

SAFEAIR

Advanced Design Tools for Mission-Critical Systems and Airborne Software

Participants: Snecma Moteurs (F), Israel Aircraft Industries LTD (IL), EADS Airbus (F),
EADS Airbus GmbH (D), Siemens AG (D), T.N.I. (F), Telelogic (F), I-Logix (IL)
OFFIS (D), Weizmann Institute, INRIA (F)

Mailing Co-ordinator Address: Centre de Villaroche 77550 Moissy-Cramayel France

Phone Number: +33 1 60598902

Fax Number: +33 1 60598925

E-mail: Philippe.Baufreton@sncma.fr

Keywords: Dependability, airborne software systems, safety critical systems

SUMMARY

SafeAir aims at the development of an *Avionics Systems Development Environment (ASDE)*, encompassing technologies, methods and tools that *meet the high dependability needs in the area of embedded control systems*. The approach is based on the integration of mature, well-accepted notations and tools integrated in a usable development environment. Salient novel features are rigorous *verification* of critical properties, automated, qualified *code generation* and *automatic validation* of the code with respect to the design.

PROBLEM

Challenges in designing and developing airborne control systems for avionics and other industrial application of similar complexity span the whole development cycle:

Requirements need to be described unambiguously and correctly, the design, code and implementation must *be checked for correctness and reliability* with respect to the requirements. At the same time the *development effort* must be kept low to meet the tight time to market.

AIM

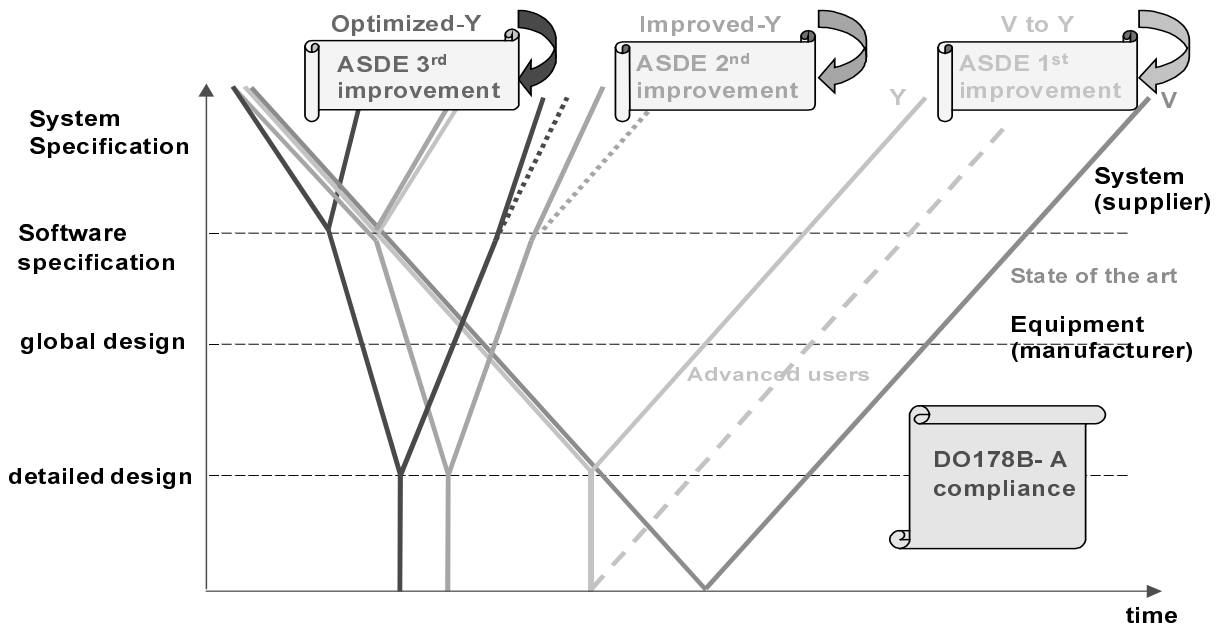
SafeAir will contribute to the overall goal of facilitating aircraft subsystem and component development in order to foster the competitiveness of the European avionics industry. Its focus is on substantially improving the electronic system development process, leading to a 35-40% reduction in development cost for airborne software systems.

ASDE will

- significantly raise the degree of error detection and reduce the validation effort at integration time through formal verification techniques,
- provide a seamless integration from system-level modelling tools to an automatic code generation tool in compliance with DO-178B standard,
- offer an innovative approach for automatically proving consistency of source and generated code supporting the complete translation chain down to the binary level, thereby eliminating potential coding errors and allowing a dramatic reduction of unit-testing.

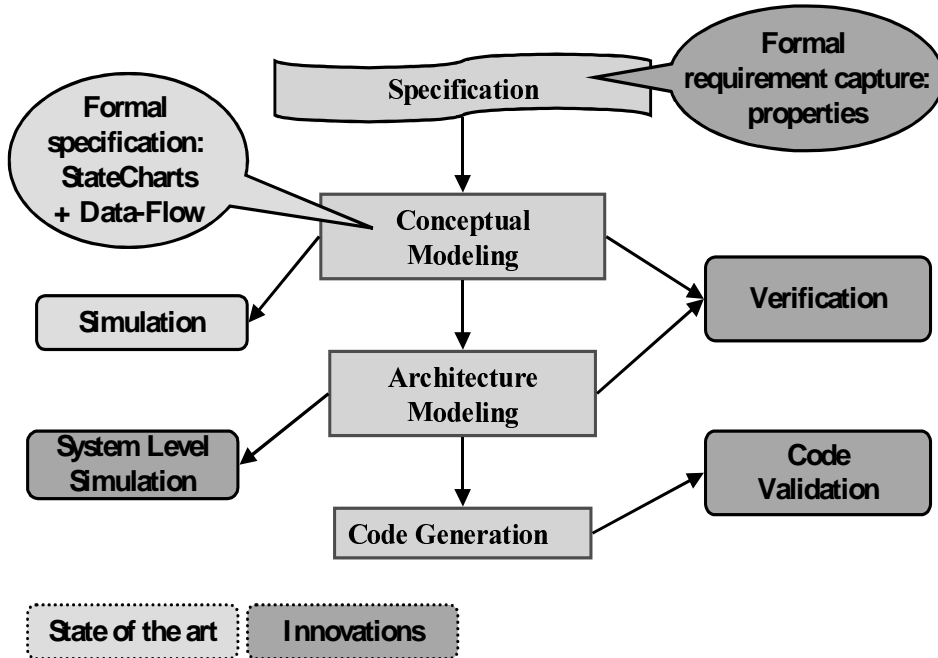
TECHNICAL APPROACH

European avionics industry typically uses variations of the V-process model to structure the development process of airborne software which will be defined as the reference model. This model is compliant with the DO-178B recommendations in commitment with certification authorities world wide: FAA and JAA. The figure below indicates, how SafeAir proposes to gradually improve a V to a Y-based process, in order to significantly reduce the design time. The slope of curves is selected to qualitatively indicate the time consumed in particular design steps.



SafeAir supports an incremental, three-stage road for process improvements, each leading to successive reductions in development costs and design time, while maintaining, or increasing, system reliability:

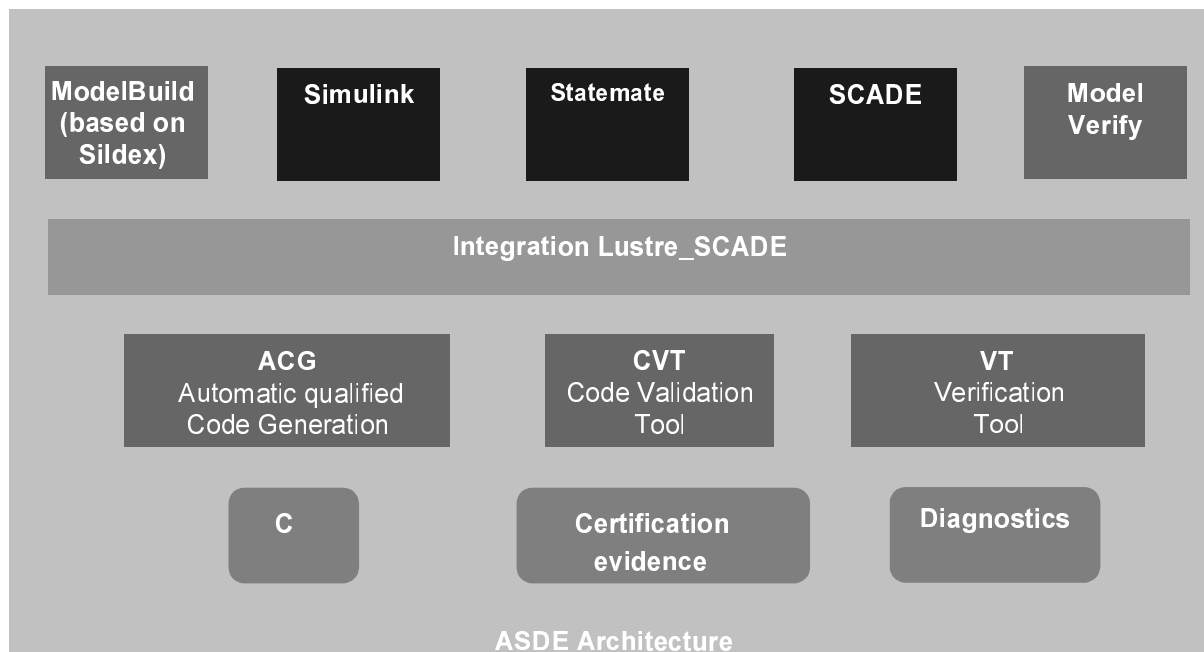
The key concepts for these improvements are a *model based design process, automatic code generation and formal verification.*



The **ASDE** integrated environment will be built on the verification and validation technologies developed in the SACRES Esprit project and expand them to a mature tool set, responsive to user needs. SafeAir will secure that proposed enhancements in the design methodology will be acceptable for the DO178B and ARP4754 certification authorities.

To ensure both the technical development and the user take-up, the project combines technology providers and vendors with skilled teams from user companies. The applications cover the entire development from system and subsystem specification to software implementation in the aeronautics sector.

ASDE is a set of tools that co-operates to allow the user to build, simulate and verify models that are composed of components modelled with different front-end tools Sildex, Simulink, Statemate, and SCADE. The communication between these components can be synchronous or asynchronous. The global model, and each of its components may be verified against properties with a dedicated tool, ModelVerify. The integration approach is by exchange of models based on SCADE files. For that purpose, gateways are part of the **ASDE** tool set.



In order to reduce the risks associated with the program, an iterative development, application, validation and assessment process ensuring close feedback from users to developers will introduce the full capabilities of the ASDE. This will assure fast feedback and appropriate changes in the ASDE architecture definition.

EXPECTED RESULTS

The major result of SafeAir will be a *validated ASDE for system and software development*.

This environment will support system specification and software specification, on the basis of formal, readable notations both at the analysis and design phase, and integrate de-facto standard modelling tools for avionics applications.

ASDE will significantly raise the degree of *early error detection* and *reduce the validation effort* at integration time through formal verification techniques for the verification of critical properties. It will provide a seamless integration from system-level modelling tools to an *automatic code generation tool* in compliance with the DO-178B standard for critical airborne embedded systems. As a result of introducing and assessing **ASDE** within aerospace engineering processes and as the basis for technology dissemination, a comprehensive *assessment* report as well as an *assimilation and training package* will be provided.