DESIGN VERIFICATION OF STABILITY CONTROLLER MODEL OF AIRPLANE USING SCADE

Presented By

Divya Udayan J

VR Lab

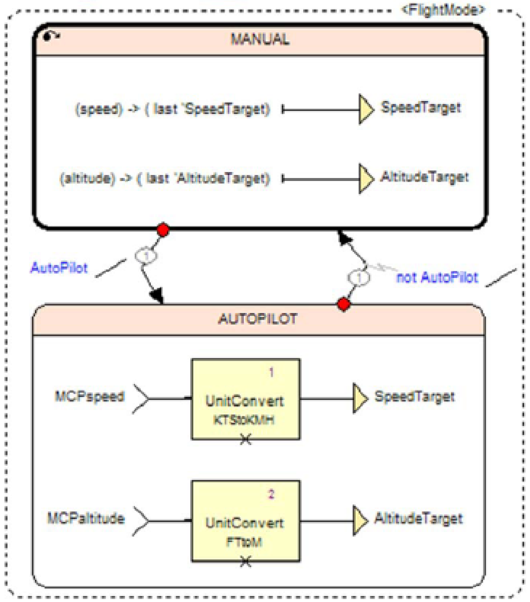
Overview

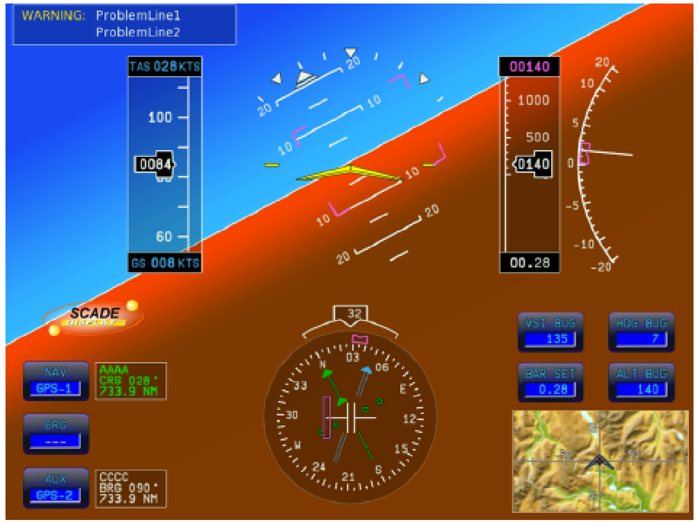
- Introduction to SCADE SUIT
- Objective of term project
- Requirement Specification
- Data flow and Control flow diagrams
- Code generation
- Verifying Design Correctness
- System Testing
- Simulation and demo
- Conclusion

Mission and Safety-Critical Design with Embedded Graphics

SCADE Suite
Integrated Data Flow & State Machines

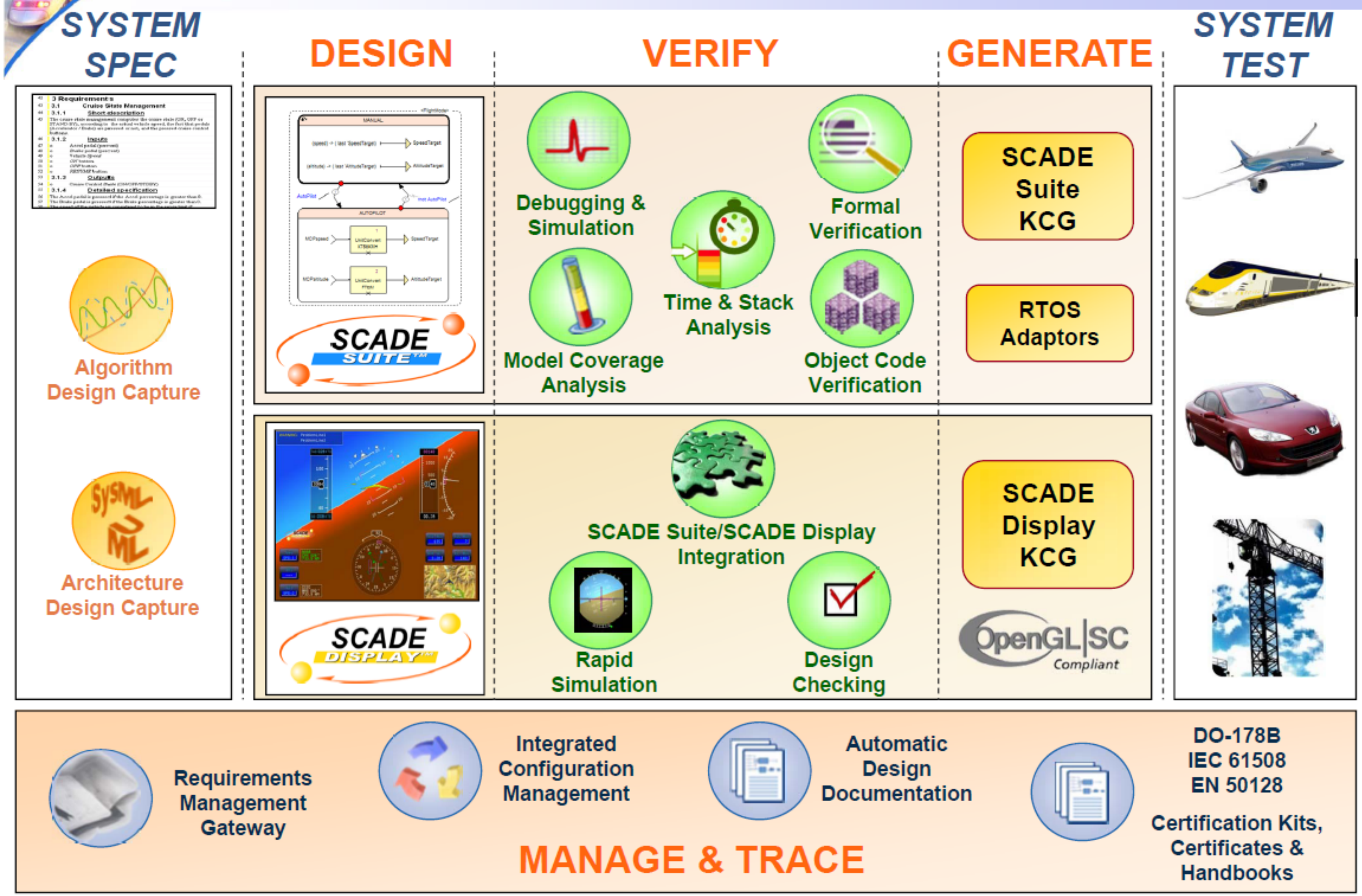
SCADE Display
Embedded Graphics

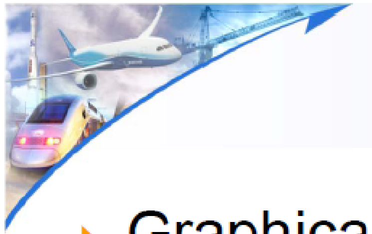




Fully Integrated Design Suite

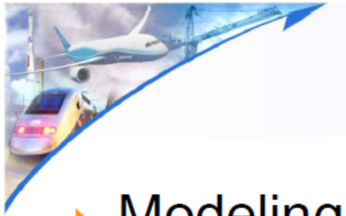
The SCADE Certified Software Factory





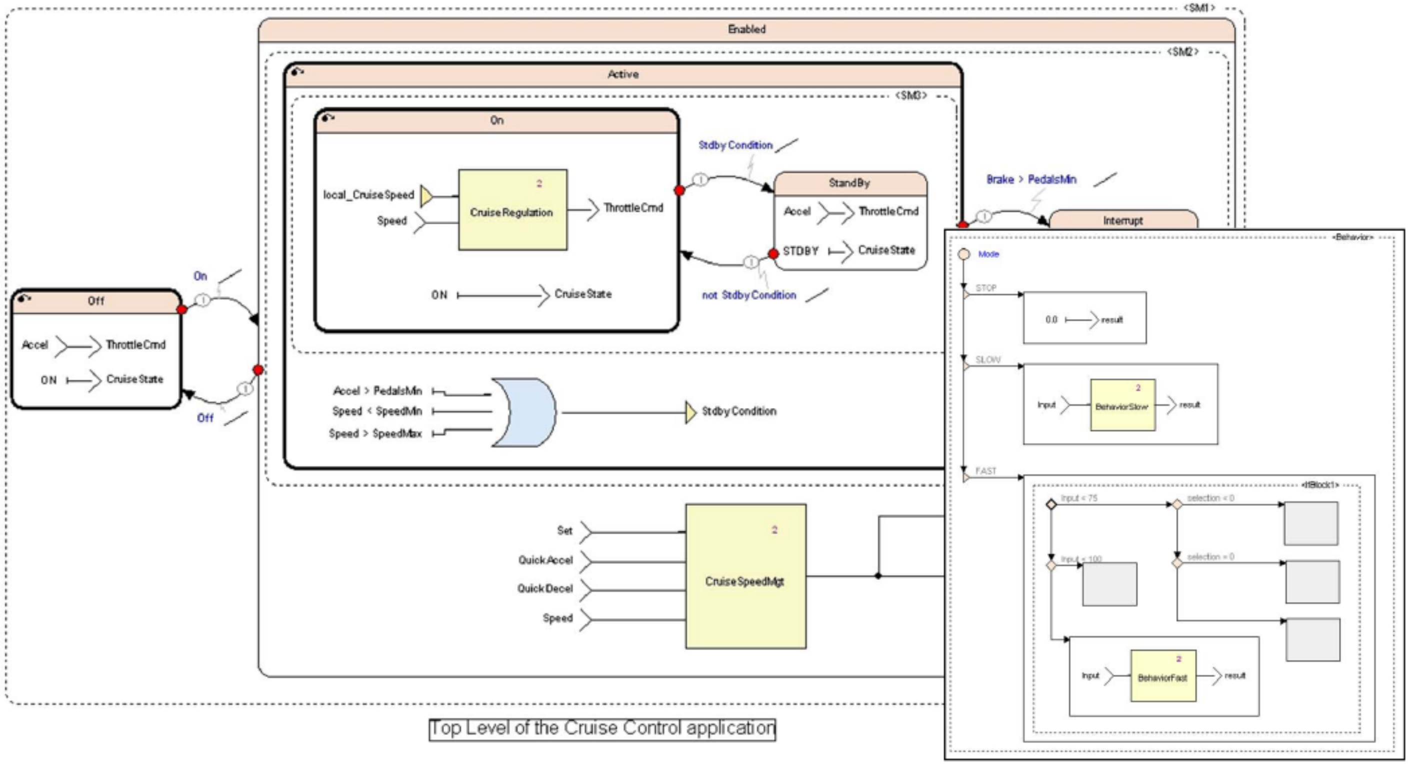
Unified Modeling Style
Modeling Capabilites

- 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

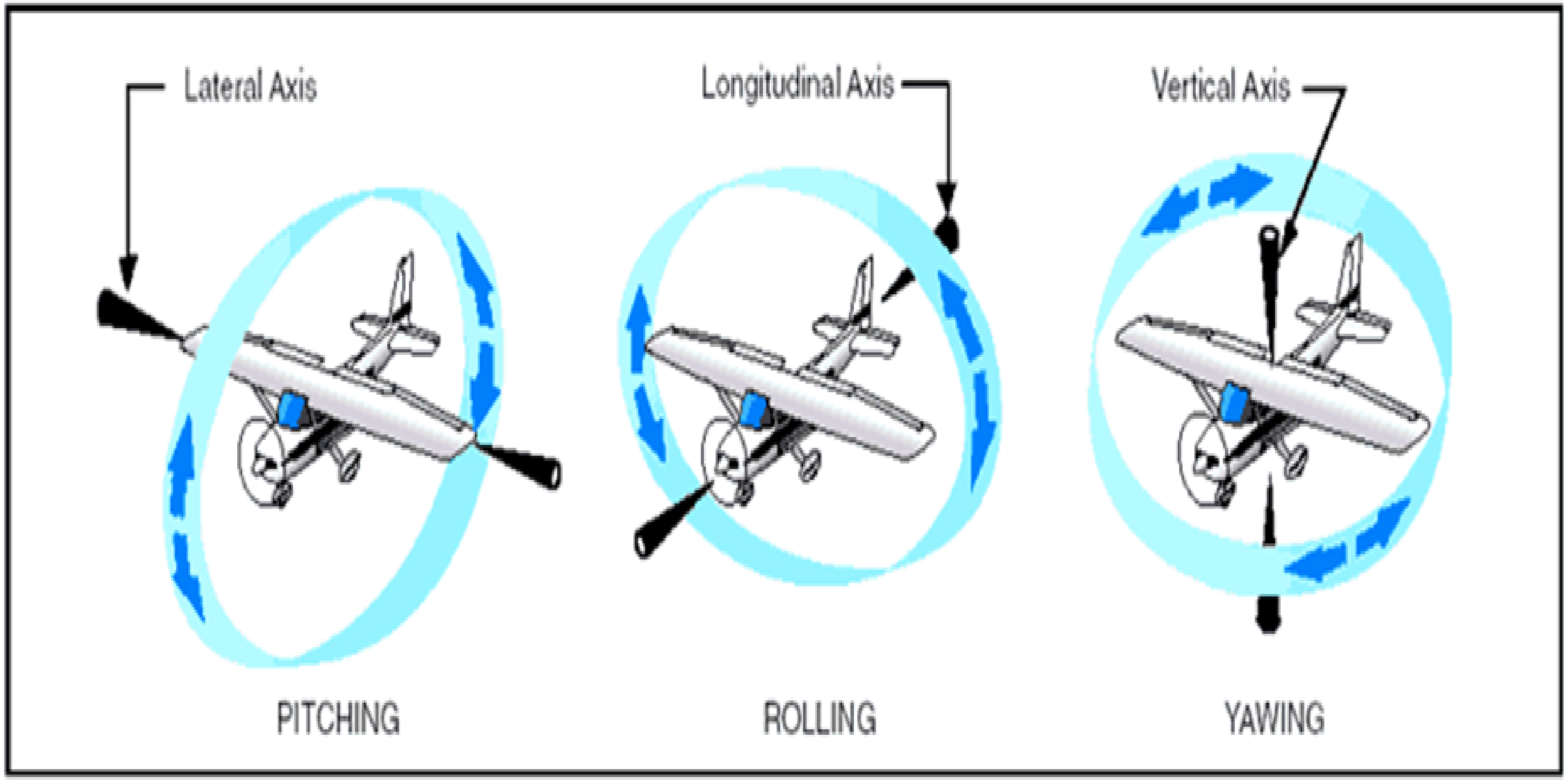
Objective

- Design verification of the stability controller for an airplane

- Checking its effect on the lateral(roll) & longitudinal(pitch)-directional dynamics of the airplane.

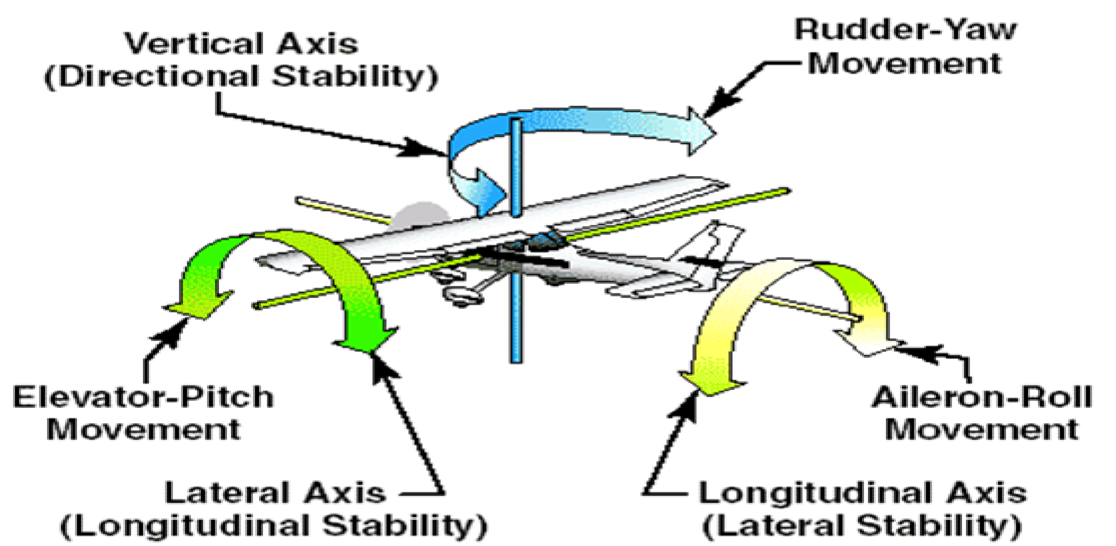
- Motivating factor for designing this controller is to simplify the piloting of the airplane.

Flight controls



Axes of an airplane

Airplane stability



PRIMARY CONTROL SURFACE	AIRPLANE MOVEMENT	AXES OF ROTATION	TYPE OF STABILITY
Aileron	Roll	Longitudinal	Lateral
Elevator/ Stabilator	Pitch	Lateral	Longitudinal
Rudder	Yaw	Vertical	Directional

Airplane controls, movement, axes of rotation, and type of stability

Requirement Specification(1/4)

1) Roll rate calculation requirement :

The roll rate calculation subsystem calculates the plane roll rate, according to a joystick command and the adverse yaw coupling effects.

Inputs : Joystick command, Adverse yaw induced by left wing, Adverse yaw induced by right wing.

Outputs : Plane roll rate

simplified coupling effect is calculated as follows:

rollCoupling = (leftAdverseYaw – rightAdverseYaw) x0.1

plane roll rate is calculated as follows:

rollRate = (joystickCmd – rollCoupling) x 0.25

The absolute value of the plane roll rate has to be saturated to 25.0.

Initialization : At system initialization, the plane roll rate is 0.0.

Requirement Specification(2/4)

2) Roll rate warning alarm requirement :

The roll rate warning alarms subsystem computes left and right warning alarms, which sound, respectively if the plane roll rate is strictly less than –15.0° per second or strictly greater than 15.0° per second.

Inputs : Plane roll rate

Outputs: Left warning alarm, Right warning alarm

Initialization : At system initialization, the left and right warning alarms do not sound.

3) Roll Mode Management

The roll mode management subsystem computes the plane "roll mode" (either Off, Nominal, or Failsoft) according to the ON/OFF button being pressed and the plane roll rate value.

Inputs : - Plane roll rate (absolute value), ON/OFF button
Output : Roll Mode

Requirement Specification(3/4)

The roll mode has three possible states:

OFF:

Active when:

• At initial state;

• Previous state was NOMINAL or FAILSOFT and ON/OFF button is pressed.

The roll mode value is then Off.

NOMINAL:

Active when:

• The previous state was OFF, the ON/OFF button is pressed, and the absolute value of the plane roll rate is less than FailSoftRoll.

• The previous state was FAILSOFT and the absolute value of the plane roll rate is less than FailSoftRoll

The roll mode value is then NOMINAL.

FAILSOFT:

Active when:

• The previous state was OFF, the ON/OFF button is pressed, and the absolute value of the plane roll rate is strictly greater than FailSoftRoll.

• The previous state was NOMINAL and the absolute value of the plane roll rate is strictly greater than FailSoftRoll

The roll mode value is then FAILSOFT.

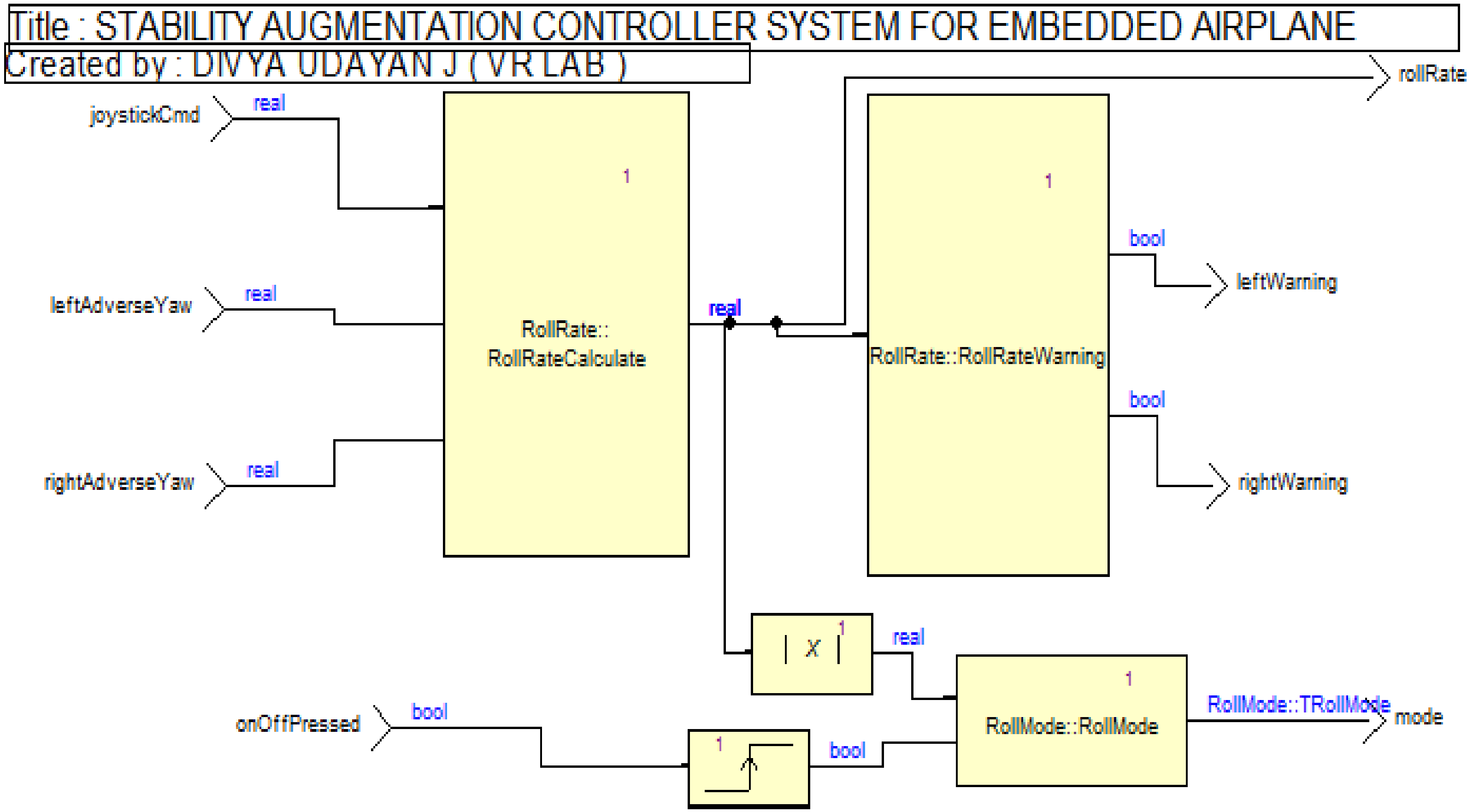
Initialization : At system initialization, the roll mode is Off.

Requirement Specification(4/4)

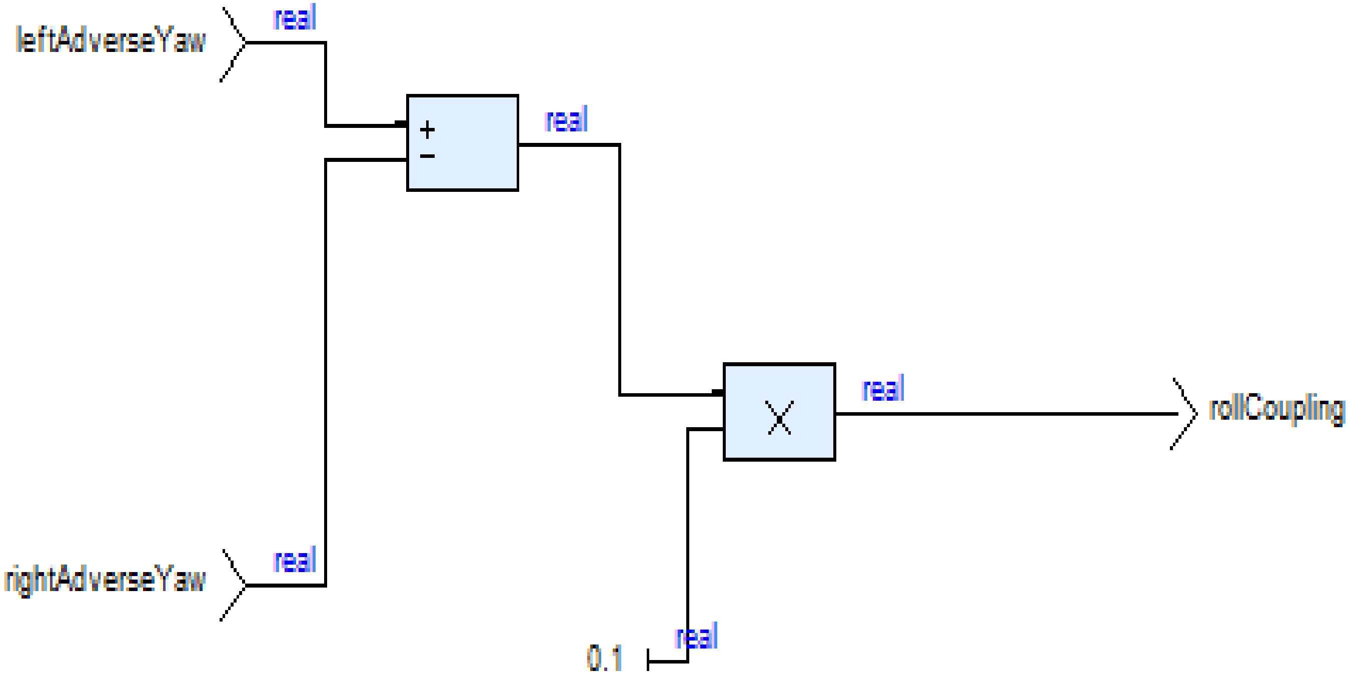
4) Constant definitions

Name	Field	Value	Unit
RollRateWarning	Left	-15.0	Degrees/sec
	Right	15.0	Degrees/sec
FailSoftRoll		20.0	Degrees/sec

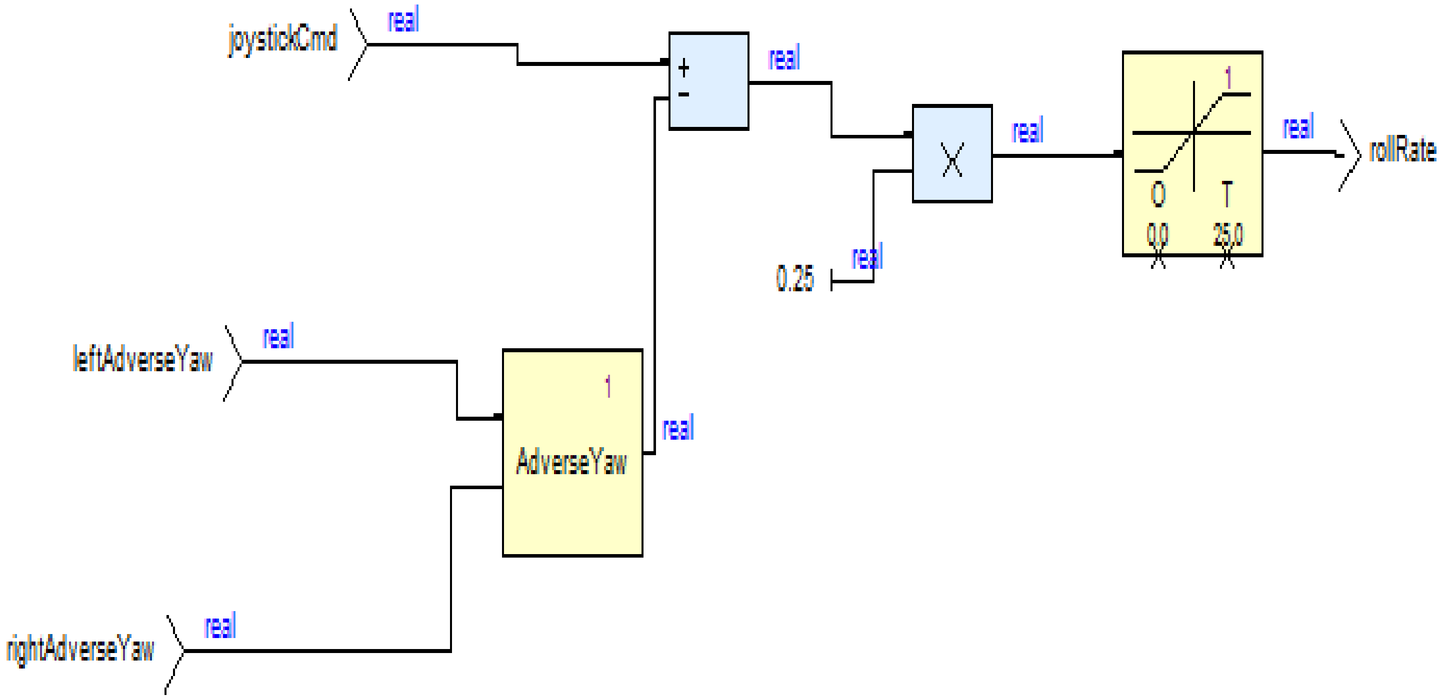
Data Flow of the Roll Controller



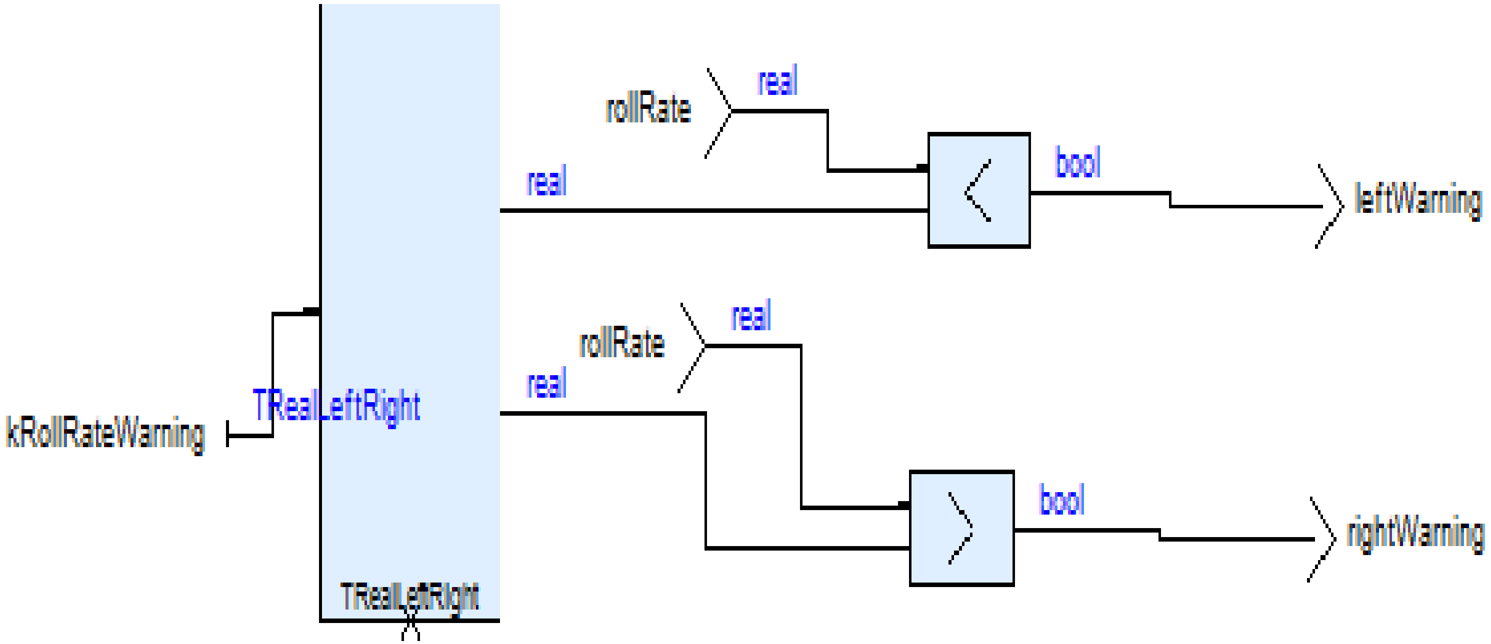
Data flow of roll coupling



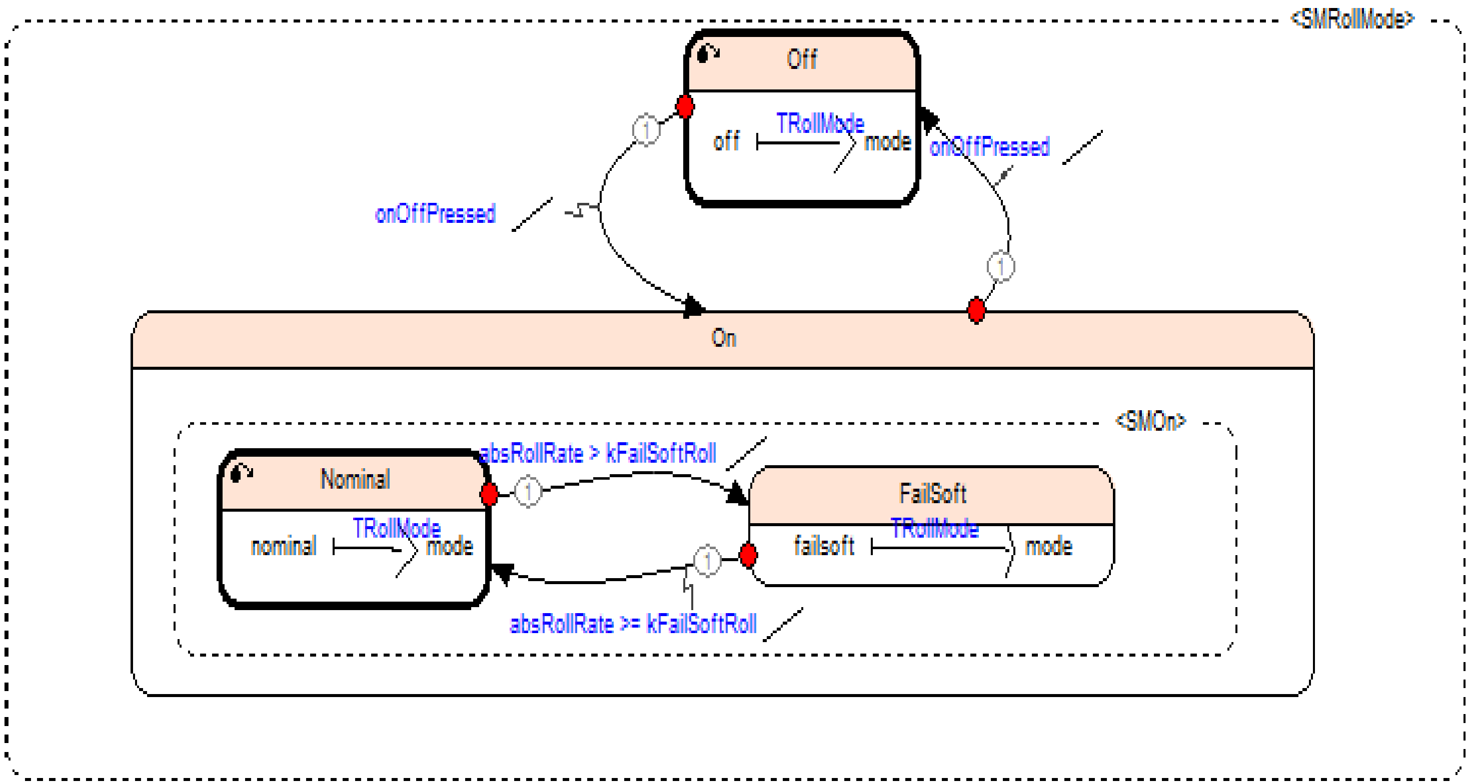
Data flow of RollRate Calculation



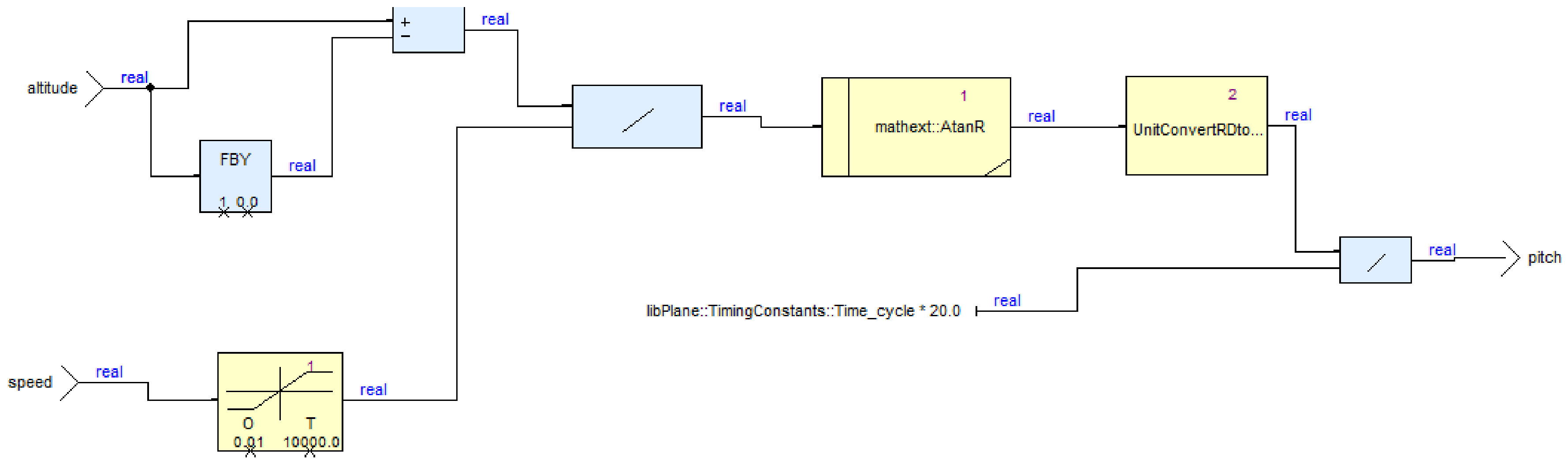
Data Flow of Rollrate warning



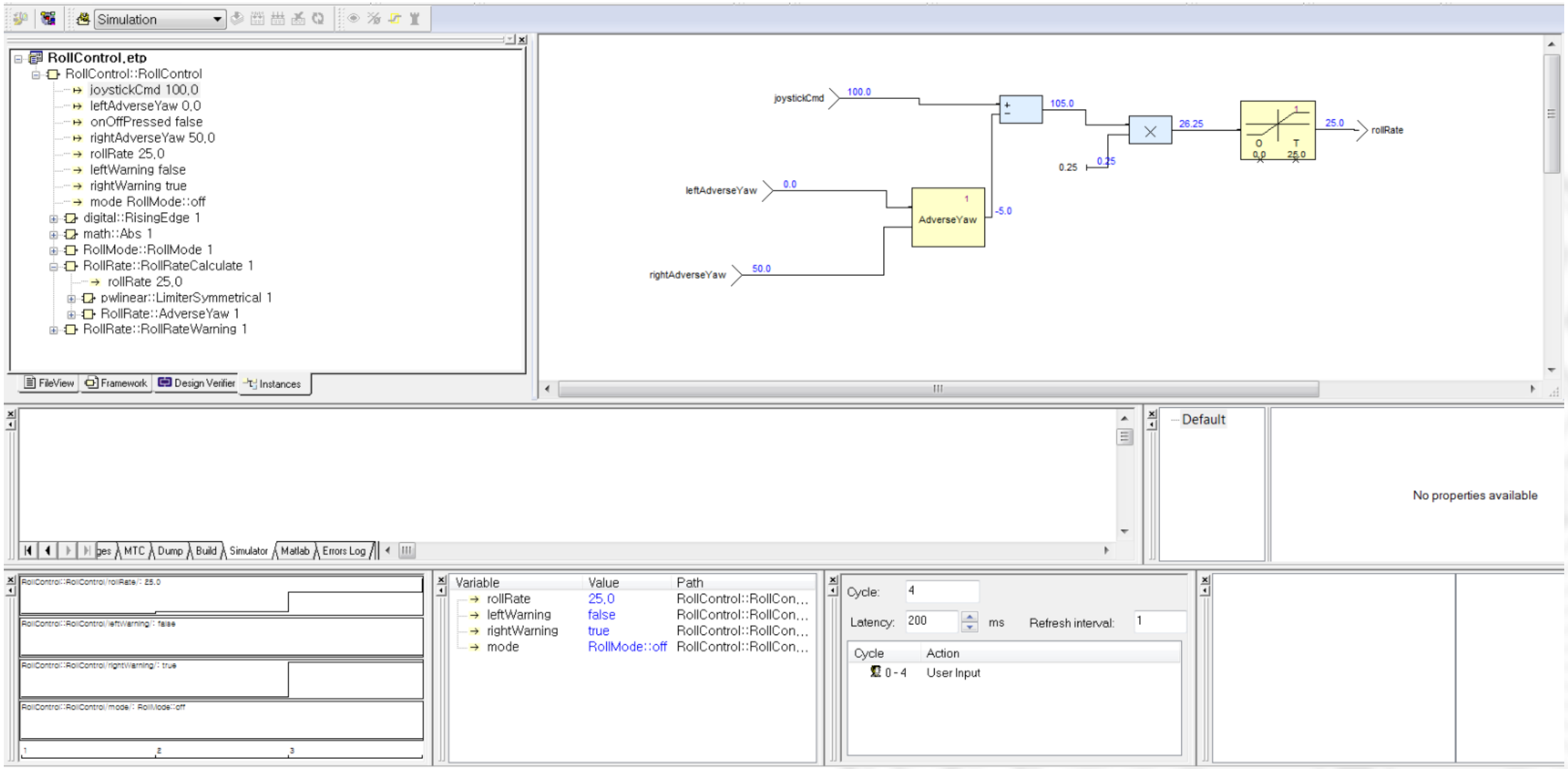
Control Flow Diagrams



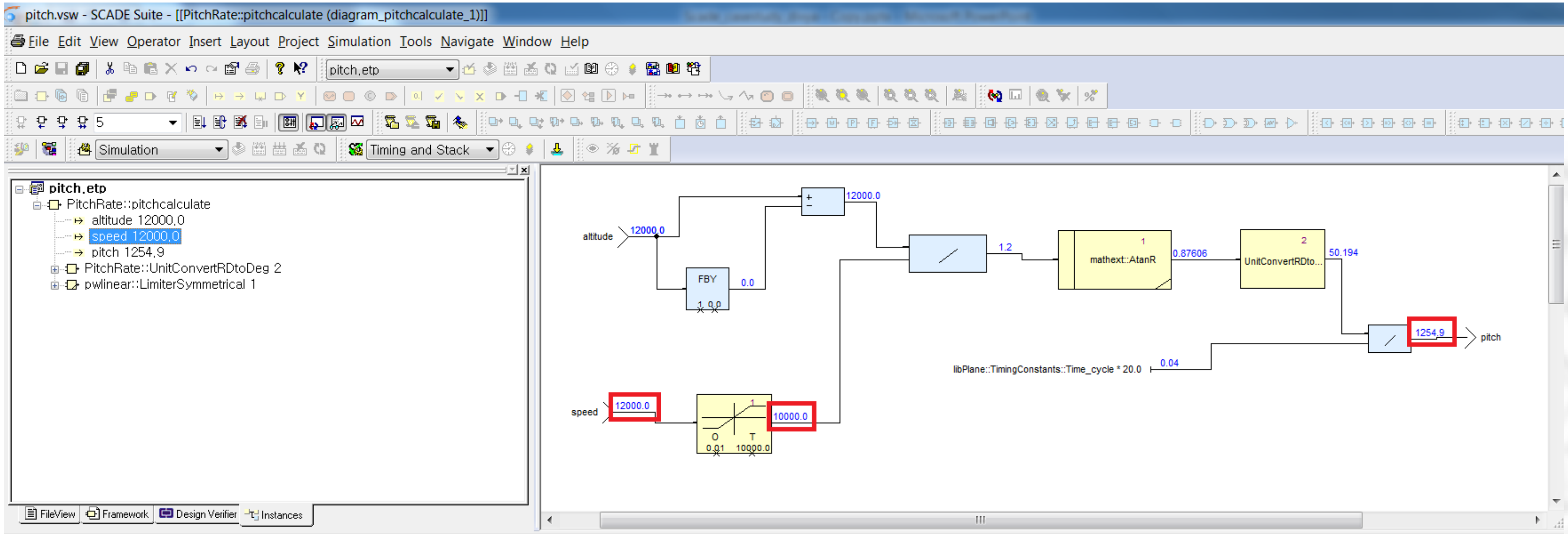
Data Flow of Pitch Control



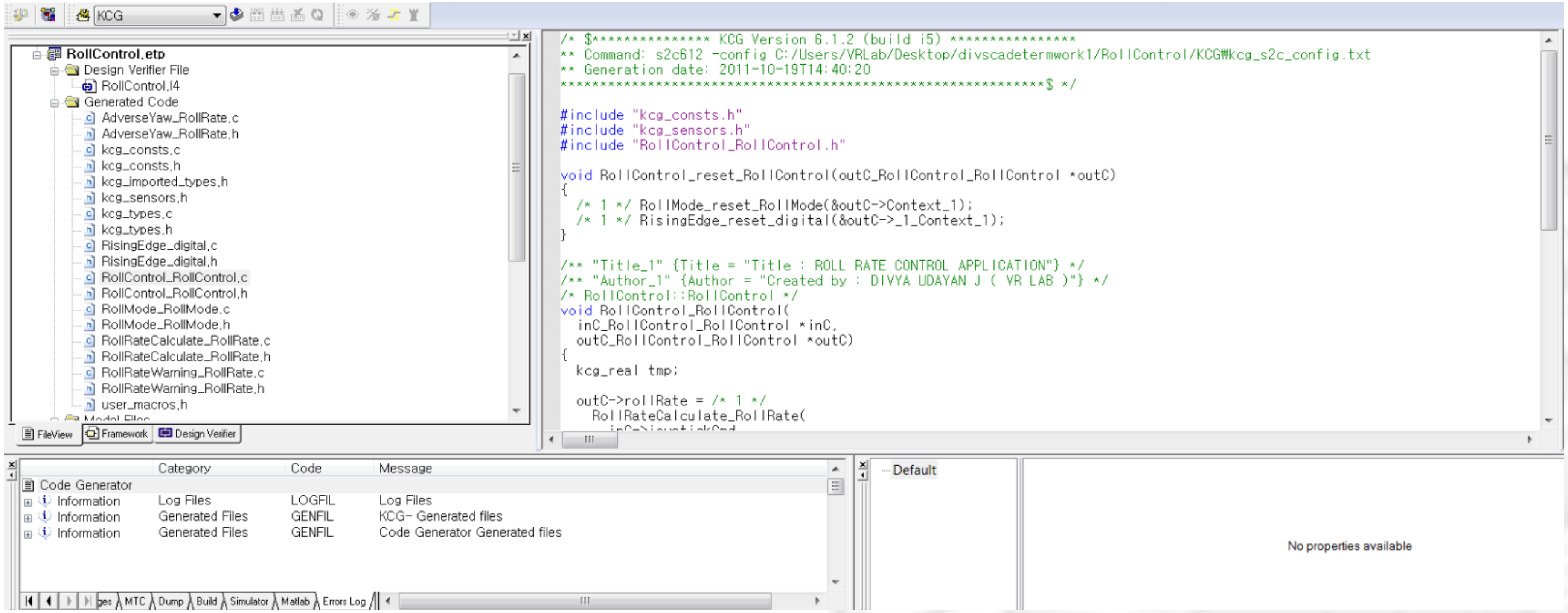
Simulation of Roll Control



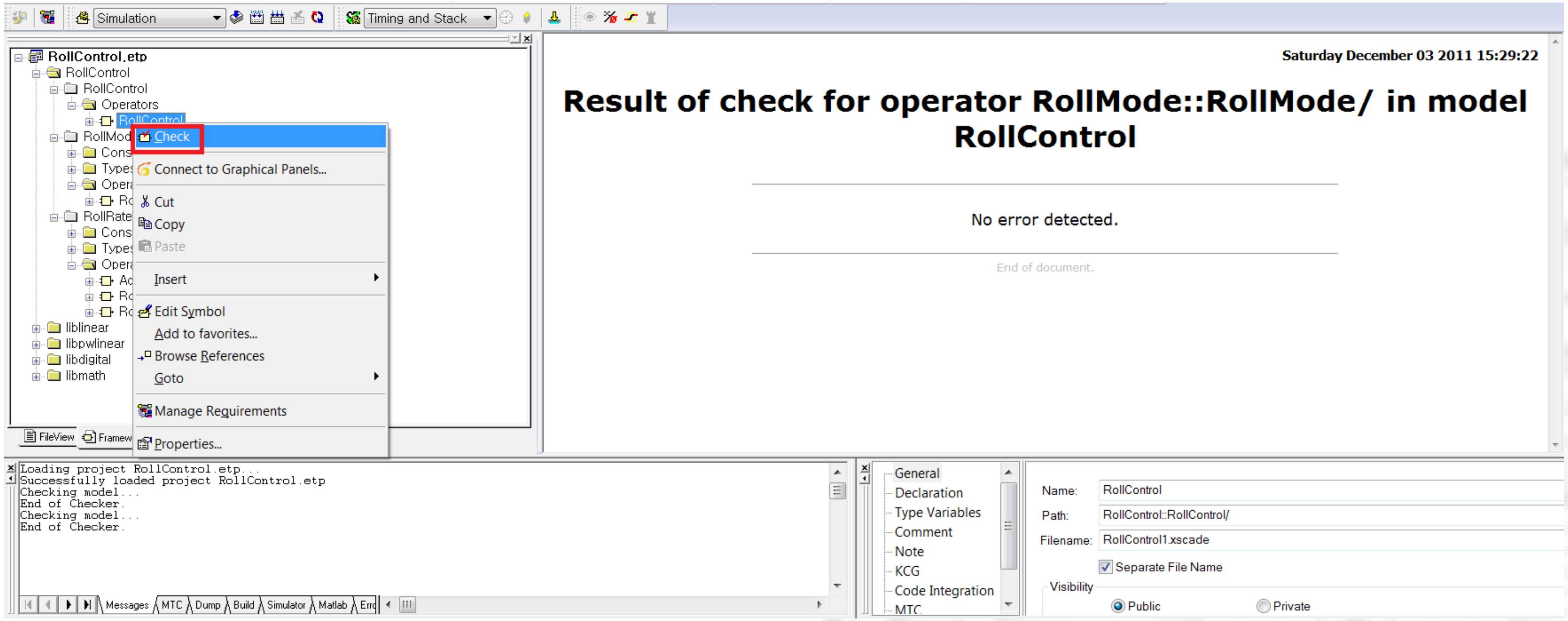
Simulation of Pitch Control



Code Generation



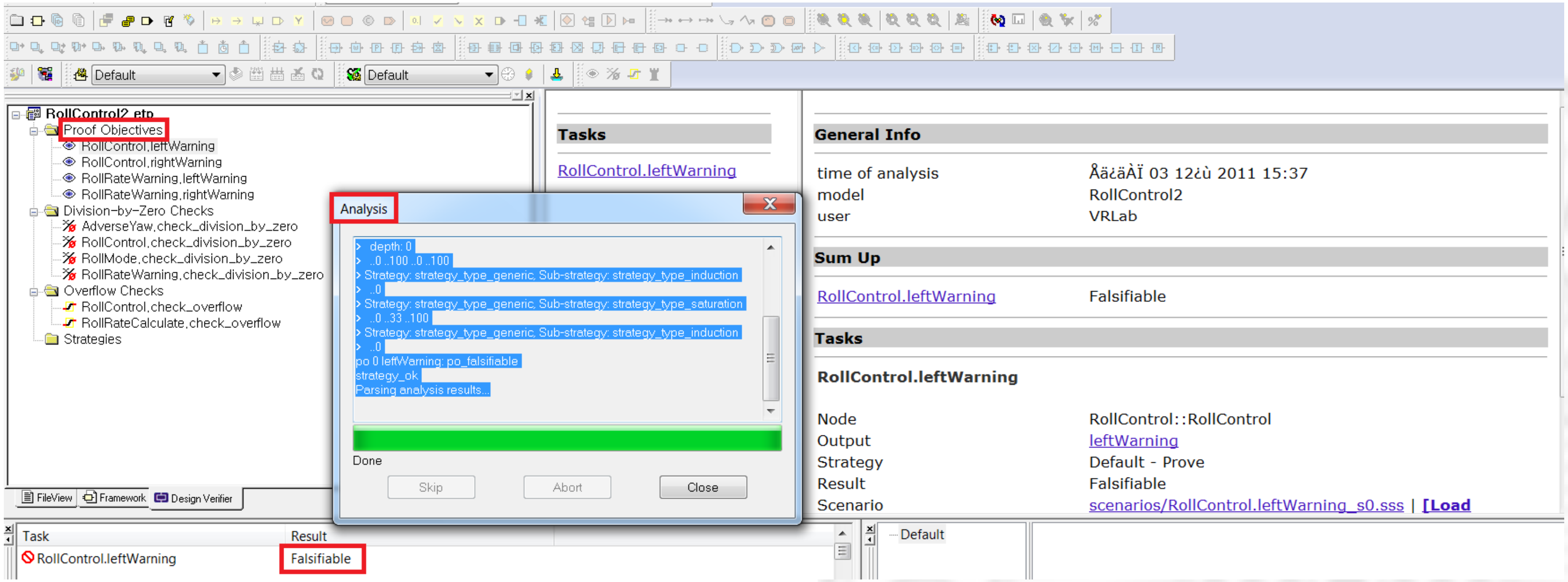
Semantic Verification



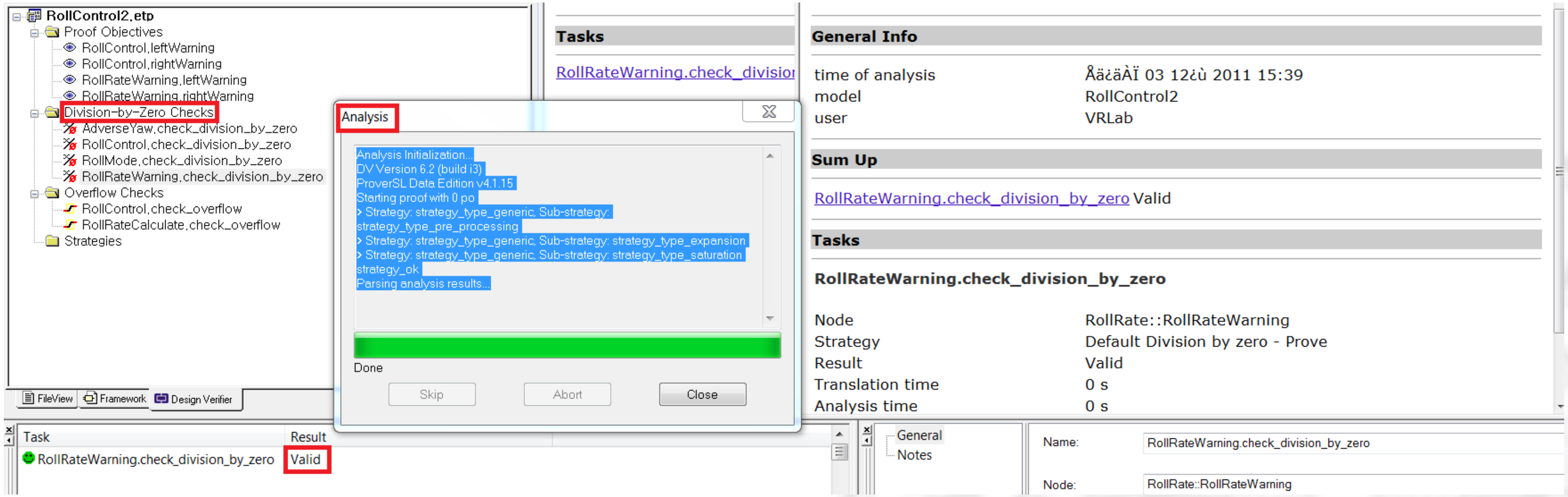
System Analysis

Verifying System Correctness(1/2)

- Using Observer Property, Divide by zero, Overflow stack



Verifying System Correctness(2/2)

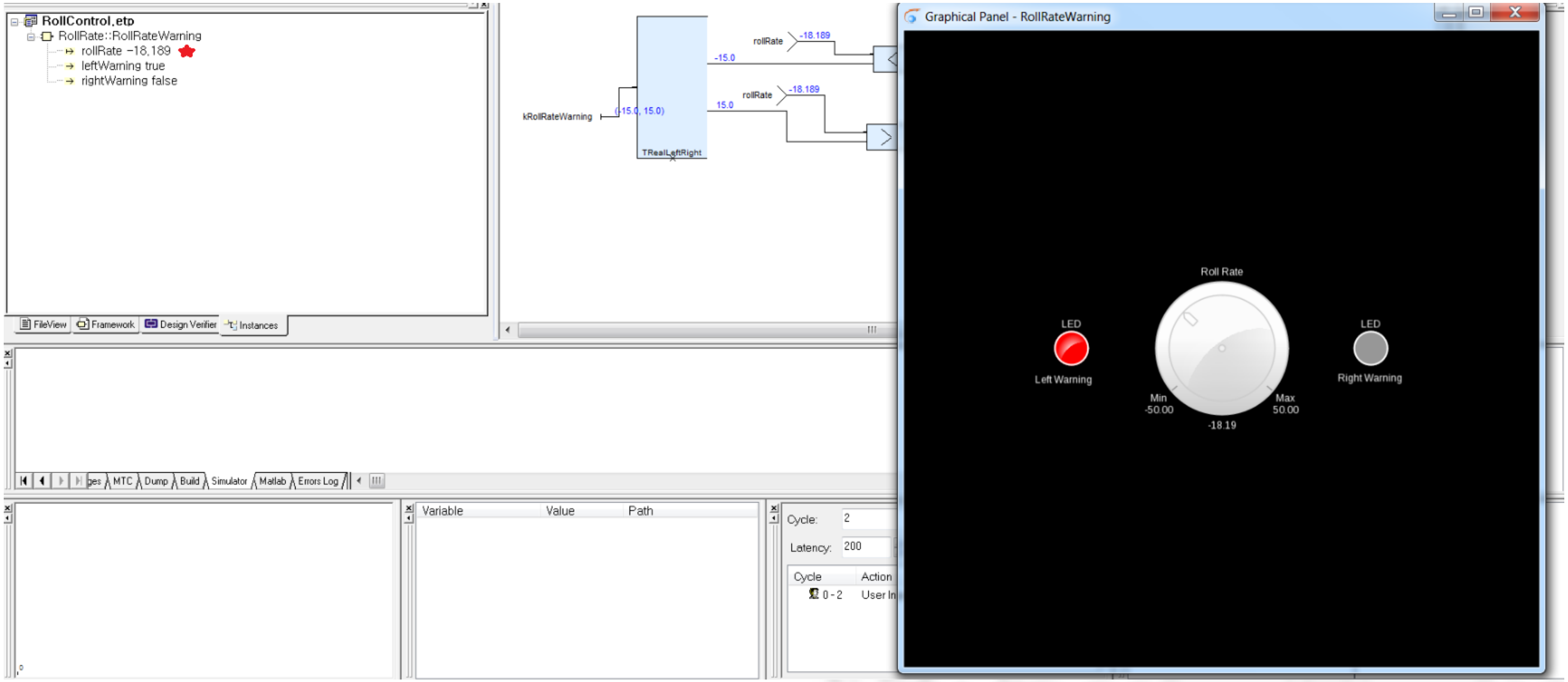


Proof Meaning

Proof result	Meaning
Valid	The verified property is always true mathematically.
Falsifiable	Property is false because Design Verifier detects a valuation of your system inputs such that the output of the observer operator is not equal to the value specified in the proof objective. Such input valuation is called a counter-example. To access the counter-example of a falsifiable property, see "Displaying Counter-Examples" on page 681.
Indeterminate	The proof reaches no significant conclusion.
Interrupted	Either you manually aborted the analysis in the status window, or Design Verifier finds no counter-example before strategy time-out (see "Setting Standard Strategy Options" on page 661).
Stop Depth Reached	The analysis reaches its execution cycle depth set in the debug strategy and Design Verifier cannot report any significant result (see "Setting Debug Strategy Options for Proofs" on page 662).
Raised an Error	The cause of error displays in the message field of the report. Possible errors are: use of unsupported Scade language features, bad syntax or semantics in your design, or an internal error of the proof engine (see "Understanding Design Verifier Error Messages" on page 677).
Error: Non Linear Property	Verification is impossible because the property is expressed with non-linear expressions or functions. Check your design and simplify the property operator or its context in the observer operator.
Contradictory	You expressed contradictory assertions in the analyzed design. Design Verifier is unable to resolve the analysis and stops the process. Revise your design to solve this error.

System Testing

- Graphical panel display



Report Generation

- Automatic report generation
- Shows the data flow diagrams and control flow diagrams
- Represent tables

Conclusion

- Model verification of the functional design with data flow and control flow of the roll and pitch of airplane.
- Automatic code generation, semantic checking
- Verifying system correctness
- Simulation using scade suit
- Scade suite graphical display verification of the stability of airplane

References

[1] www.esterel-technologies.com/products/scade-suite/


Thank You!