



SCADE Suite™

"Correct-by-Construction" Development
for Safety Critical Embedded Software



Photo courtesy of AIRBUS



Falcon 7X by Dassault Aviation



Aeroengines by Snecma
©Snecma/Studio Pons

Agenda

- ▶ Overview
- ▶ Practical Benefits Analysis
- ▶ SCAD Suite Presentation
 - ▶ *Editor*
 - ▶ *Simulator*
 - ▶ *Design Verifier**
 - ▶ *DOORS™ Link*
 - ▶ *Integration with Configuration Management Tools*
 - ▶ *Code Generators*
- ▶ Summary



* Design Verifier powered by Prover Plug-In. Prover Plug-In is a trademark of Prover Technology AB in Sweden, the United States, and other countries

Esterel Technologies- Corporate Profile

- ▶ Headquarters in Mountain View, California and Elancourt, France
- ▶ 110 employees in 5 countries
- ▶ 50+ large corporate customers
- ▶ 50+ universities worldwide teaching the use of Esterel Technologies solutions
- ▶ *2002: 50% revenue growth, SCADE revenues doubled*
- ▶ *2003: 46% to 48% revenue growth, SCADE 70% growth*



Esterel Technologies – World Class Technology

THE WORLD TECHNOLOGY
A W A R D S
2 0 0 2

- ▶ Esterel Chief Scientist, Gerard Berry, nominated as a finalist for the World Technology Award in 2001 and 2002 in the Software category.

“The World Technology Awards were created to honor those innovative individuals who most contribute to the advance of emerging technologies of all sorts for the benefit of business and society. We especially seek to honor those innovators who have done work recently which will have the greatest likely future significance and impact over the long-term...”

- ▶ All Ph.D.'s in core technology group



SCADE

Safety Critical Application Development Environment

- ▶ Technology rooted in 7 years of successful industrial application and 20 years of research
 - ▶ SCADE enters US market in 2003
- ▶ Optimized for Aerospace, Defense & Automotive
- ▶ 100% automatic generation of safe, production-quality code:
 - ▶ Ada 83/95, SPARK-compliant
 - ▶ DO-178B Level A certifiable code



Critical Embedded Software Applications

▶ Aerospace & Defense

- ▶ *Flight control systems*
- ▶ *Autopilots*
- ▶ *Engine control systems*
- ▶ *Braking systems*
- ▶ *Cockpit display and alarm management*
- ▶ *Fuel management*
- ▶ *Power management*
- ▶ *On-board communications*
- ▶ *Flight management systems*
- ▶ *Reconfiguration management*



Photo courtesy of Airbus



▶ Automotive

- ▶ *Engine regulation*
- ▶ *Airbags*
- ▶ *Display management*
- ▶ *Electrical power management*
- ▶ *Interlocking systems control*
- ▶ *Restraining systems*
- ▶ *Entertainment systems*

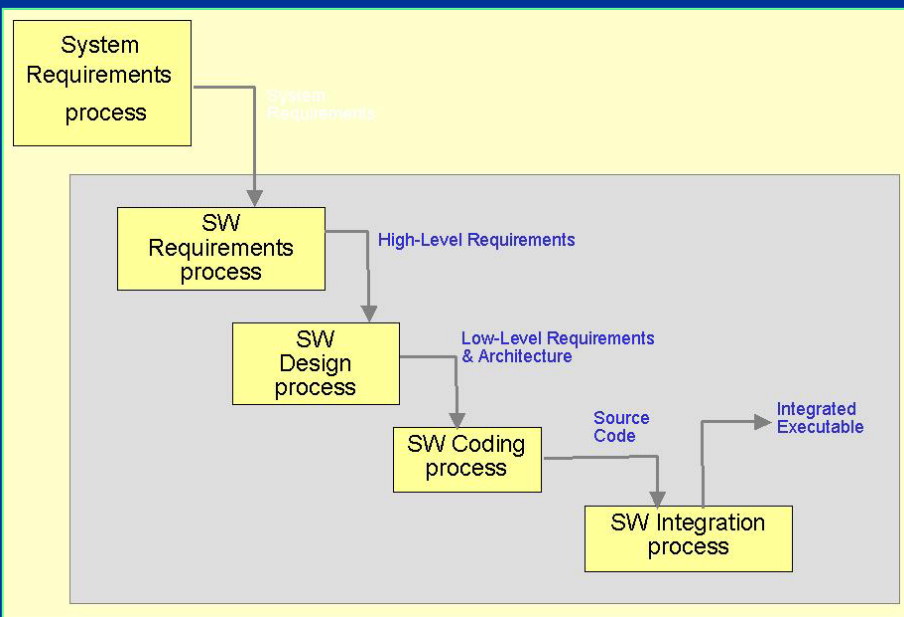


Photo courtesy of Framatome

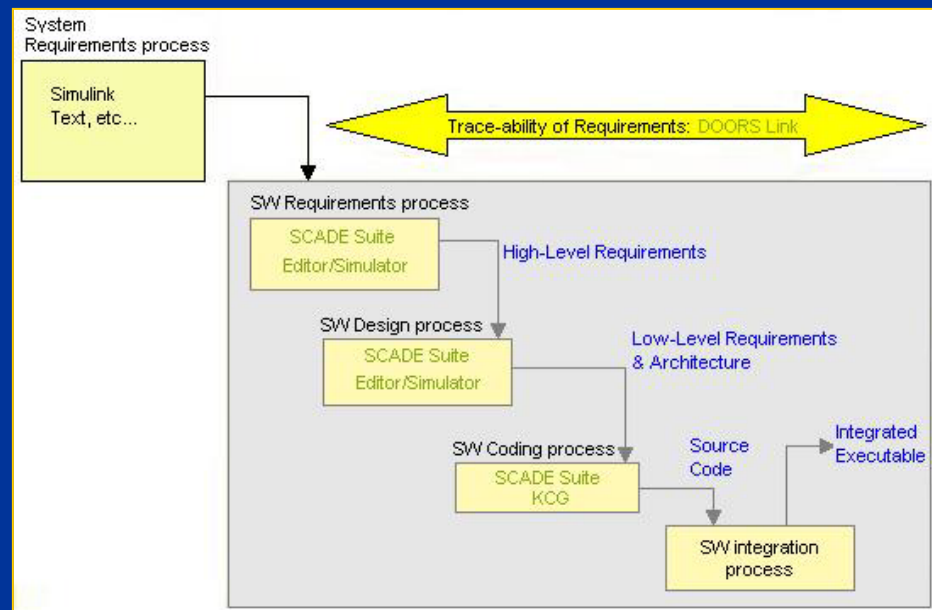
▶ Energy

- ▶ *Nuclear systems control & command*

Mapping SCADE Suite Method Into the Software Development Process



Standard Flow

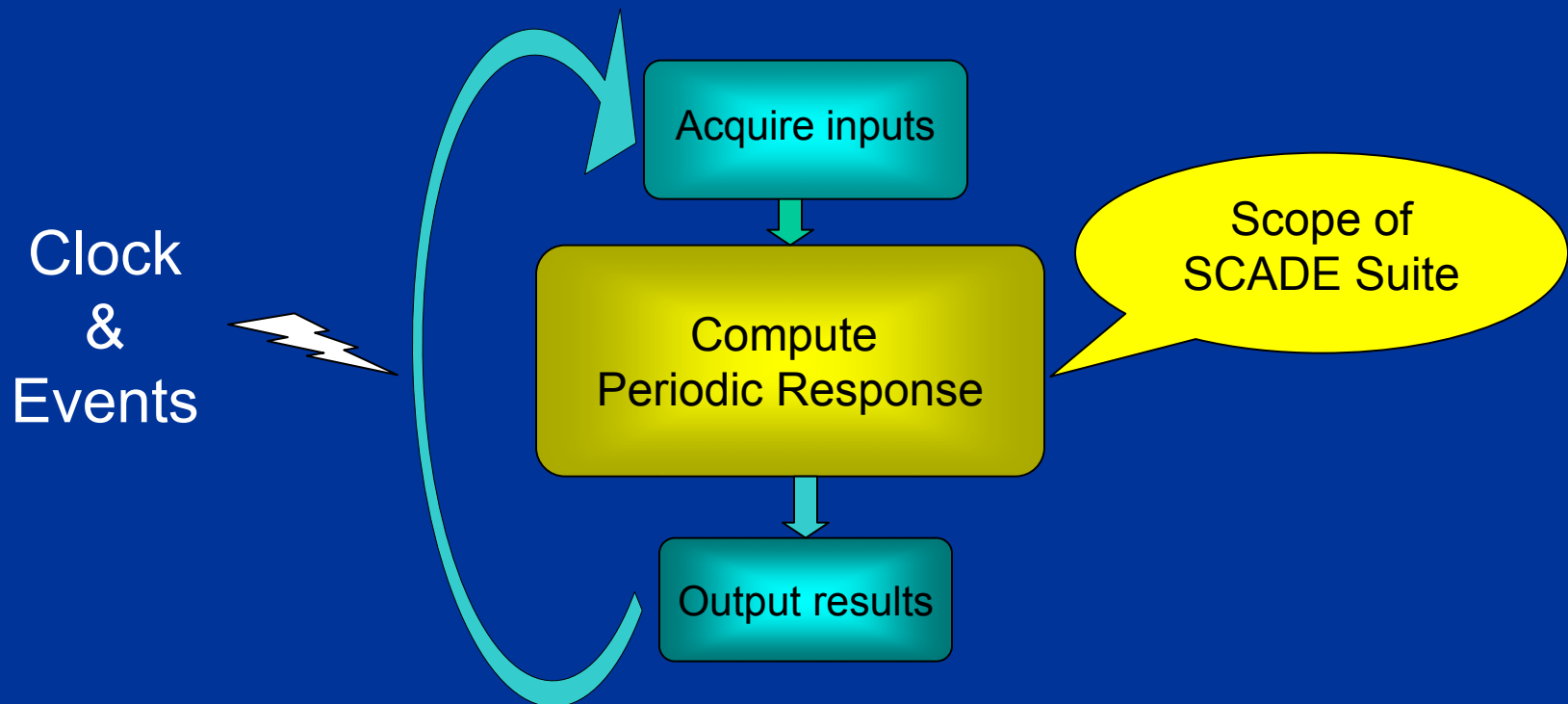


SCADE Suite

Adopt a “Safe-By-Construction” Architecture

The SCADE Suite synchronous architecture has a proven track record of success in avionics, automotive, transportation and energy.

It achieves fully deterministic behavior both for time and event-triggered systems.



SCADE Suite Platforms

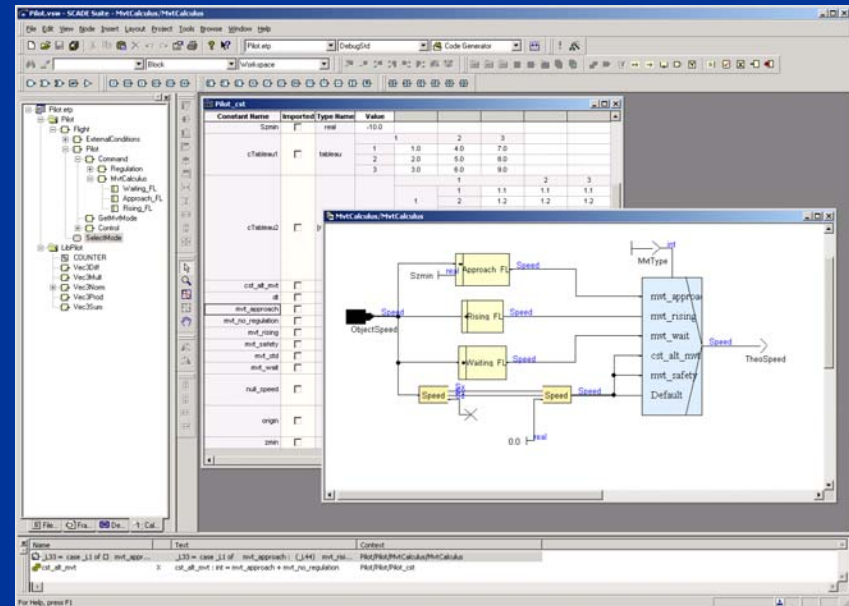
SCADE Suite is available on Windows & UNIX

▶ PC

- ▶ *Windows 2000*
- ▶ *Windows NT*
- ▶ *Windows XP*

▶ UNIX

- ▶ *Solaris 2.6*
- ▶ *Solaris 2.8*



Transparent switch from one platform to the other since project file formats and SCADE Suite MMI are identical on Windows & UNIX

Key Facts & Figures

- ▶ 70% of Airbus A340 Flight Commands software (AFCS) generated with SCADE Suite.
 - ▶ *No coding defect has ever been found.*
- ▶ Over 10 aeronautic systems successfully certified DO178-B Level A due to SCADE Suite KCG qualification.
- ▶ **100% certification success rate**
- ▶ Typical certification time improvements:
 - ▶ *Initial Eurocopter EC155 helicopter certification: 20 months*
 - ▶ *Certification with SCADE Suite qualification: 8 months*
- ▶ Typical safety-critical project development figures:
 - ▶ *654 SCADE nodes*
 - ▶ *173,000 generated lines of C code (total for 2 processors)*





- ▶ Since the 1990's a pioneer in automated code generation
- ▶ SCADE Suite KCG Code Generator used for the A340/600 secondary flight control system
- ▶ Measured Results
 - ▶ *SCADE Suite → 70% of the code*
 - ▶ **No coding error ever found in the code embedded from SCADE Suite**
 - ▶ Development costs **reduced by 50%**
 - ▶ *Specification changes & modified code were more quickly available. A repeatable reduction by a factor of 3x to 4x of the code modification cycle*

DO-178B Level A

Airbus A380

- ▶ After the objective metrics from the A340, Airbus made SCADE the corporate standard for all new airplane development. It is using SCADE on the following systems in the A380:
 - ▶ *Flight Control System*
 - ▶ *Flight Warning System*
 - ▶ *Electrical Load Management System*
 - ▶ *Anti-Icing system*
 - ▶ *Braking and Steering System*
 - ▶ *Cockpit Display System*
 - ▶ *Part of ATSU (Board / Ground Communications)*
 - ▶ *FADEC (Engine Control)*
 - ▶ *EIS2 - Specification IHM Cockpit (4 functions DU (Display Unit)) :*
 - ▼ PFD: Primary Flight Display
 - ▼ ND: Navigation Display
 - ▼ EWD: Engine Warning Display
 - ▼ SD: System Display



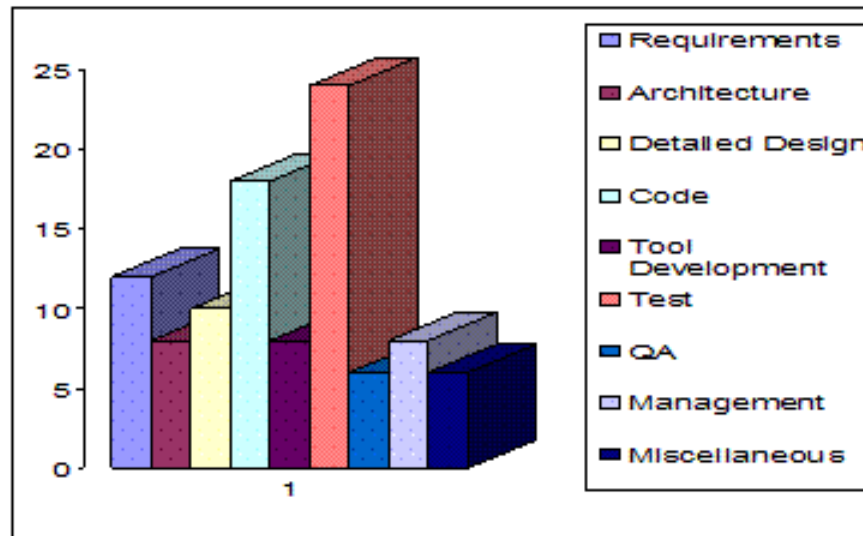
Agenda

- ▶ Overview
- ▶ **Practical Benefits Analysis**
- ▶ SCADÉ Suite Presentation
 - ▶ *Editor*
 - ▶ *Simulator*
 - ▶ *Design Verifier*
 - ▶ *DOORS™ Link*
 - ▶ *Integration with Configuration Management Tools*
 - ▶ *Code Generators*
- ▶ Summary



Where Does the Time Go?

ENEAA Where Does the Time Go on an Avionics Project? TekSci



Copyright 2003, TekSci Proprietary

Slide 72

www.teksci.com

How Does SCADE Suite Cut Costs?

▶ Cost of Coding

- ▶ *Time/Cost to write Ada and C code is greatly reduced .*
 - ▼ *Simply elaborate the design step and get 100% code generation.*
- ▶ *High cost to debug the code goes to ZERO.*
 - ▼ *Step is eliminated for SCADE Suite generated code.*

▶ Cost of Code Reviews

- ▶ *Time/Cost to do Code Reviews goes to ZERO for all SCADE Suite generated code.*
 - ▶ *Step is eliminated.*

▶ Cost of Manual Quality Practices

- ▶ *Time/Cost for requirements traceability from the point of high-level software requirements down to code goes to ZERO.*
 - ▶ *Documented by SCADE Suite hierarchy and direct relationship to code.*

How Does SCADE Suite Cut Costs?

▶ Cost of Making Changes to the Code

- ▶ *Typically cuts Time/Cost by 3X to 4X. Eliminates the need to:*
 - ▼ Update traceability tool/documentation
 - ▼ Debug the new code
 - ▼ Do a code review
 - ▼ Do unit testing (requires use of qualifiable 'C' code generator)

▶ Cost of Structural Testing (requires use of qualifiable 'C' code generator)

- ▶ *Varies for DO-178B level or CMM level, but significant (10% - 30% of project budget). Time/Cost is greatly reduced for SCADE generated code.*
 - ▶ Statement-Level Resting (Level C) – No unit testing required
 - ▶ Decision Coverage (Level B) – No unit testing required
 - ▶ Modified Condition/Decision Coverage ("MC/DC" Level A) – No unit testing required

▶ Cost of Certifying

- ▶ *Eurocopter cut the time to certify from an average of 20 months to a demonstrated 8 months using SCADE Suite (due to better requirements documentation, unquestionable traceability, less testing documentation, more reliable code, etc.)*



How Does SCADE Suite Improve Quality?

SCADE Suite addresses all 3 ways quality is compromised:

▶ Coding Defects (bugs)

- ▶ *Eliminated completely. No defect has ever been found in SCADE generated code.*

▶ Errors in Interpreting HL and LL Requirements

- ▶ *Eliminated. The HLR and LLR are graphically defined using well-known engineering notations (data flow, finite state machines) in an unambiguous, accurate and deterministic way.*

▶ Validating Software Requirements

- ▶ *SCADE Suite provides **Design Verifier**, which can process the underlying SCADE semantics and mathematically **prove** that any specified safety/mission-critical requirement or system property works 100% correctly and has no corner case bugs.*

Agenda

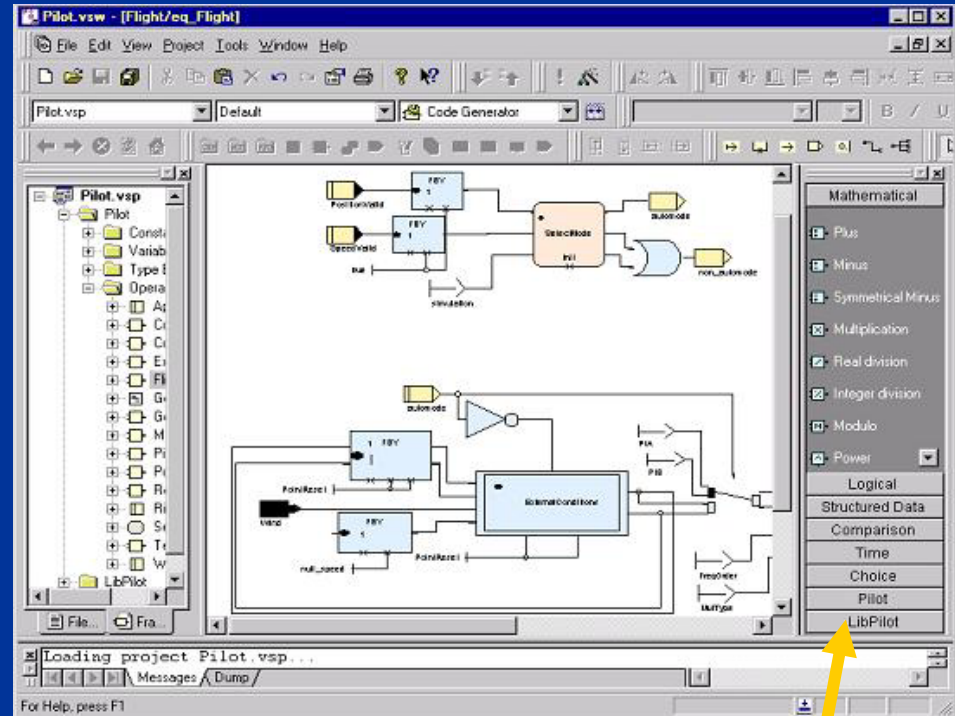
- ▶ Introduction
- ▶ Overview
- ▶ Practical Benefits Analysis
- ▶ **SCADE Suite Presentation**
 - ▶ *Editor*
 - ▶ *Simulator*
 - ▶ *Design Verifier*
 - ▶ *DOORS™ Link*
 - ▶ *Integration with Configuration Management Tools*
 - ▶ *Code Generators*
- ▶ Summary



User-Friendly

- ▶ Powerful creation & modification

- ▶ *Easy to learn and use*
- ▶ *Windows and UNIX*
- ▶ *Project creation wizards*
- ▶ *Automatic backup*
- ▶ *Global print function*
- ▶ *Easy block connections*

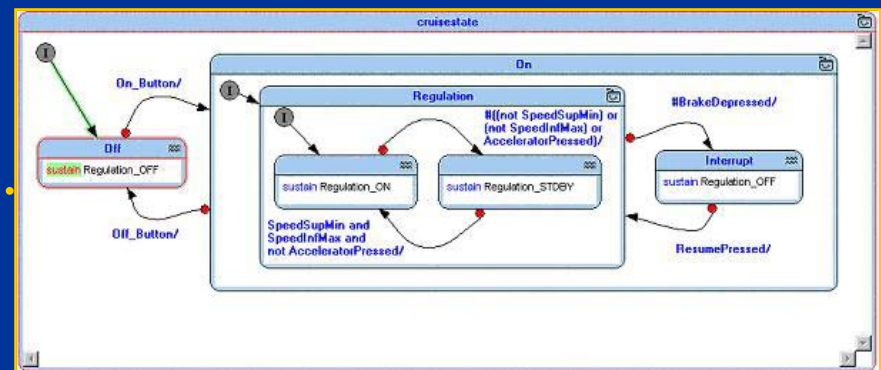
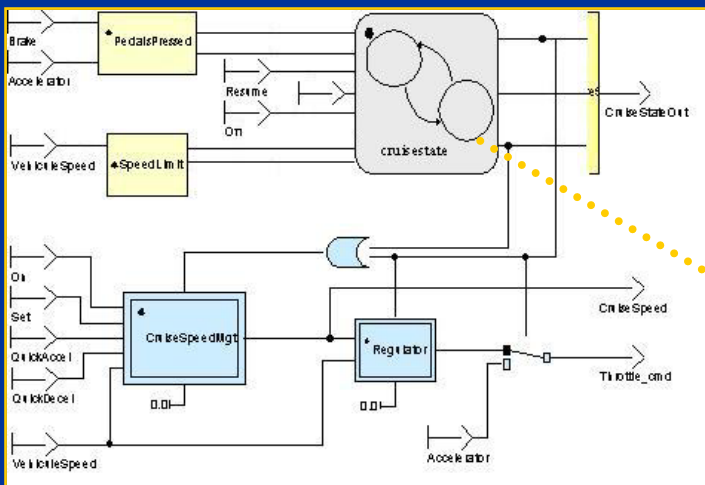


- ▶ Easy reuse of previous designs (libraries)
- ▶ Easy to read, easy to understand, easy to maintain

Libraries

Safe State Machine Diagrams

- ▶ Design a complete system with precise formalisms (non-ambiguous, deterministic)
- ▶ Simulate it right away (interactive and batch modes)
- ▶ Prove that the safety properties hold for all the possible inputs values
- ▶ The single tool to fully integrate data flows and state machines with a single code generation chain enabling automatic generation of safe production code



Automatic Documentation Generation

Reporter:

- ▶ Word (RTF) and HTML formats
- ▶ Printed entities (nodes, variables, types, etc.) can be filtered
- ▶ Customizable general parameters (author name, date, etc.)

SCADE: Detailed Design Document

Description of the application pilot

Author: Esterel Technologies
Reference: SCADE Design Document
Index: 01.01
Date: 08/04/2002

Types

Piloteage_type

Type Name	Type Definition	Comments
FullState	void*int	Item_1: Input data type: 3 coordinates and 1 flag to check the validity of the coordinate
Speed	float	Item_1: 3D vector for a speed.
SP	float	
SA	float	Item_1: X coordinate for a 3D speed vector
SA	float	Item_1: Y coordinate for a 3D speed vector
SA	float	Item_1: Z coordinate for a 3D speed vector
SP	float	Item_1: coordinates for 3D speed vector.
X	float	
Y	float	
Z	float	
point	float	Item_1: X, Y and Z coordinate in a cartesian system
X	float	
Y	float	
Z	float	
int32	int32	
int16	int16	
int8	int8	
uint32	uint32	
uint16	uint16	
uint8	uint8	
void*	void*	Item_1: Variable data type: Each field is a digit which is the 0 or 1 in the measurement which is linked to a dead.
void*	void*	
void*	void*	

Nodes

Flight

Name	Type	Check	Comment
SP	float	*	*
SA	float	*	*
SA	float	*	*
SA	float	*	*
SP	float	*	*
X	float	*	*
Y	float	*	*
Z	float	*	*

Local variables

Name	Type	Check	Annotation
int32	int32	*	*
int16	int16	*	*
int8	int8	*	*

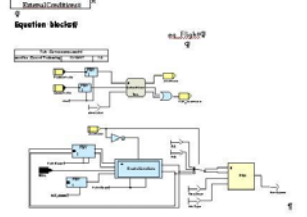
Called Operators

Name	Type	Check	Comment
int32	int32	*	*

Called Operators

Name	Type	Check	Comment
int32	int32	*	*
int16	int16	*	*
int8	int8	*	*
ExternalConstraint			

Equation blocks



Equ3Sum

Name	Type	Check	Annotation
int32	int32	*	*
int16	int16	*	*

Hidden inputs

Name	Type	Check	Annotation
int32	int32	*	*

Local variables

Name	Type	Check	Annotation
int32	int32	*	*

Outputs

Name	Type	Check	Annotation
int32	int32	*	*

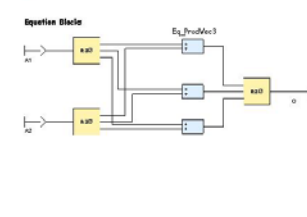
Called Operators

Name	Type	Check	Comment
int32	int32	*	*

Called Operators

Name	Equation block
int32	Equ3Sum
int16	Equ3Sum
int8	Equ3Sum

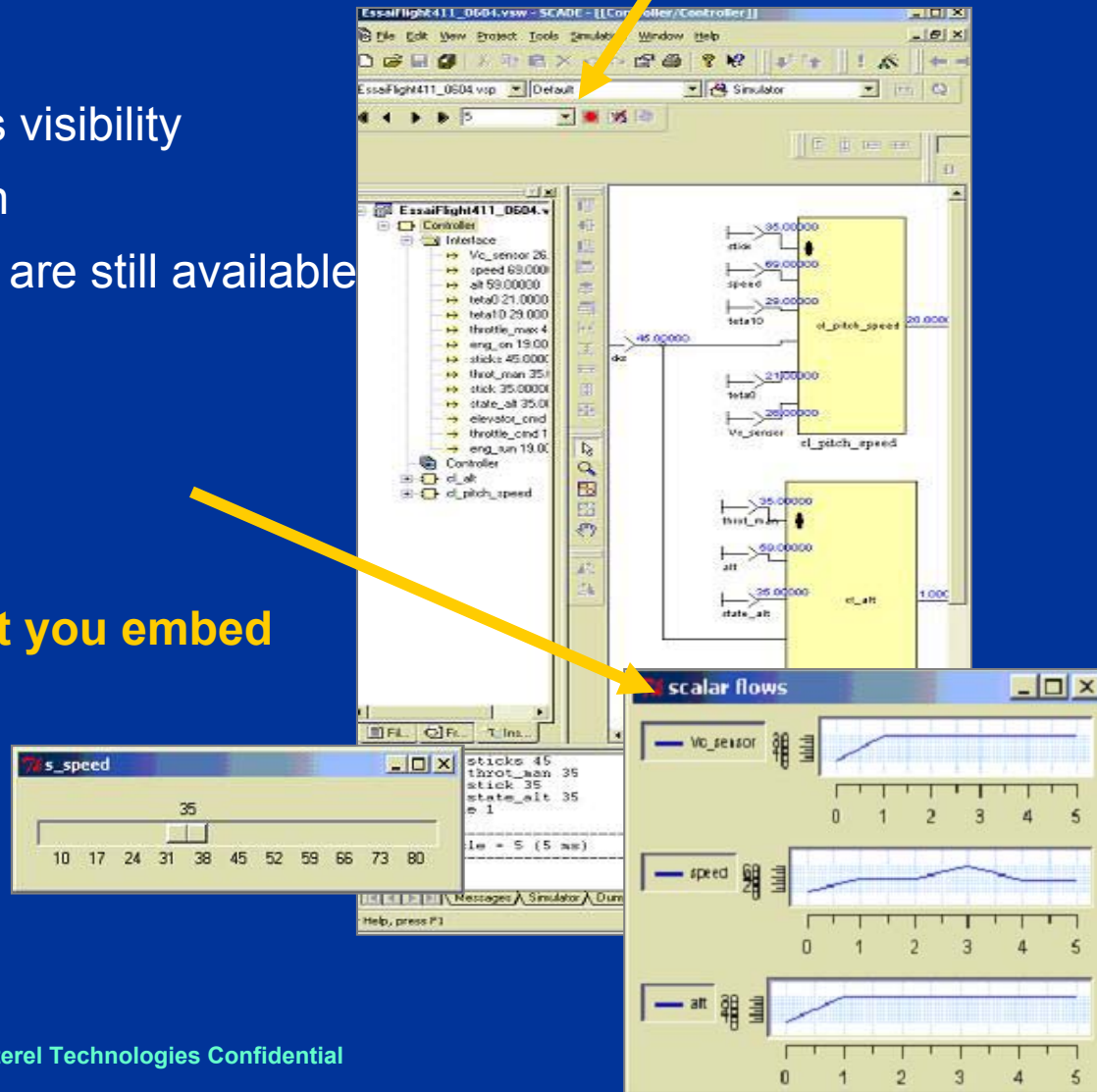
Equation Block



Graphical Simulation & Debugging

- ▶ Graphical simulator integrated in SCADE Suite GUI
- ▶ Debugging features
 - ▶ Maximization of variables visibility
 - ▶ Block-by-block simulation
 - ▶ Note that stop conditions are still available
- ▶ Graphical widgets

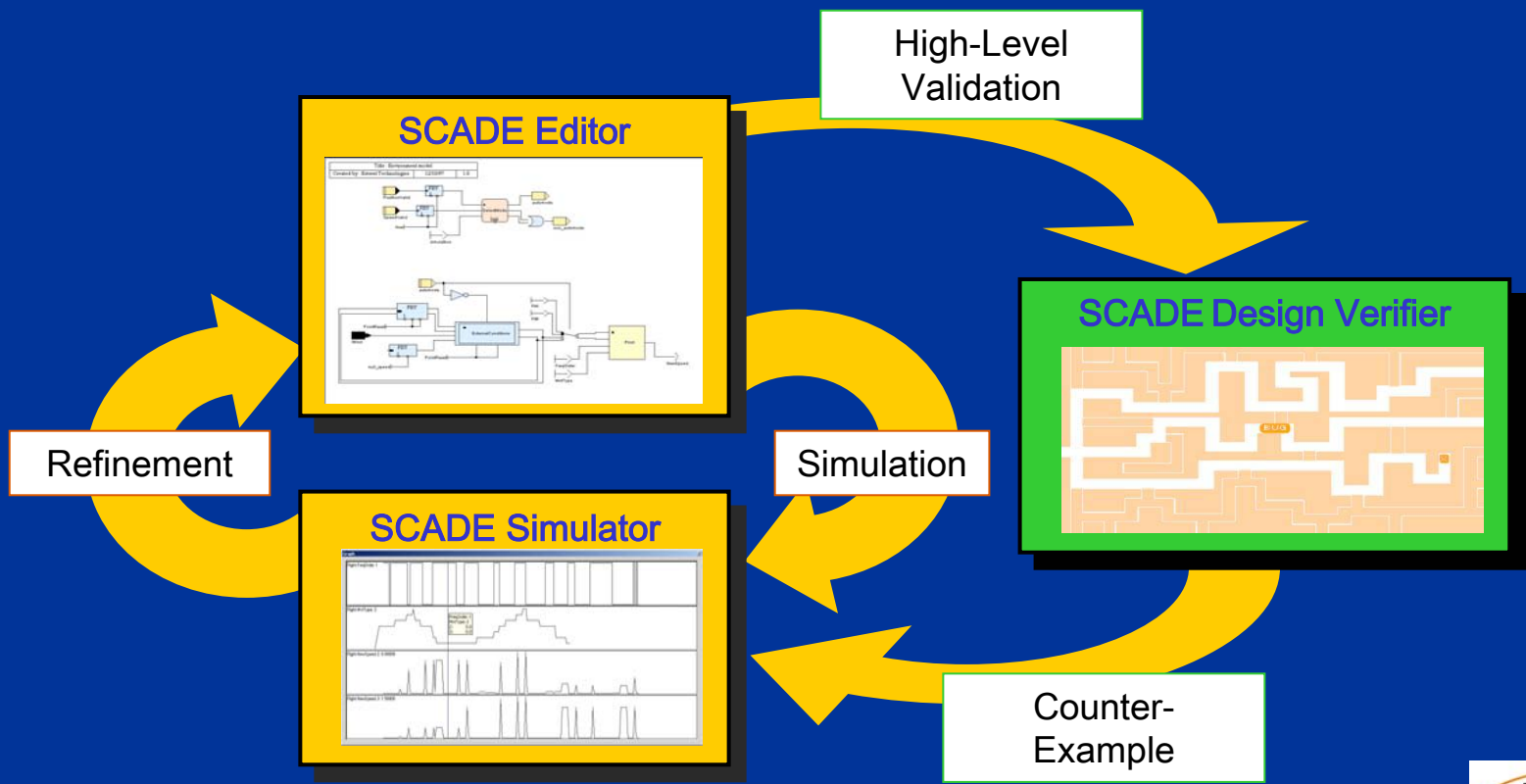
What you simulate is what you embed



Technological Breakthrough on Design Validation

SCADE Suite
Design Verifier:
Your Assistant for
Your Design Validation

- ▶ Early detection of bugs without writing tests
- ▶ Handling of both data & control flows
- ▶ Customers' designs with 100's of SCADE nodes verified in seconds



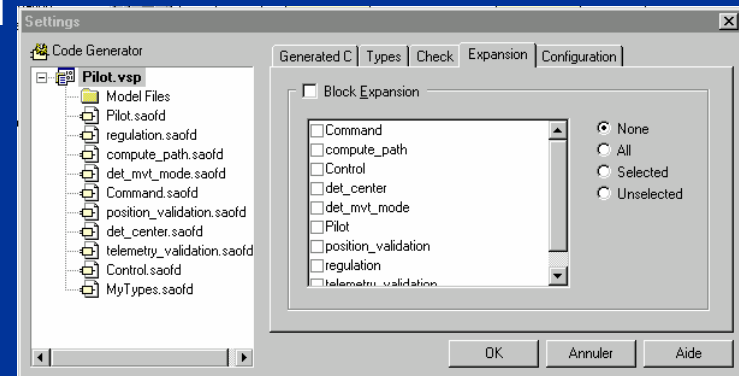
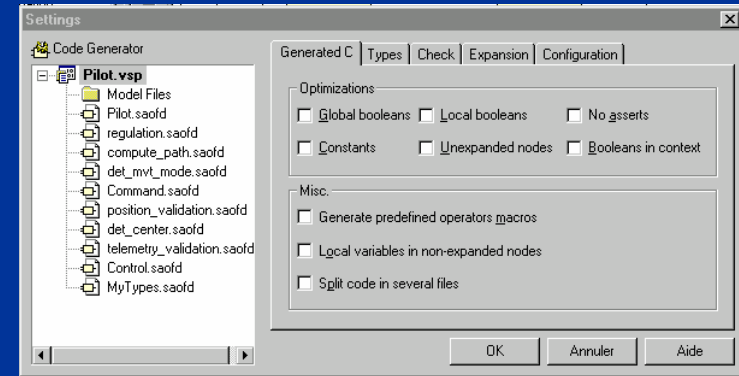


Automatic Generation of Safe Production Code That Is “Correct by Construction”

- ▶ Three code generators:
 - ▶ **Ada 83/95** Code Generator
 - ▶ Regular **ANSI C** Code Generator
 - ▶ Qualifiable C Code Generator (KCG)
 - ▼ DO-178B Level A qualifiable, as a development tool
- ▶ SCADE Suite generated code matches safety objectives
 - ▶ *Portable, strictly conforming to ANSI standards*
 - ▶ *OS independent*
 - ▶ *Static memory allocation*
 - ▶ *Bounded stack*
 - ▶ *Readable & traceable*
 - ▶ *Deterministic behavior guaranteed*

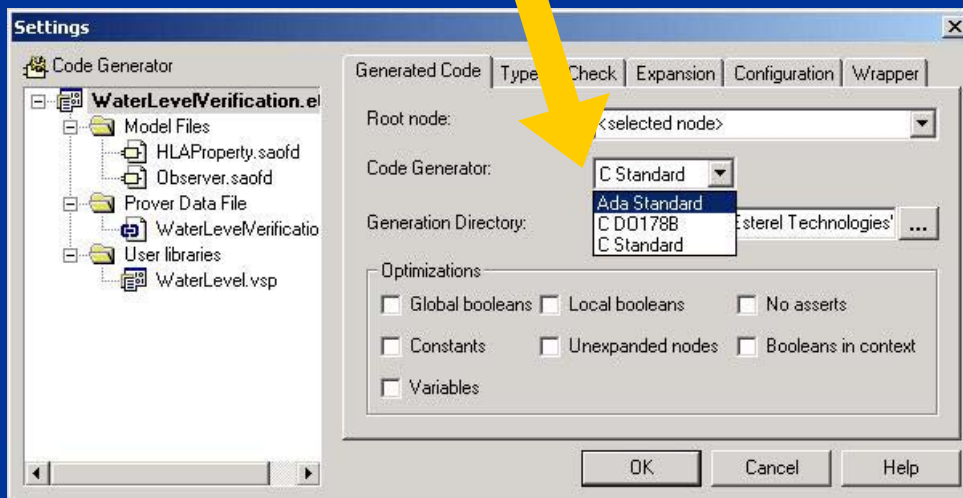
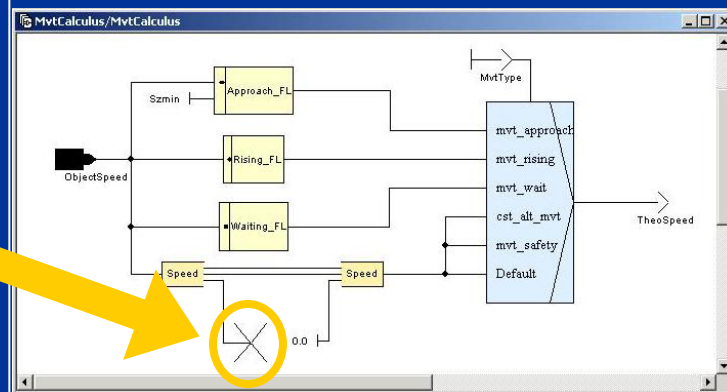
Efficient & Modular Generated Code

- ▶ No dependency loop. Every variable is computable. Clock and sub-clock processes are consistent.
- ▶ Easy and safe integration with existing code.
- ▶ Modular code generation.
- ▶ Generated code is easy to test. No complicated structures. No dead code.
- ▶ Typed variables.



Regular Ada & C Code Generation

- ▶ Embed a more efficient code
- ▶ Filter the warnings
 - ▶ *Terminators on unused outputs*
- ▶ Generate SPARK syntax-compliant Ada code with a mouse-click

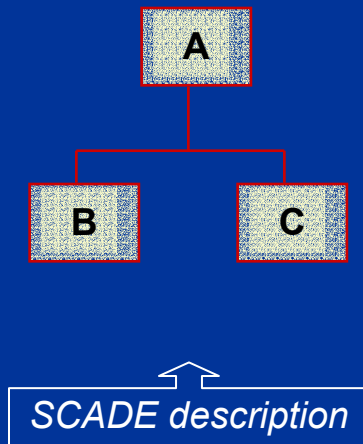


Tailor Code Generation to Target

- ▶ Code generation is **customizable** to target and project constraints

For instance:

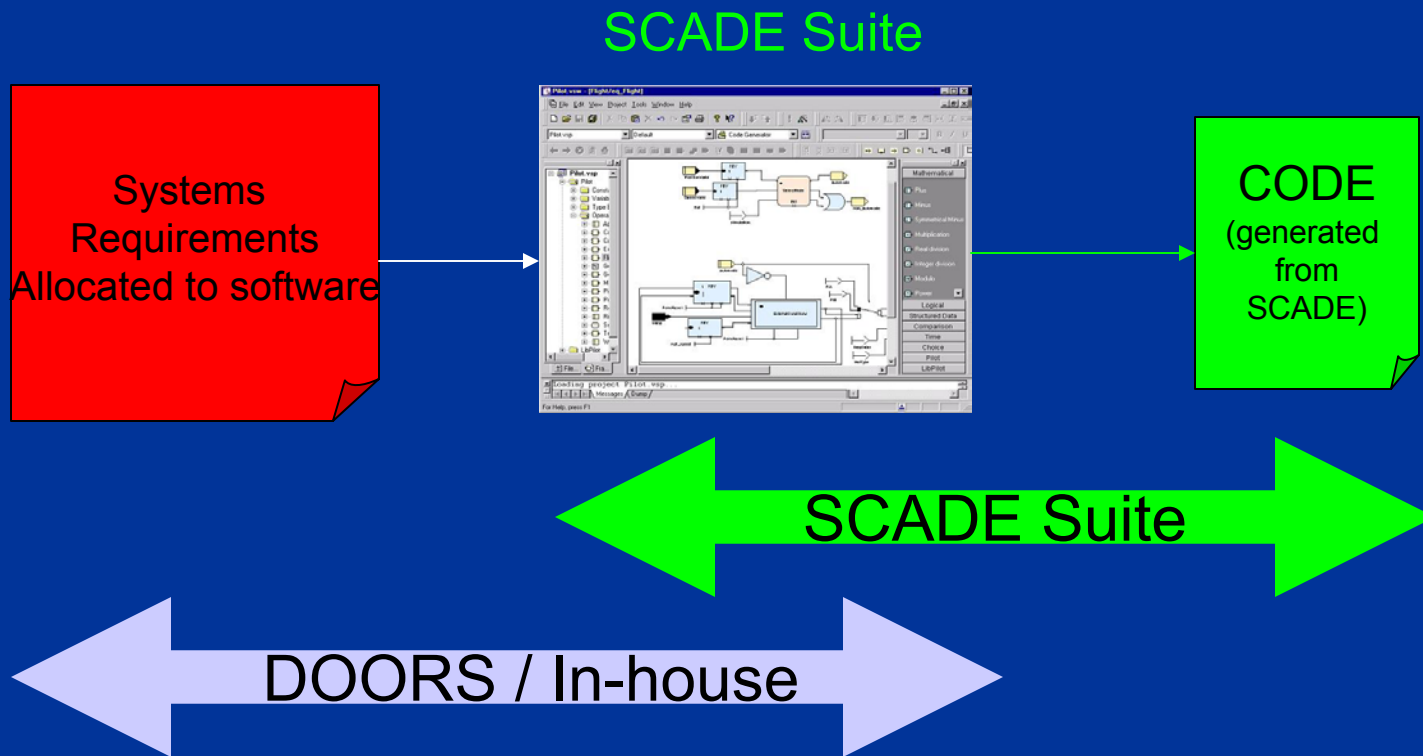
- ▶ *Call Mode: Each SCADE operator generated as a function*
- ▶ *Inline Mode: The whole sub-tree code is expanded in one function*



Call mode	Inline mode
A{	A{
...	...
B();	/*begin of B */
...	...
C();	/*end of B */
...	...
}	/*begin of C */
	...
	/*end of C */
	...
	}

Requirements Traceability

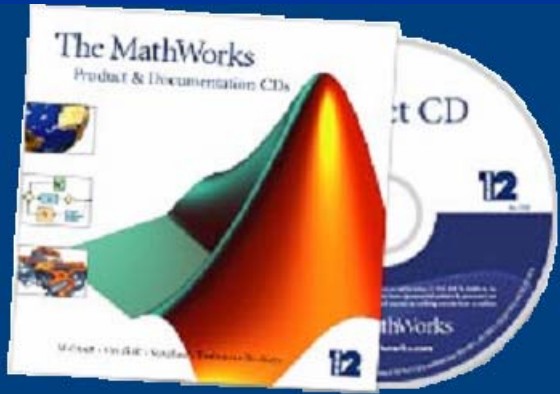
- ▶ Traceable flow from systems requirements to software design and code
 - ▶ *Since SCAD Suite generates the code, tracing to the design is the same as tracing to the code. You can eliminate the manual effort to create and maintain the links to code if you use SCAD Suite.*



A Bi-Directional Gateway

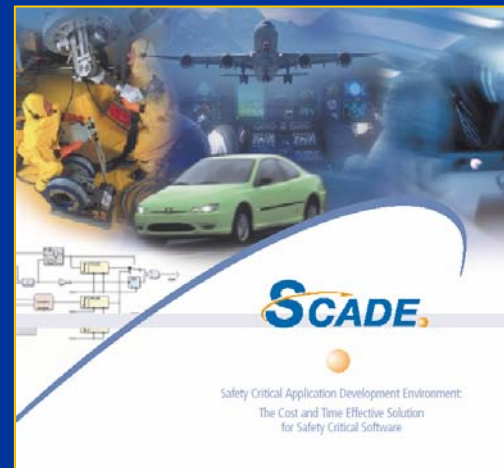
Simulink™ Gateway Translator

- ▶ Embedded software
- ▶ Deterministic behavior
- ▶ Embedded software validation
- ▶ Exhaustive proof
- ▶ Production code
- ▶ Portable code
- ▶ DO-178B Level A qualifiable code



- ▶ Physical & control laws
- ▶ Prototyping
- ▶ Global simulation & tuning

Simulink™ Gateway Wrapper as an S-function



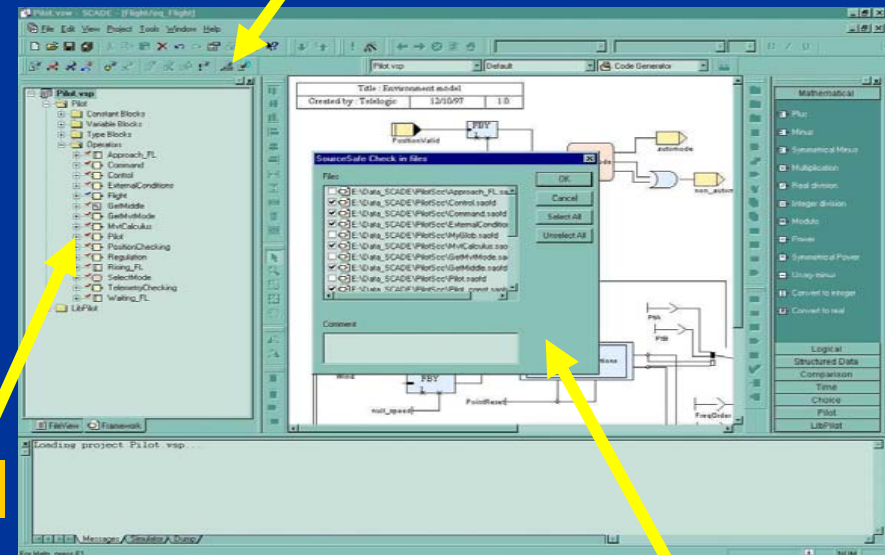
Source Code Control Integration

- ▶ Easily manage multiple design versions with the SCADA Suite plug-in integration with leading Configuration Management Tools*

- ▶ ClearCase™
- ▶ CM Synergy™ (ex-Continuus CM)
- ▶ CVST™
- ▶ eChangeMan™
- ▶ Perforce™
- ▶ PVCS™
- ▶ Visual Source Safe™

Direct access to the main version management commands ...

Visual feedback



... such as Check In

* Integration based on Microsoft® SCC API



Download Code for "Hardware in the Loop" Prototyping



SCADE Application in an Experimental Prototype

Cockpit Control Terminal

VME Exp. Computer



RDI SPARC Laptop



Summary

"If we are to obtain results never before achieved,
we must employ methods never before attempted."

Sir Francis Bacon

- ▶ **SCADE Suite is an easy to learn and use modeling tool. The heavy lifting is under the hood in the tool's rigorous semantics, code generation algorithms, and Design Verifier technology. SCADE Suite does not involve a paradigm shift or lengthy learning curve.**
- ▶ **SCADE Suite has been in production for 8 years, with documented repeated success in real-world applications. It has an unrefuted track record of cutting costs by 20% to 50%.**
- ▶ **SCADE Suite improves the quality of your code, documentation, and traceability while substantially reducing redundancy and busywork.**
- ▶ **The World Technology Award committee has twice nominated Esterel Technologies' Chief Scientist in recognition of the significance of this technology.**
- ▶ **If you are doing work regulated by DO-178B, there are no other software development tools on the market that can give you the improvements you get from SCADE Suite.**