enclosing the behavior of a hybrid system up to and beyond a zeno point. Proceedings of The First International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA), IEEE, 2013: 120-125.
[10] Rob Palin, David Ward, Ibrahim Habli, Roger Rivett. ISO 26262 safety cases: compliance and assurance. 6th IET International Conf. on System Safety, 2011: 12-50.
[11] Walid Taha, Paul Brauner, Yingfu Zeng, Robert Cartrwright, Veronica Gaspes, Aaron Ames, Alexandre Chapoutot. A core language for executable models of cyber physical systems (preliminary report). Proceedings of The Second International Workshop on Cyber-Physical Networking Systems (CPNS'12), Macau, China, 2012.
[12] Walid Taha, Roland Philippsen. Modeling Basic Aspects of Cyber-Physical Systems. Proceedings of the 3rd International Conference on Simulation, Modeling, and Programming for Autonomous Robots (SIMPAR), Workshop on Domain-Specific Languages and Models for Robotic Systems (DSLRob-12), 2012.