Simulink Users Connect with Esterel's SCADE Suite for Safe Embedded Software

Abstract

Avionics and automotive system design teams use Simulink for fly and drive by wire system modeling and control law validation. SCADE Suite™ from Esterel Technologies enables embedded software development teams to generate 'safe by construction' code from formal executable models. By using the SCADE-Simulink Gateway, embedded software development teams can ensure that their code exactly and safely meets the software design requirements, at minimum cost and in a minimum amount of time. This white paper describes the Esterel Technologies Simulink Gateway, and how typical avionics and automotive users are successfully applying SCADE Suite to meet growing safety-critical software development challenges.

Simulink Users Connect with Esterel's SCADE Suite for Safe Embedded Software

Abstract

Avionics and automotive system design teams use Simulink for fly- and drive-by-wire system modeling and control law validation. SCADE Suite™ from Esterel Technologies enables embedded software development teams to generate 'safe by construction' code from formal executable models. By using the SCADE-Simulink Gateway, embedded software development teams can ensure that their code exactly and safely meets the software design requirements, at minimum cost and in a minimum amount of time. This white paper describes the Esterel Technologies Simulink Gateway, and how typical avionics and automotive users are successfully applying SCADE Suite to meet growing safety-critical software development challenges.

Table of Contents

Introduction

Advances in electronics and software are making their way from development to practical application at ever-increasing rates. This is good news for users, whose needs are met with better, faster, and cheaper solutions, but in many applications, human safety is at risk. Mistakes cannot be tolerated when new technology is applied to safety and mission critical avionics or automotive applications such as fly- or drive-by-wire systems, yet competitive forces are growing. Time to market pressure, quality requirements, and safety regulations in these industries conspire to make verification account for more than 80% of total development costs [1].

Development teams turn to simulation to reduce system development time and cost. Matlab's Simulink is commonly used for avionic and automotive control system simulation. Esterel's SCADE (Safety and mission Critical Application Development Environment) Suite is the de-facto standard tool in the European civil avionics industry for generating safe software code for these systems. During 2002, SCADE started to see widespread use in US civilian avionics projects, and began to emerge as the de-facto standard for European automotive applications. A connection between Simulink and SCADE Suite therefore has enormous potential to increase development team productivity.

This white paper starts by summarizing the challenges facing avionics and automotive development teams and then describes the typical Simulink and SCADE Suite development flow. Esterel Technologies Simulink Gateway is then introduced and its impact on productivity examined.

Avionics Challenges

Embedded electronics systems first appeared in military applications over 50 years ago. Their use is now widespread in both military and commercial applications, and software plays a continuously growing role. Some typical applications are:

- Flight control
- Engine control
- Braking systems
- Cockpit and display systems
- Fuel and power management systems
- Alarm management systems
- Communications

Safety-critical embedded systems development environments need to allow users to build their own flows and make them feel at home [2]. For system validation and engineering, wide use of simulation built on common models is needed. The development environment must provide the means to concurrently engineer the different aspects.

The challenges facing avionics development teams are nicely summarized by the European SafeAir project [3], a collaboration of SNECMA/Hispano-Suiza, EADS/Airbus, and Israel Aircraft industries. SafeAir's goals are to reduce safety-critical embedded software development time and costs by 35-40%, while preserving safety and reliability.

Not surprisingly, safety and reliability in avionics applications are subject to regulation, and the joint Federal Aviation Administration/EUROCAE RTCA-DO-178B/EUROCAE-ED-12B is the standard in the US and Europe. When DO-178B is applied, embedded software development time and cost can be multiplied 2-3X due to traceability and stringent verification requirements.
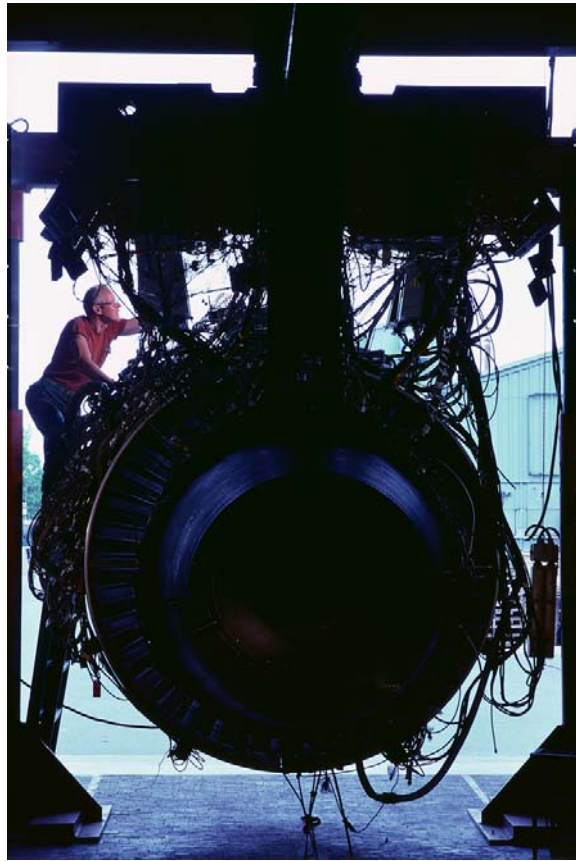
Figure 1: Full Authority Digital Electronic Control (FADEC) systems are now standard features of aircraft engines from Pratt & Whitney, GE, Rolls-Royce and SNECMA.

The Avionics Systems Development Environment (ASDE) developed by SafeAir uses model-based design, automatic code generation, and formal verification to address the following:

- Challenges
    - Clarity and correctness of requirements
    - Communication of requirements within development teams
    - Communication of requirements to suppliers and OEMs
    - Correctness of the design with respect to the requirements
    - Correctness and safety of implementation
    - Time needed to complete the project
- Safety Objectives
    - DO-178B compliance
    - Code is traceable to the requirements
    - It does not use dynamic memory allocation
    - It is fully deterministic

These are typical challenges for an avionics system development team.

Automotive Challenges

The advent of 42-volt power systems and x-by-wire technology will deliver complex and autonomous safety systems into the automobile, promising to change the way we view the automobile. 'x-by-wire' is an automotive industry term for embedded electronics control systems which replace traditional mechanical connections (e.g. drive-by-wire throttle). According to Drs Kruger and Kant of Audi, '90% of all future innovations in cars will be determined by electronics, and 80% of these will be in the area of software' [4].
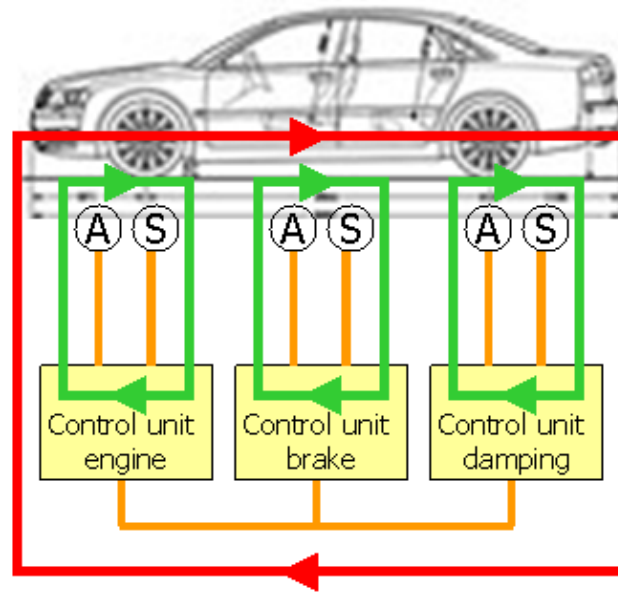
Figure 2: Companies like BMW and Audi are leading the deployment of embedded electronics systems in cars, such as engine, brake, and suspension controls, and drive-by-wire throttle.

Manufacturers are also under pressure to reduce vehicle development times to 30 months or less. A near future development process is characterized by virtual techniques and only one physical prototype cycle [5]. To achieve this, automakers must make massive use of cross-functional simulation and testing.

Some typical applications of automotive embedded systems are:

- X-by-wire (throttle, suspension, stability, braking, etc.)
- Engine management
- Airbags
- Display management
- Electrical power management
- Communications

The challenges facing the teams which develop such systems are:

- Maintaining safety and reliability
- Capturing and communicating the requirements
- Operation in a harsh Electromagnetic Inference (EMI) environment
- Cost-efficiency
- Evolving industry standards
- Size, modularity, location, and heat management

Common Challenges

Having explored some of the challenges faced by avionics and automotive development teams in the context of their respective industries, it is clear that there are commonalities in the control engineering issues which they face:

- Requirement to maintain or improve safety and reliability
- Pressure to reduce development time and costs
- Difficulty capturing requirements and communicating them within development teams and to suppliers and OEMs
- Compliance to safety standards

Common Solutions

To help meet these challenges, development teams turn to simulation. Matlab Simulink is a common control engineering environment in both the avionics and automotive industries. With SCADE Suite already the de-facto standard for safe embedded software design in civilian avionics, and a rapidly emerging presence in automotive applications, a link between the two has great productivity potential. Figure 3 shows a typical embedded software development flow and the tools used.

Why Avionics and Automotive Teams Use Simulink

Matlab and Simulink, have long been the preferred programs for graphical modeling and simulating electro-mechanical control systems. Matlab is a numerical solver. Simulink is a graphical dynamic simulator. Matlab is an intuitive language and a technical computing environment. It provides core mathematics and advanced graphical tools for data analysis, visualization, and algorithm and application development. Simulink is a simulation and prototyping environment for modeling, simulating, and analyzing real-world, dynamic systems.

Why Avionics and Automotive Teams Use SCADE Suite

An expanding number of avionics and automotive companies are choosing the correct-by-construction methodology of SCADE Suite from Esterel Technologies to shorten TTM and increase development productivity while meeting safety requirements (e.g. Airbus, Pratt & Whitney, SNECMA/Hispano-Suiza, Honeywell, Audi, Rockwell).
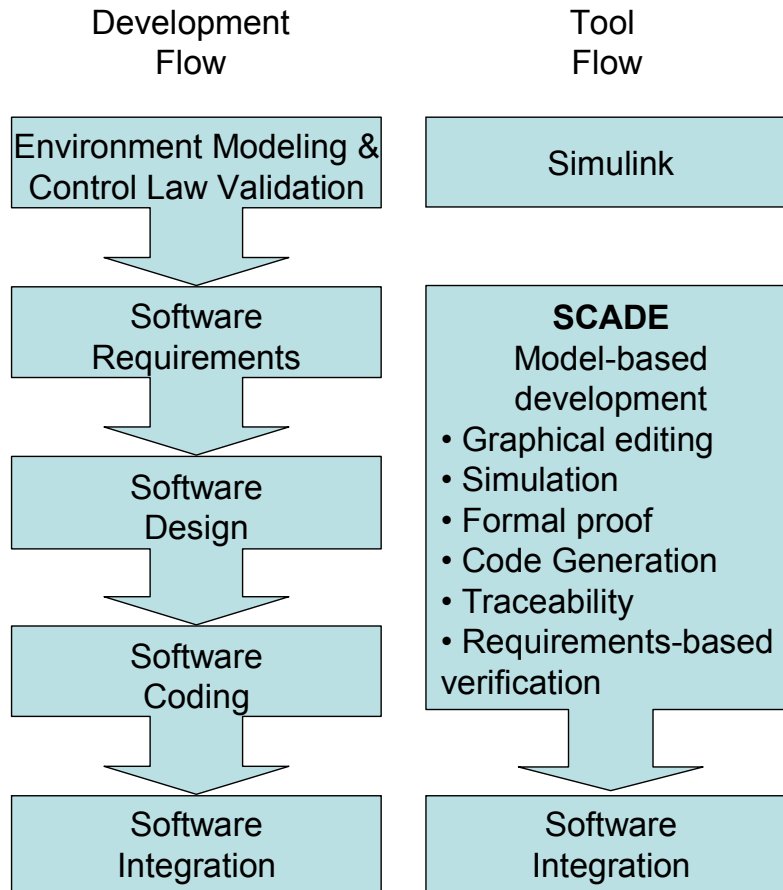
Development Flow	Tool Flow
Environment Modeling & Control Law Validation	Simulink
Software Requirements	**SCADE** Model-based development • Graphical editing • Simulation • Formal proof • Code Generation • Traceability • Requirements-based verification
Software Design	
Software Coding	
Software Integration	Software Integration

Figure 3: Typical development and tool flows.

Generating Safe Code, On Schedule and On Budget

SCADE Suite provides a graphical entry and simulation environment which allows intuitive visual representation of the control system. Requirements are unambiguously represented within SCADE. Functional testing can be performed through simulation, and SCADE Suite formal verification enables the validation of design behavior and early detection of corner case bugs. SCADE automatically generates readable, traceable, and reliable C or Ada code.

The entire code generation process is compliant to the civil avionics standard, DO-178B. SCADE Suite is the only code generator qualified at DO-178B Level A, removing the need for verification of the generated code. *Unit test with MC/DC (Modified Condition/Decision Coverage) is not necessary.*

By automating the validation and generation of embedded code, SCADE allows the early detection of design errors and shortens development time and cost.

"There is now compelling evidence that development methods that focus on bug prevention rather than bug detection can both raise quality and save time and money. A recent, large avionics project reported a four-fold productivity and 10-fold quality improvement by adopting such methods [1]."

Benefits of the SCADE Model as a Reference Model

Development team productivity can also be improved by adopting the SCADE model as the development reference model, since it effectively enforces correct- and safe-by-construction modeling.

Since SCADE Suite generates the safe embedded code and the documentation, adopting SCADE, where the model represents the requirements, makes modifications safe and fast. Eurocopter, for example, is able to fly the next test flight only 48 hours after a specification modification. The use of SCADE Suite assures that there is no risk of inconsistency between the specification, the code, and the documentation.

Over The Wall

There is one more common challenge which development teams face, that of communication difficulties between the different specialist functions within the teams. Typically there are system architects, control engineers, and software engineers. The software engineers must design and generate code which meets the requirements laid out by the system architects and control engineers. Communication with the software engineers is often stunted, and requirements thrown 'over the wall', making incorrect interpretation much more likely. System specification and control algorithm designs are done in Simulink, then thrown 'over the wall' to the software engineers for software design and code generation.

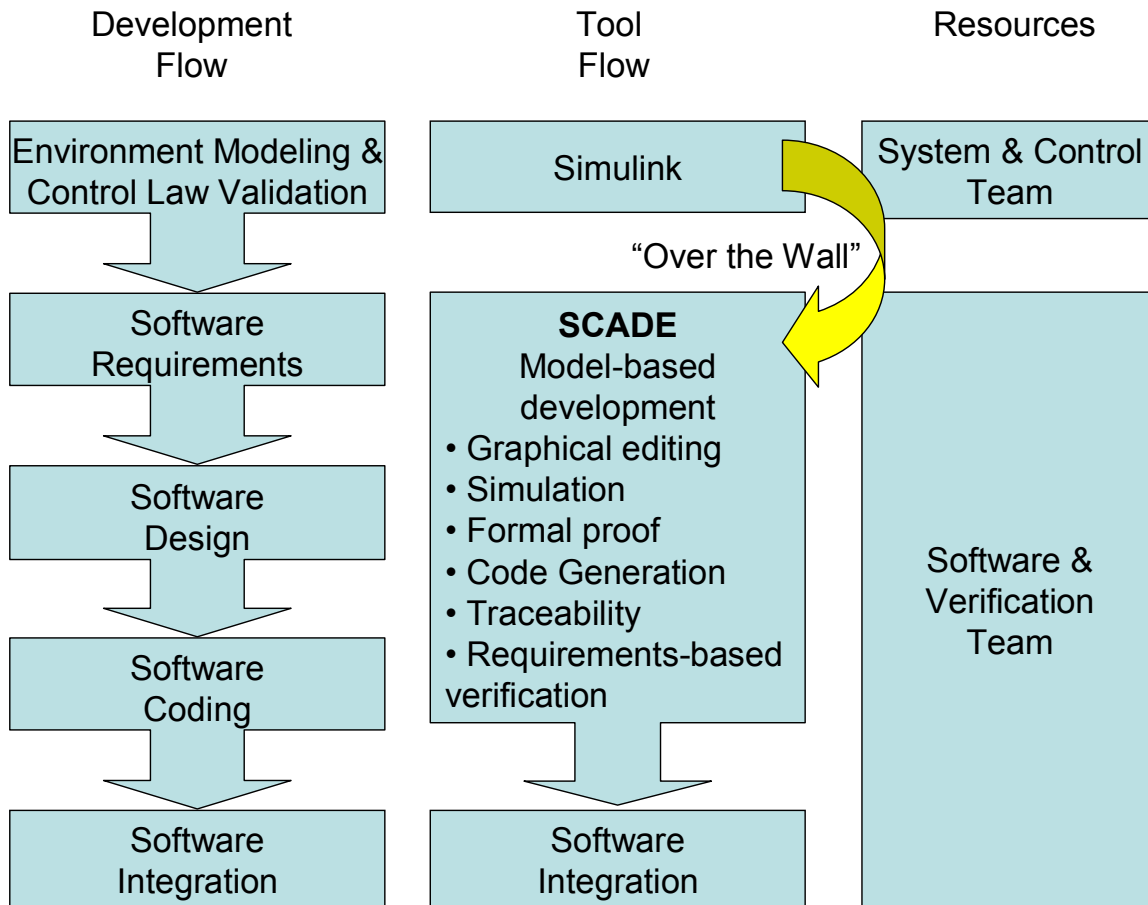| Development Flow	Tool Flow	Resources
Environment Modeling & Control Law Validation	Simulink	System & Control Team
Software Requirements	**SCADE** Model-based development • Graphical editing • Simulation • Formal proof • Code Generation • Traceability • Requirements-based verification	Software & Verification Team
Software Design		
Software Coding		
Software Integration	Software Integration	

"Over the Wall"

Figure 4: Over the wall to the software team.

The software team must often manually recreate in their own environment much of the work already done by the system and control engineers.

When the requirements must be communicated to outside suppliers or OEM customers, 'over the wall' issues can be even more severe.

The SCADE-Simulink Gateway has been created to improve flow productivity by allowing model reuse and accurate communication of requirements both within safety- and mission-critical embedded software development teams, and with their suppliers and OEM customers.

The SCADE-Simulink Gateway

The gateway provides an automatic connection between Simulink and SCADE Suite users, resulting in unambiguous communication of requirements and improved productivity for both.

SCADE and Simulink both allow the modeling and simulation of control systems, and they both allow a data flow representation. They have similar abstraction

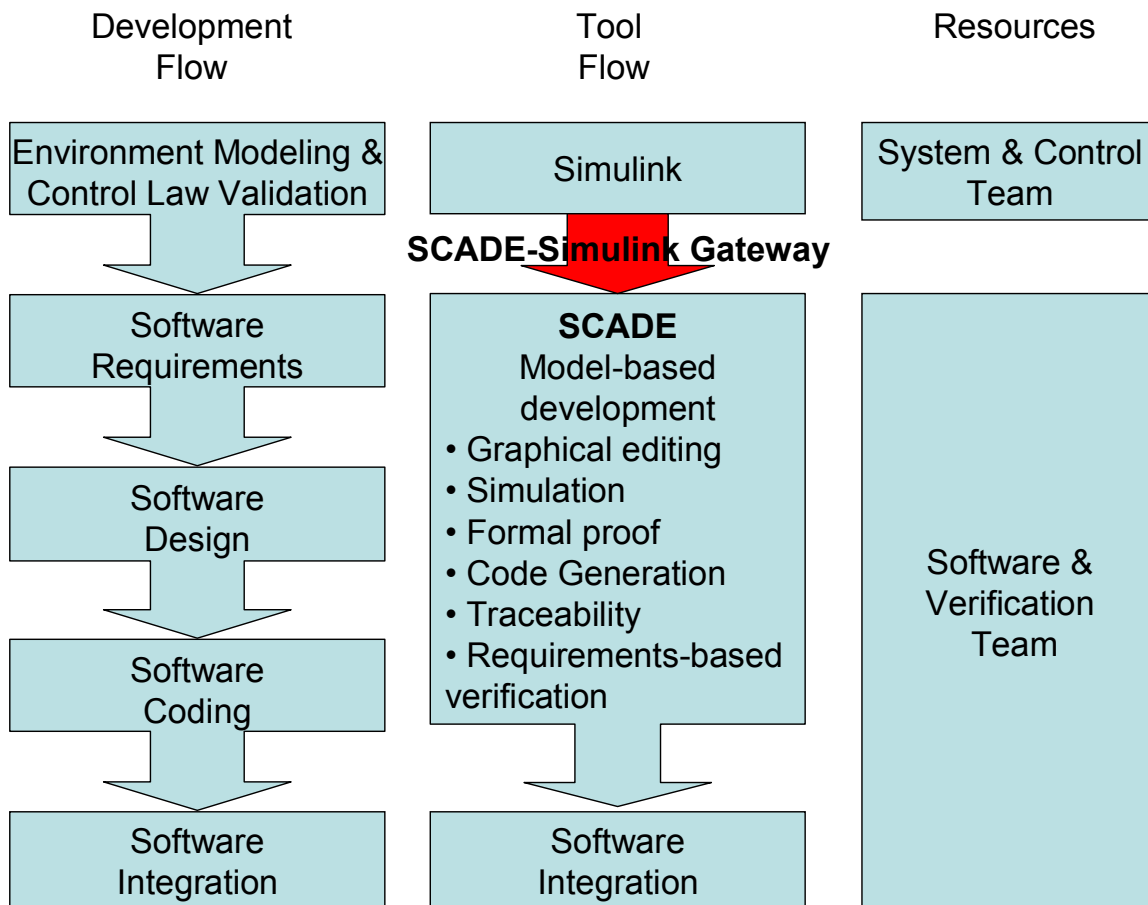mechanisms and facilitate graphical representations of control systems, but there are important differences.

Development Flow	Tool Flow	Resources
Environment Modeling & Control Law Validation	Simulink	System & Control Team
	SCADE-Simulink Gateway	
Software Requirements	**SCADE** Model-based development • Graphical editing • Simulation • Formal proof • Code Generation • Traceability • Requirements-based verification	Software & Verification Team
Software Design		
Software Coding		
Software Integration	Software Integration	

Figure 5: The SCADE-Simulink Gateway connects.

Simulink's origin is as a mathematical modeling tool, not as a software development tool. SCADE on the other hand is designed as a software specification and implementation tool. Specifically:
- SCADE models time in discrete increments whereas Simulink models time continuously. This means that a SCADE model generated by the gateway runs at the same time period used for the simulation of the equivalent Simulink model.
- SCADE is completely modular, meaning that the behavior of a SCADE subsystem does not depend on its context, whereas the behavior of an equivalent Simulink 'subsystem' does.
  - A Simulink model has implicit inputs such as the sampling times of its subsystems.
  - The Simulink GOTO/FROM constructs allow variables to cross subsystem boundaries.
  - The behavior of a Simulink model depends on its simulation options.

Simulink models which are to pass through the gateway must be discrete subsystems.

Some of the more complex Simulink constructs, and some constructs used for simulation purposes have no SCADE equivalent and are not 'safe' i.e. they can never be translated into code for a safety-critical application.

Real World Results

Both SCADE Suite and Simulink are well-proven in avionics and automotive applications. The soundness of the SCADE-Simulink translation process was verified more than 3 years ago, when Esterel assisted Peugeot SA, a SCADE user, in moving from Simulink to SCADE. This project led to SCADE-generated embedded code.

As discussed earlier in this paper, SCADE Suite and the SCADE-Simulink Gateway were chosen by the European SafeAir collaboration for its Avionics Systems Development Environment (ASDE).

A leading aircraft engine manufacturer has chosen SCADE and the Gateway for use in the development of its FADEC (Full Authority Digital Electronic Control) software.

Airbus will use the Gateway in the development of its braking system software.

Given the ubiquity of SCADE and Simulink, it is not surprising that the SCADE-Simulink Gateway is becoming a standard feature of avionics and automotive embedded software development flows worldwide.

Conclusion

Time-to-market pressure, quality, and safety requirements conspire to make verification more than half of the total embedded software development costs in safety- and mission-critical applications. Avionics and automotive developers of embedded software face similar embedded software development challenges. Development teams are turning to Esterel's SCADE Suite and its Gateway to Simulink in order to decrease verification time and costs. Avionics and automotive companies such as EADS/Airbus, Hispano-Suiza/SNECMA, and Audi are successfully improving development and verification productivity by integrating Esterel's SCADE Suite and SCADE-Simulink Gateway into their flows.

References

[1] *Correctness by Construction: Better Can Also Be Cheaper.* Peter Amey. Crosstalk Magazine, March 2002, pp24-28.
[2] *Safety Critical Embedded Systems – Orientations for the Future.* Francois Pilarski. Airbus. November 2002.
[3] *Constructing Correct Systems in the SafeAir Project*. SNECMA Control Systems. www.safeair.org (a collaboration of EADS/Airbus, Airbus Deutschland

GmbH, Israel Aircraft Industries, I-Logix, Inria, Information Societies Technology, Offis, SNECMA/Hispano Suiza Control Systems, Siemens, Telelogic, Techniques Novelles d'Informatique, and Weizmann Institute of Science). January 2002.
[4] *Software Strategy, Tools, and Development Process for X-by-Wire*. Dr Andreas Kruger & Dietmar Kant of Audi. SCADE User Conference, Toulouse 2002.
[5] *BMW AG: The Digital Auto Project.* Stefan Thomke & Ashok Nimgade. Harvard Business Review (Case). Revised November 2001