Software aspects of qualification in the SafeAir II Project

Philippe BAUFRETON
Hispano-Suiza
Etablissement de Réau BP 42 - F-77551 Moissy-Cramayel Cedex France

and

Cyrille ROSAY
CEAT (Centre d'Essais Aeronautique de Toulouse)
47 rue St Jean, BP 53123 – 31131 Balma Cedex France

PREAMBLE

The SafeAir II project (http://www.safeair2.org) is a European Commission project that was submitted under the 5th framework program. It contributes to "Dependability in Services and Technologies" in the Information Society Technologies (IST) Program and is running since July 2002 for two years.

The project partners are Hispano-Suiza (Project co-ordinator), Israel Aircraft Industries, MBDA, RENAULT, Infineon Technologies AG, OFFIS, TNI-Valiosys, Verimag, Weizmann Institute and CEAT. SafeAir II implements a comprehensive open environment that help keeping the validation effort needed to achieve the present safety level of the embedded software systems within reasonable costs despite their increasing size and complexity.

1. INTRODUCTION

European avionics industry typically uses variations of the V-process model to structure the development process of airborne software which is defined as the reference model. This model is compliant with the DO-178B recommendations in commitment with certification authorities world wide: FAA and EASA. The diagram in Figure 1 indicates, how the project propose 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 II tightly integrates ASDE "Advanced Systems Development Environment" tools in a comprehensive framework based on strongly positioned tools in the Avionics and Automotive markets with key innovative technologies: formal verification of properties and code validation tools.

2. OBJECTIVES

SafeAir II is aimed to foster the future adoption of the ASDE methodology in actual real size industrial applications in wider user communities while securing the overall tool set implementation. SafeAir II defines the adaptation process of industrial ASDE exploitation. A methodology for the adaptation process will support the ASDE technology adoption. The connection to industry-standard requirements trace-ability tools will allow a better integration in the users context, and an Automatic Test Generator (ATG) is applied when verification is not possible or fails, or for hybrid models which contain numerical values and complex algorithms.

SafeAir II supports an incremental, three-stage road for process improvements, each leading to successive reductions in development costs and design time, while maintaining, or even increasing, system reliability. The project secures that proposed enhancements in the design methodology are acceptable for the DO178B/ED12B [1] and ARP4754 [2] certification authorities. The CEAT, with its experience in the software aspects of civil aircraft certification on behalf of EASA is in charge of the analysis of the design tool items and the justification for verification and development activity reduction strategy. The capabilities of the tool set and its method to be qualified in a frame of an aircraft certification is a key issue for adoption in actual embedded applications.

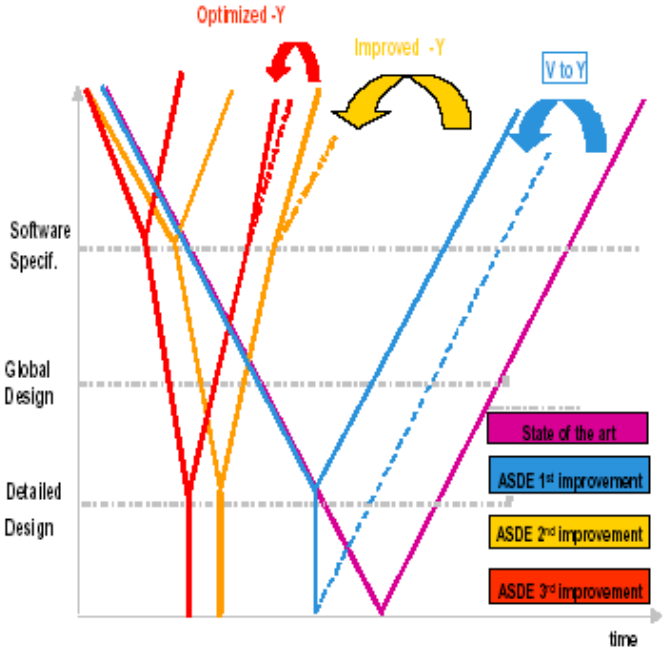

Figure 1: Life cycles over project time

3. DESCRIPTION OF THE WORK

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

verification. The ASDE Environment implementing these concepts is a set of interconnected tools evaluated in the project. Formal verification tools and code validation tools are still prototypes.

Automatically generating the production code from a validated specification alleviates many of the problems in system development. If done correctly, automated translation guarantees that the behavior of the production code is correct with respect to the formal specification. The ASDE subset of commercial tools Simulink™ from the Mathworks, Sildex™ from TNI-Valiosys and SCADE™ from Esterel Technologies are based on this idea and smoothly translate a formal or semi-formal specification down to executable code.

We successively explored the following design and V&V steps:
a) System level: tools = Simulink/Stateflows models; validation by simulation.
b) From System to Software specification: Simulink™ to Sildex™ gateway and export to SCADE™.
c) Software design: mapping the functions onto the software architecture and perform schedule-ability analysis inside Sildex™.
d) Validation by model-checking of the SCADE™ requirements in order to ensure that the entries of the previously qualified code generator will be correct (ie: implement the expected behavior of the software) before code generation.
e) From SCADE™ to embedded source code: tool "qualified" generator; validation: most of the V&V activities may be alleviated thanks to the qualification capabilities of the generator as a development tool.
f) Checking the output of the qualified code generator regarding its specification with a dedicated code validation tool CVT-C [4]
g) Validate the transformations through S-functions in Simulink™ and perform simulation with actual code.
h) From source code to embedded object code: tool : DiabData™; V&V...
i) Checking the output of the non-qualified industrial compiler by a dedicated code validation tool MCVT [5].
j) For each and every software function, test suites are elaborated on the model allowing requirements coverage of the function (including the low level requirements), as well as the structural coverage.
k) For the complete software, test suites are elaborated from the high level requirements. This would allow verification of the integration of the functions, their interfaces, scheduling and activation of every functions.

ASDE provides a seamless integration from system level modelling tools to the qualified automatic code generation tool in compliance with the DO-178B standard for critical airborne embedded systems. It significantly reduces the validation effort, in terms of time, at integration through formal verification techniques for the verification of critical properties.

The method includes a very 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. This approach constitutes a major technological breakthrough providing valuable certification evidence for the users.

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 are now available.

It was demonstrated that ASDE:

- significantly raises the degree of error detection and reduce the validation effort at integration time through formal verification techniques,
- provides a seamless integration from system-level modelling tools to the automatic code generation tool,
- offers an innovative approach for automatically proving consistency of source and generated code supporting the complete SCADE and DiabData™ translation chain down to the source level, thereby eliminating potential coding errors and allowing an eventual reduction of unit-testing.

The qualification evaluation performed by the CEAT on the Hispano-Suiza process give confidence in the acceptability of the proposed enhancements in the design methodology by the certification authorities, with respect to international applicable recommendations and regulations.

4. IMPACT

The strategic impact of SafeAir II will be a major competitive advantage for European companies, both in the avionics field and in other similar fields such ground transportation control and signalling systems, embedded car electronic units, etc. Recognition of the ASDE capability and effectiveness is expected by the qualification process of users applications and the durability of the tool set through intensive use in industrial contexts.

5. REFERENCES

[1] DO178-B **Software Considerations in Airborne Systems and Equipment Certification** - Radio Technical Commission for Aeronautics, (Ed.) 1992
[2] ARP4754 **Certification Considerations for Highly Integrated or Complex Aircraft Systems** - Systems Integration Requirements Task Group, AS-1C, ASD, SAE (Ed.) 1996
[3] SafeAir II **Project Advanced Systems Development Environment:** A methodology and a tool-set designed to develop aeronautics, automotive and space safety-critical systems. CONVERGENCE'03
[4] A. Pnueli, O. Shtrichman, M. Siegel, The Code Validation Tool (CVT) **– Automatic verification of code generated from synchronous languages** – International Journal of Software Tools and Technology Transfer (STTT), vol 2, 1999.
[5] A. Pnueli, I. Gordin, R. Leviathan, **Validating the Translation of an Industrial Optimizing Compiler**, ATVA 2003 - 2nd International Symposium on Automated Technology for Verification and Analysis Taiwan.