Towards An Ontology-Based Approach to Safety Management in Cooperative Intelligent Transportation Systems

DeJiu Chen¹, Fredrik Asplund², Kenneth Östberg³, Eugene Brezhniev⁴, Vyacheslav Kharchenko⁵

¹KTH Royal Institute of Technology, Department of Machine Design, Division of Mechatronics, Sweden
chen@md.kth.se

²KTH Royal Institute of Technology, Department of Machine Design, Division of Mechatronics, Sweden
fasplund@kth.se

³Electronics / Software, SP Technical Research Institute of Sweden, Borås, Sweden
kenneth.ostberg@sp.se

⁴National Aerospace University KhAI, Kharkiv, Centre for Safety Infrastructure Oriented Research and Analysis, Ukraine
milestone@list.ru

⁵National Aerospace University KhAI, Kharkiv, Centre for Safety Infrastructure Oriented Research and Analysis, Ukraine
V.Kharchenko@khai.edu

Abstract. The expected increase in transports of people and goods across Europe will aggravate the problems related to traffic congestion, accidents and pollution. As new road infrastructure alone would not solve such problems, Intelligent Transportation Systems (ITS) has been considered as new initiatives. Due to the complexity of behaviors, novel methods and tools for the requirements engineering, correct-by-construction design, dependability, product variability and lifecycle management become also necessary. This chapter presents an ontology-based approach to safety management in Cooperative ITS (C-ITS), primarily in an automotive context. This approach is supposed to lay the way for all aspects of ITS safety management, from simulation and design, over runtime risk assessment and diagnostics. It provides the support for ontology driven ITS development and its formal information model. Results of approach validation in *CarMaker* are also given in this Chapter. The approach is a result of research activities made in the framework of Swedish research initiative, referred to as SARIMITS (Systematic Approach to Risk Management in ITS Context).

Keywords: Cooperative Intelligent Transportation System, Safety, Ontology, knowledge, safety loop, vehicle

1 Introduction

The expected increase in transports of people and goods across Europe will aggravate the problems related to traffic congestion, accidents and pollution. As new road infrastructure alone would not solve such problems, ITS (*Intelligent Transportation System*) has been considered as a necessary initiative. In essence, the ITS-based approach emphasizes the provisions of new services for advanced collaborative and cooperative behaviors through information and communication technologies. In such a context, the perception of operational situations is supported both by in-vehicle sensors and through the V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure) communication channels [1, 2].

While traditionally focusing on traffic efficiency [3], ITS provides many new opportunities for promoting traffic safety. One main innovation would be the provision of system wide safety services by integrating the existing local sensing and safety features of individual traffic objects. This constitutes an important basis for reaching the goal of *Vision Zero* [4], i.e. that no one will be killed or seriously injured within the road transport system. On the other hand, for the automotive industry, the transition into ITS represents many technology and culture leaps. For example, an ITS-based service for traffic safety requires not only a functional conformity of traffic objects, but also a guarantee of the performance and dependability of their coordinated behaviors. This in turn implies both design-time measures (e.g. safety process) and run-time features (e.g. quality-of-service), where a consideration of multiple traffic objects beyond the traditional automotive vehicle centered view becomes necessary. In particular, due to the complexity of cooperative operational situations, novel methods and tools for the requirements engineering, correct-by-construction guarantee, variability and lifecycle management become also important. For the design of safety functions, there is a need of capturing the operational behaviors of all related traffic objects under dynamically changing conditions for behavior control and anomaly detection. Such a specification of operational behaviors is often not supported by current approaches to the design of safety functions, which rest on worst-case analyses [5].

This chapter presents an ontology-based approach to safety management in C-ITS (*Cooperative Intelligent Transportation Systems*), primarily in an automotive context. It describes the methodology where formal models play a key role both for supporting the perception of

operational situations and for dynamically assessing the safety risks and planning the behaviors. The rest of this chapter is structured into the following sections: Section 2 discusses the state-of-the-art approaches to safety management through ITS. Section 3 introduces the envisioned ontology-based approach, including the minimal version of this ontology, description of design and deployment stages.

2 Related Work

There is a wide range of approaches to the management of transport system safety using communication and information technologies. While some of these approaches focus on the integration of *strategic and tactical decisions* (dealing with long-time goals), the others deal with the integration of *operational actions* (dealing with decisions seconds into the future). In this section, we also compare some related safety management approaches in other domains.

For road transport, the integration of strategic and tactical level decisions has been studied in particular for the transport of hazardous material. For example, *dynamic risk assessment* has been suggested as a way to minimize the risk during transport routing and emergency response. One type of systems that provides such services today is ATMS (*Advanced Traffic Management Systems*). These systems typically attempt to use available traffic information to develop optimal traffic control strategies. The focus is usually on a centralized solution for monitoring and controlling traffic behavior at *macroscopic* and *mesoscopic* levels (i.e. with whole cities and large city blocks) [6]. The *microscopic* level (i.e. separate road segments) behavior is often left uncontrolled. An ATMS normally includes methods and tools to support incident detection, incident verification, etc. However, static models developed for larger geographical road systems are often inefficient when dealing with unforeseen dynamic factors such as peak hours. Tying together models at the macro- and mesoscopic levels with simulation at the microscopic level has therefore been suggested as a way of addressing these dynamic factors better. However, to avoid a too high demand on computational resources by simulations the microscopic level is typically only considered in particular “problem areas”.

An elaboration of safety-relevant requirements on ITS based rail crossings can be found in [7]. The focus is however on the support for operational (vehicle) level safety in predefined static situations. The

dynamical aspect, i.e. runtime risk assessment, is not discussed. In [8], a simulation-based approach to autonomous vehicle safety assessment is presented. The core is an ontology that stipulates the concerns in situation analysis and task planning. It is suggested that *dynamic risk assessment* (continuous evaluation of the risk of possible actions and the selection of the “best” action) can be necessary in complex and less controlled environments where *predetermined risk assessment* (analysis of possible accidents and the inclusion of protection mechanisms) is problematic to apply. An approach to offline risk analysis with Bayesian Networks for the modeling traffic accident data is given in [9]. The factors of concern include the characteristics of the road, traffic flow, time/season and the people involved in an accident. The work presented in [10] also considers the factors relating to driver behavior and vehicle dynamics including sensor uncertainty and vehicle state. In this approach, the risk level is assessed at run time by combining traffic rules, vehicle dynamics, and environment prediction. However, it does not cover cooperative behaviors and lifecycle perspective of ITS. In [11], an evaluation and testing of the two demonstrator vehicles developed for intersection driver assistance is described. The dynamic risk assessment (DRA) is supported through object tracking and classification and the communication of traffic management and driver intention.

The overall dependability of industrial installations in the nuclear, automotive, chemical and energy domains is centered on *functional safety* and *risk management* provided by IEC61508 [12] and associated standards (e.g. ISO 26262 [13]). According to these standards, a risk management lifecycle typically goes across the design, the deployment, and the post-accident analysis stages. During the design, the risk management is focused on eliminating known hazards by safety measures that keep the system in a safe state. The success can however be restricted because of a high degree of uncertainty due to a lack of knowledge, insufficient model accuracy, etc. Post-deployment risk management refers to constantly conducted safety evaluations because of changes in the system configuration, component reliability, maintenances, etc. Such measures are implemented in many industrial installations to prevent accidents. Post-accident risk assessment produces a detailed description of the incident/accident and its consequences, proposes additional prevention and protection barriers, etc.

All of these risk assessment methods are based on some assumed accident scenarios [14]. For automotive vehicles, such accident scenarios

are often given by some estimated *worst case scenarios*. From a safety engineering perspective, such deterministic estimations often abstract away details about the combinatorial effects of environmental events and system anomalies in spatial and temporal domains for the efficiency of assessment. In nuclear domain, after the Fukushima Dai-Ichi accident, when deterministic safety approaches failed, these have been complemented by probabilistic safety assessment/probabilistic risk assessment (PSA/PRA). Currently both activities are implemented during Nuclear Power Plant Instrumentation&Control System development stages. The current PSA framework has some limitations in handling the timing of automatic and personnel actions. The conventional PSA techniques (Event Tree / Fault Tree) methodology may not yet yield satisfactory results, but they open the way for use of new dynamic techniques to accurately describe system dynamics while considering e.g. state uncertainties. These new methodological approaches to risk assessment include statistical analysis of near-miss and incident data using Bayesian theory to estimate operational risk value and the dynamic probabilities of accidents sequences having different severity levels [15]; and the application of simulation models to analyze scenarios using dynamic fault trees [16]. ITS can potentially be benefited by the approaches in other safety critical industrial processes. Here, one challenge is related to the complexity of ITS where unknown emergent behaviors dominate. For example, the risk assessment, e.g. in the nuclear domain, is performed to build risk profiles for critical processes. The application of dynamic risk assessment just allows one to make these profiles dynamical.

3 An Ontology-Based Approach

By *system ontology*, we refer to the formalization of system-wide concerns in terms of models. Such concerns typically range from the definitions of system constituent units (i.e. the traffic objects and traffic environments) in regard to their boundaries, compositions, technological preferences, to the specifications of the interactions of such objects in regard to the functionalities and extra-functional constraints. As a generic support for knowledge formalization, the ontology-based approach aims to promote not only the quality management at design time across engineering disciplines and teams, but also the data treatment and decision making at run time across traffic objects.

3.1 An overview

For the functional safety of road vehicles, ISO26262 represents the domain consensus on the state-of-the-art approaches [12]. It is centered on a reference safety lifecycle through which the work tasks as well as the information to be generated and communicated for risk management and requirements engineering are stipulated. In the case of ITS, the connectivity across multiple traffic objects implies that a system-of-systems perspective on functional safety becomes necessary. This means in practice that the *safety-loop*, i.e. the loop of system safety lifecycle, now needs to cut across the safety lifecycles of involved traffic objects and infrastructure [6]. As outlined earlier, the complexity of operational situations also makes dynamic risk assessment services necessary for enabling optimized control in *a priori* unknown situations or simply for guaranteeing more qualified specification of safety goals.

The ontology-based approach described here emphasizes the provision of an integrated knowledge model both for safety engineering and for the design of advanced safety features. It in particular considers *co-ordinated driving* when two (or more) vehicles coordinate their behaviors either based on predefined traffic rules (i.e. *choreographed*), or through active communication and consolidation of intents (i.e. *cooperative*), or by active negotiation for consensus (i.e. *collaborative*). An overview of the target lifecycle phases, work tasks, and run-time services, all centered on a common ontology, is given in **Fig. 1**.

Fig. 1. The lifecycle phases, work tasks and run-time services to be benefited by a common ontology.

Post-accident analysis is supposed to be one of main stage of the ITS safety management process. The information accumulated during system runtime would be stored and processed during vehicle fault analysis through big-data and pattern elicitation. Detailed tracking and analysis of vehicle malfunctions and failures will allow the updates of failure probabilities used during design stage. Besides, it decreases uncertainties in risk and hazard analysis.

3.2 The modeling framework

There are different roles of the ontological core. During system development, the focus is on a model-based approach to risk assessment and elicitation of safety requirements. It would provide a well-structured and standardized specification of the operational situations, the system architecture in terms of functional and technical design, as well as the related safety requirements and constraints. Beyond the development time, the support is focused on the provision of a knowledge model for dynamically consolidating the monitored operational situations, coordinating the control behaviors, and handling possible anomalies. For instance, during the deployment stage, the ontology allows for transformations of information during V2V and V2I to provide a common basis for logging, shared perception and decision making. For post-accident analysis, it assures that the factors of importance for the analysis are available from the data logged by the ITS infrastructure.

The key base technology to support the deployment of such an ontology-based approach is the *EAST-ADL* (Electronics Architecture and Software Technology - Architecture Description Language). As a modeling framework, EAST-ADL represents a key European initiative towards a standardized multi-viewed description of automotive electrical and electronics systems [17]. It integrates many existing frameworks (e.g. SysML, RIF/ReqIF, ISO26262) while allowing a wide range of functional safety related concerns (e.g. hazards, faults/failures, safety requirements) to be declared and structured seamlessly along with the lifecycle of nominal system development. Based on such a structured description, EAST-ADL also provides necessary modeling support for functional safety [18]. Moreover, through its support for behavior description, the modeling framework also allows the developers to precisely capture various behavioral concerns in requirements engineering, system design, and safety engineering [19]. However, although consti-

tuting a very good basis for capturing and formalizing various aspects of ITS, current EAST-ADL does not provide any explicit methodology on the modeling and analysis of ITS systems in regard to the emergent properties and safety issues. Therefore, language extensions and specializations in regard to cooperative ITS (C-ITS) are being developed. One key modeling package being extended is the *Environment Model*, shown in **Fig 2**. In particular, the following additional concepts are introduced to support the specification of operational situations:

- *Scene* - a description of characteristics and objects that are of interest and “static” at a strategic or tactical level. Typical static scene data include: 1. Weather conditions, i.e. air density, humidity and pressure, solar radiation, temperature, etc. 2. The terms defined by the WGS 84, OpenDrive and OpenCRG standards; 3. Regions of interest, which are defined by a polygon set, a type (e.g. boundary) and an object identified (e.g. fence)
- *Situation* - a scene populated with dynamic objects, which are defined by: 1. WGS 84; 2. Mass and Speed; 3. Behavior, which is defined by a type (e.g. choreographed) and a trajectory (i.e. an intent); 4. An associated region of interest; 5. A probability distribution tied to each of these terms
- *Scenario* - a set of situations linked in time.

Fig 2. An overview of the meta-model packages of EAST-ADL.

3.3 The Case Study with Virtual Depolyment

As a first step towards analyzing the use of our ontology during the deployment stage we used *IPG CarMaker* to simulate interactions between an ego-vehicle and both uncoordinated and all types of coordinated drivers on a four lane circular track (see **Fig. 3**). If all information defined by the ontology is available, then an ego-vehicle can make informed control decisions by sharing data across all ITS levels. In real implementation, there would of course be many challenges since there is a high probability for the information being lost or corrupted (e.g. the sheer size of the data, failing sensors, transmission issues, etc.). As a fundamental requirement, such problems would not result in risk, but rather in a lower level of certainty of the dynamic assessment outcome that would in turn imply the activation of ADAS function (for involving the human driver in the loop as the fail-safe).

Fig. 3. CarMaker Simulation

A related problem of concern is that each ego vehicle will have to evaluate the *trustworthiness* of each piece of information provided via ITS. For legal reasons it is unreasonable to assume that the manufacturer of a vehicle will be able to completely trust and coordinate with all *other* manufactures of vehicles and infrastructure. This implies two things. Firstly, that the probability distribution tied to each piece of information will have to be subjective for each ego-vehicle in the ITS system. Secondly, that the probabilities of most importance to dynamic risk assessment in an ITS systems are not those related to the outcomes an ego-vehicle set of possible actions, but rather those related to the validity of the provided decision support. Support for reasoning about such uncertainty, such as that provided by *Dempster-Shafer Theory* and *Belief Propagation*, across ITS levels is therefore likely to be a well-

motivated research direction. It is also likely that those objects in ITS on which a specific vehicle can trust completely are going to become important as evaluators of other entities. For example, a trusted vehicle driving in front of a less trusted vehicle can be used to evaluate the accuracy of the latter vehicle's sensors; trusted infrastructure can estimate the speed of a vehicle, which can then be compared with the broadcasted value.

4 Conclusions

Deployment of ITS is expected to bring the many benefits for all traffic participants. ITS will help to improve the transport efficiency, passengers comfort, decrease environmental contamination, etc. Due to the inherent complexity of ITS, it is impossible to cover all of the possible traffic scenarios during the design stages. The traditional approaches to safety management in ITS would not be sufficient due to their heavy reliance on worst case assumptions. The approach proposed by this paper is based on an ontology that allows one to formally capture the concerns in temporal and spatial domains and thereby constitutes a basis for a novel safety lifecycle with *knowledge-in-the-loop*. The approach emphasizes the interplay of model-based system development and the design of advanced system services, through which meta-knowledge for robust perception and safe operation will be deployed and maintained at system run-time.

5 References

1. Sussman, J.: Perspectives on Intelligent Transportation Systems, Springer, New York, NY (2005)
2. Vision for ITS. Proceedings of the National Workshop on Intelligent Vehicle/Highway systems sponsored by Mobility 2000, Dallas, TX 1990 (available here: http://ntl.bts.gov/lib/jpodocs/repts_te/9063.pdf - accessed June 2014)
3. Papageorgiou, M.: ITS and Traffic Management. Handbook in OR&MS, Vol.14, DOI:10.1016/S0927-0507(06)14011-6 (2007)
4. Tingvall, C.: Vision Zero - An ethical approach to safety and mobility. Proceedings of the 6th ITE International Conference Road Safety & Traffic Enforcement: Beyond 2000, Melbourne (1999)
5. Chen, D. et al.: A systematic approach to risk management in ITS context – challenges and research issues. Радіоелектронні і комп'ютерні системи, 2014, № 5 (69) ISSN 1814-4225, 11 p. (2014)
6. Östberg, K. et al.: Intelligent Transport Systems - the Role of a Safety Loop for Holistic Safety Management. SAFECOMP 2014 Workshops, LNCS 8696, 3–10 p., Springer International Publishing Switzerland (2014)

7. Larue, Gregoire S., et al.: Methodology to assess safety effects of future Intelligent Transport Systems on railway level crossings. Proceedings of Australasian Road Safety Research, Policing and Education Conference, 4-6 October, Wellington, New Zealand (2012)
8. Wardzinski A.: Dynamic Risk Assessment in Autonomous Vehicles Motion Planning. Proceedings of the first International Conference on Information Technology, DOI:10.1109/INFTECH.2008.4621607 Gdansk, Poland (2008)
9. Simonic, M.: A Bayesian Network Model of Two-Car Accidents, Journal of Transportation and Statistics, vol. 7, 2/3 (2004)
10. Hong Cheng, et al.: Interactive Road Situation Analysis for Driver Assistance and Safety Warning Systems: Framework and Algorithms. IEEE transaction on Intelligent Transportation System, Volume 8, Issue 1, pp. 157-167 (2007)
11. Fuerstenberg, K. et al.: (Results of the EC-Project INTERSAFE. Advanced Microsystems for Automotive Applications VDI-Buch, pp. 91-102 (2008)
12. International Electrotechnical Commission. IEC 61508:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems (2010)
13. International Organization for Standardization. ISO 26262:2011, Road vehicles - Functional safety (2011)
14. Swaminathan, S. et al.: The Event Sequence Diagram framework for dynamic Probabilistic Risk Assessment Reliability Engineering and Systems Safety 63, pp. 73-90 (1999)
15. Anjana Meel, A.: Plant-specific dynamic failure assessment using Bayesian theory. Chemical Engineering Science 61, pp. 7036-7056 (2006)
16. Hong, Xu.: Combining Dynamic Fault Trees and Event Trees for Probabilistic Risk Assessment Reliability and Maintainability, Annual Symposium - RAMS ISBN: 0-7803-8215-3, pp. 214-219 (2004)
17. EAST-ADL. EAST-ADL Domain Model Specification, Version M.2.1.12. 2014. <http://www.east-adl.info/>
18. D. Chen, R. Johansson, et al.: Integrated Safety and Architecture Modeling for Automotive Embedded Systems. e&i, vol. 128, Number 6. Springer (2011)
19. D. Chen, L. Feng, et al.: An Architectural Approach to the Analysis, Verification and Validation of Software Intensive Embedded Systems. Computing, Springer. DOI: 10.1007/s00607-013-0314-4 (2013)