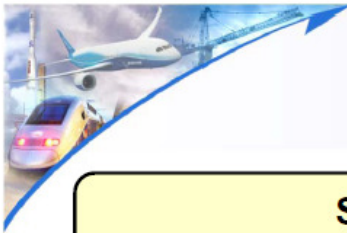


# SCADE – Safety Critical Application Development Environment

Presented By

Divya Udayan J

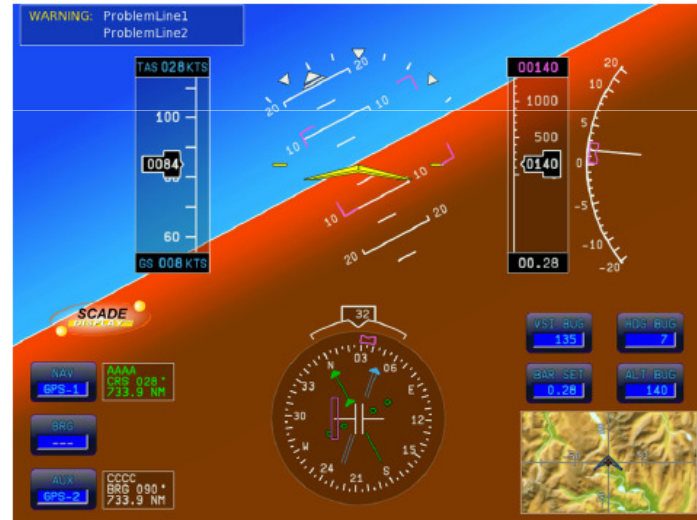
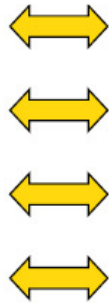
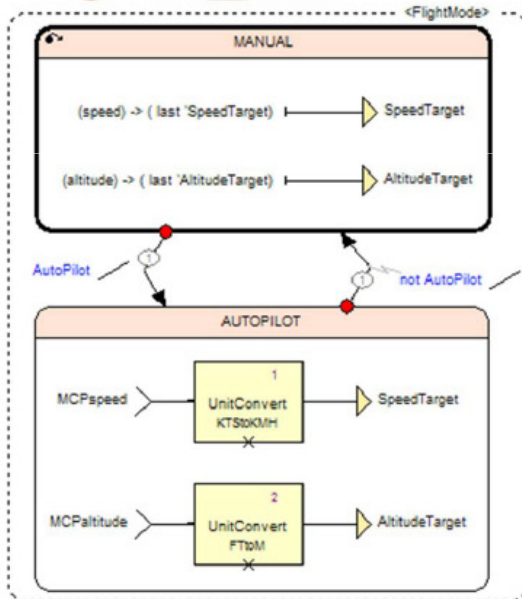
VR Lab



# Mission and Safety-Critical Design with Embedded Graphics

**SCADE Suite**  
Integrated Data Flow & State Machines

**SCADE Display**  
Embedded Graphics



**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

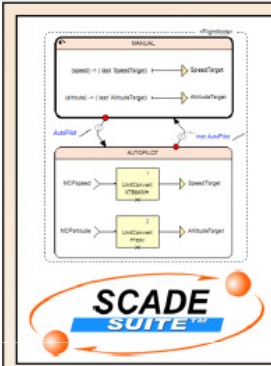
## SYSTEM SPEC

3 Requirements  
3.1 Cruise State Management  
3.1.1 Short description  
3.1.2 Inputs  
3.1.3 Outputs  
3.1.4 Detailed specification

Algorithm Design Capture

Architecture Design Capture

## DESIGN



## VERIFY

Debugging & Simulation

Model Coverage Analysis

Formal Verification

Time & Stack 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

The screenshot displays the SCADE Suite Editor interface for a project named "CruiseControl.vsw". The main workspace shows a state machine diagram titled "Top Level of the Cruise Control application". The diagram is organized into nested states: "Enabled", "Active", "On", "Standby", and "Interrupt".

- Enabled State:** Contains the "Active" state and an "Interrupt" state. Transitions include "Brake > PedalSpin" and "Resume".
- Active State:** Contains the "On" state and a "Standby" state. Transitions include "BrakeCondition" and "not BrakeCondition".
- On State:** Contains a "CruiseRegulation" block. Inputs include "local\_CruiseSpeed" and "Speed". Output is "ThrottleCmd".
- Standby State:** Contains a "STDEV" block. Output is "CruiseState".
- Interrupt State:** Contains an "INT" block. Output is "CruiseState".

Below the "Active" state, there is a logic block for "BrakeCondition" with inputs: "Accel > PedalSpin", "Speed < SpeedLim", and "Speed > SpeedMax".

At the bottom, a "CruiseSpeedMgt" block has inputs: "Set", "QuickAccel", "QuickDecel", and "Speed". It has outputs: "local\_CruiseSpeed" and "CruiseSpeed".

The left sidebar shows a project tree for "CruiseControl.etp" with folders for Constants, Types, Operators, Proof, System, and various libraries (libdigital, liblinear, libmath, libmathext, libpwnear, Car, CarType, libverif).

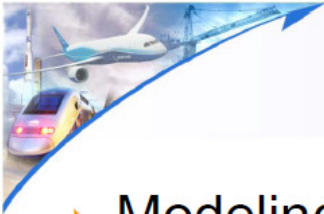
The bottom panel shows the "General" properties for the "CruiseControl" component, including Name, Path, Filename, and Visibility (Public/Private).



## Unified Modeling Style

*Modeling Capabilities*

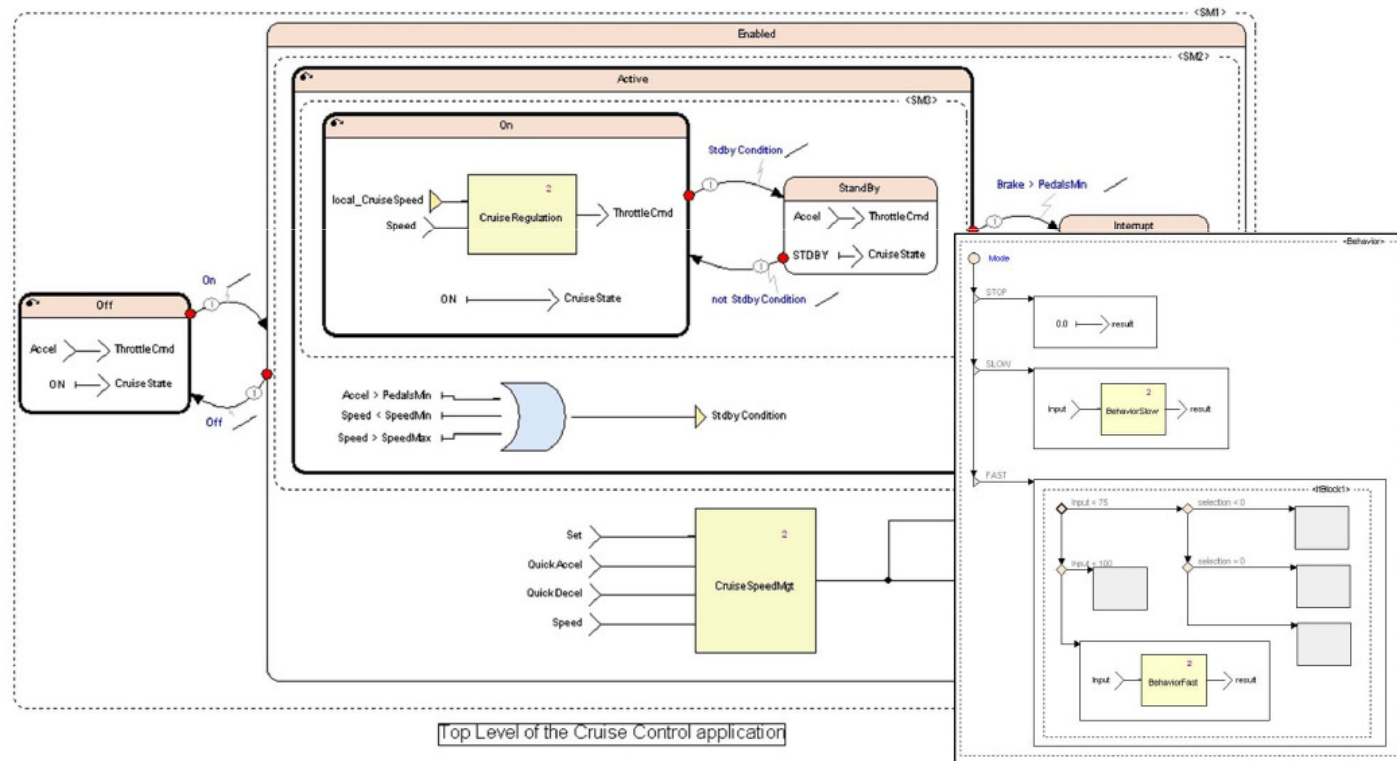
- ▶ Graphical formalism
  - ▶ Block diagrams, to specify the algorithmic part of applications, such as control laws and filters
  - ▶ Hierarchical state machines, to model the control part of applications
  - ▶ Decision diagrams
  - ▶ Packages, data types, constants
  - ▶ Arrays & iterators
  - ▶ Libraries
- ▶ 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



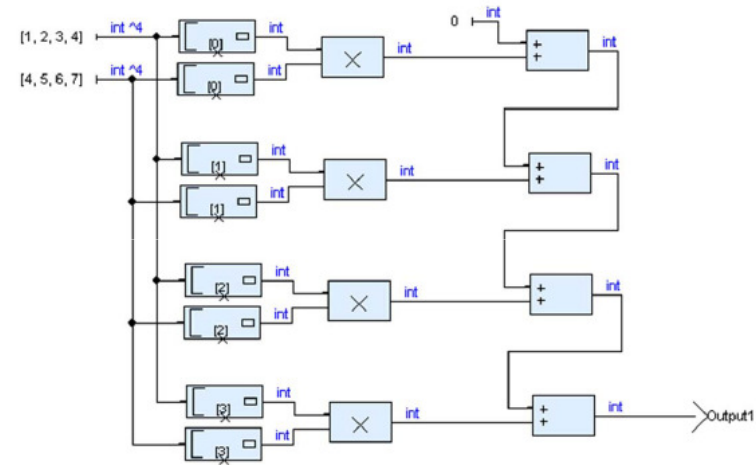


## Unified Modeling Style

### 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

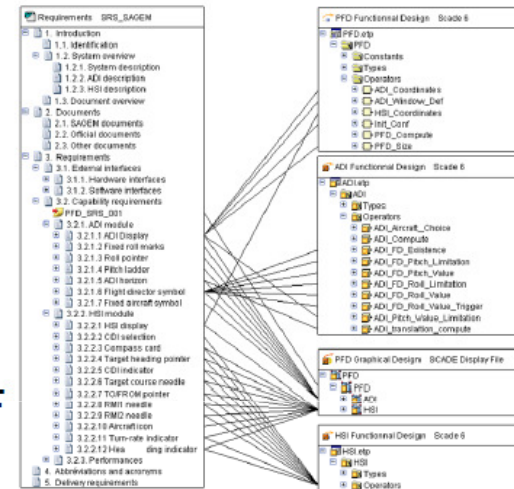


# Requirements Management Gateway

## Integrated Requirements Management & Traceability

### Supported Tools & Formats

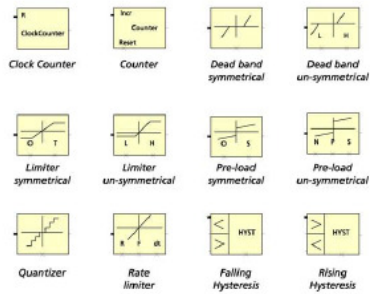
- ▶ **Microsoft® Office** tools: Word, Excel®, Access®, Visio®
- ▶ **Code files** (C, C++, test log files)
- ▶ **Technical Communication** tools: Adobe® FrameMaker® and Acrobat® PDF
- ▶ **Requirements Management** tools: IBM® DOORS®, Rational RequisitePro®, CaliberRM™
- ▶ **Modeling & Design** tools: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





# SCADE Suite Libraries

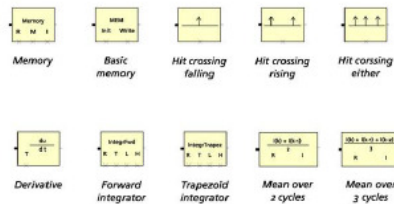
## libpwnlinear pwnlinear package



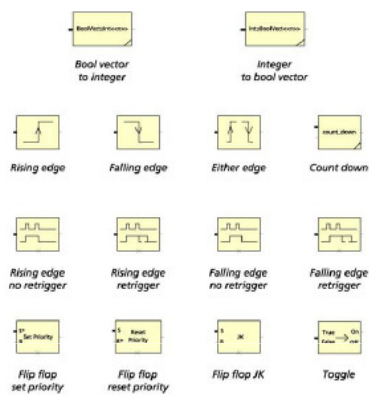
## lut package



## liblinear linear package



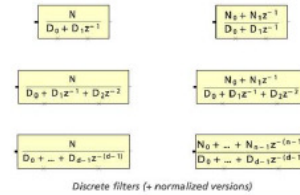
## libdigital digital package



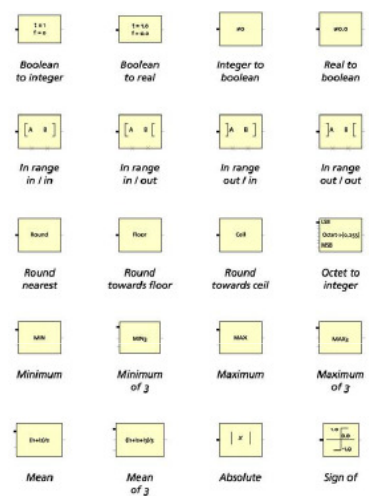
## truthtables package



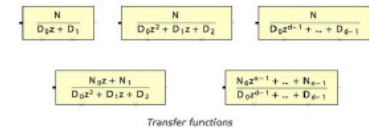
## filters package



## libmath math package



## vect package





## 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

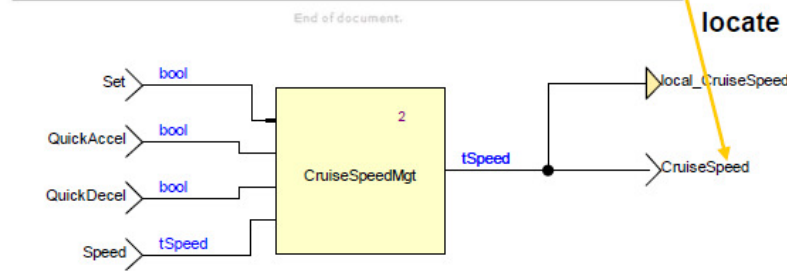
Friday January 11 2008 14:30:55

### 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 <a href="#">CruiseControl::CruiseControl/CruiseSpeed/</a> This expression has type (real) but is here used with type (bool)

Error message:  
Incompatible type  
interface







## 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

Pilot.vsw - SCADE - [[FlightSimulations:FlightSim (FlightSimulations:FlightSim)]]

File Edit View Operator Insert Layout Project Simulation Tools Browse Window Help

Simulation

**Pilot etp**

- FlightSimulation:FlightSim
  - Positions ([[2.0,false],[6.0,false]],[[0.0,false],[0.0,false]],[[0.0,0.0,false],[0.0,false]])
  - NewMvt true
  - MvtType Pilot.mvt\_undefined
  - Wind (10.0,5.0,1.0)
  - Simulation false
  - Velocity (4524,2.2622,0.0)
  - AutoPilot true
  - PositionValid true
  - TelemetryValid false
  - VelValid false
  - ExternalConditions:ExternalConditions 2
    - WindVel
    - ObjectVel
    - Points ([[1248.0,true],[1248.0,true]],[[624.0,true],[624.0,true]])
    - ExternalConditions:CalculateNewPoint 1 ((MAP))
    - ExternalConditions:CalculateNewPoint 1[[0]]
    - ExternalConditions:CalculateNewPoint 1[[1]]
    - ExternalConditions:CalculateNewPoint 1[[2]]
    - PreviousRedundantPointPositions
    - ObjectVel
    - WindVel
    - NewRedundantPointPositions ([[111.79,true],[111.79,true]])
    - ExternalConditions:AddPointPosition 1 ((MAP))
    - ExternalConditions:AddPointPosition 1[[0]]
    - Add
    - NewPointPosition ([[111.79,true]])
    - ExternalConditions:AddPointPosition 1[[1]]
- Pilot: Pilot 3
  - SelectMode
    - Manual
    - Auto (Active)
    - Simu

**State Machine Diagram (SelectMode):**

```

stateDiagram-v2
    state Manual
    state Auto
    state Simu

    Manual --> Auto: last PositionValid and last VelValid
    Manual --> Simu: Simulation
    Auto --> Manual: not (last VelValid and last PositionValid)
    Simu --> Manual: not Simulation
  
```

**Logic Diagram:**

Inputs: AutoPilot (true), Wind (10.0,5.0,1.0), Pilot:Info (0.0,0.0,0.0), ExternalConditions:NavVel (0.0,0.0,0.0).

Logic: A central 'ExternalConditions: ExternalConditions' block receives inputs and outputs to 'Positions' and 'Pilot: Pilot'.

Outputs: Velocity (4524, 2.2622, 0.0), PositionValid (true), VelValid (false), TelemetryValid (false).

**Variable Table:**

Variable	Value
FlightSimulation:FlightSimPositions/	[[[2.0, false], [6.0, false]], [[0.0, false], [0.0, false]]]
Positions/0/0	[[2.0, false], [6.0, false]]
Positions/0/0/valid	2.0
Positions/0/0/valid	false
Positions/0/1	[[6.0, false], [0.0, false]]
Positions/0/1/valid	6.0
Positions/0/1/valid	false
Positions/1	[[0.0, false], [0.0, false]]
Positions/2	[[0.0, false], [0.0, false]]

**Simulation Control:**

Cycle: 40 / 4000 ms Latency: 200 ms

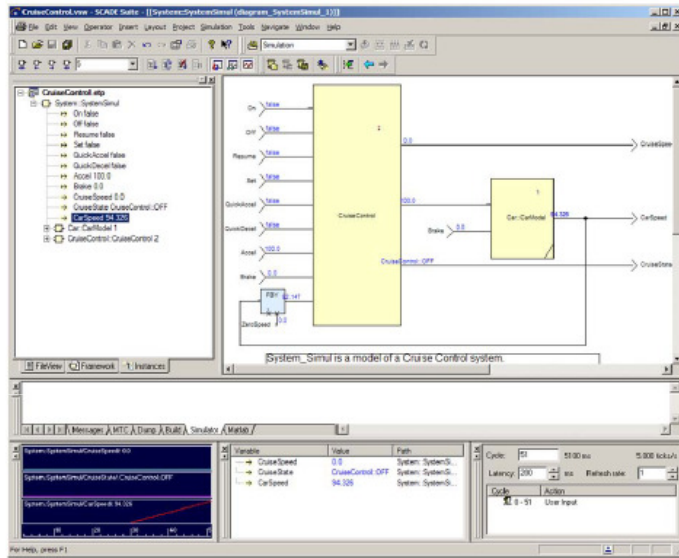
Cycle	Action
0-2	Back
3-40	User Input

For Help, press F1

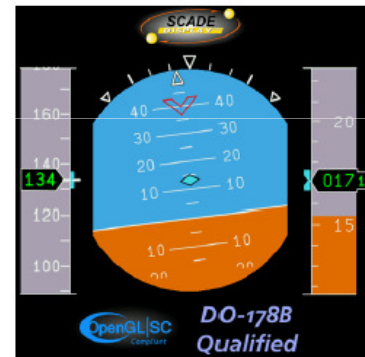
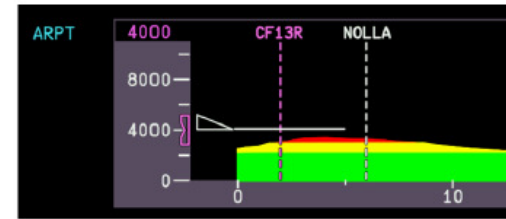




# Integrated Simulation with SCADE Display



SCADE Suite Simulator



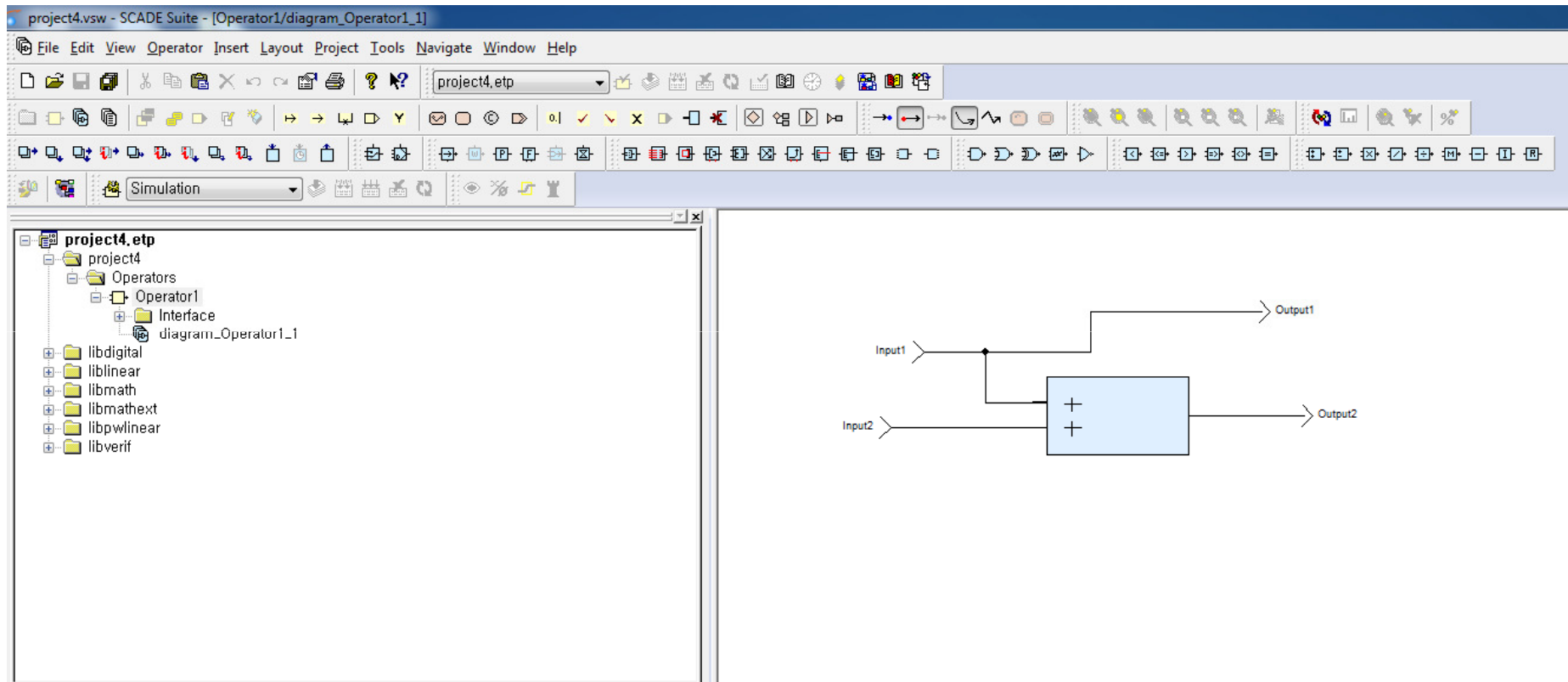
SCADE Display Panels

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



# DESIGN EXAMPLE

# Modeling & Interfacing



# Model Checking(1/4)

Wednesday September 28 2011 14:13:30

## Result of check for operator Operator1/ in model project4

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

Category	Code	Message
Semantic Error	ERR_103	Numeric constraint violated at <a href="#">Operator1/ L2=</a> Unsatisfiable numeric constraint bool (inputs of binary operator + must be numeric)

End of document.

FileView Framework Design Verifier

```
Loading project project4.etp...
Successfully loaded project project4.etp
Checking model...
End of Checker.
```

Messages MTC Dump Build Simulator Matlab Errors Log

No properties available

# Model Checking(2/4)

Wednesday September 28 2011 14:13:30

## Result of check for operator Operator1/ in model project4

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

Category	Code	Message
Semantic Error	ERR_103	Numeric constraint violated at <u>Operator1/ 1.2</u> Unsatisfiable numeric constraint bool (inputs of binary operator + must be numeric)

End of document.

Messages / MTC / Dump / Build / Simulator / Matlab / Errors Log /

General  
Declaration  
Clock  
Comment  
Note  
KCG  
Traceability

Type: bool  
 bool  
Last:  char  
 digital  
Default:  filters  
 int  
Kind:  linear  
 lut  
 math  
 mathext  
 multilinear

# Model Checking(3/4)

Wednesday September 28 2011 14:18:48

### Result of check for operator Operator1/ in model project4

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

Category	Code	Message
Semantic Warning	WAR_151	Internal state expected at <u>Operator1/</u> Node Operator1 has no internal state (it should probably be declared as a function)

End of document.

Messages / MTC / Dump / Build / Simulator / Matlab / Errors Log /

General  
- Declaration  
- Type Variables  
- Comment  
- Note  
- KCG  
- Code Integration  
- MTC  
- Traceability

Node  Function  
 Imported Source file:   
 Specialize   
Symbol file:   
Note Category:

# Model Checking(4/4)

The screenshot displays the SCADE Suite interface. The main window shows the results of a model check for 'Operator1' in 'project4'. The results indicate that 0 errors and 1 warning were detected. A table below provides details for the warning, 'WAR\_151', which is a semantic warning about missing internal state for the operator.

Wednesday September 28 2011 14:18:48

### Result of check for operator Operator1/ in model project4

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

Category	Code	Message
Semantic Warning	WAR_151	Internal state expected at <u>Operator1/</u> Node Operator1 has no internal state (it should probably be declared as a function)

End of document.

At the bottom right, the 'Node' radio button is selected and circled in red.

Messages: \MTC \ Dump \ Build \ Simulator \ Matlab \ Errors Log /

# Automatic generation of code(1/2)

The screenshot displays the SCADE Suite interface for a project named 'project4.vsw'. The main window shows the source code for 'Operator1.c', which was automatically generated by KCG Version 6.1.2 (build i5) on 2011-09-28T14:25:35. The code includes headers for 'kcg\_consts.h', 'kcg\_sensors.h', and 'Operator1.h'. It defines a function 'Operator1\_reset' and a function 'Operator1' that takes an input 'inC' and returns an output 'outC'. The 'Operator1' function implements a simple logic: 'outC->L1' is assigned to 'inC->Input1', 'outC->L3' is assigned to 'inC->Input2', 'outC->L2' is the sum of 'outC->L1' and 'outC->L3', 'outC->Output1' is assigned to 'outC->L1', and 'outC->Output2' is assigned to 'outC->L2'.

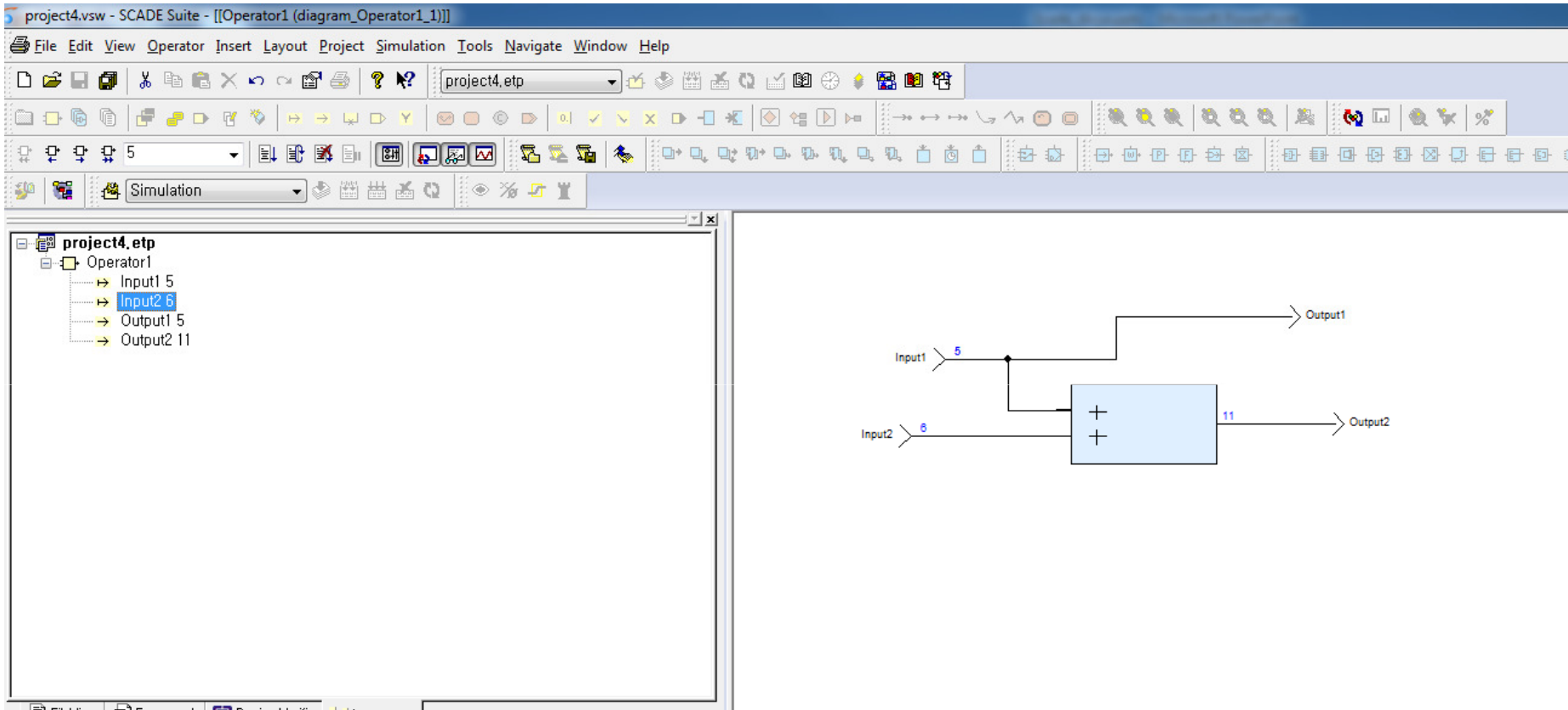
The interface also shows a project tree on the left with 'Operator1' selected, and a bottom panel with a 'Messages' window listing generated files like 'kcg\_log', 'kcg\_s2c\_config.txt', and 'Operator1.c'. A right-hand panel shows properties for 'Operator1', including its name, path, and visibility settings.

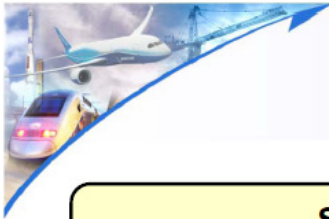
# Automatic generation of code(2/2)

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



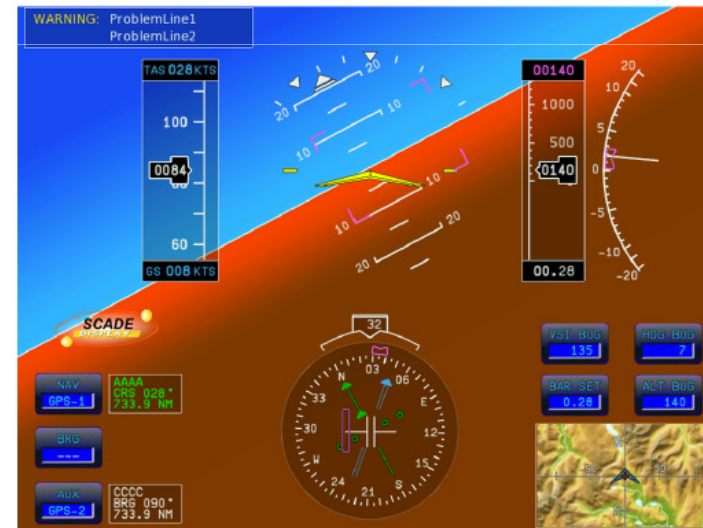
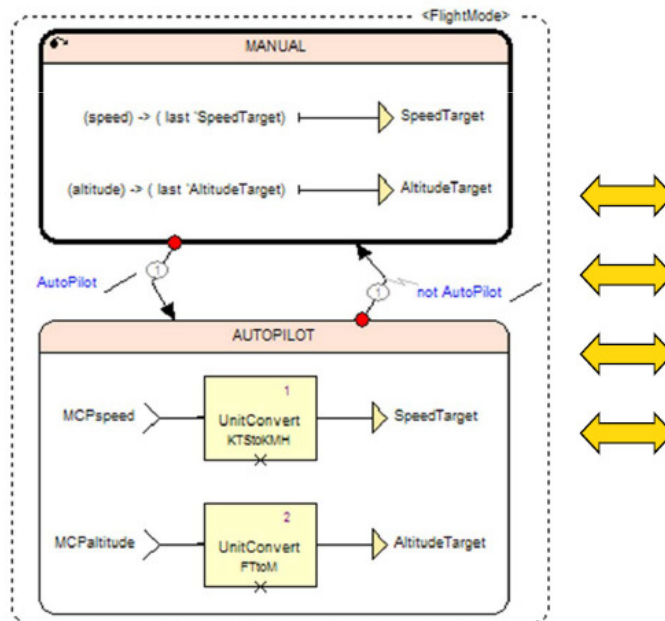


# Data Flow, Safe State Machines & Embedded Graphics

**SCADE Suite**  
Integrated Data Flow & State Machines



**SCADE Display**  
Embedded Graphics

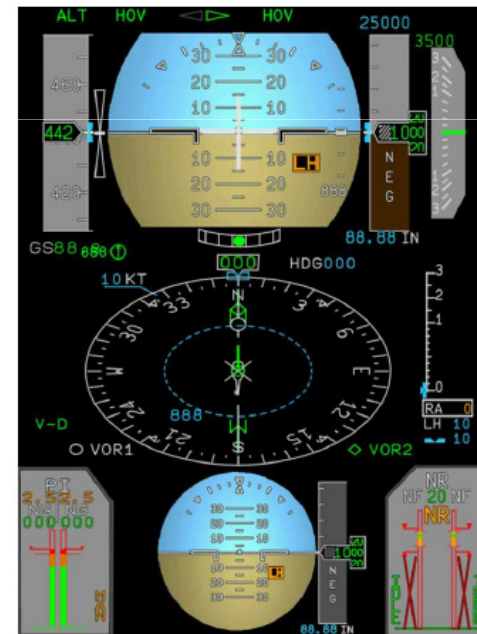




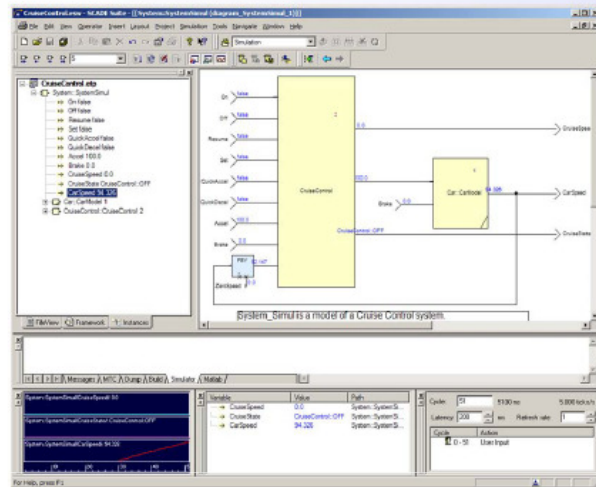
# SCADE Display Modeler

*Modeling Productivity & Full Compliance with OpenGL*

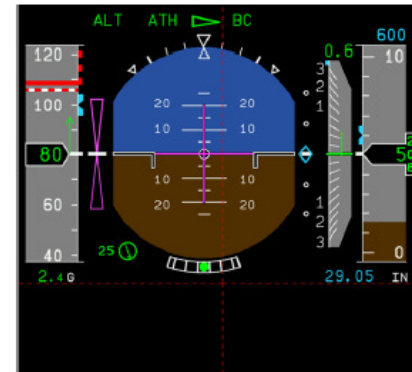
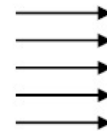
- ▶ Graphics capabilities are based upon an **advanced graphics library**
  - ▶ Improved rendering quality vs. OpenGL
  - ▶ More powerful and more expressive OpenGL-based primitives
- ▶ High-level graphics primitives enable **more productive design** while still generating OpenGL commands, and so ensuring **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](http://www.esterel-technologies.com)