Traffic Sequence Charts –

Werner Damm
Chairman, OFFIS Transportation
Chairman, SafeTRANS
Director Center for Critical Systems Engineering of Socio-Technical Systems of the Carl von Ossietzky Universität Oldenburg
Joint work with Astrid Rakow, Eike Möhlmann, Thomas Peikenkamp, Sebastian Gerwinn
Structure of Presentation

• The Application Context
• Traffic Sequence Charts:
  – relevance
  – key concepts
  – semantics
• Why we need a formal semantics
• References
Verification challenges for autonomous driving

1. Can we capture at design time the space of all possible traffic situations and environmental factors relevant for determining safe trajectories for autonomous vehicles?

2. Can we characterize the environmental conditions for all elements in the perception chain under which identification of objects can be guaranteed for a given desired confidence level?

3. Can we characterize the variability of dynamics of other participants to allow safe predictions of future evolution of traffic situations for a given confidence level?
The safety impact of object identification

- State uncertainty
- Existential uncertainty
- Classification uncertainty
- Inaccurate or counterfactual characteriz. of situation
- Inaccurate or counterfactual prediction of evolution
- Inadequate plans
- Inadequate actions & decision (trajectory, cooperation scheme, conflict resolution, level of automation, ...)

Impact of perceptual insufficiencies on overall risk

- Different harsh conditions
- Fuse all input to one model
- Deal with uncertainty
- Plan safe actions under current conditions

Operational situations

System performance monitoring
- Measure reliability and uncertainty
- Improve future data acquisition
- Decision on function availability and degradation

Scene understanding
- Situation characterization
- Planning of provable safe actions

Functions

Mid-Range Radar

IR

C2X
Overall Approach

Application perspective

Database containing critical scenarios

Scenario-specific criticality measure / phenomena

Safety requirements

Formal foundations

Build mathematical models of
- Criticality
- Behavior of traffic participants
- Addressing uncertainty
- Composable building blocks
  - Models of environment
  - Models of perception/sensing

Labelled data base of traffic situations
Addressing ghost images and other automation risks through learning

- Injection of non-nominal behaviours (such as ghosts objects)
- Fault-injection
- Analysis
- Refinement
- Intended functionality
- Initial environment and functional model
- Refinement of environment model and/or functional model
- Simulation based analysis of anomalies: fake or true risk?
- Yes
- No
- Add Scenario to catalogue of identified automation risks
- Identify Scenarios ensuring Safety of the intended function (SOTIF)
- Truly Critical Scenario?
- Add Scenario to catalogue of identified automation risks
Safety through Guided Simulation

Data base: Formal characterization of scenarios

Functional model

- Environment perception
- Tracking / Planning
- Decision

Injection of failures/uncertainties:
- Ghost objects
- Position / velocity uncertainty
- Prediction uncertainty
- ...

Probabilities of occurrence:
- Guaranteed probability of being safe
- Level of confidence in safety

Scenarios:
- Extract scenario data base from real-world scenes
- Generation of test cases
- Coverage of real-world scenes

Source: Arne Bartels, Volkswagen

Source: Bosch
SafeTRANS Recommendations: Learning in the Field
Structure of Presentation

• The Application Context
• **Traffic Sequence Charts:**
  – relevance
  – key concepts
  – semantics
• Why we need a formal semantics
• References
Design Objectives  TSCs

• To provide a concise, intuitive specification language for capturing expected and forbidden behaviours of autonomous vehicles in the space of all possible traffic situations

• To prevent exponential blow up in requirement capture

• To serve as a formal basis for scenario catalogues in a type approval

• To serve as a formal basis for testing on all levels (MIL, HIL, runtime monitoring)
Highly Automated Lane Change Assistant

DRL TS
More than pictures

- Formal world model (unbounded composition of (probabilistic) hybrid automata)
  - defines type, attributes, and relations of objects
  - Physical aspects (e.g. dynamics)
More than pictures

- Traffic snapshot describe a traffic situation as invariants
  - captures infinitely many possible real life situations surrounding the ego vehicle

\[
\exists \text{ego}: \text{CAR}: \text{ego}.\text{pos} = (X_{\text{ego}}, 2) \text{ and } \\
\forall c: \text{CAR}: c.\text{pos}.y = 1 \rightarrow c.\text{pos}.x \notin [X_{\text{ego}} - 50, X_{\text{ego}} + 50]
\]
More than pictures

- Traffic snapshot charts describe evolution over time

- timers and end-to-end latencies
- probabilities
- mandatory vs optional vs forbidden
- negation, concatenation, concurrency, and alternatives
- activation mode (initial, always), quantification mode (universal, existential)
- activation conditions (pre-charts)
  - e.g. only if health-state=nominal and light-conditions are good
  - e.g. only if initially relative speed and distance are good
- Mandatory conditions and case splitting
Canonical extension to cooperative car2x based maneuvers

- Interplay with the well-known concept of Live Sequence Charts (LSCs)
Translation from Charts to Formulae

- Formal semantics of one TSC translates to formula in first-order multi-sorted real-time logic
  - Existential TSCs describe possible scenarios
  - Universal TSCs describe requirements
- Formal semantics of sets of TSC given by conjunction
  - Hence, no need for specifying all possible combinations requirements in each possible scenario

If ego signals a lane change and intends to change to right lane with sufficient free space then ego has to signal the lane change
Benefits

• Staged requirement analysis processes
  – from sketches (possible behaviors) to requirements (mandatory behaviors or forbidden behaviors)
  – from ideal observer to object identification through sensor fusion and exchange of perceived world models
  – from nominal behavior to degraded behaviors
  – from ego perspective to cooperative situation awareness and cooperative maneuvers

• Verification of consistency of requirements

• “Play out” generate set of all possible runs for validation of requirements

• Automatic generation of monitors
  – For design time verification on all levels (MIL, HIL, VIL of ADF)
  – For runtime verification and detection of disallowed activations of ADF

• Automatic test case generation for requirement-based/scenario-based testing
Why we need a formal semantics

- (C1) Given the ill-structuredness of the space of real world traffic situations, how can we achieve completeness of scenario catalogs, i.e. demonstrate with high confidence that all relevant real-world situations have been captured?

- Challenge C1 will be addressed by generalizing from data bases of observed traffic flows. A minimal requirement for checking for completeness is thus the need to formally define, whether a particular observed traffic behavior is already covered or not by the current scenario catalog, thus requiring the definition of a formal satisfaction relation.

- Moreover, as experienced in the play-out approach for Live Sequence Charts, a formal semantics provides a basis for playing out the current scenario catalog, thus generating traffic flows which an expert can judge for unrealistic or missing real-life traffic flows.
Why we need a formal semantics

• (C2) Given the remaining likelihood of experiencing failures in perception and interpretation after deployment, how can we establish process learning from field incidents and accidents leading to updates of the scenario catalog avoiding re-occurrence of this incident in the field?

• Challenge C2 requires a formal semantics to identify the gaps between the space of possible worlds described in the scenario catalog, and the concrete in-field incident or accident. Specifically, forthcoming regulations will require autonomously driving cars to record all those perceived environmental artifacts relevant to trajectory planning as well as the car’s trajectory control for a sufficiently long time-period. A formal semantics allows to check the failed scenario(s), offering a basis for refining the scenario specifications to cope with the observed failure in perception or interpretation of the real world.
Why we need a formal semantics

• (C3) Given the complexity space of real-world traffic situations, how can one at all achieve sufficiently concise specifications to make construction of scenario catalogues viable?

• Challenge C3 demands the use of a declarative specification language, where one single scenario specification stands for a possibly extremely large set of real world traffic situations, defined unambiguously through the satisfaction relation. Also, declarative specification languages allow for separation of concerns, such as focusing on particular kinds of critical situations in isolation, knowing that the car can only pass the test if all scenarios are passed.
Why we need a formal semantics

(C4) How can we assure, that the interpretation of scenarios and thus interpretation of test results is unambiguous across all test platforms?

Challenge C4 can be addressed by automatically synthesizing monitors for compliance testing, using the reference formal semantics.
Related Work: OpenScenario

– emerging industry standard
- Definition of ontology
- No formal semantics
- Correspond to existential TSCs

- Links: http://www.openscenario.org/

VIRES Simulationstechnologie GmbH. OpenDRIVE, 2015.
VIRES Simulationstechnologie GmbH. OpenCRG, 2016.
Papers on TSCs

- A formal semantics for TSCs, Principles of Modelling, Festschrift to the honor of Edward Lee, LNCS 10760, 2018
- Statistical Model Checking for Scenario-based verification of ADAS, Sebastian Gerwinn, Eike Möhlmann, Anja Sieper, in Proc Workshop on "Control Strategies for Advanced Driver Assistance Systems and Autonomous Driving Functions“, Springer Verlag, 2018
- Exploiting Learning and Scenario-based Specification Languages for the Verification and Validation of Highly Automated Driving, Werner Damm, Roland Galbas, to appear in Proc SEFAIAS 2018, First Workshop on Software Engineering for AI in Autonomous Systems co-located with ICSE 2018
Background Material

• SafeTRANS Recommendations on Verification of Highly Autonomous Systems
• The Enables Project
• The Pegasus Project
• Recommendations of the Ethik-Kommission of the German Ministry of Transportation
• Acatech Study Neue Automobilität
Other Relevant Links

- [http://www.enable-s3.eu/](http://www.enable-s3.eu/)

LSCs

  [https://doi.org/10.1023/A:1011227529550](https://doi.org/10.1023/A:1011227529550)
- David Harel, Rami Marelly: “Come, Let’s Play”  