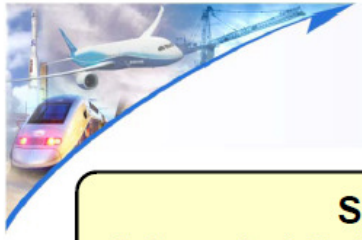
SCADE – Safety Critical Application Development Environment

Presented By

Divya Udayan J

VR Lab



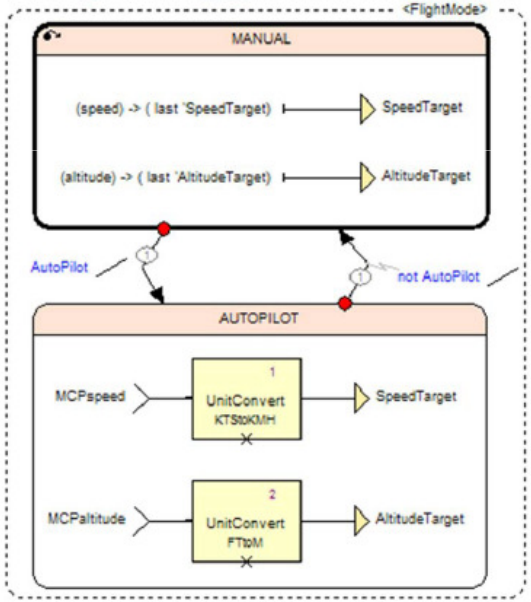
Mission and Safety-Critical Design with Embedded Graphics

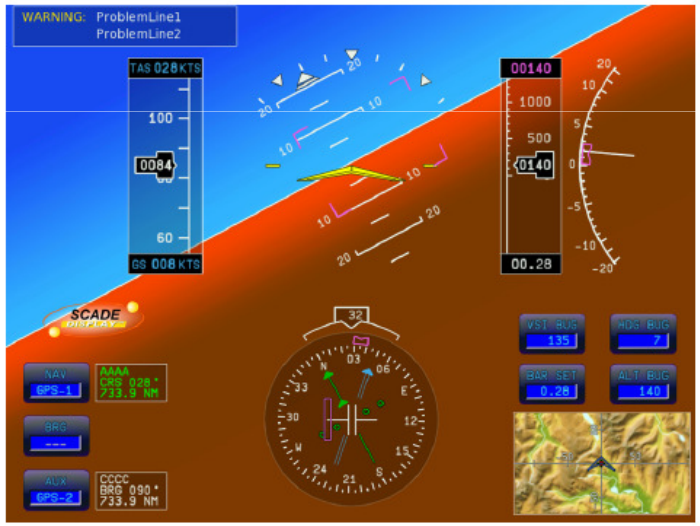
SCADE Suite
Integrated Data Flow & State Machines

SCADE Display
Embedded Graphics

SCADE SUITE™

SCADE DISPLAY™





Fully Integrated Design Suite

What is Unique About SCADE ?

- SCADE is being developed specifically to address mission and safety-critical embedded applications

- SCADE is certified/qualified according to following international safety standards:
  - **DO-178B** qualification up to Level A – Aerospace & Defence
  - **IEC 61508** certification up to SIL 3 – Transportation & Industry
    - In use on SIL 4 applications
  - **EN 50128** certification up to SIL 3/4 – Rail Transportation
  - **IEC 60880** full compliance – Nuclear Industry

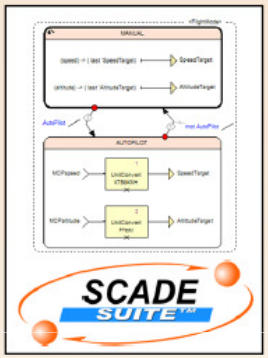
The SCADE Certified Software Factory

SYSTEM SPEC

Algorithm Design Capture

Architecture Design Capture

DESIGN



VERIFY

Debugging & Simulation

Formal Verification

Time & Stack Analysis

Model Coverage Analysis

Object Code Verification

SCADE Suite/SCADE Display Integration

Rapid Simulation

Design Checking

GENERATE

SCADE Suite KCG

RTOS Adaptors

SCADE Display KCG

OpenGL|SC Compliant

SYSTEM TEST

MANAGE & TRACE

Requirements Management Gateway

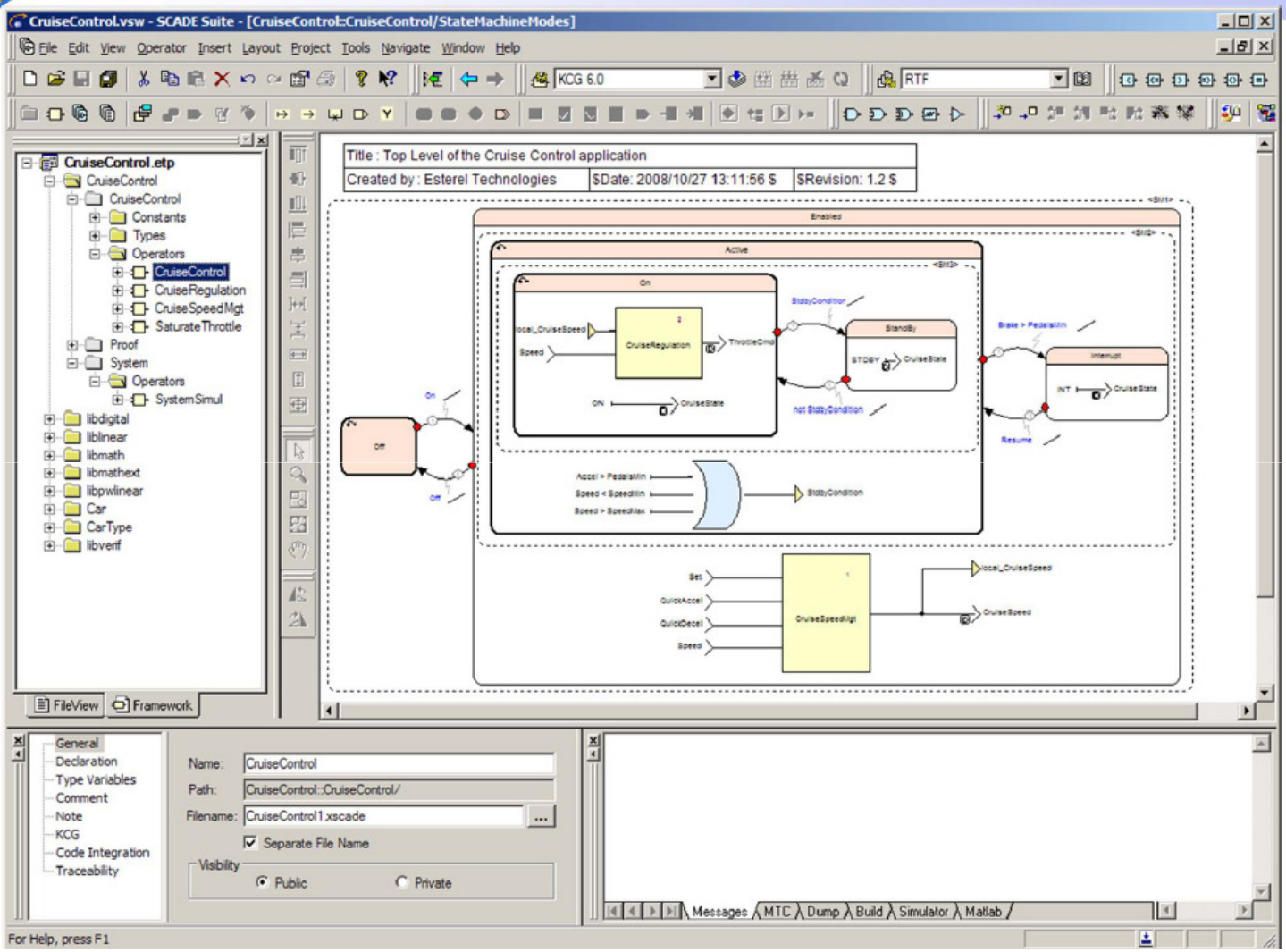
Integrated Configuration Management

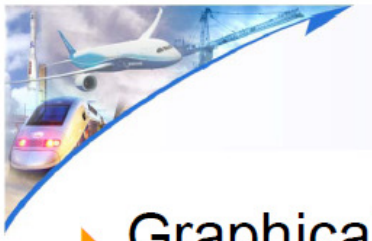
Automatic Design Documentation

DO-178B
IEC 61508
EN 50128

Certification Kits, Certificates & Handbooks

SCADE Suite Editor





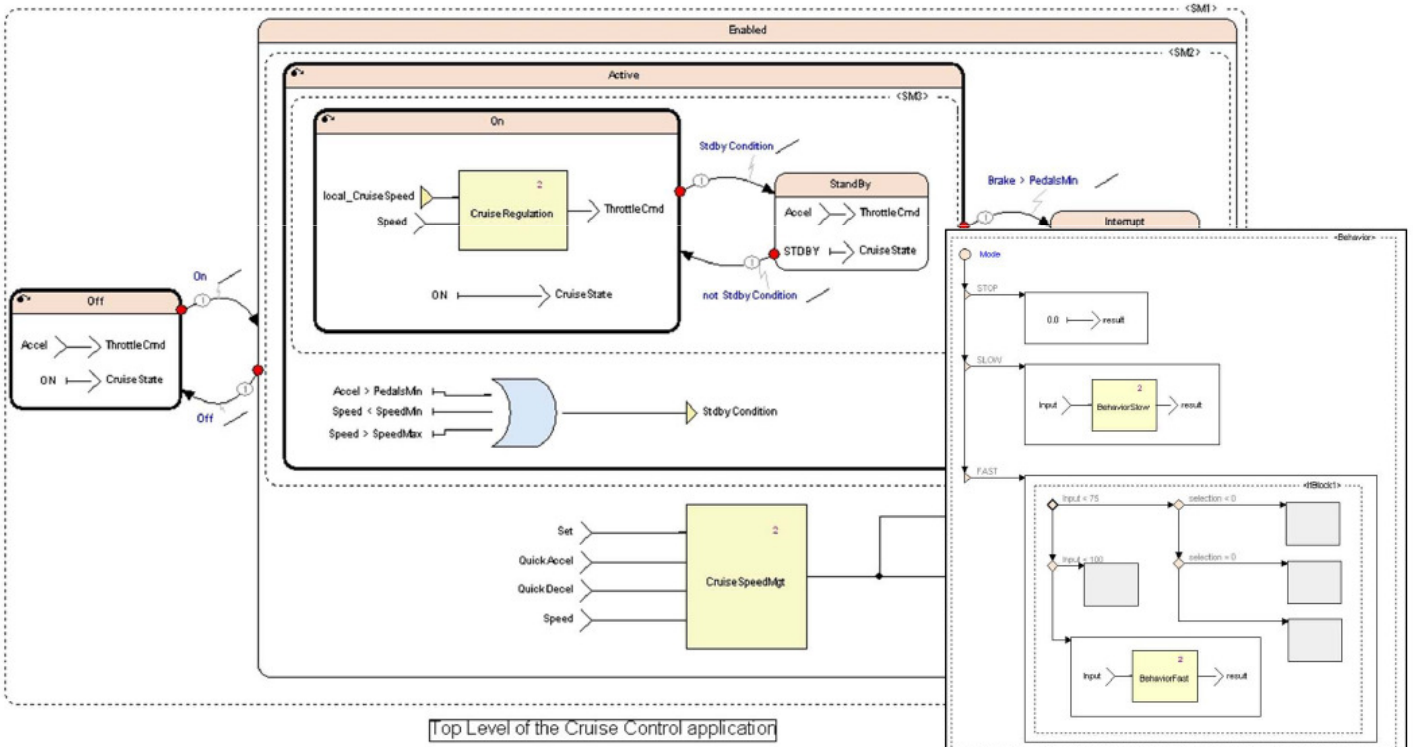
Unified Modeling Style
Modeling Capabilites

- Graphical formalism
  - Block diagrams, to specify the algorithmic part of applications, such as control laws and filters
  - Hierarchical state machines, to model the control part of applications
  - Decision diagrams
  - Packages, data types, constants
  - Arrays & iterators
  - Libraries
- The unique **integration of data flow and safe state machines** allows you to model the whole application with the same formalism

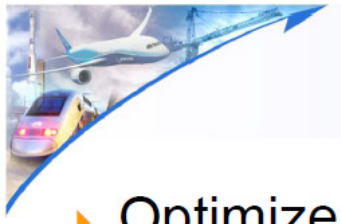
Unified Modeling Style

Integrated Data Flow & State Machines

- Modeling flexibility:
  Power of nested data flow & control flow



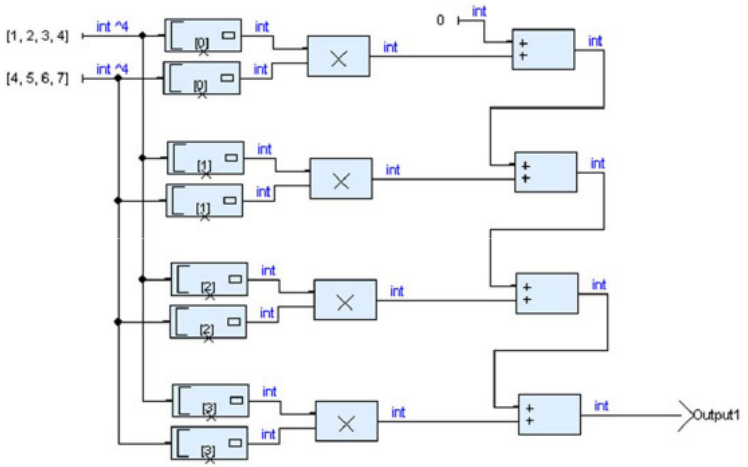
Top Level of the Cruise Control application



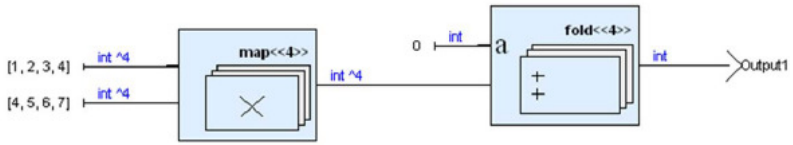
Unified Modeling Style
Arrays & Iterators

- Optimize the design, while preserving safety
  - Example Scalar Product

Without iterators

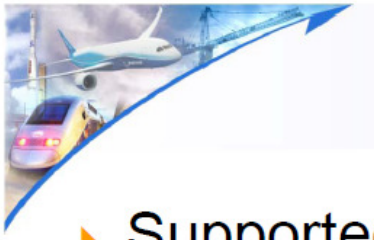


With SCADE 6 iterators



SCADE Suite was created for Safety

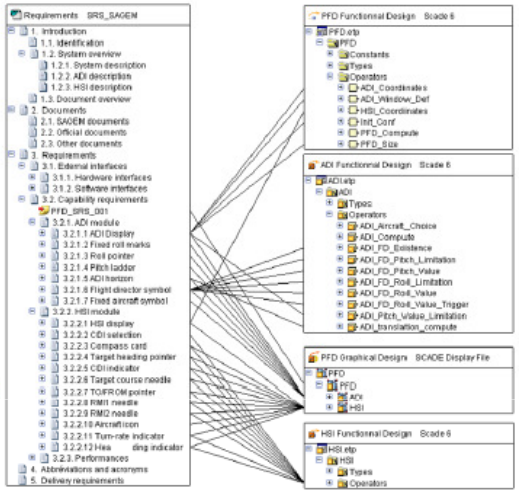
- The Scade language is **formally defined** with **key safety objectives**:
  - Fully deterministic models only comprising **safe constructs**
  - The language is simple and stable
  - Modular, strongly typed, explicit specification
  - Interpretation of a Scade model does not depend on the reader nor its environment
  - Very active research work for more than 10 years
- Designed in close collaboration with certification authorities in the aeronautics, transportation & nuclear energy domains
  - SCADE Suite KCG is a C code generator developed with DO-178B level A, EN 50128 & IEC 61508 certification objectives



Requirements Management Gateway

Integrated Requirements Management & Traceability

- Supported Tools & Formats
  - **Microsoft® Office** tools: Word, Excel®, Access®, Visio®
  - **Code files** (C, C++, test log files)
  - **Technical Communication** tools: Adobe® FrameMaker® and Acrobat® PDF
  - **Requirements Management** tools: IBM® DOORS®, Rational RequisitePro®, CaliberRM™
  - **Modeling & Design** tools: The Mathworks™ Simulink®, Stateflow®, Artisan Studio®
  - **Test** tools: Rational® Test RealTime



SCADE Suite Libraries

libpwlinear

pwlinear package

Clock Counter · Counter · Dead band symmetrical · Dead band un-symmetrical

Limiter symmetrical · Limiter un-symmetrical · Pre-load symmetrical · Pre-load un-symmetrical

Quantizer · Rate limiter · Falling Hysteresis · Rising Hysteresis

lut package

1D Look-up table · 2D Look-up table

+ variants

liblinear

linear package

Memory · Basic memory · Hit crossing falling · Hit crossing rising · Hit corssing either

Derivative · Forward integrator · Trapezoid integrator · Mean over 2 cycles · Mean over 3 cycles

libdigital

digital package

Bool vector to integer · Integer to bool vector

Rising edge · Falling edge · Either edge · Count down

Rising edge no retrigger · Rising edge retrigger · Falling edge no retrigger · Falling edge retrigger

Flip flop set priority · Flip flop reset priority · Flip flop JK · Toggle

truthtables package

Truth table · Exhaustive truth table · Index only truth table

filters package

$$\frac{N}{D_0 + D_1 z^{-1}} \qquad \frac{N_0 + N_1 z^{-1}}{D_0 + D_1 z^{-1}}$$

$$\frac{N}{D_0 + D_1 z^{-1} + D_2 z^{-2}} \qquad \frac{N_0 + N_1 z^{-1}}{D_0 + D_1 z^{-1} + D_2 z^{-2}}$$

$$\frac{N}{D_0 + \ldots + D_{d-1} z^{-(d-1)}} \qquad \frac{N_0 + \ldots + N_{n-1} z^{-(n-1)}}{D_0 + \ldots + D_{d-1} z^{-(d-1)}}$$

Discrete filters (+ normalized versions)

$$\frac{N}{D_0 z + D_1} \qquad \frac{N}{D_0 z^2 + D_1 z + D_2} \qquad \frac{N}{D_0 z^{d-1} + \ldots + D_{d-1}}$$

$$\frac{N_0 z + N_1}{D_0 z^2 + D_1 z + D_2} \qquad \frac{N_0 z^{n-1} + \ldots + N_{n-1}}{D_0 z^{d-1} + \ldots + D_{d-1}}$$

Transfer functions

libmath

math package

Boolean to integer · Boolean to real · Integer to boolean · Real to boolean

In range in / in · In range in / out · In range out / in · In range out / out

Round nearest · Round towards floor · Round towards ceil · Octet to integer

Minimum · Minimum of 3 · Maximum · Maximum of 3

Mean · Mean of 3 · Absolute · Sign of

vect package

Matrix . matrix · Matrix . vector · Vector . matrix · Scalar product

Checker
Design Consistency Checks

- SCADE Editor Checker performs **specification integrity verification** at model level
  - Semantic verification, Strong data typing, Sub clocks, Data dependencies, Cycle detection
  - HTML report with hyperlinks to locate the errors

Friday January 11 2008 14:30:55

Result of check for operator CruiseControl::CruiseControl/ in model CruiseControl

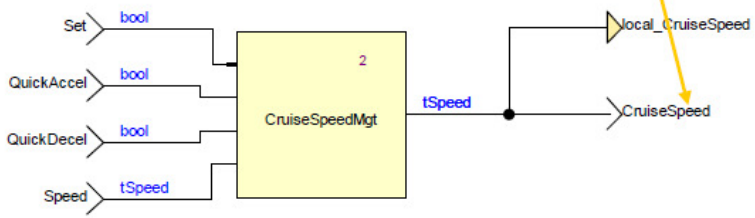
1 error(s) detected - 0 warning(s) detected

Category	Code	Message
Semantic Error	ERR_100	**Type: Type mismatch at** CruiseControl::CruiseControl/CruiseSpeed/ This expression has type (real) but is here used with type (bool)

End of document.

Error message: Incompatible type interface

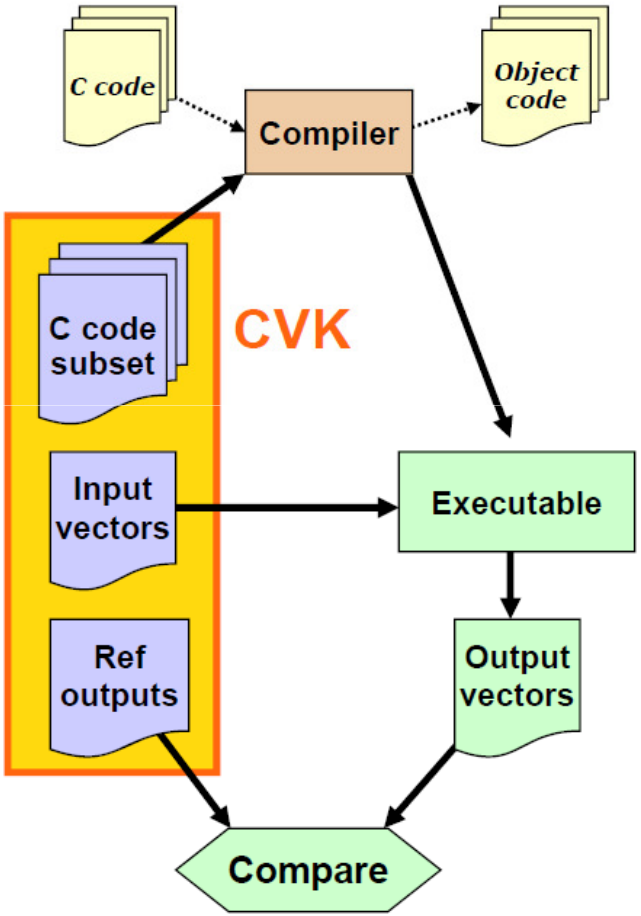
locate



Compiler Verification Kit (CVK)

Object Code Verification

- SCADE Suite CVK is:
  - A **complete subset of C constructs** that can be generated from SCADE Suite
  - A series of inputs & reference output vectors **ensuring MC/DC coverage at object code level**
- This approach is accepted by safety authorities **(CAST-12 §h)**

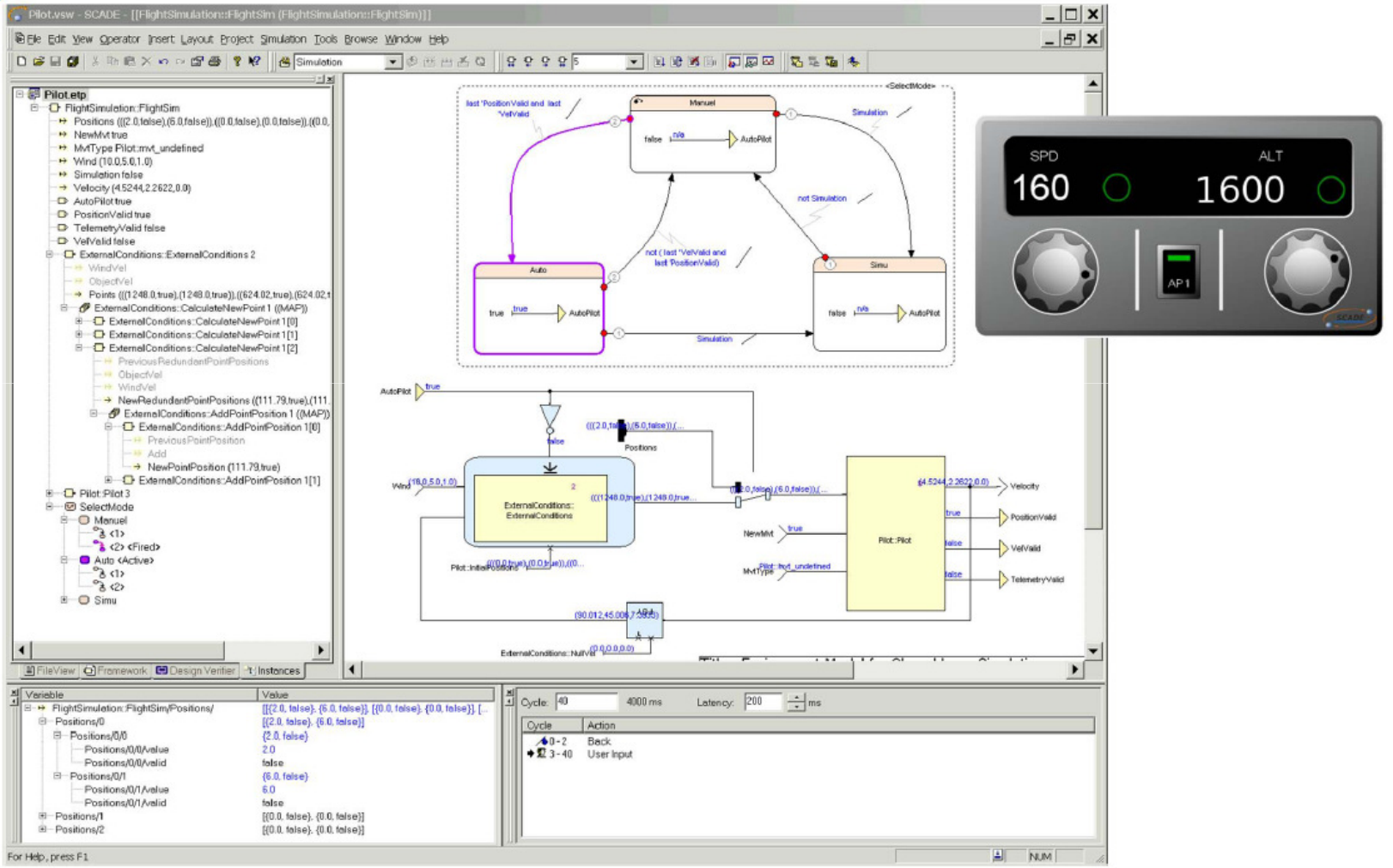


SCADE Suite KCG
Generated Code Properties

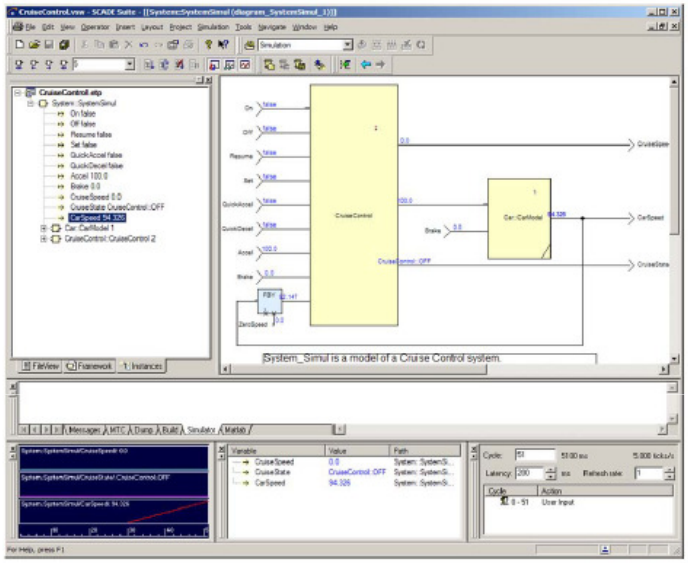
- SCADE Suite KCG produces simple C code that fits the constraints of safety-critical embedded software
  - **Portable** (ANSI C, compiler, target and OS independent)
  - **Readable** and **traceable** with respect to the design (name / annotation propagation)
  - **Optimized** code for all constructs
  - Structured (by functions or by blocks)
  - Static memory allocation
  - No pointer arithmetic
  - No recursion, bounded loops only
  - Bounded execution time

Simulator

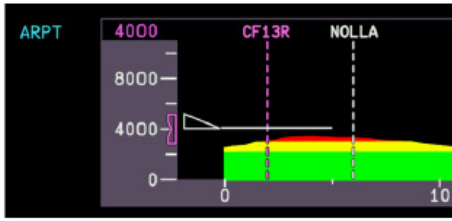
Debugging & Simulation at Model Level

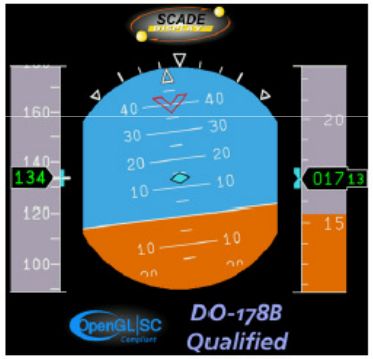


Integrated Simulation with SCADE Display



SCADE Suite Simulator



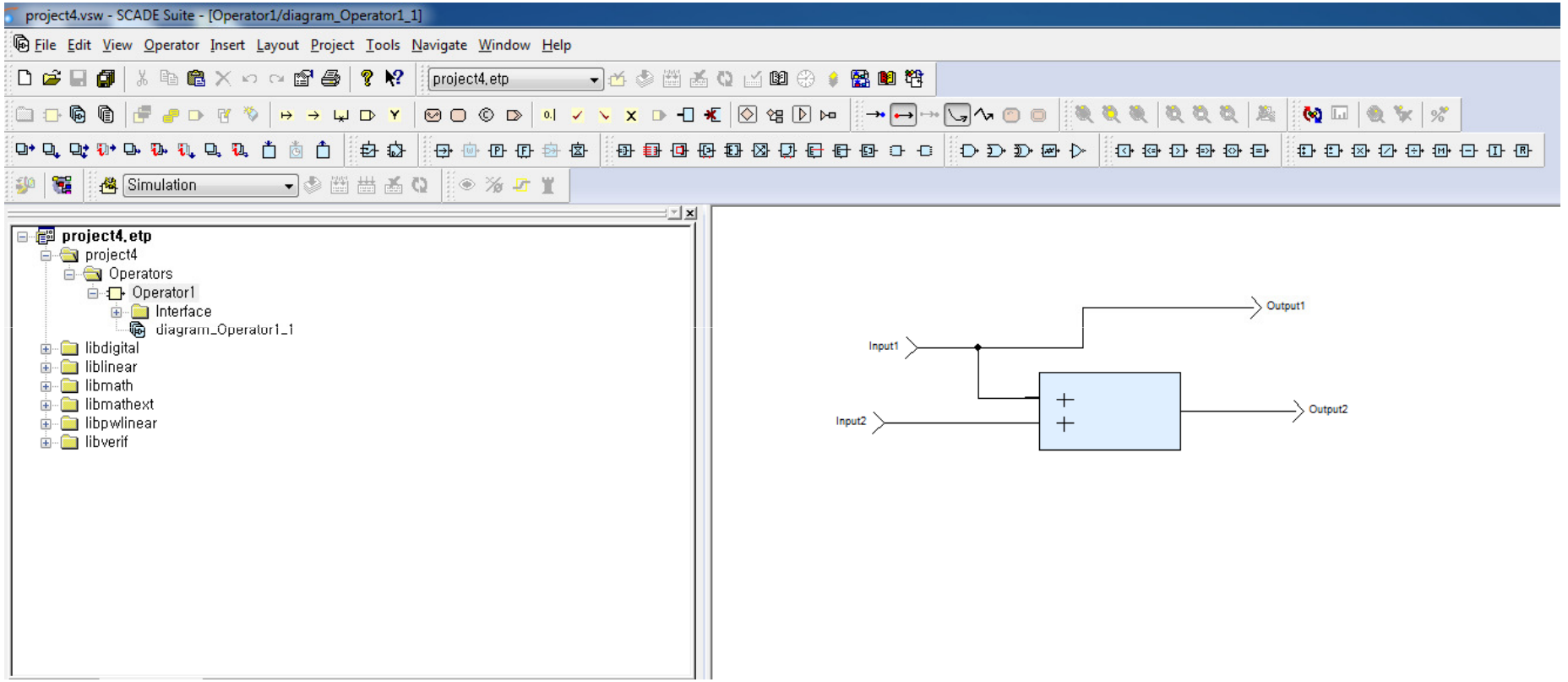


SCADE Display Panels

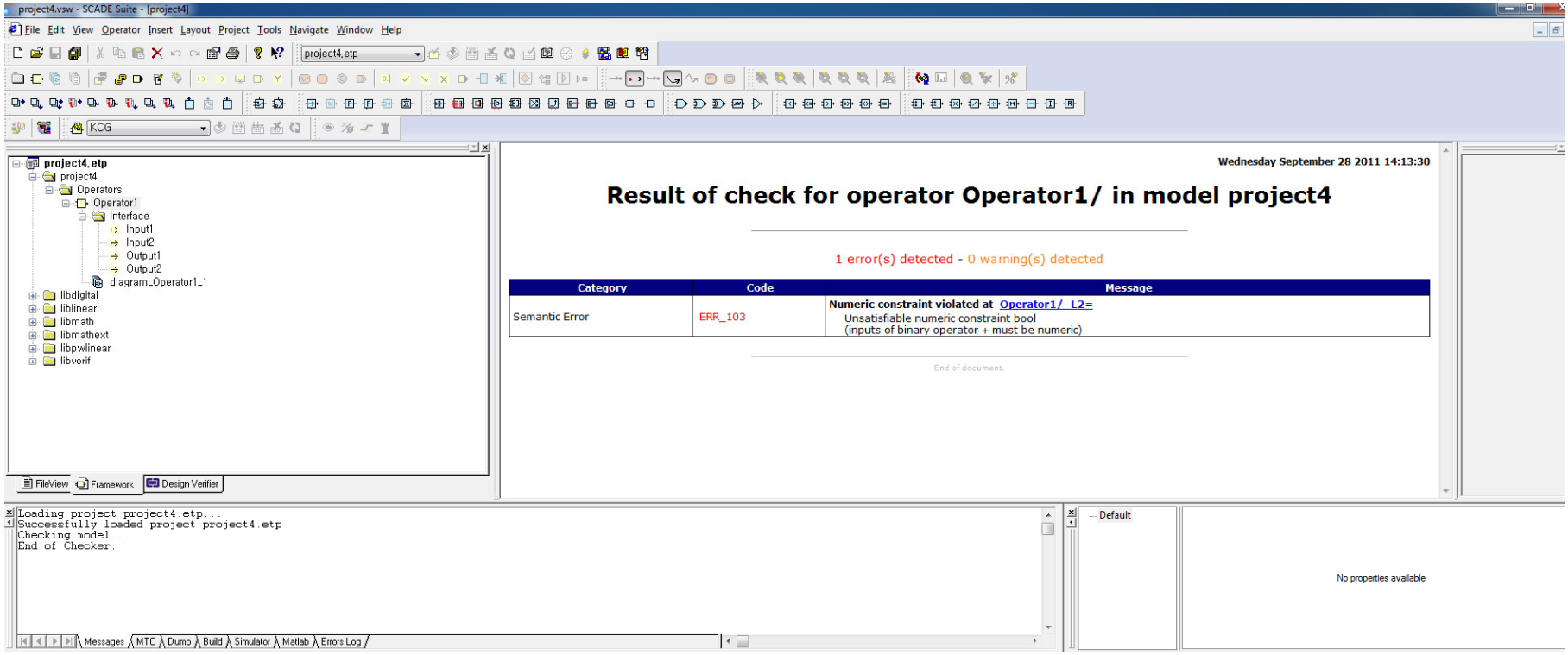
- Integrated simulation capabilities
  - Tight integration of SCADE Suite & SCADE Display generated code ensures good simulation performance

DESIGN EXAMPLE

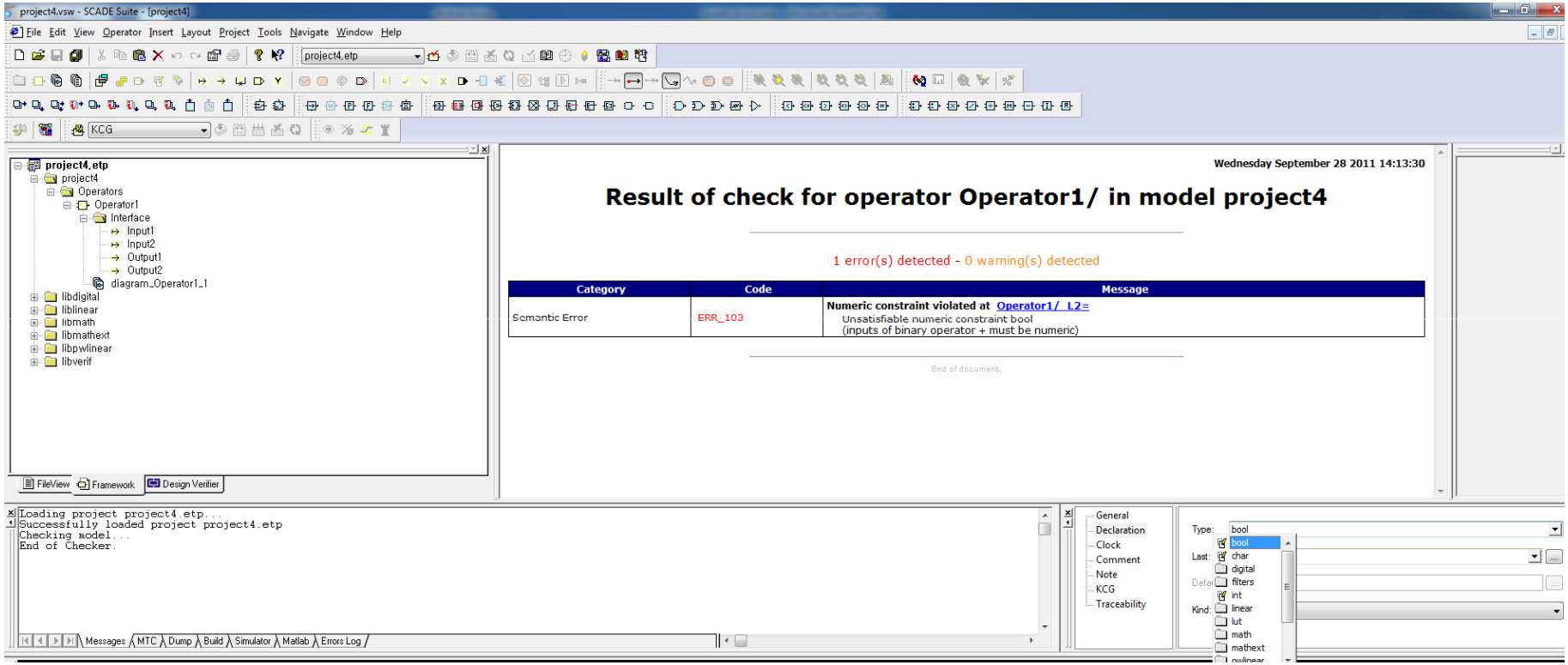
Modeling & Interfacing



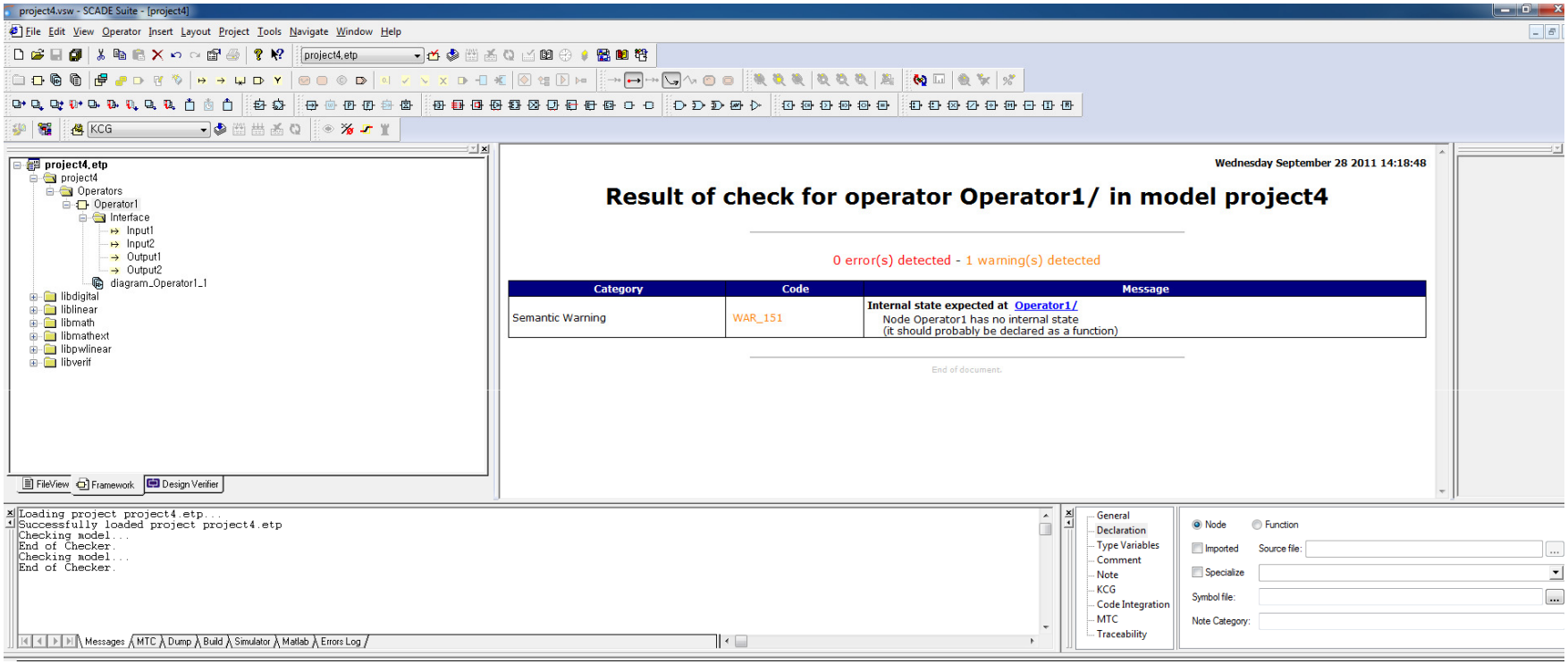
Model Checking(1/4)



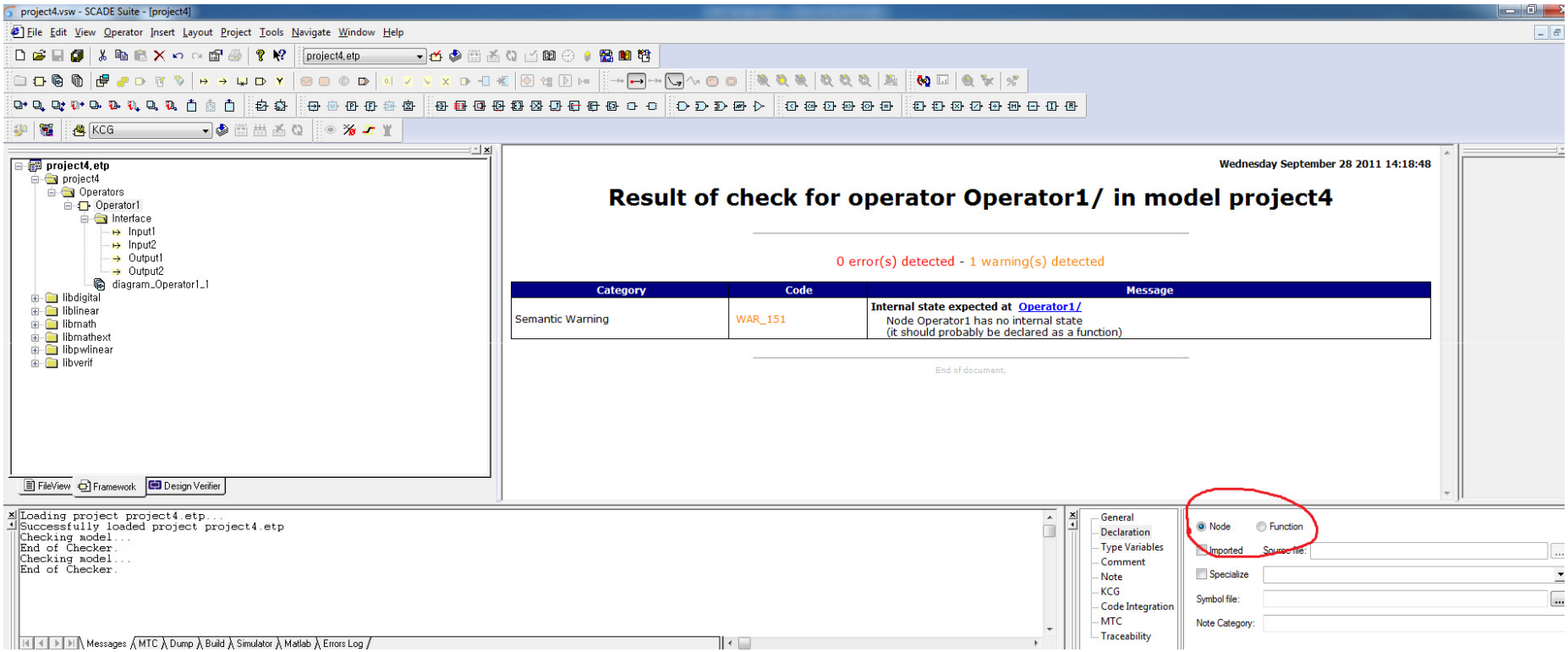
Model Checking(2/4)



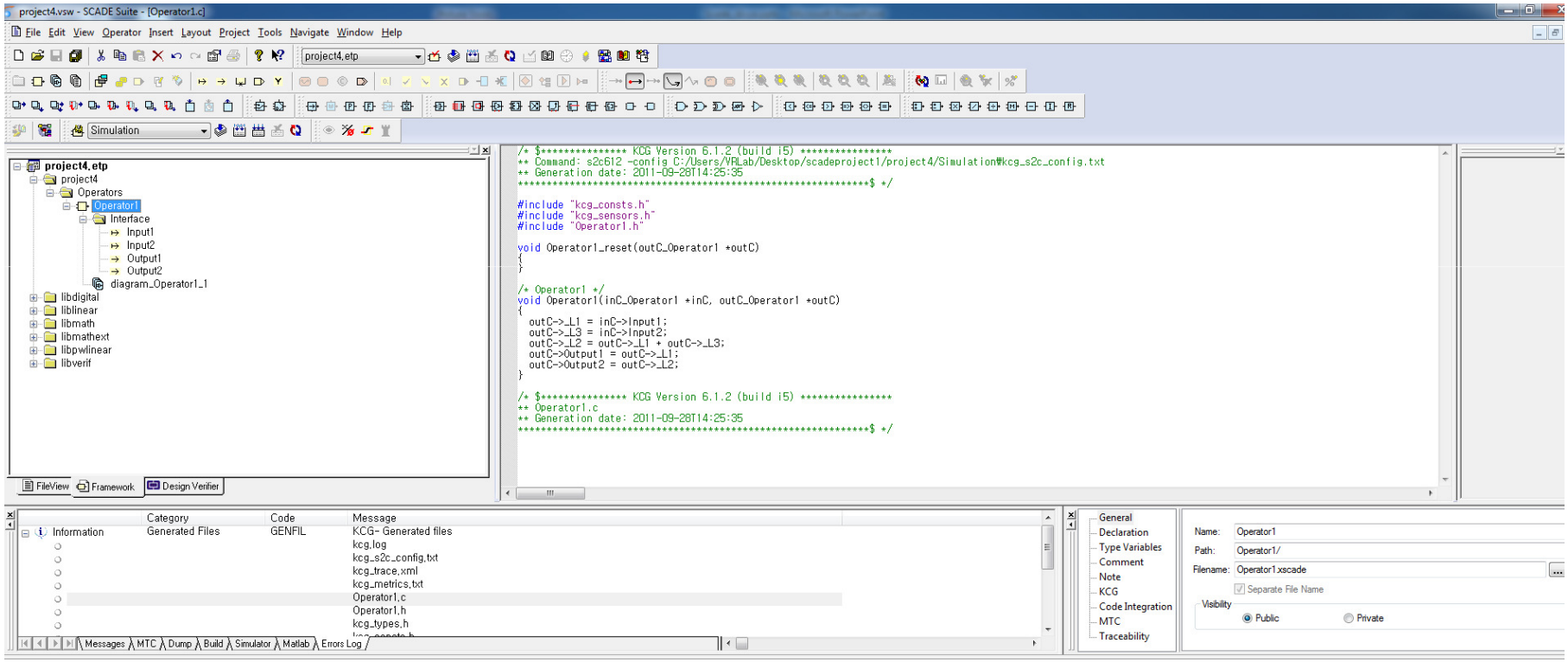
Model Checking(3/4)



Model Checking(4/4)



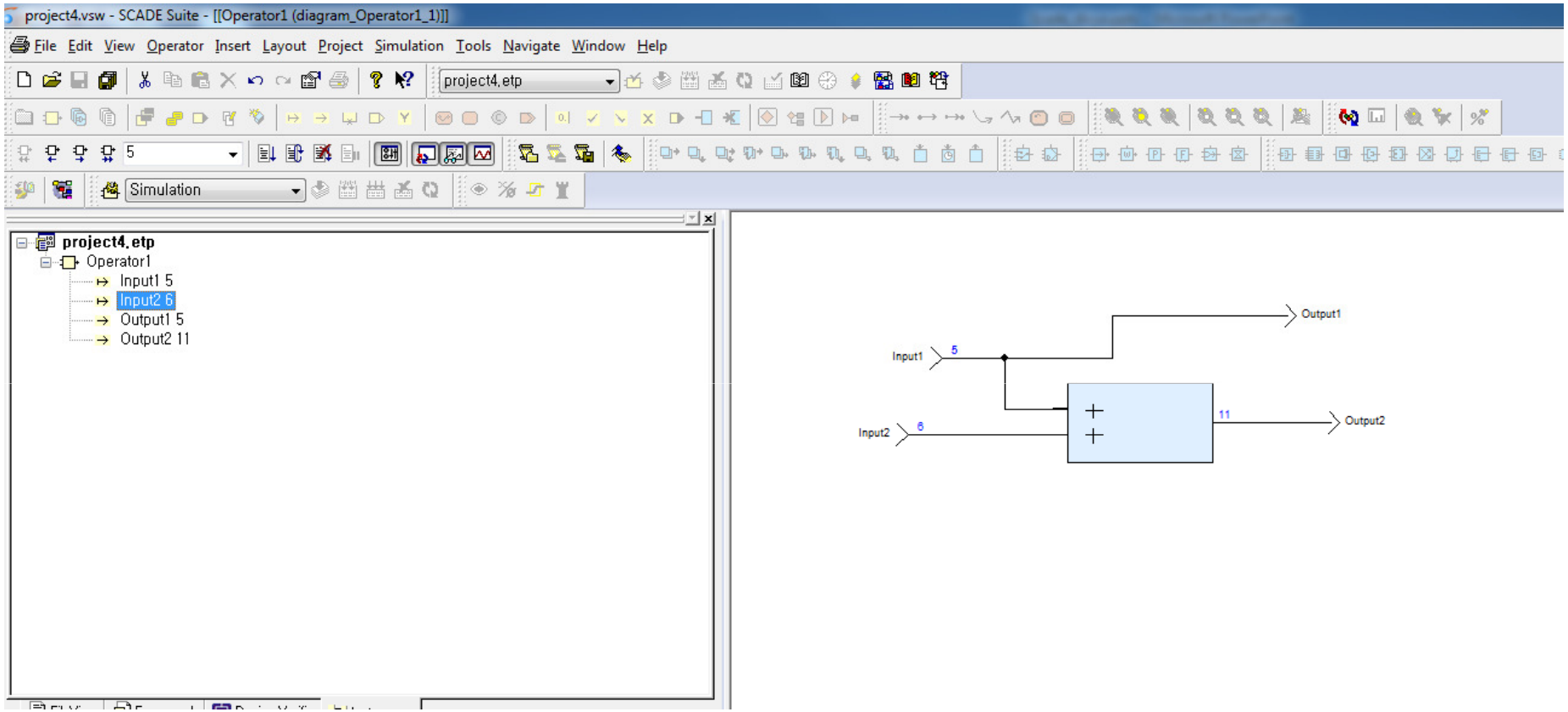
Automatic generation of code(1/2)

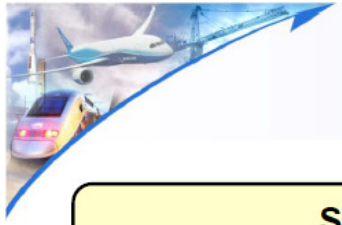


Automatic generation of code(2/2)

```
/* $*************** KCG Version 6.1.2 (build i5) ****************
** Command: s2c612 -config C:/Users/VRLab/Desktop/scadeproject1/project4/Simulation₩kcg_s2c_config.txt
** Generation date: 2011-09-28T14:25:35
*****************************************************************$ */

#include "kcg_consts.h"
#include "kcg_sensors.h"
#include "Operator1.h"

void Operator1_reset(outC_Operator1 *outC)
{
}

/* Operator1 */
void Operator1(inC_Operator1 *inC, outC_Operator1 *outC)
{
  outC->_L1 = inC->Input1;
  outC->_L3 = inC->Input2;
  outC->_L2 = outC->_L1 + outC->_L3;
  outC->Output1 = outC->_L1;
  outC->Output2 = outC->_L2;
}

/* $*************** KCG Version 6.1.2 (build i5) ****************
** Operator1.c
** Generation date: 2011-09-28T14:25:35
*****************************************************************$ */
```

Simulation


project4.vsw - SCADE Suite - [[Operator1 (diagram_Operator1_1)]]
File Edit View Operator Insert Layout Project Simulation Tools Navigate Window Help
project4.etp
Simulation
project4.etp
Operator1
Input1 5
Input2 6
Output1 5
Output2 11
Output1
Input1
5
Input2
6
11
Output2



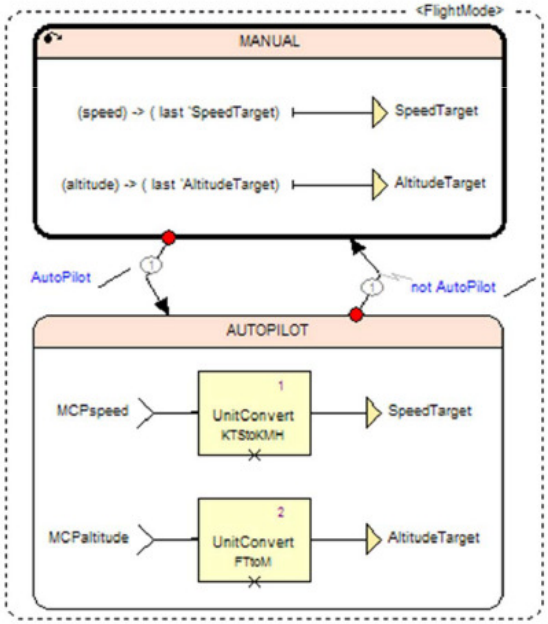
Data Flow, Safe State Machines & Embedded Graphics

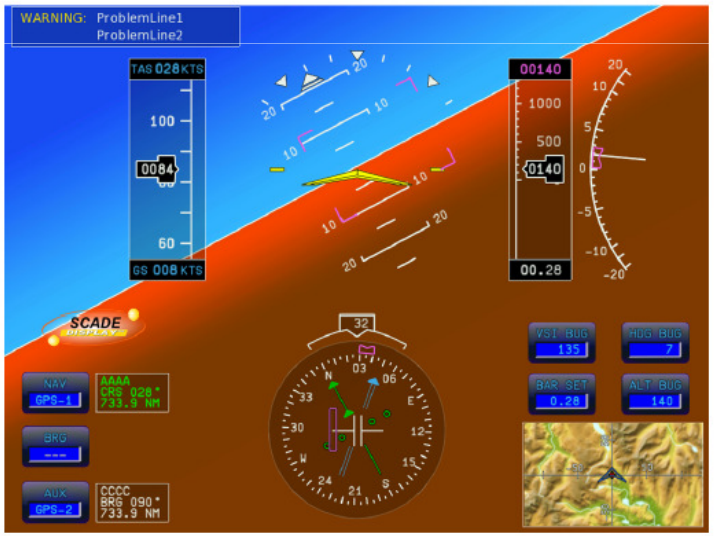
SCADE Suite
Integrated Data Flow & State Machines

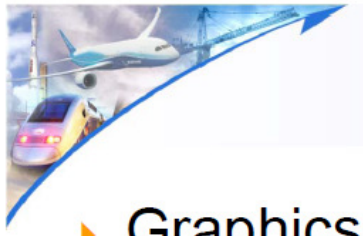
SCADE SUITE™

SCADE Display
Embedded Graphics

SCADE DISPLAY™



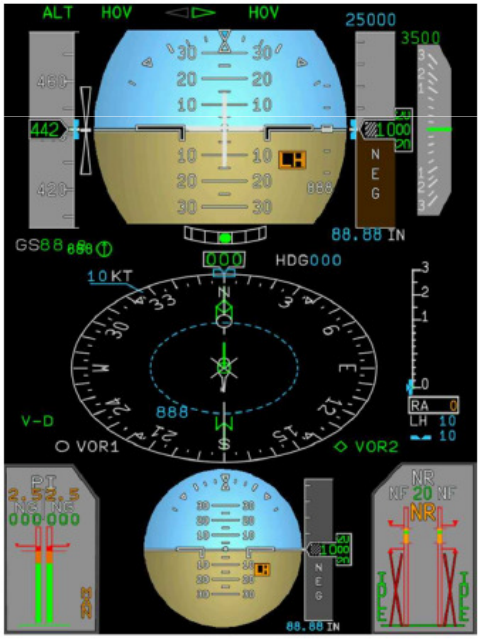




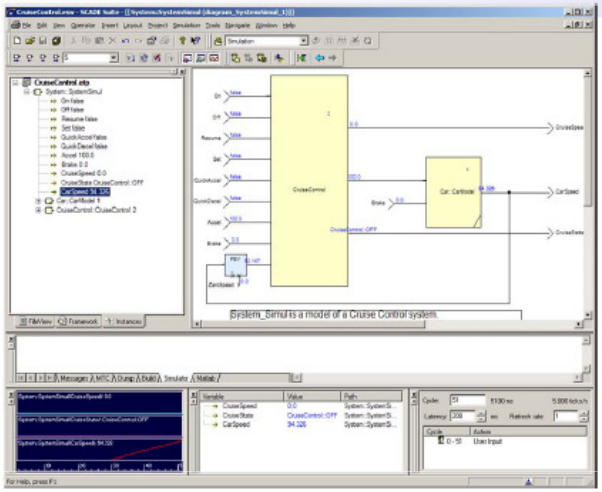
SCADE Display Modeler

Modeling Productivity & Full Compliance with OpenGL

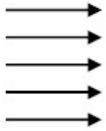
- Graphics capabilities are based upon an **advanced graphics library**
  - Improved rendering quality vs. OpenGL
  - More powerful and more expressive OpenGL-based primitives
- High-level graphics primitives enable **more productive design** while still generating OpenGL commands, and so ensuring **full compliance with OpenGL standard**

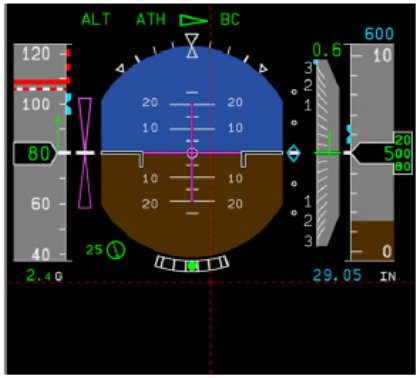


Integrated Simulation with SCADE Suite



SCADE Suite Simulator





SCADE Display Specification (execution of generated code)

- Integrated simulation and debug capabilities
  - Benefit from SCADE Suite Simulator capabilities (step-by-step / continuous modes, scenario management, graphical debugging, etc.)
  - Relies on generated code for both SCADE Suite & SCADE Display
  - Simulate / Debug SCADE Suite & SCADE Display at the same time
  - Tight integration of generated code ensures optimal simulation performance

Why Esterel SCADE is the solution …

Standards	Esterel SCADE provides a common representation between systems and software teams sharing Esterel models
Portability	Esterel SCADE generates portable C or ADA Code which is RTOS, hardware & bus platform independent
Support	Esterel Technologies has worldwide training and support capabilities in *your* language
Partners	Esterel SCADE has been integrated to leading Requirements Mgt, Traceability, RTOSes, IDEs, Compilers, Testing and Code analysis tools
Results	Esterel SCADE users have experienced a 2X speed-up improvement in time-to-certification and a 37% reduction in project development costs!

Reference

- www.esterel-technologies.com