



RISE
IST-2001-38117
Reliable Innovative Software for
Embedded Systems

Final Report

Report Version: Deliverable D0.2

Report Preparation Date: 4 February 2005

Contract Start Date: 1 August 2002 **Duration:** 31 months

Project Coordinator: Esterel Technologies S. A.

Partners: Audi AG - D,
TTTech Computertechnik AG - A,
Universite Joseph Fourier - F,
Centre National de la Recherche Scientifique - F,
Insitut National Polytechnique de Grenoble - F



Project funded by the European
Community under the
"Information Society Technology"
Programme (1998-2002)

Table of Contents

1. Executive summary	5
1.1. Original research objectives	5
1.2. Deliverables.....	6
1.3. Methodology and Guidelines.....	7
1.4. Demonstrator.....	7
1.5. Theoretical Support.....	8
2. Technical activities.....	9
2.1. Introduction	9
2.2. WP1 - Concepts and methods.....	9
2.2.1. Requirements	9
2.2.2. Training	9
2.2.3. Time and event mix	9
2.2.4. Methodology.....	11
2.3. WP2 – Tools.....	12
2.3.1. Simulink Gateway improvements	12
2.3.2. Translating imperative features of Simulink into SCADE/Lustre.....	13
2.3.3. SCADE – TTP toolset	14
2.3.4. Middleware.....	15
2.3.5. Code generation - Fixed-point data handling in implementation	15
2.3.6. Integration.....	16
2.4. WP3 – Experimentation.....	16
3. Publications and conferences.....	19
3.1. Main RISE dissemination events	19
3.2. Publications.....	21
3.3. Participation in Workshop and Conferences.....	23
3.4. MSc and PhD-Thesis	24
4. Deliverables	25
4.1. D1.1: User requirements definition.....	26
4.2. D1.2.1 and D1.2.2: Report on mixing time and events theory	26
4.3. D1.3.1 and D1.3.2 : Methodology for the design of software embedded on cars	27
4.4. D2.1 and D2.1.2 : Specification of the toolset.....	28
4.5. D2.3.1 and D2.3.2: Translating imperative features of Simulink into SCADE-Lustre.	28
4.6. D2.7 : Middleware.....	29
4.7. D3.1 : Evaluation outline report	30
4.8. D3.3 : Conclusion report.....	30

4.9. *RISE methodology and toolset demonstration*..... 31

5. Project Management33

5.1. *Management of the project*..... 33

5.2. *Meetings*..... 33

5.3. *Main risks* 34

6. Conclusion37

1. Executive summary

1.1. Original research objectives

The objective of the RISE project is to provide support for the development of embedded reactive software, in particular for cars, by developing:

- Concepts and methods for the developments of such embedded reactive software
- An integrated toolset supporting the concepts and the method, covering the analysis, design and development phases of such embedded reactive software.

It is based on synchronous techniques both for the development of the applicative software and for the middleware. Dependable real time systems are at the heart of planes and cars. Europe has shown a high ability to develop such systems both in the avionics and automotive industry. In order to keep the technological leadership in this important field of advanced distributed and embedded systems in Europe, it is necessary to remain proactive and to develop the next generation of real time systems, combining dependability constraints similar to avionics, with low costs mandated by the car industry.

Three levels of architecture are required for the deployment of such systems:

- A safe communication **infrastructure**
- Safe **computers**, on top of the infrastructure
- Safe **applicative software**, embedded in those computers

The synchronous paradigm is the best-known approach to build reliable, deterministic systems. In this project, the synchronous paradigm is used both for the communication infrastructure and the applications running in the computing units:

- For the specification and implementation of the **applicative** software, the Lustre/SCADE language, based on the synchronous paradigm has proven to be efficient for safety critical systems. Lustre/SCADE is being used extensively by the aeronautics industry to develop high-dependability software for flight control and other applications. It was the role of the RISE project to answer the specific needs of the automotive industry.
- For the communication **infrastructure**, the Time-Triggered Architecture (TTA) is suited to high-dependability distributed systems. TTA is based on the synchronous paradigm, where an autonomous communication subsystem establishes a fault-tolerant global time base and exchanges autonomously and predictably the information among nodes that are connected to replicated communication channels. The foundations of this infrastructure were addressed in the “Next TTA” project.

RISE is complementary of the previous “Next TTA” IST project:

- Next TTA focused on the communication infrastructure (hardware and middleware)

RISE focuses on the development of the application software in the Computing Units, on top of the middleware

1.2. Deliverables

Besides the general goals agreed upon between the project partners, the construction of seamless workflows, the creations of guidelines and the test of these workflows and guidelines in concrete automotive projects resulted in the following deliverables:

Seamless Interface between Prototyping/Model Simulation and Software Development

A seamless flow between Model Simulation/Rapid Prototyping tools and Software Development Tools is needed:

- A typical tool for Model Simulation/Rapid Prototyping is MatLab/Simulink™ and Stateflow™ from TheMathWorks. It is widely used for physical environment modeling, simulation and visualization.
- A typical model-based software development tool is SCADE from Esterel Technologies. SCADE is widely used for graphical software development, software simulation, formal verification (via property checking) and automated code generation.

An objective of the RISE project was the development and enhancement of an interface allowing the direct transfer of high-level requirements modeled with SimuLink/Stateflow™ into an extended SCADE toolset so that safe software can be developed and verified in a cost-effective manner. This guarantees a seamless workflow from physical modeling to production of safe and high quality code. The components of the SCADE toolset include:

- Effective translation from Simulink/Stateflow™ to the SCADE language
- Efficient and partially automated implementation of SCADE models onto target architecture that may rely on fixed-point arithmetic (in the case a floating-point unit is ruled out for cost reasons)
- Guidelines to model preemptive scheduling, and generate corresponding code, to support in a safe way the mix of event and time triggered application tasks
- Formal Verification of the (implemented) SCADE model in order to statically check safety properties of the application software
- Safe C code generation from the implemented model. (Although certification is out of the scope of the RISE project, issues related the certification of the code generator with respect to the IEC 61508 standard have been considered as well.)
- Connection of the SCADE model to the initial description of the requirements through an interface to the DOORSTM product from Telelogic.
- Management of versions and configuration of the SCADE model through compliance to the Microsoft SCCITM standard interface for source control.

Seamless Interface between Network Management and Software Development

The usage of time-triggered protocols requires a detailed modeling of the complete network. Tools that enable precise network scheduling both on network and node level exists. Other tools that automatically adjust network drivers cooperate here. The tools TTP Plan and TTP Build from TTTech fulfill these tasks and are widely in use.

A key deliverable of the project is the development of an interface between SCADE and TTP Plan / TTP Build called TTP SCADE Link that guarantees a seamless workflow between network and application software development.

The RISE project with its focus on automotive use of the TTA included the development of new components for the TTA middleware and its configuring tools. The new components bring new solutions for the support of basic needs for event-triggered communication, diagnostic services and calibration in a time-triggered environment. The calibration tool TTP-Calibrate is already productized.

1.3. Methodology and Guidelines

Managing this complexity also requires a new methodology. This is the aim of the RISE Methodology document that provides guidelines for the development of distributed automotive applications software addressing the following phases:

- Design
- Formal verification
- Automatic code generation
- System integration.

The general concepts of the methodology are presented and they build upon a classical V-Model largely improved by the systematic use of Model-Based Development. Relation to the IEC 61508 standard is explained.

1.4. Demonstrator

During the RISE project a force feedback steering wheel was developed to demonstrate the results of other workpackages. The force feedback algorithm itself is determined to be safety critical and should therefore be developed close the methods recommended or even highly recommended for safety integrity level 3 of the IEC61508. These methods include the use of formal- and semi-formal methods if formal methods are not applicable. Therefore the algorithm was developed within a model driven process, which enforces the use of semi-formal methods at the beginning and the gets more and more formal by the use of guidelines and tools. At the end the formal prove of requirements can be shown with a method, which guarantees completeness. The demonstrator shows also how the integration into the development process of Audi can be performed. Therefore the demonstrator can also be seen as reference project for further integration activities. The demonstrator is already well known in Audi because it is shown on several internal events and international conferences.

Furthermore a second demonstrator was developed to show diagnosis as application for the middleware developed in the RISE project. The CAN emulation layer can be used to show, how the migration can be performed on ECU's, which are now communicating via CAN and in the future will exchange information via a time-triggered network.

Calibration is also a very important issue in the automotive industry and can be shown on the third demonstrator, which provides complete Steer by Wire technology including also the artificially generated feedback. This demonstrator was also shown on the AEV day in Audi.

1.5. Theoretical Support

The extensions of model-based development that are described above rely on strong theoretical background. The research work that was needed is also an output of the RISE project.

A study of the semantics issues that are raised in the translation from the semi-formal notation of Simulink and StateflowTM to the formal notation of Lustre/SCADE was needed. In particular, the translation from StateflowTM to Lustre was studied in depth leading to practical guidelines for the use of Stateflow diagrams within the RISE toolchain and a reference translator which can be used to verify Stateflow designs.

The role of pre-emption in a Lustre execution model to handle urgent events were formally studied. A general method for ensuring simulation accuracy was proposed and formally proven.

2. Technical activities

2.1. Introduction

The project is organized in work packages. Besides the “Management” workpackage (WP0), and the “Exploitation and Dissemination” workpackage (WP4), the technical work is decomposed into 3 workpackages, each leading to deliverables that report the work performed:

- WP1: “Concepts and methods”
- WP2: “Tools”
- WP3: “Experimentation”

The objectives and results reached in each of these work packages are detailed in this chapter.

2.2. WP1 - Concepts and methods

2.2.1. Requirements

During the first period of the project AUDI presented user requirements for the software development tool set. In particular, following the evaluation of the current Simulink Gateway (WP3 work), a precise list of required evolutions for this tool has been produced. Other requirements have also been identified for the code generation (MISRA compliance).

The requirements for the tool set are listed in deliverable D1.1 (detailed in 4.1). This document covers the requirements in the wide area of software development in the automotive industry. This includes the software development process, method and tools, which support the software development process. The User Requirements Document is an important input for the Concepts and Methods, which are developed in WP1, the tools, which are developed in WP2 and the Experimentation and Validation, which is run in WP3.

Since the “User requirement definition”, deliverable D1.1, Audi raised new requirements while pursuing the use of the tool set components available (Simulink Gateway, SCADE Code Generator, TTTech tools). The whole set of requirements is reported in the second version of the “Specification of toolset” deliverable with links to the tool evolutions done in WP2.

2.2.2. Training

Three persons from Esterel-Technologies attended a full TTA training by TTTech Computertechnik AG from 9th – 12th December 2002 in Vienna. The training consists of a 2 day seminar that gives an overview over the time triggered architecture and another 2 days of workshop.

A consulting day on SCADE tools has been run at AUDI’s site for AUDI and TTTech experts.

Two persons from TTTech attended a full SCADE training by Esterel Technologies from 19th – 21st August 2003 in Toulouse.

2.2.3. Time and event mix

Verimag studied how such systems could be modelled in Simulink and SCADE using triggered subsystems (with periodic triggers for the time-triggered case) and shown that

a pre-emptive strategy is required to successfully model the priorities implicit in the system being modelled.

In particular, we noted that event and time-triggered systems should be able to pre-empt each other depending on their relative priorities. This creates a difficult problem for the scheduling algorithm since, traditionally, mixed systems have been partitioned into separate event and time-triggered components. Hence we have reviewed the well-studied method of deadline monotonic scheduling which promises the capability of scheduling a mixed system such as we have described. We also reviewed a more recent model which has been used in the automotive industry and gives an iterative scheduling of mixed event and time-triggered system which is very similar to ours with the exception that time-triggered tasks must have higher priority than event-triggered tasks. Thus we conclude that scheduling mixed-priority time and event-triggered tasks should be possible at the expense of some slight pessimism in the scheduling.

We then studied the question of preserving the functional semantics of the translation process.

This is required to guarantee the fidelity of the simulation with respect to the executing program generated from it. This is couched in terms of the Caspi-Halbwachs framework within which we can express both the ideal semantics of the simulation and the real-time semantics of the execution making some assumptions about temporal ordering of events. We showed how unit delays can be used to preserve this ordering and illustrate how problems with pre-emption could be solved using a multiple buffering mechanism. A quite complete proof of this mechanism has been provided.

The real-time operating system is intended to conform to the OSEK standards which include a pre-emptive operating system OSEKVDX suitable for event-driven execution and a time-triggered variant OSEKTIME which executes under more rigorous constraints. The two can coexist but only with the event-triggered system executing within the time-triggered system's idle time. This creates a problem for our system but we point out that urgent events could be modelled as interrupts within the OSEKTIME system. This is not currently supported by the OSEKTIME standard, however.

Demonstration of the way pre-emptive scheduling can be done from SCADE without losing the synchronous properties is the main result from the study Verimag performed. This breakthrough in linking theory and practice has been presented at the 1st review, reported it in deliverable D1.2.2, second version of "Report on mixing time and events theory" (detailed in 4.2), and published at ECRTS04 conference (reference in 3.2).

Esterel Technologies applied the result on the pre-emptive scheduling modelling in an extension of the SCADE toolset. The technical details on the mapping of SCADE nodes onto OSEK task are reported in the deliverable D2.1 "Specification of the toolset" (detailed in 4.4). This specification has been fully implemented, including the generation of the OIL file for the configuration of the OSEK OS.

2.2.4. Methodology

The RISE methodology that underlines all the studies and tool development performed through the project has been explained in a comprehensive report, deliverable D1.3 “Methodology for the design of embedded software in cars” (detailed in 4.3). The effort invested in that work lead to high quality material that will be exploited by marketing teams from the tool providers.

The software development methodology mainly introduces three phases:

- *System Engineering*, a phase where system engineers and architects write and design the system requirements. Control laws and algorithms may be studied using a tool such as Simulink.
- *SCADE Software Specification*, a first software engineering phase where the SCADE tool is used as the basis for describing a software model, gathering various pieces from Simulink descriptions, together with the specification of the distribution of this model, either onto several OSEK tasks or on a TTA architecture.
- *SCADE Software Implementation*, a phase where the initial SCADE model is implemented using fixed-point data, in order to ensure the required efficiency on current processors used in the automotive domain. The code is finally generated either onto several OSEK tasks or onto the processors of a TTA cluster.

In this phase, code can be generated using either the standard SCADE code generator (CG) or the qualified code generator (KCG), whose qualification with respect to the IEC 61508 SIL 4 regulations is under way with TUV. Although this qualification is outside the scope of the RISE project, it heavily contributes to the efficiency of the proposed RISE methodology.

The following figure pictures the RISE methodology.

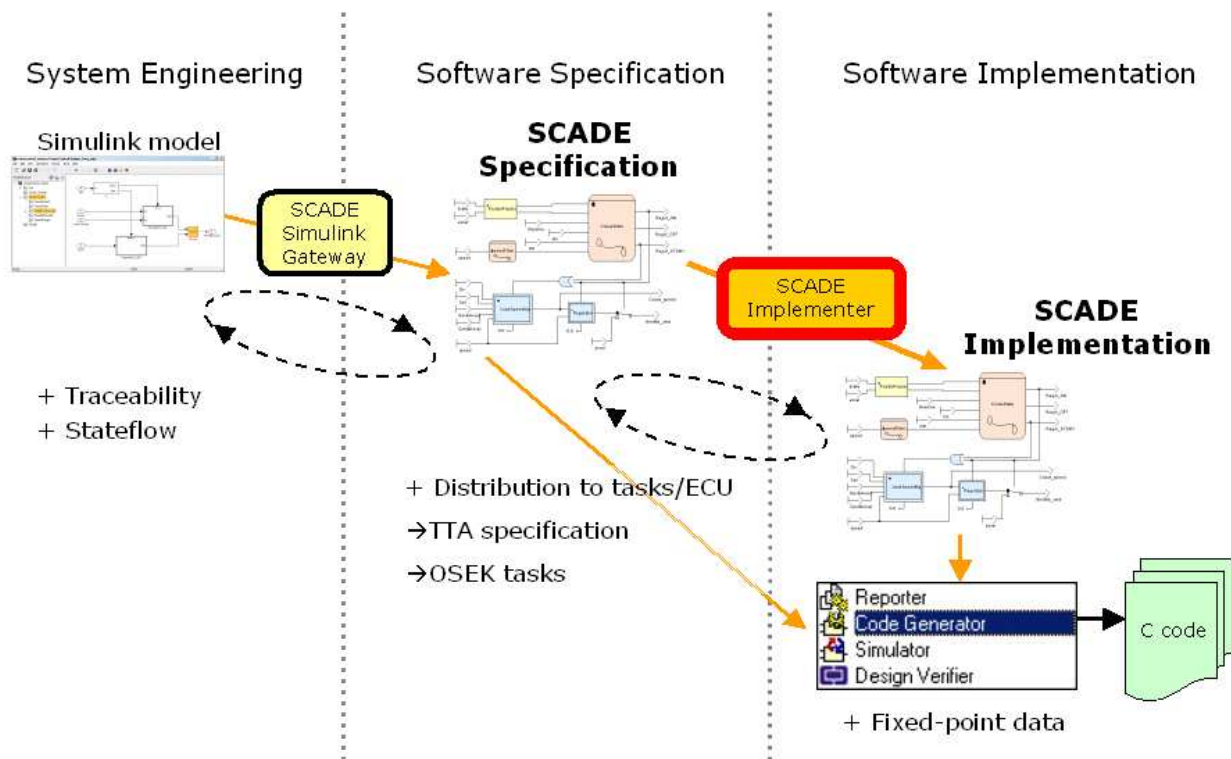


Figure 1: The phases in the RISE software development methodology

2.3. WP2 – Tools

The SCADA tools that have been enhanced or newly developed will all be all integrated in a single delivery for the partners in November 2004, so 2 months before the end of the project. This package contains:

- Simulink Gateway
- Stateflow to SCADA importer,
- OSEK coupling
- SCADA - TTA coupling tool
- SCADA implementer

The evolutions of the tools will be pursued before the end the project in the way described below:

2.3.1. Simulink Gateway improvements

At the RISE project launch, a first version of the Simulink to SCADA translator provided by Esterel technologies was evaluated carefully by AUDI. The outcome of the evaluation was that several evolutions are required for convenient usage and for the generation of an efficient SCADA model.

Several evolutions have been implemented to make the tool usable on automotive industrial models:

- Better type inference,
- Better translation of Matlab variables,

- Support for latest version of Simulink,
- Support of user libraries.
- Configurable level of each message raised by Simulink Gateway,
- Error reporting in Simulink editor,
- Translation of incomplete model,
- Improvement of the translation of triggered subsystems to ease formal proofs,
- Translation of new Simulink control blocks If, Switch Case, Action Subsystems, and Merge blocks
- Translation of the Simulink Fcn block into SCADE textual node in order to allow formal verification
- Increase of the configurability of the mapping rules by allowing expression as parameter for the SCADE nodes
- Use of the Simulink wires name to name the corresponding SCADE local variables,
- Improvement of the ergonomics of the GUI.
- “Traceability information generation”: for the model-based methodology we enforce, it is important that the SCADE model generated by Simulink Gateway is very traceable w.r.t. the Simulink model. The evolution consists in generating a textual file that exhibits a fine grain traceability between each SCADE objects (nodes, I/Os, constants, etc.) and the Simulink block it corresponds to. The first use of this information is a direct graphical locate feature from any SCADE object selected in SCADE editor to its correspondence in Simulink editor. This feature allows in a friendly way the process “Simulate in SCADE, Draw in Simulink” that is described in the methodology report, deliverable D1.3 (detailed in 4.3).
- “White box co-simulation”: AUDI expressed as a strong requirement the capability of having both the Simulink and the SCADE simulator communicating and displaying simulation values dynamically for fine grain debugging of software SCADE models embedded into realistic environment modeled in Simulink. In the first version of the tool, only black box co-simulation was possible.
- Pick-up Matlab variable definitions directly from Matlab workspace as a work around of too complex M-file to compile,

The precise specification of these evolutions is detailed in the “Specification of toolset” deliverable.

2.3.2. Translating imperative features of Simulink into SCADE/Lustre

The deep study by Verimag of Stateflow, the finite state machine system description integrated with Simulink, showed the difficulties of translating this formalism into the well defined synchronous languages we’re interested in (Lustre, SCADE, SSM). This work has been reported in deliverable D2.3.1 “Translating imperative features of Simulink into Scade-Lustre (V1)” (detailed in 4.5), and presented at the 1st review.

Despite the inherent difficulty of the task, the user requirement from AUDI in providing a solution, even if only partial, is very strong because of legacy Stateflow models. So the work has been pursued in two complementary directions, both reported during the 2nd review:

- Verimag has worked on an incremental translation of Stateflow to LUSTRE. The idea is to provide a "semantic by translation" for Stateflow. This translation starts from a very simple subset of Stateflow and will go increasing according to the growth of potentialities for static analysis of Stateflow designs. A prototype has been developed to demonstrate this approach.
- Esterel Technologies proposed a "translation assistant" that translates a Stateflow graphics into another graphics that looks similar, the Safe State Machine. The idea is to provide a faithful translation for the "safe" subset of Stateflow, a partial helpful translation for the "unsafe" subset. The development of a prototype based on this idea has been done during the 4th semester period. It has been demonstrated as part of the complete demonstration of the toolset during the 3rd EC review.

Both works are reported in deliverable D2.3.2 "Translating imperative features of Simulink into Scade-Lustre (V2)" (detailed in 4.5). One very interesting aspect of the two approaches is that they can be used together to obtain an exact and safe SSM model from a Stateflow design: the translation assistant generates an incomplete, graphical, SSM that is completed "by hand" by the user. The semantic translator provides a reference of the behavior in SCADE-Lustre. SCADE Design Verifier can be used to prove that the two models are equivalent, simply by connecting together the corresponding inputs of the models, and the corresponding outputs to equality operators.

2.3.3. SCADE – TTP toolset

TTTech and Esterel-Technologies strongly cooperated in developing a coupling solution for SCADE and TTA. The result of that design is detailed in the "Specification of the toolset" document, deliverable D2.1 (detailed in 4.4). Large effort has been spent on development of the solution, with integrated GUI in SCADE editor for the mapping of SCADE nodes onto hosts, launching of TTTech tools from SCADE editor, exchanging architecture description as a XML file between the tools, and generating glue code that "connects" the code generated by SCADE Code generator on one hand to the code generated by TTPbuild on the other hand.

The prototype developed has been first demonstrated on a toy example during the 2nd review in Bruxelles, and is been used successfully by AUDI on the version of the Force Feedback demonstrator.

One task remains: design and extend the tools to generate the global synchronous model that includes all the functional units of the SCADE-TTA design. This subject has been studied in technical meetings with Esterel Technologies, TTTech and Verimag. We are pretty confident that this is feasible, but did not had time to actually develop a tool for that. Esterel Technologies and TTTech will pursue their cooperation to make this breakthrough as a follow-up of the RISE project. The DECOS IST project, which goal is wider than the RISE objective, but in which both SCADE and TTA are core tools, offers the opportunity to reach this goal.

2.3.4. Middleware

At the review meeting in Brussels it was agreed upon that a separate deliverable should summarize the middleware activities at TTTech. The report D2.7 "RISE Middleware Development" (detailed in 4.6) was finished within this reporting period.

In the last reporting period the work focused on the integration of the middleware prototype components into the Audi demonstrator and on the integration of components into the configuration tools for the middleware.

On behalf of Audi the setup of the prototype shown at the final meeting changes: additionally to the Force Feed Back actuator from Audi a complete Steer-by-Wire prototype setup will be shown. Due to hardware incompatibilities between the two setups on the level of the physical layer and due to different network topologies -bus versa star- the diagnostic prototype application had to be modified. In order to allow a convenient work-flow configurable I/O blocks from the TTTech I/O driver libraries for Matlab/Simulink had to be migrated to the SCADE environment.

The ASAM2 parser for the calibration was adapted. At the final review a standalone tool developed will be used as user interface for the calibration. The idea to integrate calibration directly into the SCADE environment as it was realized with TTP-Calibrate into the Matlab/Simulink environment was dropped due to the necessary maintenance effort of such an interface. It is planned to integrate calibration after the end of the RISE project with the Tool TTP-View. This avoids the development of two very similar graphical display tools.

The knowledge gained during the development of the configuration tool extensions for the RISE project for TTP-Plan and TTP-Build have been used to start the development of a single solution that can be used both for the SCADE and the Matlab/Simulink integration. This work will be finished after the end of the RISE project.

The concepts developed for the CAN Emulator in the RISE project and its efficiency have already risen interest for the development of CAN emulation for other time-triggered networks. The CAN Emulator is a very important step for the migration of existing CAN based solutions to a time-triggered environment.

2.3.5. Code generation - Fixed-point data handling in implementation

Following the requirement from AUDI to have generated code compliant with the MISRA rules, Esterel Technologies has undertaken a precise analysis of the code generated by SCADE Code Generator w.r.t. these rules. A detailed report on this conformance has then be written.

The main lack of the tool chain we propose for automotive embedded applications is the non-support of native fixed-point data handling. This is a key difference from the avionics applications SCADE has been used for where ECUs always have floating point unit. The solution developed by the competitors consists in a complex code generator that generates directly fixed-point code from an annotated Simulink model.

Following our model based methodology a step further, Esterel Technologies imagined a different solution that provides several advantages. Instead of adding complexity in the code generator that would have as consequence a more difficult certification process, we propose an intermediate model, the SCADE implementation model, which uses fixed-point data types for the data flows. Being a SCADE model, this implementation model allows simulation, and even formal verification taking into account the changes from floating point data (modelled as mathematical real numbers) to fixed-point data (modelled as a fixed size of bits).

Esterel Technologies has first developed a library of imported data types and operators (the libimplementation library) that allows users to transform the specification model into implementation models.

But for a true model based methodology (and also because this manual work is tedious), this manual process must be automatized. We have then developed a configurable tool, the SCADE “Implementer”, that can generate the SCADE implementation model from a specification model annotated by the user.

The solution and the implementer tool has been specified in the “Specification of the toolset” D2.1 deliverable (detailed in 4.4). The Implementer tool will be demonstrated during the final EC review.

Finally we have worked on the generation of information conforming to the ASAM2 standard for calibration activity, so that the demonstrator running SCADE code on TTA middleware can be calibrated during the final review.

2.3.6. Integration

The toolset set-up in the RISE project includes numerous components (all evolutions and new components described in deliverable D2.1 “Specification of the toolset”, detailed in 4.4). A very interesting outcome of the RISE project is that the tools developed by Esterel technologies and TTEch are well integrated, all accessible from the SCADE GUI. This includes the configuration and traceability management, so that all the steps of the RISE methodology detailed in deliverable D1.3 “Methodology for the design of embedded software in cars” (detailed in 4.3) are covered.

The complete methodology and all tools are experimented on a simple Cruise Control model. This experimentation is described step by step in a report “RISE methodology and toolset demonstration”.

2.4. WP3 – Experimentation

At the project launch AUDI experimented the first version of the Simulink Gateway product from Esterel Technologies in the first period. One important outcome was a refinement of the requirements on that tool to be usable on real Simulink designs from AUDI. These requirements serve as major inputs for the Simulink Gateway improvements.

Audi has started defined a prototype demonstrator for experimentation and validation activities. This prototype demonstrator includes an application, which is essential for the by Wire technology, a force feedback steering wheel functionality. This application is

safety critical and suitable for demonstration of the results, which are developed during this project.

The application prototype detailed in deliverable D3.2 “Prototype demonstrator based on simulation” is developed with Simulink and successfully translated into SCADE. The SCADE-TTA integration has been used on the model generated by the SCADE Simulink gateway. The demonstrator has been set up together with TTTech at Audi.

Audi had also looked for an appropriate pilot scheme to evaluate the Simulink Gateway enhancements, the Stateflow support and the fixed point implementation. For the Simulink Gateway there was a pilot scheme called data-path project, which generates requirements described in the User requirements document.

The force feedback algorithm does not require fixed-point arithmetic or Stateflow support up to now, but is appropriate to evaluate the Simulink Gateway and to investigate formal verification. There has also been several small case studies in Audi from different departments, which were used to demonstrate formal verification on a real model. Some demonstration has arisen new requirements for the Simulink Gateway, the Design Verifier and the Simulator, which were reported to Esterel. To evaluate the Stateflow Importer in detail there was started a common pilot scheme together with Volkswagen. Most parts of the model contain only Stateflow. This work is an ongoing task.

The fixed point implementer was presented several times in Audi and the feedback was very good. This was presented to different departments in Audi to collect the requirements on fixed point arithmetic. Most of these requirements were implemented and demonstrated to the same department. All the attending engineers were impressed how far these requirements have been implemented in a product in this short time. Also a look at the generated code have shown that there are great improvements.

The RISE toolset delivered with SCADE 5.0beta version has been evaluated corresponding to the user requirements.

Pilot schemes and case studies had been used to investigate the RISE methodology. Furthermore investigations had been made to facilitate the integration of the RISE methodology into the development process of Audi. This includes the development of modeling guidelines, requirement-templates and performance analyses.

With regard to methodology, which is also a very important part of this project, there has been started a working group for defining a new standard for a software development process for safety critical systems in the automotive industry. At the moment there is no appropriate standard development process for the automotive industry with regard to safety. There is one generic standard, the IEC61508, which is independent from the industry sector, but focuses on the plant construction industry. It is not possible to use these development guidelines one to one for the automotive industry, but it is possible to adjust this norm to the special needs of this industry. This tailoring characteristic is also addressed in the IEC61508 standard. This work is performed within two automotive working groups. One working group has the focus of the overall system safety (the car) and the second one has the focus on the software development process. Of course the

results of both working groups should complement each other. Audi is one partner in both working group.

With regard to experimentation it has been checked, if the methodology and tools, which are developed in this project, can be integrated in the software development process according to the part 3 of the IEC 61508 (the software part of the norm). The result is that the IEC 61508-3 recommends formal methods, but the tools, which are widespread in the automotive industry are not formal but only semi – formal. The evolving standard cannot require less than the original one. Therefore the developments done in the RISE project will have a lot of users in the future, not later than the new standard is released.

3. Publications and conferences

Dissemination of the technical activities performed in the RISE project have received particular attention.

Numerous papers have been published and the partners attended several conferences, all listed below. Moreover, RISE results have been presented specific industrial events, with potential customer audience.

A RISE web site has also been set-up to allow the non-direct contacts from the partners to be aware of the goals and results from the project:

www.esterel-technologies.com/rise

3.1. Main RISE dissemination events

The main events where the RISE project has been presented were:

- “TTTech Cross industry info day”, November 20, 2003 – Toulouse.
More than 50 attendees, most from large companies, attended to this workshop organized by TTTech. AUDI gave a presentation of the model based Workflow for AUDI. Esterel Technologies gave a presentation of the SCADE-TTA coupling.
- SAE world congress, March 2004 - Detroit, USA
Three presentations from TTTech and Esterel-Technologies showed results from the RISE project:
 - “Correct-By-Construction Methods for the Development of Safety-Critical Applications” by Bernard Dion – Esterel Technologies
 - “Supporting MBD with Unambiguous Specification, Formal Verification and Correct-by-Construction Embedded Software” by Jean-Marc Talbot – Esterel Technologies
 - "Virtual CAN Networks over TTP – Integrating Legacy Systems within the Time-Triggered-Architecture", Christian Eder – TTTech
- The milestone meeting within the Volkswagen and Audi electronic strategy at the 25th and 26th of September 2003. This was an event where a lot of high level managers and developers from Volkswagen and Audi could see the work.
- The AEV day, August 2004.
Presentation to AUDI’s manager and technicals teams of the RISE demonstrator



Figure 2: Posters and demonstrators, which were presented to the developers and managers of Audi

- The SCADE User Conference, May 2003 and October 2004, Toulouse. These events, organized by Esterel-Technologies are a very important marketing activity to promote the use of SCADE in industries.
 - TTech had a booth there where the SCADE-TTA integration was demonstrated.
 - AUDI gave a talk “Concepts, Methods & Tools for Software Development in the Automotive Industry“ at the first SCADE user conference,
 - Esterel Technologies gave a talk “RISE project” at the second one.
 - Verimag attended these events to have attention to the current expectations from SCADE industrial users.

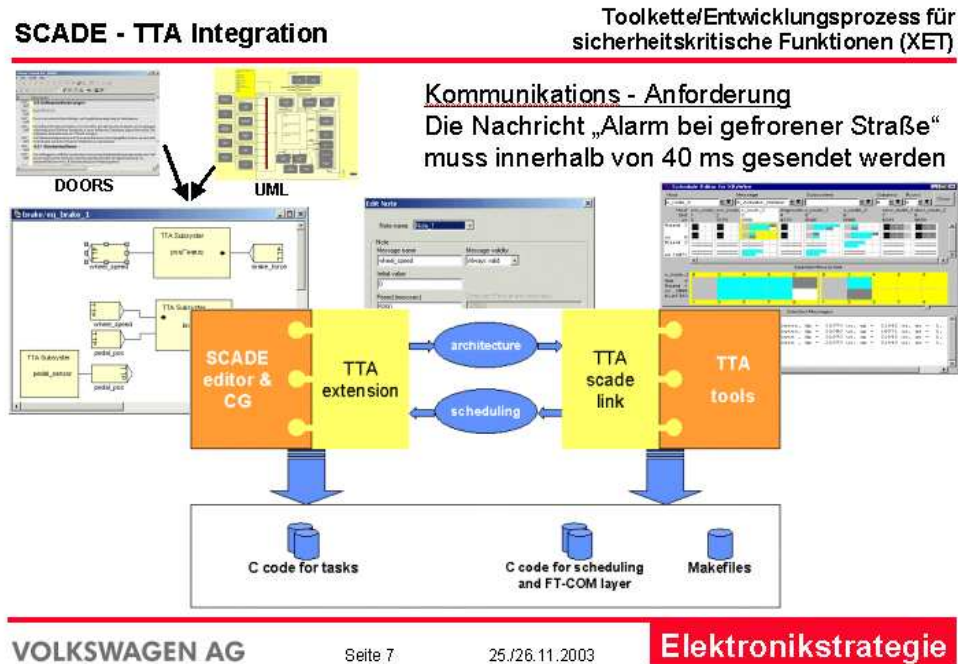


Figure 3: Slide, which was presented to the developers and managers of Volkswagen and Audi

3.2. Publications

- F. Maraninchi and Y. Rémond: “Mode-Automata: a new Domain-Specific Construct for the Development of Safe Critical Systems”, Science of Computer Programming (SCP), v. 46, 2003.
- K. Altisen, A. Clodic, F. Maraninchi and E. Rutten: “Using Controller Synthesis to Build Property-Enforcing Layers”, European Software and Programming Symposium, 2003.
- Paul Caspi and Albert Benveniste: “Toward an Approximation Theory for Computerised Control”, EMSOFT2002, v.2491 in LNCS, October 2002.
- Albert Benveniste, Paul Caspi *et al.*: “The synchronous languages, twelve years later” Proceedings of the IEEE, v 91(1), January 2003.
- M. Buhlmann. “Necessary software structures and process steps for development of distributed controls”. 3rd Dec. 2003, “Haus der Technik” (house of technique), Düsseldorf, Germany

- A. Benveniste, P. Caspi, P. Le Guernic, H. Marchand, J.P. Talpin and S. Tripakis
"A Protocol for Loosely Time-Triggered Architectures"
In Proc. EMSOFT 2002, Grenoble, France, Oct. 2002,
Springer, LNCS series, volume 2491.
- P. Caspi, A. Curic, A. Maignan, C. Sofronis, S. Tripakis and P. Niebert
"From Simulink to SCADE/Lustre to TTA: A Layered Approach for Distributed
Embedded Applications"
In Proc. LCTES 2003, San Diego, CA, June 2003
Published by ACM-SIGPLAN.
- Wolfram Hohmann
"Modellbasierter Entwurf und Formale Verifikation von Embedded Software"
Design and Verification, July 2003
Publishing Industry
- Krüger, D. Kant, M. Buhlmann.
"Software Development Process and Software-Components for X-by-Wire Systems".
Submitted to the SAE WorldCongress, March 2003, Detroit, USA.
- Christian Eder, "Virtual CAN Networks over TTP – Integrating
Legacy Systems within the Time-Triggered-Architecture",
SAE World Congress, Detroit, MI, USA, March 2004
- Martin Schwarz, Reinhard Maier, "Communication Platform
Requirements for Modular Avionics", 22nd Digital Avionics
Conference, Indianapolis, Indiana, USA, October 2003
- Georg Stöger, Andreas Krüger, Gerhard Könighofer,
"Network Management in time-triggered communication
systems", VDI, Baden-Baden, Germany, September 2003
- B. Hardung, M. Wernicke, G. Wagner, A. Krüger, F. Wolgemuth, "Entwicklungsprozess
für vernetzte Elektroniksysteme", VDI, Baden-Baden, Germany, September 2003
- P. Caspi, A. Curic, A. Maignan, C. Sofronis, S. Tripakis
"Translating Discrete-Time Simulink to Lustre"
EMSOFT'03, Philadelphia, October 2003.
Springer, LNCS series, volume 2855.
- S. Tripakis
"Folk theorems on the determinization and minimization of timed automata"
In FORMATS, September 2003
- M. Buhlmann, D. Kant, "Software-Entwicklungsprozess und Methoden für
sicherheitskritische Funktionen" 24th Conference Elektronik im Kraftfahrzeug in Haus der
Technik, Essen, Germany, June 2004

- N. SCAIFE and P. CASPI
"Integrating model-based design and preemptive scheduling in mixed time- and event-triggered systems"
ECRTS04, Catania, July 2004, IEEE Computer Society
- Bernard Dion, Thierry Le Sergent, Bruno Martin, Herbert Griebel
"Model-Based Development for Time-Triggered architectures"
23rd DASC (Digital Avionics Systems Conference), Salt Lake City, US, October 2004.
- N. Scaife, C. Sofronis, P. Caspi, S. Tripakis, and F. Maraninchi
"Defining and translating a "safe" subset of Simulink/Stateflow into Lustre",
4th ACM International Conference on Embedded Software (EMSOFT'04), Pisa,
September 2004.
- Andreas Koehler, Dietmar Kant
"Use of Formal Verification for the Software Development in the Automotive Area"
FORMS / FORMAT 2004, Formale Techniken für Automatisierungs- und
Sicherheitssysteme im Eisenbahn- und Automotivbereich Submitted at the 27th of
August 2004 to the Technical University of Braunschweig.

The following have not yet being published but are already accepted for publications:

- P. Caspi, A. Curic, A. Maignan, C. Sofronis, S. Tripakis
"Translating Discrete-Time Simulink to Lustre"
Accepted to ACM Transactions on Embedded Systems
- P.Caspi, O. Maler
"From Control Loops to Real-Time Programs"
in "Handbook of Networked and Embedded Control Systems" (D. Hristu and W.Levine
editors), Springer, 2005 (to appear)

3.3. Participation in Workshop and Conferences

In addition to the conferences where the listed above publications have been presented, the partners attended the following workshop:

- TTA-Group Forum, November 15, 2002, Munich, Germany
"Tools for safety critical systems" by E. Bantegnie – Esterel Technologies
Attended by Markus Buhlmann, Dietmar Kant.
- EMSOFT'02, October 2002
Attended by Jean-Louis Colaço – Esterel Technologies
- SAE World Congress 2003, Detroit, Michigan, 2003 (TTTech)

- “Tools and Algorithms for the Construction and Analysis of Systems”, ESOP'03, Warsaw, Poland, April 2003 (Verimag)
- ETAPS'04 (European Joint Conferences on Theory and Practice of Software), Barcelona, March 2004
- Artist2 Hard Real-Time meeting, Roma, January 2005
P. Caspi - Verimag

3.4. MSc and PhD-Thesis

The work performed for the RISE project has been mostly done by confirmed researchers and developers. One PhD student has started to work on the Stateflow to SCADE/Lustre translation at Verimag with Norman Scaife, but this PhD thesis will be finished only after the end of the RISE project.

4. Deliverables

The whole list of deliverables expected during the project is given in the following table. The table has been updated to be coherent with the 2nd review report deliverable table. The “Actual delivery date” column is updated at the end of each period. The “(demo)” information is for the prototype deliverables that are presented in the report “RISE methodology and toolset demonstration” delivered month 25. The “(P)” information means that the deliverable is a Prototype that is ready at the given month, but is not delivered because of its nature (software and hardware).

Del. no.	Deliverable name	Actual delivery date	Due to (proj. month)
D0.1.1	Periodic Progress Reports 1	7	7
D0.1.2	Periodic Progress Reports 2	14	13
D0.1.3	Periodic Progress Reports 3	20	19
D0.1.4	Periodic Progress Reports 4	25	25
D0.2	Final Report	31	30
D1.1	User requirements definition	11	9
D1.2.1	Report on mixing time and events theory V1	14	14
D1.2.2	Report on mixing time and events theory V2	25	23
D1.3.1	Methodology for the design of software embedded on cars V1	20	14
D1.3.2	Methodology for the design of software embedded on cars V2	31	30
D2.1	Specification of the toolset	13	12
D2.1.2	Specification of the toolset (added because D2.1 has been rejected)	20	20
D2.2.1	Framework tools V1	13	14
D2.2.2	Framework tools V2	25 (demo)	23
D2.3.1	Translating imperative features of Simulink into Scade-Lustre (V1)	13	14
D2.3.2	Translating imperative features of Simulink into Scade-Lustre (V2)	25	23
D2.3.3	Simulink to SCADE translator	25 (demo)	24
D2.4	Modelling toolset	25 (demo)	24
D2.5	Toolset for mapping function to architecture	25 (demo)	24
D2.6	Code generator	25 (demo)	24
D2.7	Integration layer with middleware	(P) 24	24
D3.1	Evaluation Outline report	13	14
D3.2	Prototype demonstrator based on simulation	(P) 23	23
D3.3	Conclusion Report	31	30
D4.1	Project Presentation	11	4
D4.2	DUP	11	6
D4.3	TIP V1		cancelled
D4.5	TIP V2	31	28
D4.5.x	Publications	31	15-30

Figure 4 : Deliverables table

The Main technical reports are summarised here; they are:

- D1.1: User requirements definition
- D1.2.1 and D1.2.2 : Report on mixing time and events theory
- D1.3.1 and D1.3.2 : Methodology for the design of software embedded on cars
- D2.1 : Specification of the toolset
- D2.3.1 and D2.3.2 : Translating imperative features of Simulink into Scade-Lustre
- D2.7 : RISE Middleware development
- D3.1 : Evaluation outline report.
- D3.3 : Conclusion report.

The prototype deliverables demonstrated during the reviews are:

- D2.2.2: Framework tools
- D2.3.3: Simulink to SCADE translator
- D2.4: Modelling toolset
- D2.5: Toolset for mapping function to architecture
- D2.6: Code generator

In order to demonstrate the way they are integrated to support the methodology detailed in D1.3 report, we have ran a complete demonstration using all these prototypes, and detailed this demonstration in a single report. This report, "RISE methodology and toolset demonstration", is also summarized below.

4.1. D1.1: User requirements definition

The user requirements were elicited during the first evaluation of the tools and several presentations of the goals of this project in Audi. Mainly two user groups had expressed their requirements. On the one side traditional C-programmer are the target group of the RISE methodology and on the other side the requirements from control engineers should be met by this methodology as well. To guarantee a broad acceptance several application domains have to be considered. For this purpose several pilot schemes have been performed to have the practical view on the real problems. From this point of view new requirements have been arisen and communicated to the project partners. Several discussions had revealed that several improvements have to be made not only on tool level but also on the process level.

4.2. D1.2.1 and D1.2.2: Report on mixing time and events theory

Model-based design is advocated as the method of choice when dealing with critical systems as well as high quality systems. However, it often abstracts implementation details such as execution times. This can be a problem when dealing with urgent events whose implementation requires pre-emptive scheduling.

We have studied how such systems could be modelled in Simulink and SCADE using triggered subsystems (with periodic triggers for the time-triggered case) and shown that a pre-emptive strategy is required to successfully model the priorities implicit in the system being modelled.

We have also designed an original inter-task communication mechanism on top of a fixed-priority deadline monotonic pre-emptive execution scheme, which preserves the ordering of computations validated in a "zero-time" synchronous framework such as provided by Simulink/Stateflow and SCADE/SSM modelling and simulation. This is required to guarantee the fidelity of the simulation with respect to the executing program generated from it. We show how unit delays can be used to preserve this ordering and illustrate how problems with pre-emption could be solved using a multiple buffering mechanism. This method also ensures deterministic executions which are considered a key feature of synchronous and time-triggered approaches.

The communication mechanism has been fully mathematically formalised and then model-checked using LUSTRE and the LESAR model-checker. This allows us to formally guarantee the correctness of the approach. Thanks to this formalisation, SCADE itself can be used to implement the protocol. However, a JAVA implementation and simulation are also provided can act as specifications for lower-level implementations (C for instance).

A preliminary SCADE implementation, restricted to pre-emptive multi-periodic systems has been described in RISE deliverable D.2.1. The event-triggered part is still to be prototyped.

4.3. D1.3.1 and D1.3.2 : Methodology for the design of software embedded on cars

This document defines the RISE methodology for the development of distributed automotive applications software addressing the following phases:

- Design,
- Formal verification,
- Automatic code generation,
- System integration.

The general concepts of the methodology are presented: it builds upon a classical V-Model largely improved by the systematic use of Model-Based Development. It is related to the IEC 61508 standards, including the safety-related aspects and the tool certification aspects of this standard.

The three main phases of the RISE methodology have been identified:

- *System Engineering*, a phase where the system requirements are designed. Control laws and algorithms may be studied using a tool such as Simulink™.
- *SCADE Software Specification*, a first Software Engineering phase where the SCADE tool is used as the basis for describing a software model, taking various pieces from Simulink™ descriptions, together with the specification of the distribution of this model, either onto several OSEK tasks or on a TTA architecture.
- *SCADE Software Implementation*, a phase where the initial SCADE model is implemented using Fixed-point data in order to ensure the required efficiency on current processors used in the automotive domain. Also, the code is generated either onto several OSEK tasks or onto the processors of a TTA cluster.

When dealing with these various steps of the methodology, the artifacts that are specifically produced are described and the consequences of the use of the RISE methodology on the various project roles (system architect, system safety manager, etc) are examined.

4.4. D2.1 and D2.1.2 : Specification of the toolset

The specification of the toolset report is based on the description of User requirements (deliverable D1.1) and on the RISE Methodology (deliverable D1.3). This document only describes the new tools that have been created in the course of the RISE project, like the SCADE TTA coupling or the StateflowTM to SSM translator, and the major evolutions of the various tools that are necessary so that the RISE methodology can be used, like the evolutions of the SimulinkTM to SCADE gateway.

The RISE toolset relies on:

- The SimulinkTM to SCADE gateway to import SimulinkTM block diagrams into SCADE, while warning the users of all the constructs that have to be fixed so that a safe software implementation can be obtained.
- The StateflowTM to SSM translator to convert StateflowTM state machines into the Safe State Machines of SCADE.
- The SCADE OSEK coupling to distribute SCADE generated code onto several OSEK tasks
- The SCADE TTA coupling to distribute SCADE generated code onto a TTA architecture.
- The TTA middleware to make this distribution efficient.
- The SCADE Implementer to automate the efficient implementation of a Fixed-point SCADE model onto a processor having integer arithmetic only.
- The SCADE Code Generator to produce MISRA compliant C code from the implemented SCADE model.

4.5. D2.3.1 and D2.3.2: Translating imperative features of Simulink into SCADE-Lustre

The semantics of Simulink and STATEFLOW are defined by their only implementations and they have no formal definition. SCADE and LUSTRE have very similar semantics and are formally defined. The lack of a formal semantics for Simulink and Stateflow means that we are obliged to describe the translation process in anecdotal terms only.

Previous work in this area includes translators from Simulink into SCADE and LUSTRE and we give an overview of these systems.

We mainly studied Stateflow, the finitestate machine system which is implemented under Simulink.

The Stateflow interpretation algorithm was studied since this embodies the semantics and we then point out, by a brief enumeration of various cases, some of the problems with translating this into SCADE/LUSTRE, in particular the influence of graphical layout upon the system's behavior. Esterel technologies have recently produced their own

finite state machine system called Safe State Machines (SSM) based upon the semantics of the ESTEREL language which already addresses many of these problems so we reviewed the current state of this system.

We also compared SSM with Stateflow with a view to defining a safe subset of Stateflow which we can target for translation.

Initially, this may look very similar to SSM but we would like to extend the range of features which can be handled. Finally, we outlined this subset. Since it is not possible to formally define Stateflow itself we described the subset by a short set of tests for which, if all these tests are passed, then the Stateflow model conforms to our subset. We briefly studied the choice of source and target systems which is not straightforward given multiple routes for the same translation system.

We have developed a translator from Stateflow to LUSTRE. The idea was to provide a "semantic by translation" for Stateflow. Originally, the translator was thought of as very simple and incremental. Instead, the translator we designed is quite powerful: it can even translate unbounded STATEFLOW diagrams, provided a bound on the stack is given by the user. There can be several uses of this translator:

- As a code generator
- To provide Stateflow with a formal semantic
- To check the correctness of semi-automatic Stateflow to SSM translation
- To model-check several desirable properties of a diagram, confluence and insensitivity to graphical ordering, stack boundedness, ...

More examples of these uses have already been provided, using the LESAR model-checker.

Esterel technologies has developed a tool framework to help translating graphically Stateflow charts into SSM. The tool framework is integrated in the SCADE development environment. The aim of the framework is two-fold:

- Warn the user about the presence of unsafe constructs
- Provide the designer with a partial SSM that reproduces a large part of the Stateflow into SSM leaving some finishing work for the designer.

The finishing work consists mainly in rewriting the Stateflow state and transition action expressions into the SSM action language syntax, and in performing the addition modeling to change the unsafe constructs according to the system requirements.

4.6. D2.7 : Middleware

Concepts and a prototype implementation for event-triggered communication over TTP shall be developed.

The event-triggered communication layer shall be compatible to the HIS (Hersteller Initiative Software) standard for CAN API.

Concepts and a prototype implementation for calibration in a time-triggered automotive network shall be developed.

The calibration system shall be compatible with the ASAM 2 standard.

Concepts for the integration and a prototype shall be developed for the integration of automotive diagnosis in a time-triggered network.

The prototype shall integrate a diagnostic service according to the ISO 14229-1 (KWP 2000).

The transport protocol for the prototype shall be according to Volkswagen group standard TP 2.0.

The middleware shall offer support for urgent events.

The middleware shall support SCADE data types as messages.

The middleware configuration tools shall support a convenient prototyping environment.

4.7. D3.1 : Evaluation outline report

The Evaluation outline report describes how to proceed with the evaluation. Firstly the evaluation has proceeded with the investigation which requirements imposed by the users are fulfilled by the SCADE suite 5.0 beta2 release. To get a broad user acceptance of the RISE methodology existing tools had to be applied on pilot schemes and case studies. This step should reveal further bottlenecks and gaps of today's development processes as well as on the applied tools. Thirdly the integration of the methodology in the development process of Audi had to be evaluated. This included also the development of modelling guidelines, templates for the specification of formal requirement and performance analysis of the verification tool. At the last step of evaluation the results of the other workpackages had to be applied to the demonstrators developed in the context of the RISE project.

4.8. D3.3 : Conclusion report

The conclusion reports gives a detailed overview of the requirements described in the User Requirements Document and how they are satisfied by the released tools. Furthermore the evaluation results w. r. t. the integration of the RISE methodology into the development process of Audi is described. This includes the description of some rules of the modelling guidelines, templates for the specification of formal requirement and results of the performance analysis of the verification tool. For the purpose of integration of the RISE methodology into the development process of Audi pilot schemes and case studies had brought also a lot of useful information and are therefore also described in this report. It can be seen, what changes if the RISE methodology is applied instead of traditional development. The advantages are clearly emphasised as well as the problems, which occurs during the evaluation. The results of applying the RISE methodology to the demonstrator are described at the end of this report.

4.9. RISE methodology and toolset demonstration

This report is a step-by-step demonstration following the methodology detailed in report “Methodology for the design of software embedded on cars”. The model used is a simple Cruise control application for a car. Each step is illustrated with screen copies of the tools used:

- MS-Word, DOORS, and Simulink for the requirements,
- Simulink Gateway,
- Stateflow to SCADE importer,
- SCADE-DOORS gateway,
- SCADE-SCCI gateway for configuration management,
- SCADE simulator and design verifier,
- SCADE-OSEK coupling,
- SCADE-TTA coupling,
- SCADE implementer and code generator.

5. Project Management

5.1. Management of the project

No management difficulty arose during the project; the working atmosphere was friendly, the plan has been followed, and the results reached, and even overstepped, the expectations the partners had on the project.

All partners have signed a consortium agreement, late in the project, but before the end of it (last semester).

5.2. Meetings

Several meetings have been hosted by all partners during the whole duration of the project. Technical meetings with two or three partners for active brainstorming on specific topics, plenary meetings where all partners discussed the progress made and actions to pursue, and four reviews with the project officer and the reviewers.

The main meetings held are listed below.

First 12 months period (August 2002 – July 2003)

The following meetings have been held:

- The Kick off meeting in Toulouse on 26th and 27th of September 2002.
- Join NextTTA – RISE technical meeting, AUDI 21st November 2002
- 2nd Plenary meeting Ingolstadt on 15th and 16th of January 2003.
- Technical meeting on configuration and traceability management with SCADE Suite, in Munich on the 20th of March 2003
- 3rd Plenary meeting Toulouse on 21st of May 2003.
- The 1st EC review, in Brussels on the 3rd of June 2003.

Second 12 months period (August 2003 – July 2004)

The following meetings have been held:

- August 2003 – Toulouse, TTTech and Esterel Technologies
 - o 19-21 : TTTech SCADE training
 - o 22 : SCADE-TTA brainstorming
- 4th Plenary meeting, October 2, 2003 – Vienna
- 5th Plenary meeting, January 30, 2004 – Grenoble
- 2nd EC review, in Brussels on the 18th of February 2004

Last 7 months period (August 2004 – February 2005)

The following meetings have been held:

- 9 September 2004 – Toulouse, TTTech, Verimag and Esterel Technologies for a technical meeting
- 6th Plenary meeting, September 10, 2004 – Toulouse
- 3rd EC review, in Brussels on the 22nd of September 2004
- Several technical meetings to set up the demonstrator – Ingolstadt and Pfaffenhofen, August 2004, January and February 2005,
- 4th EC review, in Ingolstadt on the 28th of February 2005

5.3. Main risks

The reviewers have pointed out during the second review several risks for the success of the RISE project. We list them here, and explain how they have been handled.

1) Ambitious toolset

The amount of subjects to study, and tools to build and integrate to provide a complete toolset for the development of safety critical embedded software in cars is high. There is a risk of not finishing the work in the RISE timeframe.

The possible exploitation of the results of the project are very important for all partners, user, tool providers, and academic. This makes the motivation and involvement of the partners in the project very high. This is a key in the success of the project. The others keys to fulfil this ambition are:

- Focus on the needs of the user AUDI, in order to define solutions to real difficulties and not to hypothetical problems,
- Rely on the technologies provided by TTTech and Esterel Technologies that have already been proven to have good qualities in this area,
- Strong cooperation between the tool providers and the academic partner Verimag to tackle the most difficult points (pre-emptive scheduling, Stateflow semantics).

Esterel Technologies in particular has invested a large effort during the second year of the project in order to meet the expectations from SCADE tools before the end of the project. This result in a effort reported higher than planned, but the objective has been reached.

2) Application domain of the Stateflow gateway

The study performed by Verimag showed the gap that exists between the wish in importing any Stateflow diagram in our toolset, and the semantic problems of Stateflow. The risk identified is that the work we can do in that area does not match the legacy Stateflow diagram of users.

As described in deliverable D2.3.2 "Translating imperative features of Simulink into Scade-Lustre" we addressed the problem by following two different solutions, each with a development of a prototype. AUDI has been able to use these prototypes on his Stateflow models.

3) Perpetuation of the SCADE-TTA coupling

One of the interesting results of the RISE project is coupling of the SCADE and TTTech tools. Of course the tools from each company will have several releases in the future, so there is a risk in the continuity of the support of this coupling in the future.

Technically, the coupling is based on exchanging files that describe at a high level the architecture and timing constraints of the model. These files have an XML format defined together by TTTech and Esterel Technologies (we plan to look at standards

such as the FIBEX description to see if this can be used at the place of the XML format, but did not have time to go on with that study during the RISE project)
The internal details from SCADE and from TTTech tools are not stored in this file, so its format needs not to be frequently updated.

Note that the first prototype that what running with SCADE 4.2.1/TTTools version 6. It has been upgraded without difficulties to SCADE 4.2.1/TTTools version 7, and then to with SCADE 5.0/TTTools version 7.

Commercially, the sales agreement signed between TTTech and Esterel Technologies is a good sign to not let down the technical work done.

6. Conclusion

The RISE project is a true success: the objective reminded here has been fully reached:

The objective of the RISE project is to provide support for the development of embedded reactive software, in particular for cars, by developing:

- Concepts and methods for the developments of such embedded reactive software
- An integrated toolset supporting the concepts and the method, covering the analysis, design and development phases of such embedded reactive software.

The success of the RISE project has been built on the competence and complementarities of the partners:

- Audi as a mayor car manufacturer, for the evaluation of the re-existing tools, definition of the required improvements in the these tools and on new tools, and in setting up a demonstrator well suited to show the result from the RISE project,
- TTTech and Esterel Technologies as tool providers, with a string motivation to fulfil the automotive requirements, and a large effort investment to build a comprehensive tool chain,
- Verimag as academic expert, in taking care of the two main difficulties raised from the requirements, and establishing and adequate answer to each of them, for the tool provider

Several breakthroughs have been reached. Dissemination or exploitation of each of them is given here.

1) Modelling of pre-emptive scheduling

Preemptive scheduling is compulsory when time-triggered tasks are to be mixed with urgent event-triggered tasks and several techniques and associated schedulability tests have been extensively studied in the past. However, studies linking these scheduling techniques with the semantics problems of model-based design, as found in Simulink/Stateflow and Scade were lacking. The basic questions to be investigated were:

- a. Was it possible to model both time and event-triggered tasks in the Rise modelling framework?
- b. Could we find implementations techniques based on preemptive scheduling such that the behaviour of the implementation be consistent with the model, a key issue when it comes to model-based design?

Positive answers to these two questions have been found. This result has been published.

2) SCADE-TTA global model

The integration of a synchronous language with a synchronous communication layer opens very attractive possibilities for the design and development of Safety Critical embedded application with functionalities distributed onto several ECUs.

A first paper describing this coupling has been published to the 23rd Digital Avionics Systems Conference (DASC). Work will be pursued after the RISE project to generate the global model for simulation and formal verification purposes.

TTTech and Esterel Technologies have signed a sales agreement to promote the integrated solution, and several customers have already been visited, in Europe and in the US.

3) Integrated toolset from informal specification to safety critical embedded code

This is the core and aim of the RISE project. The toolset together with the underlying methodology is demonstrated in the “RISE methodology and toolset demonstration” report. This will be exploited this year by Esterel Technology marketing team.

4) Definition of the safe subset of Stateflow

This work performed by Verimag and Esterel Technologies has lead to the documentation of guidelines that have been exploited by AUDI.

5) The milestone for the middleware

The milestone defined for workpackage 2.7 has been reached. A prototype has been built that is based on the CAN emulator and the diagnostic subsystem.