UDC 004.94

D. CHEN[1], F. ASPLUND[1], K. ÖSTBERG[2]

[1] ***KTH Royal Institute of Technology, Department of Machine Design, Division of Mechatronics, Brinellvägen 83, 10044 Stockholm, Sweden***
[2] ***Electronics / Software, SP Technical Research Institute of Sweden, Borås, Sweden***

A SYSTEMATIC APPROACH TO RISK MANAGEMENT IN ITS CONTEXT –CHALLENGES AND RESEARCH ISSUES

Intelligent Transportation System (ITS) with autonomic functions that are cyber-physical in nature is of rapidly increasing importance for traffic efficiency and safety. Current engineering approaches to such functions often rely on worst-case assumptions, originally used for safety engineering, due to the difficulty and cost involved in precisely modeling and analyzing the system boundaries and emergent behaviors in a highly dynamic configuration of system-of-systems. This can lead to the loss of many of the benefits in regard to traffic efficiency, but also to conditions where the transport system as a whole is prone to unacceptable high risks. We envisage a systematic approach to the development of autonomous functions in ITS resting on the basis of a formal modeling framework. This paper presents our vision for achieving such a goal on the basis of EAST-ADL, which is an ISO26262 compatible architecture modeling language and methodology for the development and management of automotive Electrics & Electronics systems. Especially, this paper elaborates on some key challenges and outlines related research issues to be regarded in a Swedish research initiative, referred to as SARMITS (Systematic Approach to Risk Management in ITS Context).

Keywords*: intelligent transportation system, safety engineering, cyber-physical functions, system-of-systems, model-based development, ontology, EAST-ADL.*

Introduction

Intelligent Transportation System (ITS) - with the support of autonomous vehicles, V2V and V2I infrastructure - provides new opportunities for traffic efficiency and safety, which could lead to many societal and economic benefits. It could for instance be one of the foremost technologies for reaching the goal of *Vision Zero* (1), i.e. that no one will be killed or seriously injured within the road transport system. However, as the transition into ITS represents such a large technology and culture leap, ITS features are likely to be first deployed to facilitate fully autonomous cooperative driving scenarios with human-in-the-loop unfeasible or excluded by nature. This is unfortunately misaligned with the state-of-the-art approaches to the design of advanced safety functionality of vehicles, which often rests strongly on *worst-case analyses* (2).

The *SARMITS (Systematic Approach to Risk Management in ITS Context)* initiative aims to advance the methodologies and technologies required to build advanced autonomous functions in ITS by consolidating the expected interplay between engineering methods/tools and safety features such as proactive accident prevention.

The rest of this paper is organized as follows: Section 2 provides a background discussion regarding the limitations of current approaches; Section 3 elaborates on some key design issues to be addressed; Section 4 presents some related state-of-the-art technologies to be considered; Section 5 provides details of the SARMITS research objectives and work tasks; Finally, Section 6 provides a summary and conclusion.

1. Background

From a safety engineering point of view, hazardous events and therefore the related safety risks are due to the combinatorial effects of environmental factors and the behavior of the vehicle in focus. For example, the causes of a critical situation can range from unacceptable driving styles and unexpected interplay between vehicles, to unfavorable weather and road conditions (3). A worst-case based approach to the design of safety functions, dominated by a priori assumptions about the operational situations originally used for safety engineering, can therefore be very restrictive in regard to traffic efficiency. For instance, such an approach could result in unnecessarily strict safety margins in regard to vehicle speed or distance between vehicles. Notably, such an approach can also lead to conditions where the transport system as a whole is prone to unacceptable high risks, mainly due to the fact that a violation of the safety margins in many practical situations is often not perceived as risky. If the drivers of individual vehicles can bypass the functions implement-

ing worst-case safety margins to achieve benefits in a practical situation, results from other domains show they are likely to start doing so (4). In other words, the introduction of safety features without an elaborated reasoning about vehicle status, operational situations, and driver behaviors may in combination with worst case assumptions lead to the decay of the overall system safety.

Consider for instance the scenario when ITS allows a vehicle to drive down a highway at a speed unfeasible for a human driver to control. Instead of a simple worst-case analysis based design of safety functions, an elaborated analysis of the driving scenarios and the interplay among vehicles would call for advanced features supporting both strategic decisions during normal driving and tactical decisions in critical situations:

1. Braking as hard as possible may be the correct choice, for instance if traffic is sparse or all vehicles are autonomously driven.

2. Smooth braking may be required if traffic is dense or weather conditions have made the road slippery.

3. Driving off the road may be preferable if a truck is about to hit a bus, but the road environment consists of plains devoid of natural obstacles. At the same time, choosing to hit a car instead of a bus may be acceptable if the road environment consists of sheer cliffs.

4. A front-to-side collision with a car may be preferable to hitting a pedestrian, but not if it will push that car into oncoming traffic and thereby create a collision involving several vehicles.

5. A front-to-side collision may be preferable, but if a front-to-end collision is possible it may be a better choice. However, this might depend on the manufacture, model and year of both vehicles.

Surrounding the vehicles, there are both a *road* and a *traffic environment*. While the road environment constitutes the infrastructure and road conditions, the traffic environment is characterized by a dynamically changing configuration of adjacent vehicles, pedestrians, and other stakeholders of heterogeneous types. Therefore, a realization of advanced safety features requires support for monitoring and assessing the actual external and internal conditions, perceiving the allowed and prohibited behaviors, and planning for proactive measures. Through such runtime measures, any plausible violations of safety rules can be detected before the system of concern has already reached an unacceptable state with high risk.

2. Key Design Issues

In general, advanced safety features, like pre-crash planning, crash mitigation, and automated post-crash diagnostics, relies strongly on autonomic functions that are *cyber-physical* (CP) in nature. While the physical aspect is related to the energy flows under control, the cyber aspect is related the embedded control and cognitive loops making the control decisions. ITS will provide many unique opportunities for cooperative control decisions by individual vehicles. The infrastructure basically constitutes a sensor network that allows an exchange of monitored operational information from a variety of sources, a consolidation of context understanding in vehicular and infrastructural nodes (i.e. data fusion), and a coordination of behavior planning and control decisions. Still, the success requires a well-formed specification of the *System-of-Systems* (SoS) characteristics. The issues of particular concern include but are not limited to: *boundary configurations, data fusion, emergent behaviors, treatment of decision uncertainties and failure modes*. As the development often involves multidisciplinary teams, a well-defined methodology as well as advanced methods and tools for work management, decision support and traceability, and system synthesis are all necessary.

In particular, for deciding best courses of actions in complex scenarios, a vehicle needs to perceive the operational status of its environments and its own. Here, such a system feature is referred to as *context-awareness* (5). Typically, some data underlying context-awareness could be obtained through direct monitoring and communicating about the operational situations, such as the relative positions, speeds, events and types of adjacent vehicles. However, to cope with the uncertainties and interferences, other *contractual data* also become necessary. For example, when a vehicle is planning its own driving behavior on a road, it needs to estimate risk zones and plausible crash scenarios. For this, information about the contractual assumptions, promises, and invariants of other vehicles and the ITS would be of vital importance. Obviously, all context-awareness information, if communicated or logged, could also be valuable for automated post-incidents or accidents diagnosis.

Given a support for context-awareness, a further topic is related to the *provision of knowledge* (5) underlying the in-vehicle reasoning for the purposes of task planning or control. To these ends, one key factor is concerned with how to create an *information-model* for a standardized parameterization and structuring of a wide range of concerns in the SoS context, and how to formalize such an information-model in terms of *ontology* to support effective design, implementation, diagnostics and maintenance.

For advanced safety features, it is not trivial to derive such an ontology. Whilst some of those related factors are well known, others remain to be explored. Due to the complexity of the related operational scenarios multidisciplinary sources with potentially rich and varying semantics will have to be consulted. These will range from vehicle and ITS architectures, to risk perception and proactive safety planning algorithms, and to emergent vehicle and driver behaviors.

3. Base Technologies and Related Work

DySCAS (Dynamically Self-Configuring Automotive Systems) is a middleware architecture for context-awareness and dynamic configuration management of automotive embedded systems (5). The context information includes both internal operating conditions and external environment situations, such as levels of resource utilization, connected devices, faults detected etc. The self-management is governed by the use of policies distributed throughout the middleware components. DySCAS also provides an information-model that stipulates a set of predefined data types for formalizing various architectural and executional concerns in system configurations. As a first step towards self-managing automotive systems, DySCAS provides a very good basis for understanding the fundamental functional and technical issues in regard to embedded reasoning of dynamic properties.

EAST-ADL represents one domain-specific approach to multi-viewed system description with the aim of promoting separation-of-concerns and thereby effective quality management in general (6). EAST-ADL allows 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 precisely defining the related error behaviors for safety analysis (7). Furthermore, EAST-ADL allows the developers to precisely capture various behavioral concerns in requirements engineering, system design and safety analysis based on a hybrid-system model (8). However, although constituting a very good basis for capturing and formalizing various aspects of ITS, current EAST-ADL does not provide an explicit methodology on the modeling and analysis of ITS systems in regard to the emergent properties and safety issues.

Related formalization efforts exist, such as the work by NASA to formalize safety cases described in Goal Structured Notation (9).

There is a wide range of methods and tools aiming to support safety analysis, see e.g. (10) for a discussion. However, there exists no standard for system safety specifically for systems like ITS. While it can be foreseen that any safety standardization work for co-operative systems of vehicles will affect and be affected by the ISO 26262 standard (2), it is highly likely that input will be required also from safety discourse outside those targeting *functional safety*. One might for instance consider the discussion on how control of safety based on empirical evidence is likely to continuously become unreliable due to *"compensatory adaptation to changes governed by local, situational features"* as work systems become more dynamic and self-organizing (12). Instead of modelling the cause-effect leading up to accidents as chains of events, it might therefore be better to view systems as migrating towards states of high risk in which any one of several otherwise acceptable deviations could lead to an accident. This would imply that it would be important to enable a safety analysis in ITS that builds on identifying, highlighting and managing elevated states of risk, rather than striving to control all deviations.

4. Research Objectives and Work Tasks

A first step towards the ontology envisioned in Section 3 would be an analysis of the boundaries between ITS and vehicular Electrics & Electronics (E&E) systems, considering some key reference features, a variety of cooperation scenarios, and system internal conditions. This would constitute a basis for constructing an *information-model* that allows a systematic and formal definition of context-awareness data *in each individual system,* supporting any autonomous features of which the loops of control involve the monitoring, consolidation, and assessment of environmental and internal conditions. A natural base for this type of information-model would be some of the already existing, common reference models of ITS (e.g. ETSI) and E&E systems (e.g. EAST-ADL, AUTOSAR).

A second step would be to construct a formal specification of environmental and contractual data required for effective run-time task planning. This would create a formal basis for understanding and specifying latent risks (strategic planning), risk avoidance (seconds to crash) and minimizing the effect of hazards (crash is imminent or has already occurred). The scope would have to include, but not be limited to, possible characteristics of the road environment, the traffic environment and the involved stakeholders, properties and invariants of safety (i.e. weather conditions, the mass and deformation zones of different vehicles, driving styles at different times and geographical locations, etc.). This specification would allow a preliminary *information-model* for a standardized *parameterization and structuring of a wide range of concerns in the SoS context* and provide an understanding of how to formalize such an information-model in terms of an ontology for effective engineering. It would also enable a run-time match between task design and actual operating situations to decide what is safe and what is unsafe in a dynamic and uncertain environment. In addition, it would allow for a more accurate off line analysis of a real accident given that data from the LDM/ITS has been logged in a driving recorder.

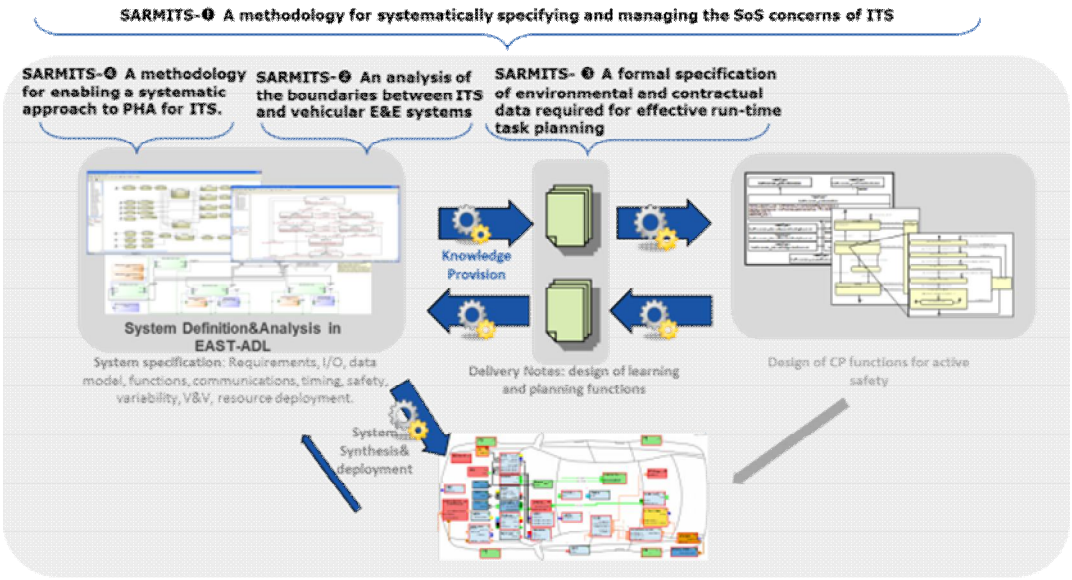

Fig. 1. Quick Iterations from Design to Runtime

A third step would then be to design a methodology for enabling a systematic approach to preliminary hazard analysis (PHA) for ITS. This would include the elicitation of safety goals in the ITS context, while emphasizing the usage of models to understand the different aspects that may influence the behaviors of cooperative driving vehicles in critical situations (types of vehicles, information shared, communication failures, sensor failures, etc.). The work would ideally (when appropriate) be in accordance to ISO26262 and other state-of-the-art approaches to system safety, functional safety, structured and formal safety analysis techniques.

By building on these three steps one could then design a methodology for systematically specifying and managing the SoS concerns of ITS. The design would still require the elicitation of ITS specific requirements on structuring, formalization, and multi-view representation of use cases, operational situations, functional and extra-functional requirements. However, once the requirements, information models, hazard analysis approach and overall methodology is in place, then quick iterations through design-time modeling/simulation, deployment, run-time decisions and post-crash information can be enabled (see Fig. 1).

This work would ideally be based on EAST-ADL, which is a methodology and modeling framework developed by Volvo, KTH, and other industry and academia partners.

Conclusions

The ITS systems of tomorrow will probably be the most complex systems humans have ever built. It is highly likely that not all initial design decisions will be correct and that there – as a result – will be accidents. Unfortunately a worst-case analysis approach to designing for safety is neither a guarantee for system safety, nor appropriate for the successful realization of the traffic efficiency gains promised by ITS.

ITS is most likely to be introduced in steps and to maintain public acceptance we therefore suggest the creation of a methodology for systematically specifying and managing the SoS concerns of ITS. This would require:

1. An information-model that allows a systematic and formal definition of context-awareness data in each individual system participating in ITS.

2. An information-model for a standardized parameterization and structuring of a wide range of concerns in the SoS context.

3. A methodology for enabling a systematic approach to preliminary hazard analysis for ITS.

Based on such a methodology for specifying and managing the concerns of ITS the feedback loops through design-time modeling/simulation of safety, deployment, run-time decisions and post-crash information can be sped up. This would minimize the impact of safety by invalid assumptions and enable an increasing public trust in ITS.

References

1. Tingvall, C. Vision Zero – An ethical approach to safety and mobility [Text] / C. Tingvall, N. Haworth // Melbourne: u.n., 1999. Proceedings of the 6th ITE International Conference Road Safety & Traffic Enforcement: Beyond 2000.

2. ISO 26262:2011. International Organization for Standardization [Text]. – Road vehicles – Functional safety. 2011.

3. Martensen, H. Forecasting Road Traffic Fatalities in European Countries: Model and First Results [Text] / H. Martensen // Deliverable 4.2 of the EC FP7 project DaCoTA. 2010.

4. Rasmussen, J. Risk Management in a Dynamic Society: A Modelling Problem. Safety Science [Text] / J. Rasmussen. – 1997. – Vol. 27. – P. 183 – 213.

5. Autonomic Middleware for Automotive

Embedded Systems [Text] / R. Anthony, D. Chen, M. Törngren, D. Scholle, M. Sanfridson, A. Rettberg, T. Naseer, M. Persson, L. Feng. – Autonomic Communication: Springer US, 2009.

6. EAST–ADL Association. EAST–ADL – An architecture description language for automotive E&E systems [Electronic resource]. – Available to: http://www.east–adl.info/ – 07.03.2014.

7. Elektrotechnik und Informationstechnik, Integrated safety and architecture modeling for automotive embedded systems [Text] / D. Chen, R. Johansson, H. Lönn, H. Blom, M. Walker, Y. Papadopoulos, S. Torchiaro, F. Tagliabo, A. Sandberg. – Springer–Verlag, 2011. – Vol. 128. – ISSN: 0932–383X.

8. An architectural approach to the analysis, verification and validation of software intensive embedded systems [Text] / D. Chen, L. Feng, T. N. Qureshi, H. Lönn, F. Hagl. – Springer Vienna, 2013. – Vol. 95. – ISSN: 0010–485X.

9. Denney, E. A Formal Basis for Safety Case Patterns [Text] / E. A. Denney, G. Pai. – Springer Berlin Heidelberg, 2013. – Vol. 8153. – ISBN: 978–3–642–40792–5.

10. Modelling Support for Design of Safety–Critical Automotive Embedded Systems [Text] / D. Chen, R. Johansson, H. Lönn, Y. Papadopoulos, A. Sandberg, F. Törner, M. Törngren. – Springer Berlin Heidelberg, 2008. – ISBN: 978–3–540–87697–7.

11. Rasmussen, J. Risk Management, Adaptation, and Design for Safety [Text] / J. Rasmussen ; edit by Nils–Eric Sahlin, Berndt Brehmer. – Springer Science, Business Media, 1994.

Поступила в редакцию 11.03.2014, рассмотрена на редколлегии 24.03.2014

Рецензент: д-р техн. наук, проф. В. А. Заславский, Киевский национальный университет имени Тараса Шевченко, Киев, Украина.

СИСТЕМНЫЙ ПОДХОД К УПРАВЛЕНИЮ РИСКАМИ В ИТС – ПРОБЛЕМЫ И ЗАДАЧИ ИССЛЕДОВАНИЯ

Д. Чен, Ф. Асплунд, К. Остберг

Интеллектуальные транспортные системы (ИТС) с автономными функциями, которые являются по своей природе кибер-физическими, имеют все большее значение для повышения эффективности и безопасности движения. Для обеспечения техники безопасности в таких функциях, текущие инженерные подходы базируются на предположениях наихудших сценариев, это связанно с трудностями и затратами при точном моделировании и анализе границ систем. Это может привести к потерям эффективности движения и к высоким рискам. Мы предполагаем системный подход к разработке автономных функций в ИТС на основе формального фреймворка моделирования. Данная статья представляет наше виденье для решения этой цели на основе языка EAST-ADL, который совместим с языком моделирования архитектуры и методологией для разработки и управления автомобильными электронными системами из стандарта ISO26262. Подробно рассмотрены ключевые вопросы и связанные с ними задачи исследования.

Ключевые слова: интеллектуальные транспортные системы, техника безопасности, кибер-физические функции, система систем, разработка на основе моделей, онтология, EAST-ADL.

СИСТЕМНИЙ ПІДХІД ДО УПРАВЛІННЯ РИЗИКАМИ В ІТС – ПРОБЛЕМИ ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

Д. Чен, Ф. Асплунд, К. Остберг

Інтелектуальні транспортні системи (ІТС) з автономними функціями, які є за своєю природою кібер-фізичними, мають все більше значення для підвищення ефективності та безпеки руху. Для забезпечення техніки безпеки в таких функціях, поточні інженерні підходи базуються на припущеннях найгірших сценаріїв, це пов'язано з труднощами і витратами при точному моделюванні та аналізі меж систем. Це може привести до втрат ефективності руху і до високих ризиків. Ми припускаємо системний підхід до розробки автономних функцій в ІТС на основі формального фреймворка моделювання. Дана стаття являє наше бачення для вирішення цієї мети на основі мови EAST-ADL, який сумісний з мовою моделювання архітектури та методологією для розробки та управління автомобільними електронними системами зі стандарту ISO26262. Докладно розглянуті ключові питання і пов'язані з ними завдання дослідження.

Ключові слова: інтелектуальні транспортні системи, техніка безпеки, кібер-фізичні функції, система систем, розробка на основі моделей, онтологія, EAST-ADL.

De-Jiu Chen – Associate Professor at Sweden KTH Royal Institute of Technology, Department of Machine Design, Division of Mechatronics, e-mail: chen@md.kth.se.

Fredrik Asplund – PhD at Sweden KTH Royal Institute of Technology, Department of Machine Design, Division of Mechatronics, e-mail: fasplund@kth.se.

Kenneth Östberg – at Sweden Electronics / Software, SP Technical Research Institute of Sweden, Borås, Sweden, Kenneth, e-mail: Ostberg@sp.se.