



Contract number: 2004 - 026976

Advancing Traffic Efficiency and Safety through Software Technology (ATESST)

Report type	Deliverable D6.2.1
Report name	Case study and demonstrator plan with early case study release
Disemination level	PU
Status	Final
Version number	1.1
Date of preparation	2006-04-21

Authors**Editor**

Rolf Johansson

E-mail

MGH (rolf_johansson@mentor.com)

Contributors

Lars-Olof Berntsson

Volvo Technology Corporation (lars-olof.berntsson@volvo.com)

Hans Blom

VTEC (hans.blom@volvo.com)

Ali Botorabi

Daimler Chrysler AG (ali.botorabi@daimlerchrysler.com)

DeJiu Chen

KTH (chen@md.kth.se)

Philippe Cuenot

Siemens VDO (philippe.cuenot@siemens.com)

Jörg Donandt

DC (joerg.donandt@daimlerchrysler.com)

Ulrich Freund

ETAS (ulrich.freund@etas.de)

Sebastien Gerard

CEA (sebastien.gerard@cea.fr)

Istvan Horvath

MGH (istvan_horvath@mentor.com)

Fredrik Jernqvist

MGH (fredrik_jernqvist@mentor.com)

Rolf Johansson

MGH (rolf_johansson@mentor.com)

Henrik Lönn

Volvo Technology Corporation (henrik.lonn@volvo.com)

Mark-Oliver Reiser

TUB (mark-oliver.reiser@web.de)

David Servat

CEA (david.servat@cea.fr)

Jianlin Shi

KTH (Jianlin@md.kth.se)

Carl-Johan Sjöstedt

KTH (carlj@md.kth.se)

Patrick Tessier

CEA (patrick.tessier@cea.fr)

Martin Törngren

KTH (martin@md.kth.se)

Matthias Weber

DC (matthias.n.weber@daimlerchrysler.com)

The Consortium

Volvo(S)

DaimlerChrysler (D)

Siemens (F)

ETAS (D)

Mentor Graphics (Hu)

CEA (F)

The Royal Institute of Technology (S) Technische Universität Berlin (D)

Carmeq GmbH (D)

Volvo Cars (S)

Mecel (S)

Revision chart and history log

Version	Date	Reason
0.1	2006-03-22	Creation (Rolf Johansson – MGH)
0.2	2006-03-24	Update after initial comments (Rolf Johansson – MGH)
0.3	2006-03-27	Siemens VDO update
0.4	2006-04-04	review chap 1.4 Siemens VDO
0.5	2006-04-06	minor consistence corrections (MGH-RJ)
0.6	2006-04-18	new document template (MGH-RJ)
1.0	2006-04-21	document release (MGH-RJ)
1.1	2007-07-04	Updated according to observations/comments from EC review 29/03/2007, Review no. 1 covering project month 1 to 12 (01/01/06 – 31/12/06)

List of abbreviations

Abbreviation	Description
AADL	Architecture Analysis & Design Language
ACC	Adaptive Cruise Control
ADL	Architecture Description Language
ATESST	Advancing Traffic Efficiency and Safety through Software Technology
AUTOSAR	Automotive Open System Architecture
DOW	Description Of Work
EAST-EEA	Embedded Architecture & Software Technologies-Embedded Electronic Architecture
EAST ADL	Architecture Description language developed in the EAST-EEA project
ECU	Electronic Control Unit
E/E Architecture	Electrical/Electronic Architecture
FMEA	Failure Mode Effect Analysis
FTA	Fault Tree Analysis
ISS	Integrated Safety Systems
MARTE	Modeling and Analysis of Real-Time and Embedded systems
MDD	Model Driven Development
MIC	Model Integrated Computing
OMG	Object Management Group
RT/E	Real-Time/Embedded
SAE	Society of Automotive Engineers
SysML	System Modeling Language
UML	Unified Modeling Language
V&V	Verification and Validation

Table of contents

Authors	2
Revision chart and history log.....	3
List of abbreviations.....	4
Table of contents	5
List of Figures	6
1 Introduction	7
2 Case Study and Demonstrator Plan	8
2.1 Active Safety	8
2.2 System Description	9
2.3 Scenarios	9
2.4 Realization Phases	10
2.5 Physical View.....	11
2.6 Options	11
3 Contribution to overall ATESSST objectives.....	13

List of Figures

Figure 1 Crash Mitigator	8
Figure 2 Speed Moderator.....	8
Figure 3 Demonstrator system, functional block view.....	9
Figure 4 Demonstrator system, physical block view.	11

1 Introduction

Improvement of automotive safety, efficiency and environmental-friendliness relies heavily on the usage of electronics and software. Recent systems provide optimization and coordination of functions within the vehicle but also externally between vehicles and road infrastructure (environment). The complexity induced by the electronic architecture and increasingly by the applications, needs to be managed adequately. The goal of the ATESST project is to deliver an Architecture Description Language suitable for these systems. This provides a means to handle the complexity and improve safety, reliability, cost, and development efficiency of automotive electronic systems.

The ATESST results will be based on the EAST-ADL (Architecture description language developed in the ITEA EAST-EEA project). A completely revised version of EAST ADL will be delivered, EAST-ADL2.0, where existing constructs are validated and adjusted, and additions are made where needed. In particular, environment modeling and behavior specification will be refined. These areas are both important aspects of handling application complexity. Also, the support for variability and re-use will be amended. Variability of automotive system increases the complexity that engineers are facing and is a major threat to safety and reliability.

EAST-ADL2.0 will be formalized through the definition of a UML2 (Unified Modeling Language) profile. This profile will take into account the new Object Management Group standard for real-time and embedded systems called MARTE (Modeling and Analysis of Real-Time and Embedded systems) as well as the Society of Automotive Engineers' Architecture Analysis & Design Language, AADL.

The ATESST results will be validated through the implementation of a prototype tool based on the Eclipse framework and an automotive demonstrator. The demonstrator will contain safety-related functions, such as crash mitigation and speed moderation.

This Case study and demonstrator plan is the early definition of the scope of the demonstrator. This task will be refined throughout the project ending with the complete demonstrator in the end of the project.

2 Case Study and Demonstrator Plan

This document serves as input both for the case study and the demonstrator that will be used in the ATESST project. At the end of the project there will be a demonstrator that will serve as proof of concept for external stake-holders, demonstrating the capabilities of the EAST-ADL2.0. During the project the case study will also serve as a common example for all WPs. Along the project, WP6 validates proposed concepts by ensuring that the identified language needs are met in the context of this case study based on scenarios defined in D6.1.

Because ATESST targets the specific needs of safety applications, we have chosen some safety-related functions to be central in the case study. For this purpose, the example system includes a longitudinal distance control system with ACC, collision mitigation by braking, and a speed moderator that will be distributed over several ECU.

As well the crash mitigator as the speed moderator is considered as an active safety function, and the ACC is seen as a safety-related function.

2.1 Active Safety

The Crash Mitigator will become active if there is an obstacle (e.g. another vehicle) ahead of the car, and the driver at the same time is trying to brake, but not hard enough. To detect if there is an approaching obstacle ahead of the car, there is a radar sensor in the car detecting the longitudinal distance. Not to introduce more hazards, the Crash Mitigator will only become active if the driver has a foot on the brake pedal.

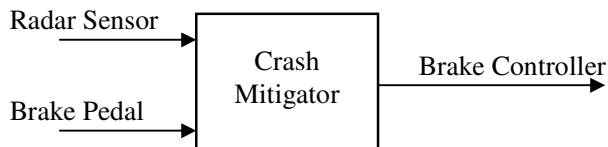


Figure 1 Crash Mitigator

The Speed Moderator will become active if it is raining and the driver, or the ACC, is trying to drive faster than what is considered safe with respect to the weather.

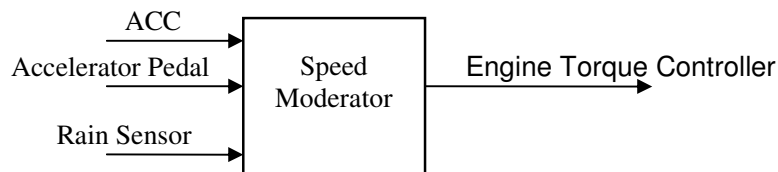


Figure 2 Speed Moderator

2.2 System Description

Given the active safety functions described above, and the safety-related function: ACC, the system studied is made complete by E/E functionality for the engine and braking systems. On the system border there will be environmental models, modelling such things as vehicle dynamics, driver behaviour, weather, and other cars.

The system model is depicted in a functional view in the figure below. In each functional block is also noted what ATESST partner that is responsible for the modelling.

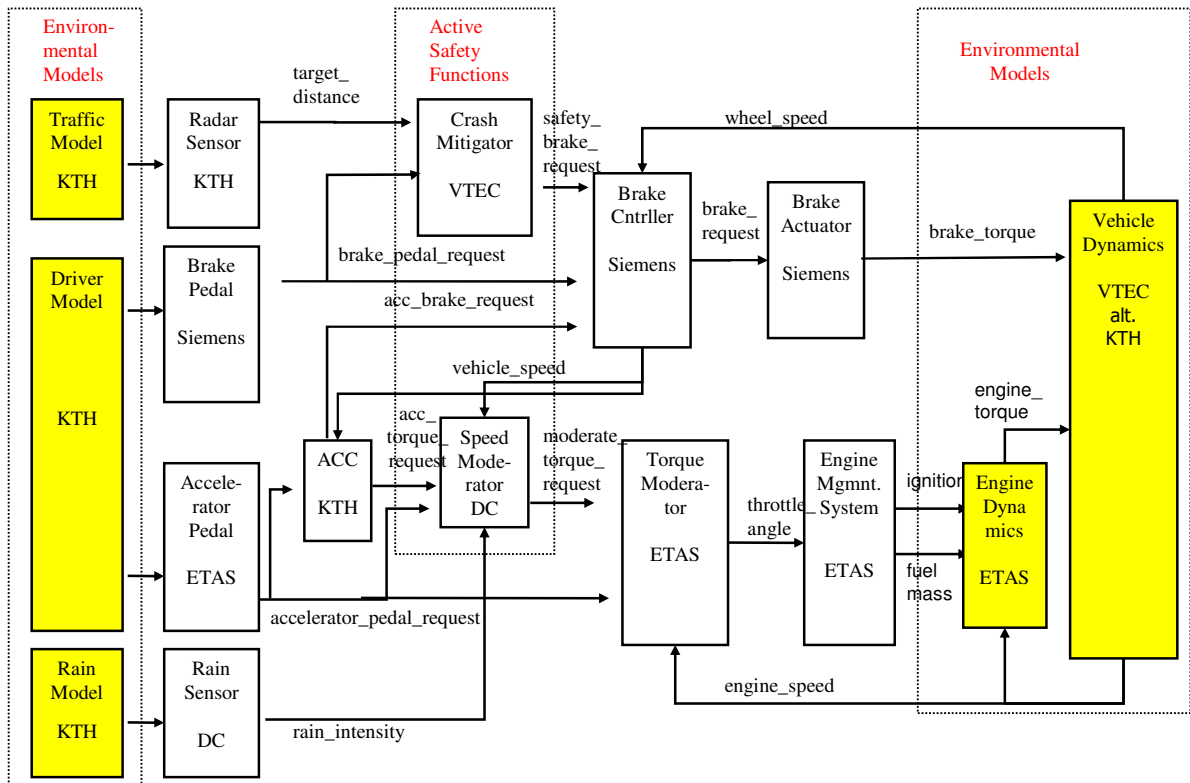


Figure 3 Demonstrator system, functional block view

2.3 Scenarios

The case study will be the target of the scenarios where these two safety-related functions are in focus. This has been initiated directly from the start of the project as a part of WT6.1 (see D6.1 documentation). It will then be refined throughout the project, serving as a case study also for WP2 through 5, and for dissemination purposes in WP7.

2.4 Realization Phases

The realisation of the example system into a case study for final demonstrator at the end of the project will be done in three main stages.

The first stage will be a description in Simulink of all functions (Figure 3). This is scheduled to be ready in July 2006, getting Simulink models executable.

Starting with EAST-ADL modeller available in July 2006, the second stage will then be to do initial EAST-ADL2.0 models with Intermediate profile defined in M2, scheduled to be finalized in November 2006. Integration of initial models into hardware into a physical view (Figure 4) will be targeted starting in December 2006. In parallel dedicated scenarios for final demonstrator purpose will be fixed to target dissemination material as demonstration show.

Finally, case study will extended to support ADL language improvements and dedicated extension of development environment based on an iterative scenario. First release based on advanced profile defined in M3 will integrate evaluation of requirement plug-in for March 2007. Then case study will be refined for adaptation versus behaviour and variability, compliant to modelling environment with dedicated plug-ins in June 2007. Finally, final profile defined for October 2007 for M4, will serve as final update of the case study and experimentation of ATESSST methodology. During this period iterative exchange and improvement of tool environment and case study versus initial ADL requirement of dedicated WP2 – 3 – 4 will be preformed based on milestones defined up (3 month period for major iteration loop).

During all these evolutions, ADL requirements for all WP will be stored in D6.3.3 report document in order to capitalize information and exchange, for final summary report.

Final demonstrator material with hardware allocation, demonstration scenarios and physical view, will be capitalization of case study versus WP2-3-4 methodology assessment, will be completed for November 2007 based on case study and final profile definition.

2.5 Physical View

In the picture below is shown one possible way to build the demonstrator.

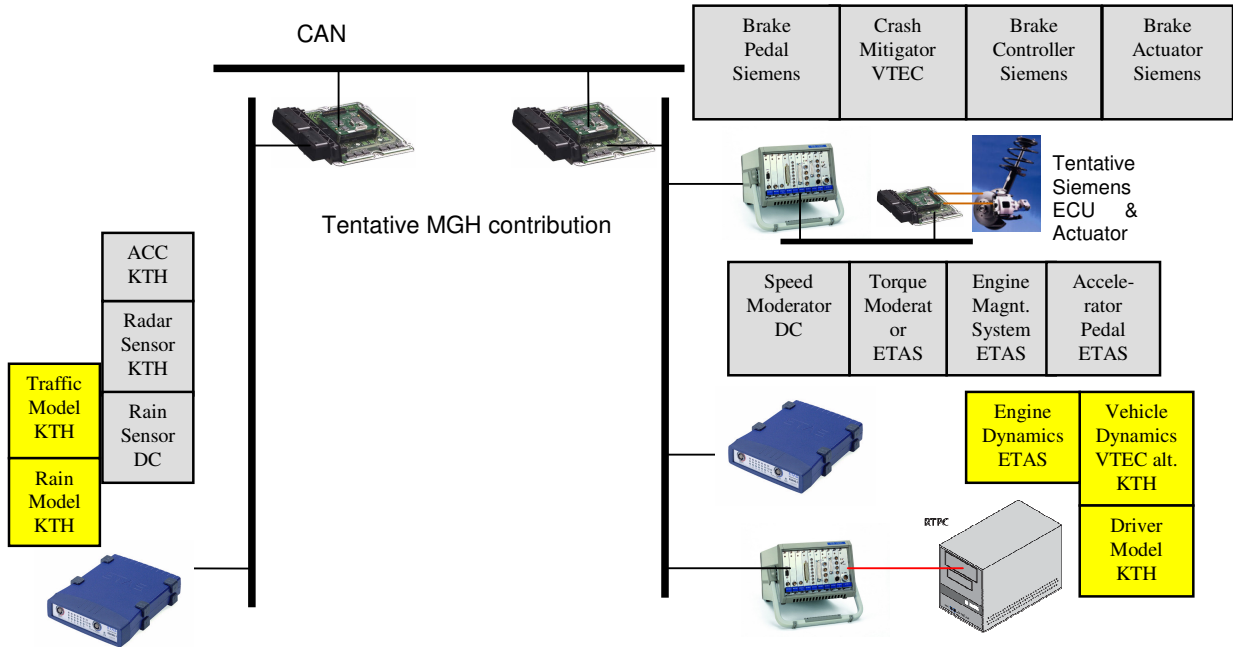


Figure 4 Demonstrator system, physical block view.

In this demonstrator suggestion, physical ECUs will be emulated by ECU emulators (ES900) from ETAS. There are a number of CAN bus segments representing different busses in a car. The definition of the physical realization definition will be refined during the following phases of the project, when the Simulink and EAST ADL2.0 models are fulfilled.

2.6 Options

Tentatively to support case study extension and dissemination material a potential material could be a model truck called SAINT. SAINT is a small national project where KTH collaborates with Scania and ENEA. The purpose of the project is to evaluate a range of measures to improve the modularity and configurability of an automotive embedded system. Another purpose is to develop a demonstrator useful for further research in the area of automotive embedded systems. The currently ongoing project will end June 1st, 2006.

There are several advantages that make the SAINT platform interesting for use in the ATESST project:

- The results are fully open

- The system is fairly complete in terms of a demonstrator and exposes most of the behaviors, structures and issues of interest to model in the EAST-ADL2.0.
- The project will end mid 2006, this is a good timing.

However there are also certain obstacles as follows:

- It is not now fully clear how ready developed various parts of the demonstrator will be in June 2006, e.g. how fully fledged and operational the advanced functions will be.
- Although many features are inherent in the SAINT demonstrator, not all of them have been explored or documented. For example, no safety analysis has been performed, and the existing models will mainly be limited to Simulink functionality models, word documentation, an information model in a PDM system, some UML-models and C-code.

Nevertheless, the SAINT platform might be very interesting and could tentatively be used as a partial case study or demonstrator within ATESSST, for example to model and evaluate aspects of the EAST-ADL2.0 with respect to safety analysis, variability and V&V issues.

3 Contribution to overall ATESST objectives

This Case study and demonstrator plan is the early definition of the scope of the demonstrator. This task will be refined throughout the project ending with the complete demonstrator in the end of the project.