



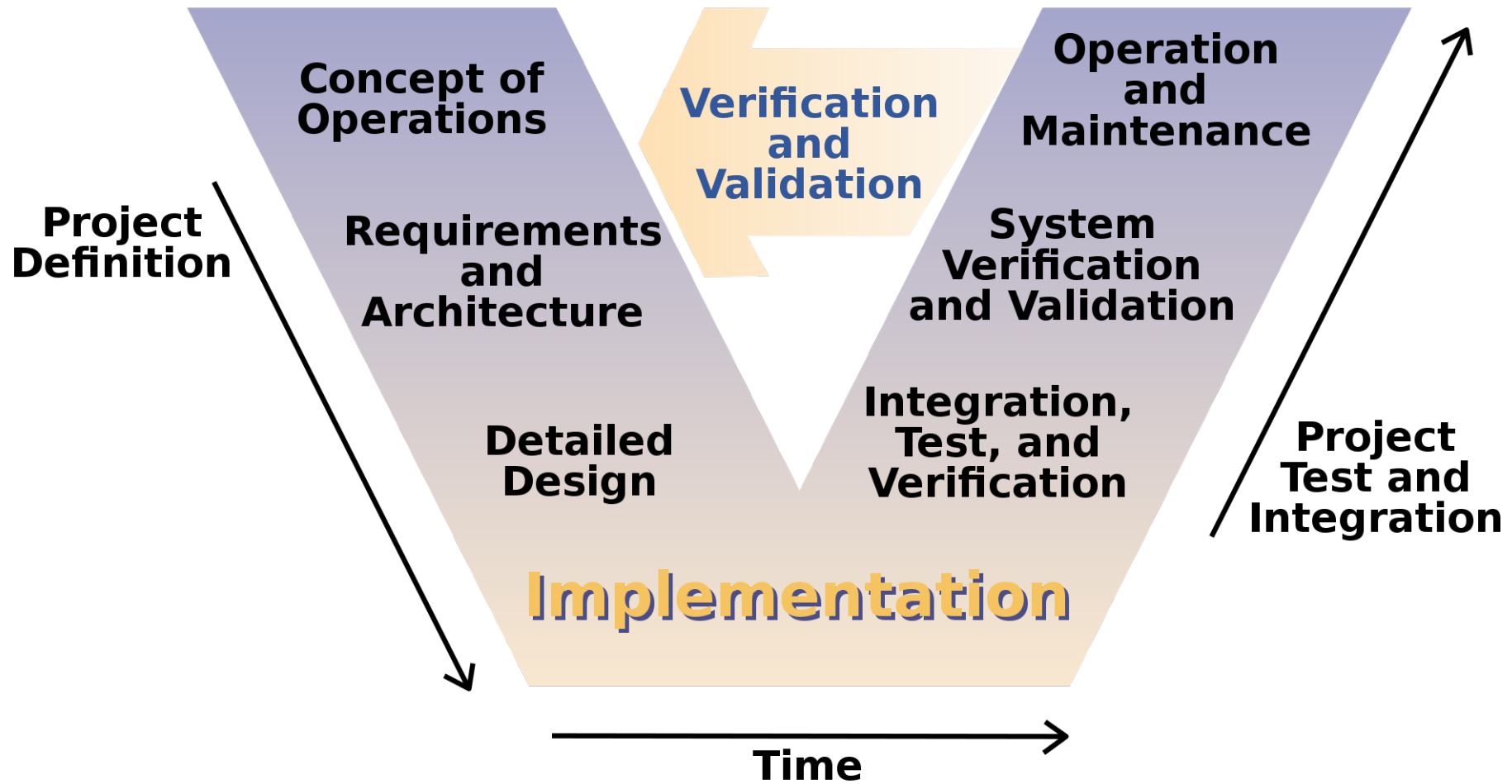
INTELLIGENT
SYSTEMS
DIVISION



CoCoSim Tutorial

Contract-based Compositional Verification of Simulink Models

Andreas Katis





NSSDCA Master Catalog Search

- + Spacecraft
- + Experiments
- + Data Collections
- + Personnel
- + Publications
- + Maps
- + New/Updated Data
- + Lunar/Planetary Events



Mariner 1

NSSDCA ID: MARIN1
COSPAR ID:

Description

This was to be the first Mariner mission. It was intended to perform a Venus flyby. The vehicle was destroyed by the Range Safety Officer 293 seconds after launch at 09:26:16 UT when it veered off course. The booster had performed satisfactorily until an unscheduled yaw-lift (northeast) maneuver was detected by the range safety officer. Faulty application of the guidance commands made steering impossible and were directing the spacecraft towards a crash, possibly in the North Atlantic shipping lanes or in an inhabited area. The destruct command was sent 6 seconds before separation, after which the launch vehicle could not have been destroyed. The radio transponder continued to transmit signals for 64 seconds after the destruct command had been sent.

The failure was apparently caused by a combination of two factors. Improper operation of the Atlas airborne beacon equipment resulted in a loss of the rate signal from the vehicle for a prolonged period. The airborne beacon used for obtaining rate data was inoperative for four periods ranging from 1.5 to 61 seconds in duration. Additionally, the Mariner 1 Post Flight Review Board determined that the omission of a hyphen in coded computer instructions in the data-editing program allowed transmission of incorrect guidance signals to the spacecraft. During the periods the airborne beacon was inoperative the omission of the hyphen in the data-editing program caused the computer to incorrectly accept the sweep frequency of the ground receiver as it sought the vehicle beacon signal and combined this data with the tracking data sent to the remaining guidance computation. This caused the computer to swing automatically into a series of unnecessary course corrections with erroneous steering commands which finally threw the spacecraft off course.

Spacecraft and Subsystems

The Mariner 1 spacecraft was identical to Mariner 2, launched 27 August 1962. Mariner 1 consisted of a hexagonal base, 1.04 meters across and 0.36 meters thick, which contained six magnesium chassis housing the electronics for the science experiments, communications, data encoding, computing, timing, and attitude control, and the power control, battery, and battery charger, as well as the attitude control gas bottles and the rocket engine. On top of the base was a tall pyramid-shaped mast on which the science experiments were mounted which brought the total height of the spacecraft to 3.66 meters. Attached to either side of the base were rectangular solar panel wings with a total span of 5.05 meters and width of 0.76 meters. Attached

Alternate Names

Facts in Brief

Launch Date: 1962-07-22
Launch Vehicle: Atlas-Agena B
Launch Site: Cape Canaveral, United States
Mass: 202.8 kg

Funding Agency

- NASA-Office of Space Science Applications (United States)

Disciplines

- Planetary Science
- Space Physics

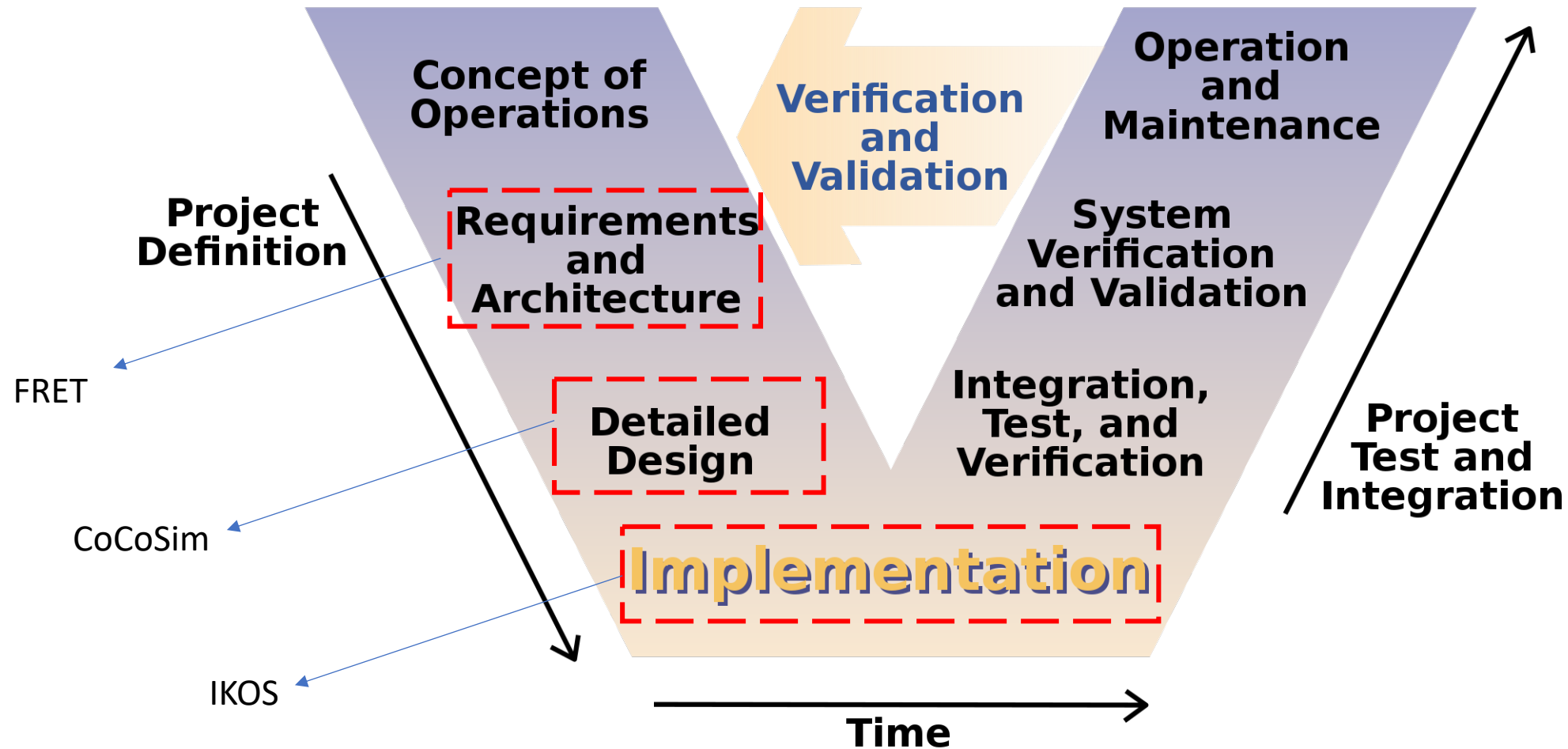
Additional Information

- Launch/Orbital information for Mariner 1
- Telecommunications information for Mariner 1
- Experiments on Mariner 1
- Data collections from Mariner 1

Questions and comments about this spacecraft can be directed to: Dr. David R. Williams

“...The vehicle was destroyed by the Range Safety Officer 293 seconds after launch...”

“...Additionally, the Mariner 1 Post Flight Review Board determined that the omission of a hyphen in coded computer instructions in the data-editing program allowed transmission of incorrect guidance signals to the spacecraft.”

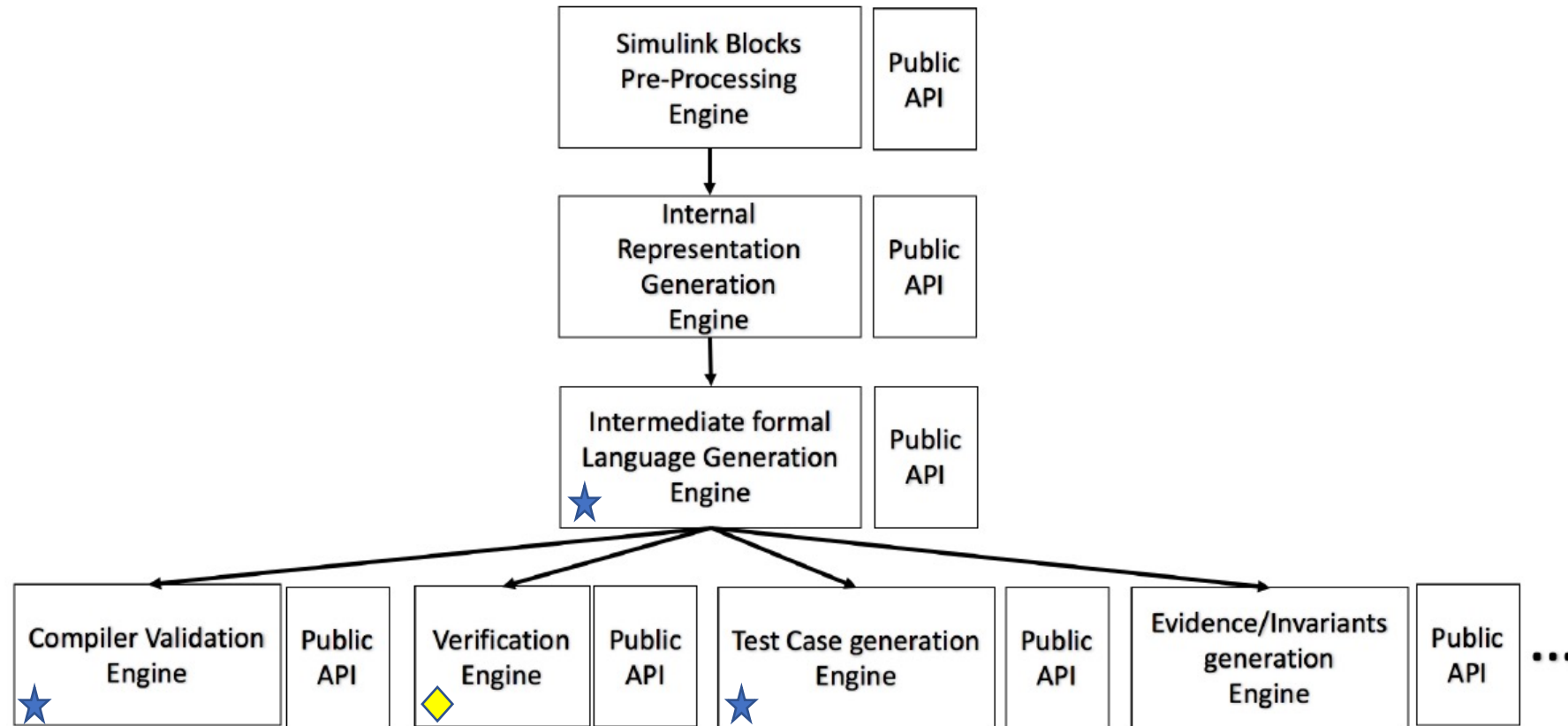


<https://github.com/NASA-SW-VnV>

CoCoSim: an open-source MATLAB plugin for

- Contract-based Compositional Verification of Simulink/Stateflow Models
 - Simulink/Stateflow translation to Verimag Lustre / C
 - Work in progress: Link with requirements specification tools (FRET), Test Case Generation
-
- Bourbouh, Hamza, Marie Farrell, Anastasia Mavridou, Irfan Slijivo, Guillaume Brat, Louise A. Dennis, and Michael Fisher. "Integrating formal verification and assurance: an inspection rover case study." In *NASA Formal Methods Symposium*, pp. 53-71. Springer, Cham, 2021.
 - Mavridou, Anastasia, Hamza Bourbouh, Dimitra Giannakopoulou, Thomas Pressburger, Mohammad Hejase, Pierre-Loïc Garoche, and Johann Schumann. "The ten lockheed martin cyber-physical challenges: formalized, analyzed, and explained." In *2020 IEEE 28th International Requirements Engineering Conference (RE)*, pp. 300-310. IEEE, 2020.
 - Mavridou, Anastasia, Hamza Bourbouh, Pierre Loïc Garoche, Dimitra Giannakopoulou, Thomas Pessburger, and Johann Schumann. "Bridging the gap between requirements and Simulink model analysis." In *Joint 26th International Conference on Requirements Engineering: Foundation for Software Quality Workshops, Doctoral Symposium, Live Studies Track, and Poster Track*. 2020.
 - Bourbouh, Hamza, Pierre-Loïc Garoche, Thomas Loquen, Éric Noulard, and Claire Pagetti. "CoCoSim, a code generation framework for control/command applications An overview of CoCoSim for multi-periodic discrete Simulink models." In *10th European Congress on Embedded Real Time Software and Systems (ERTS 2020)*. 2020.
 - Bourbouh, Hamza, Guillaume Brat, and Pierre-Loïc Garoche. "CoCoSim: an automated analysis framework for Simulink/Stateflow." In *Model Based Space Systems and Software Engineering-European Space Agency Workshop (MBSE 2020)*. 2020.

CoCoSim Architecture

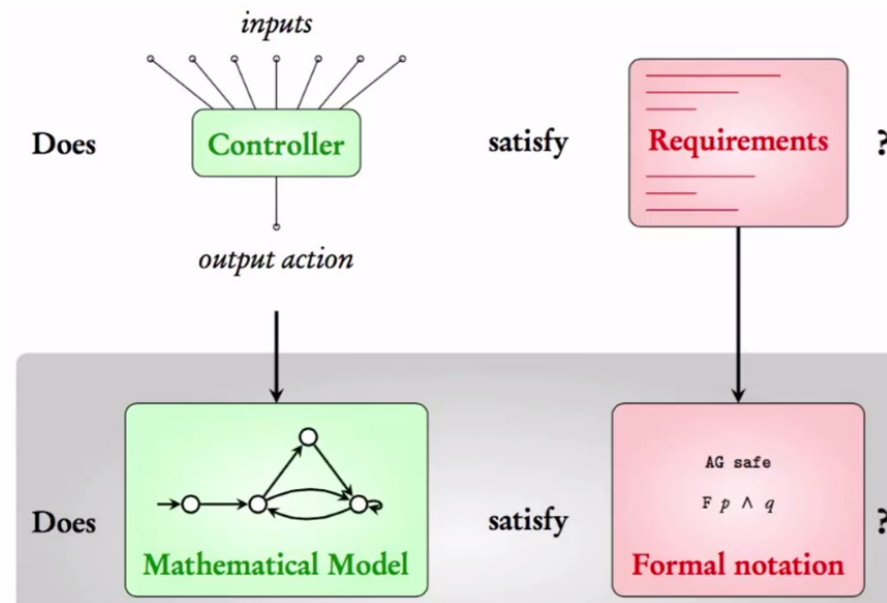


★ LustreC

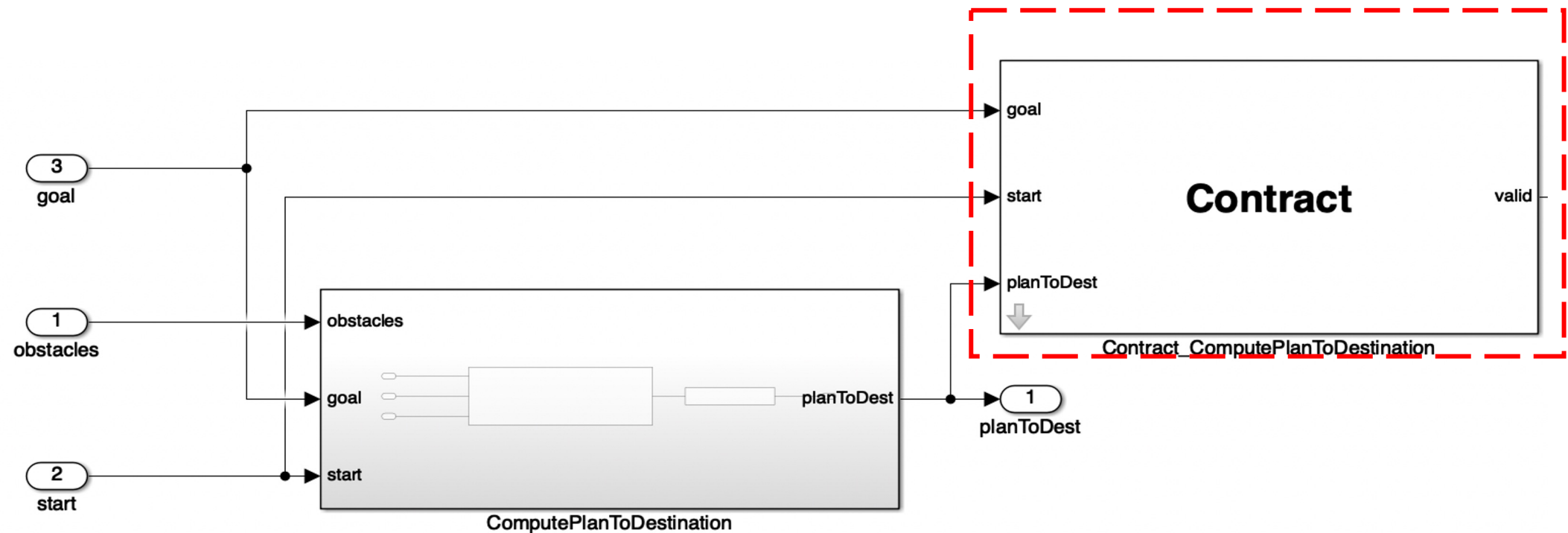
◆ Kind 2

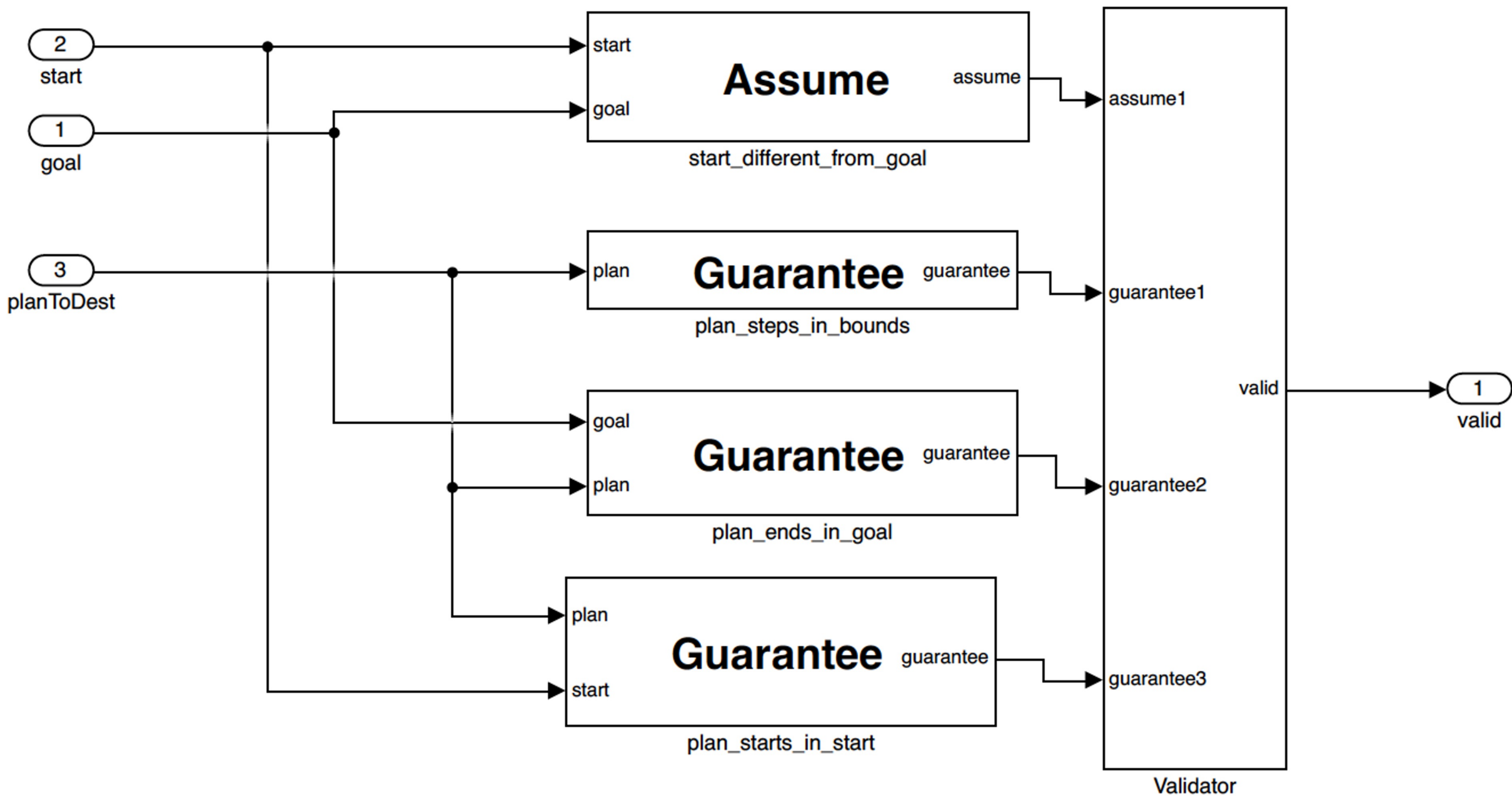
Verification

- Formal verification: Prove that a system **always** conforms to our requirements
- By constructing a mathematical proof!
- Model checking



Requirements are expressed using the CoCoSim library.





HOME

PLOTS

APPS

New Script

New Live Script

New

Open

Find Files

Compare

Import Data

Save Workspace

Open Variable

Clear Workspace

Favorites

Analyze Code

Run and Time

Clear Commands

Simulink

Layout

Preferences

Set Path

Add-Ons

Help

Community

Request Support

Learn MATLAB

Search Documentation

Sign in

home

akatis

Documents

CoCoSim

demo

Current Folder

absolute.slx

Command Window

New to MATLAB? See resources for [Getting Started](#).

>> start_cocosim

WELCOME TO COCOSIM (NASA Ames)

... Starting cocoSim configuration
From https://github.com/NASA-SW-VnV/CoCoSim
* branch installation_fix -> FETCH_HEAD
Already up to date.
Already on 'cocosim_nasa'
Your branch is up to date with 'origin/cocosim_nasa'.
From https://github.com/coco-team/cocoSim2
* branch cocosim_nasa -> FETCH_HEAD
Already up to date.
Already on 'master'
From https://github.com/hbourbough/cocosim-external-libs
* branch master -> FETCH_HEAD
Already up to date.
(warning)[tools_config] VICES2 is not found in */home/akatis/git/CoCoSim/tools/verifiers/linux/bin/yices-
(warning)[tools_config] You can ignore the previous warning if you are not going to use VICES2 with Kind:
Tools config is already run and will be ignored.
To force it run "tools_config" in your Matlab Command Window.

Click [here](#) to change pre-processing configuration.
... Configuration is Done

Click [here](#) to start with a simple verification example.
fx >>

Workspace

Name	Value
cocosim_verb...	0

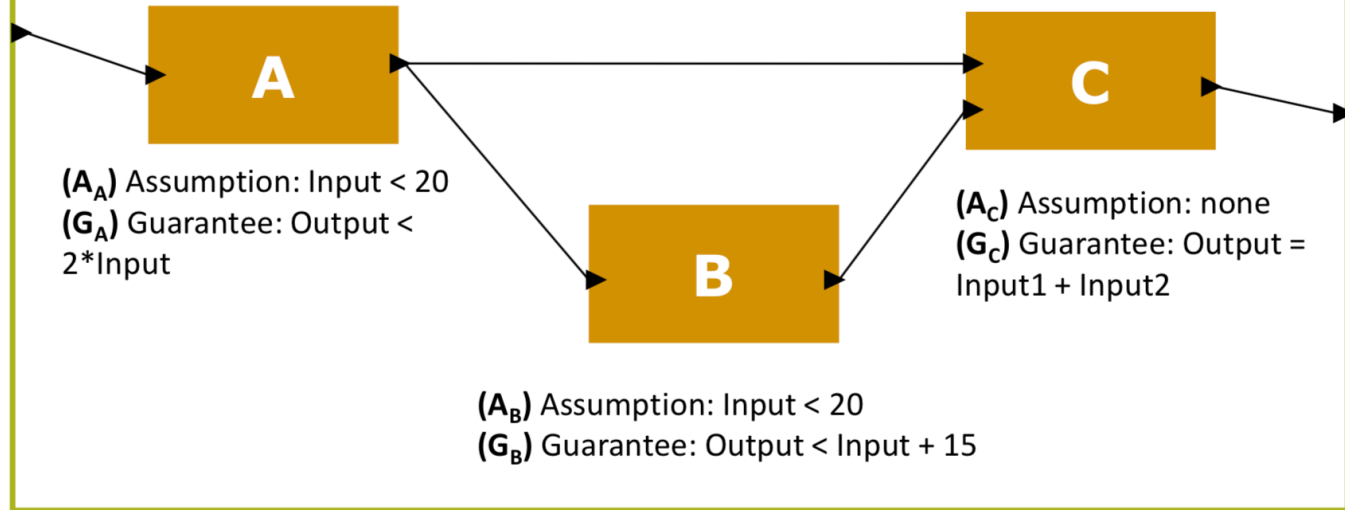
Details

Compositional Verification

Example (to prove)

$A_S \rightarrow A_A$
 $A_S \wedge G_A \rightarrow A_B$
 $A_S \wedge G_A \wedge G_B \rightarrow A_C$
 $A_S \wedge G_A \wedge G_B \wedge G_C \rightarrow G_S$

(A_S) Assumption: $\text{Input} < 10$
 (G_S) Guarantee: $\text{Output} < 50$



$\text{Input}_A = 9, \text{Output}_A = 17, \text{Output}_B = 31, \text{Output}_C = 48$

HOME

PLOTS

APPS

New Script

New Live Script

New

Open

Find Files

Compare

Import Data

Save Workspace

New Variable

Open Variable

Clear Workspace

Favorites

Analyze Code

Run and Time

Clear Commands

Simulink

Layout

Preferences

Set Path

Add-Ons

Help

Community

Request Support

Learn MATLAB

Search Documentation

Sign In

home

akatis

Documents

CoCoSim

demo

Current Folder

Command Window

Workspace

Name

Value

cocosim_output

cocosim_verb... 0

ABC.slx

ABC_PP.slx

absolute.slx

absolute_PP.slx

ABC.slx (Simulink Model)

New to MATLAB? See resources for [Getting Started](#).

>> start_cocosim

WELCOME TO COCOSIM (NASA Ames)

... Starting cocoSim configuration

From <https://github.com/NASA-SW-VnV/CoCoSim>

* branch installation_fix -> FETCH_HEAD

Already up to date.

Already on 'cocosim_nasa'

Your branch is up to date with 'origin/cocosim_nasa'.

From <https://github.com/coco-team/cocoSim2>

* branch cocosim_nasa -> FETCH_HEAD

Already up to date.

Already on 'master'

From <https://github.com/hbourbough/cocosim-external-libs>

* branch master -> FETCH_HEAD

Already up to date.

(warning)[tools_config] YICES2 is not found in */home/akatis/git/CoCoSim/tools/verifiers/linux/bin/yices-

(warning)[tools_config] You can ignore the previous warning if you are not going to use YICES2 with Kind

Tools config is already run and will be ignored.

To force it run "tools_config" in your Matlab Command Window.

Click [here](#) to change pre-processing configuration.

... Configuration is Done

Click [here](#) to start with a simple verification example.

>>

Compositional Verification

Example (to prove)

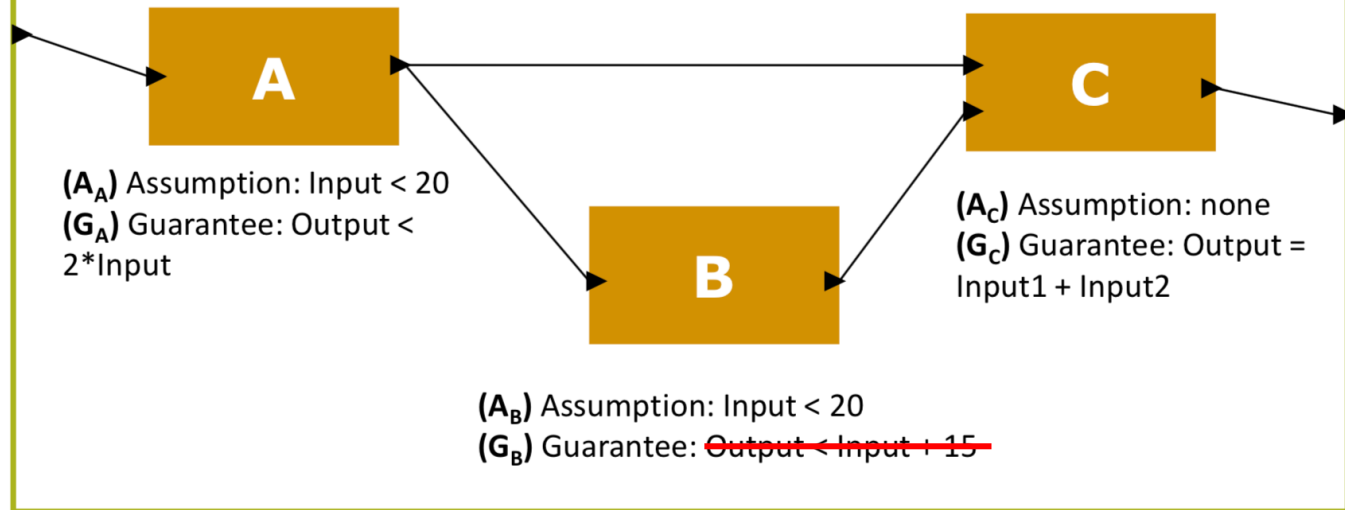
$$A_S \rightarrow A_A$$

$$A_S \wedge G_A \rightarrow A_B$$

$$A_S \wedge G_A \wedge G_B \rightarrow A_C$$

$$A_S \wedge G_A \wedge G_B \wedge G_C \rightarrow G_S$$

(A_S) Assumption: $\text{Input} < 10$
 (G_S) Guarantee: $\text{Output} < 50$



$$G_B = \text{Output} < \text{Input} + 50$$

Verification Summary

ABC_PP/S/C__abstracted/C

Result
✓

ABC_PP/S/B__abstracted/B

Result
✓

ABC_PP/S/A__abstracted/A

Result
✗

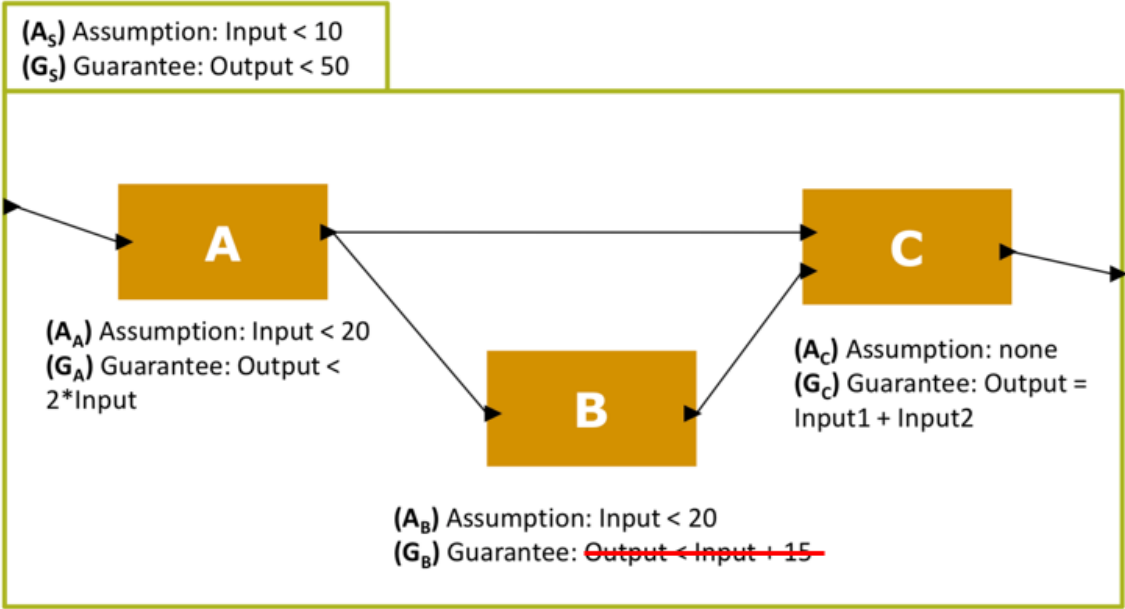
ABC_PP/S

Abstract C	Abstract B	Abstract A	Abstract C	Result
✓	✓	✓	✓	✗
✓	✗	✓	✓	✓

The new contract for B is not sufficient to prove the system-level contract!

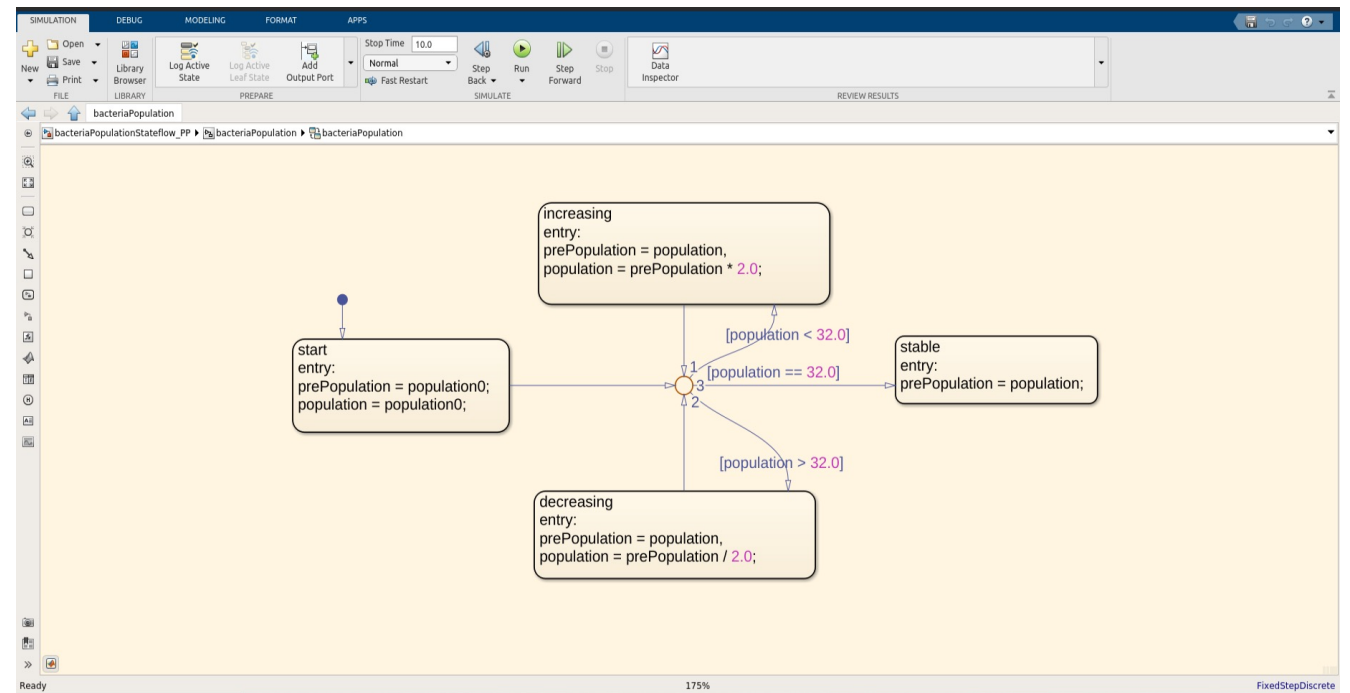
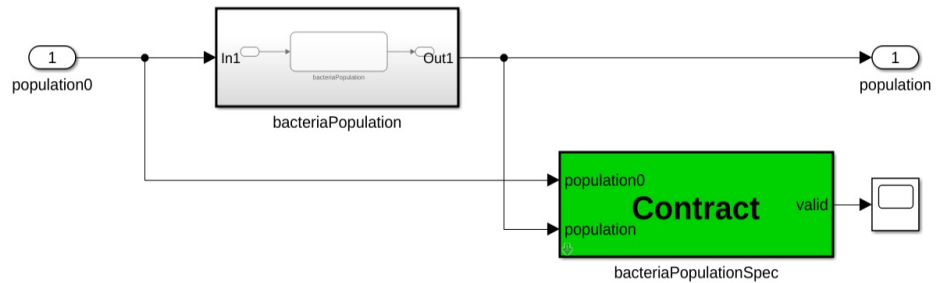
ABC_PP/S

Time	0
Input (input)	9
Output (output)	50
C__abstracted (local)	50
A__abstracted (local)	17
B__abstracted (local)	33



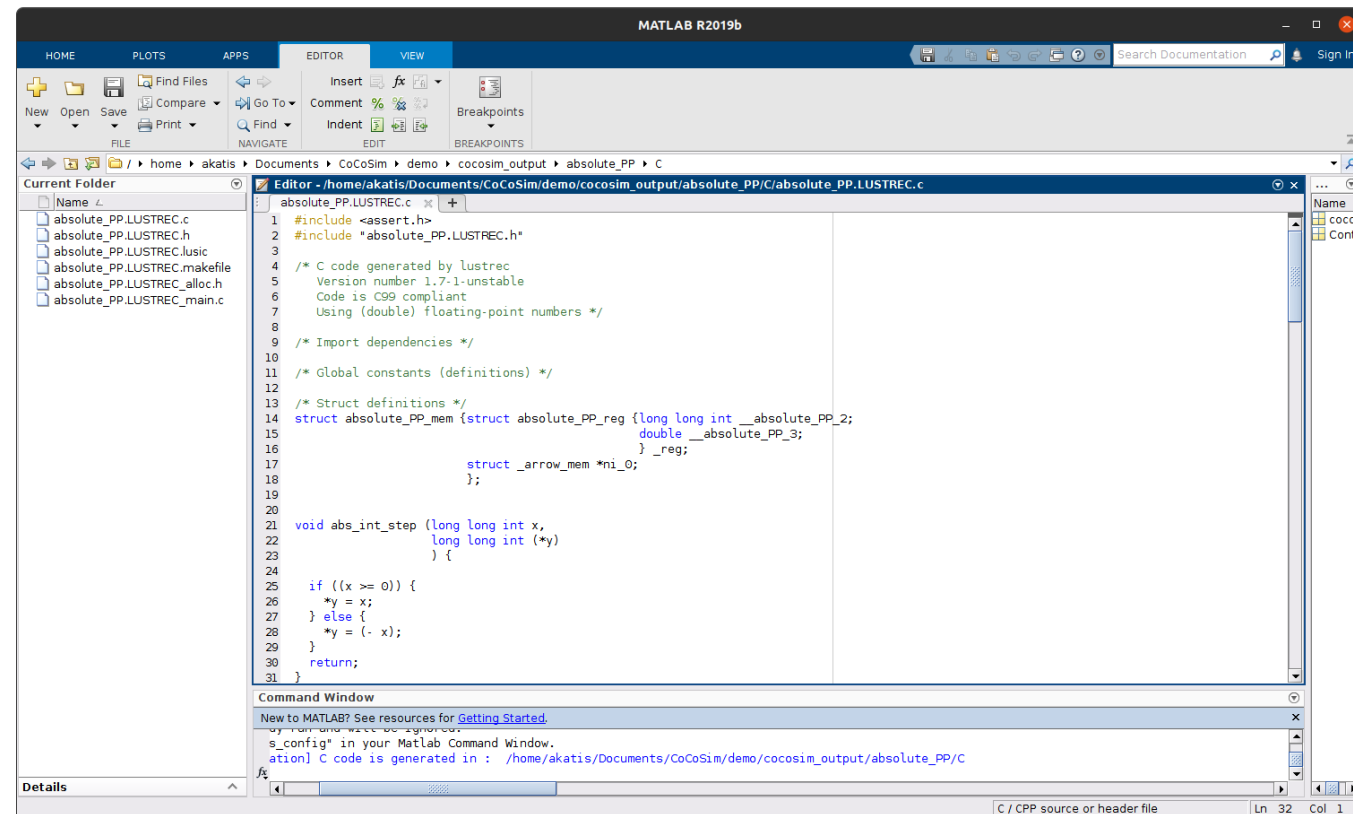
$G_B = Output < Input + 50$

Stateflow verification



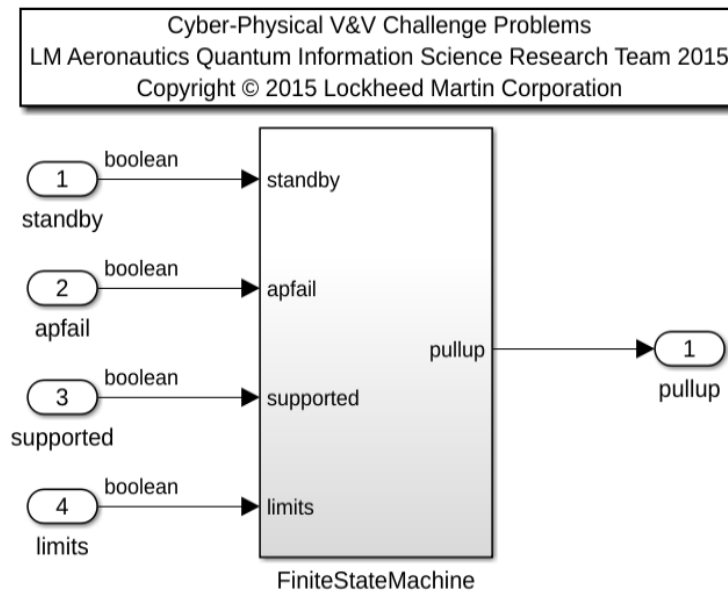
Code Generation

- Verimag Lustre & C (through LustreC)
- Rust (through Kind 2)
- Compiler validation through equivalence testing and equivalence checking



Connection with FRET

- Import FRET requirements in CoCoSim
- Automated generation of Simulink monitors based on traceability data
- Analysis results can be traced back to original FRET requirements



FRET Requirements

FRET

Requirements: CoCoSim_FSM

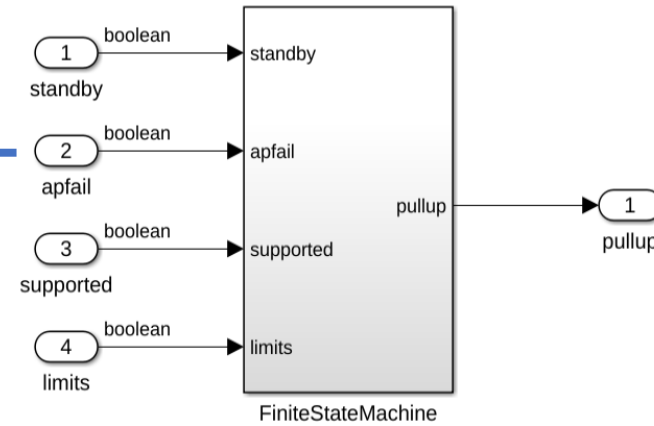
Search requirements

Status	ID ↑	Summary	Project
✓	FSM-001V1	FSM shall always satisfy (limits & standby & apfail & supported) => pullup	CoCoSim_FSM
✓	FSM-001V2	if autopilot & pre_autopilot & pre_limits FSM shall immediately satisfy pullup	CoCoSim_FSM
✓	FSM-001V3	if htlore3_autopilot & htlore3_notpreprelimits & pre_limits FSM shall immediately satisfy pullup	CoCoSim_FSM
✓	FSM-002	FSM_Autopilot shall always satisfy (standby & state = ap_transition_state) => STATE = ap_standby_state	CoCoSim_FSM
✓	FSM-003	FSM_Autopilot shall always satisfy (state = ap_transition_state & good & supported) => STATE = ap_nominal_state	CoCoSim_FSM
✓	FSM-004	FSM_Autopilot shall always satisfy (! good & state = ap_nominal_state) => STATE = ap_maneuver_state	CoCoSim_FSM
✓	FSM-004V2	FSM_Autopilot shall always satisfy (state = ap_nominal_state & ! good & ! standby) => STATE = ap_maneuver_state	CoCoSim_FSM
✓	FSM-005	FSM_Autopilot shall always satisfy (state=ap_nominal_state & standby) => STATE = ap_standby_state	CoCoSim_FSM
✓	FSM-006	FSM_Autopilot shall always satisfy (state = ap_maneuver_state & standby & good) => STATE = ap_standby_state	CoCoSim_FSM
✓	FSM-007	FSM_Autopilot shall always satisfy (state = ap_maneuver_state & supported & good) => STATE = ap_transition_state	CoCoSim_FSM

Rows per page: 10 1-10 of 19

Model Information (JSON)

Cyber-Physical V&V Challenge Problems
LM Aeronautics Quantum Information Science Research Team 2015
Copyright © 2015 Lockheed Martin Corporation



Export CoCoSpec (Lustre) + Traceability data

FRET

Requirement Variables to Model Mapping: LM_requirements

Export Language *

Autopilot EXPORT

FSM EXPORT

Corresponding Model Component
fsm_12B/FiniteStateMachine/Manager IMPORT

FRET Variable Name ↑	Model Variable Name	Variable Type	Data Type	Description
APFAIL	apfail	Input	boolean	
AUTOPILOT		Internal	boolean	
HTLORE3_AUTOPILOT		Internal	boolean	
HTLORE3_NOTPREPRELIMITS		Internal	boolean	
LIMITS	supported	Input	boolean	

FRET

Requirement Variables to Model Mapping: LM_requirements

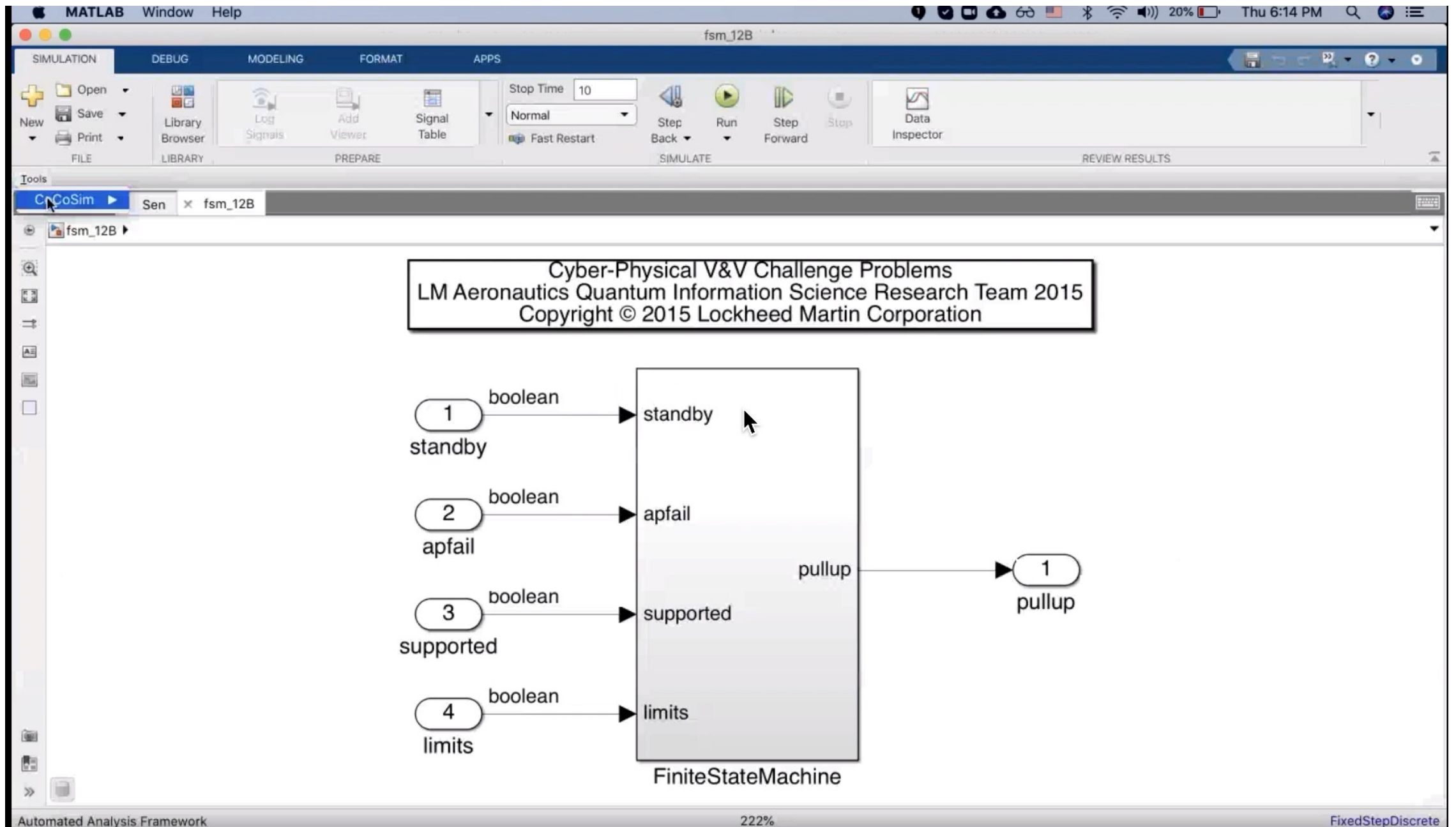
Export Language *
CoCoSpec

Autopilot EXPORT

FSM EXPORT

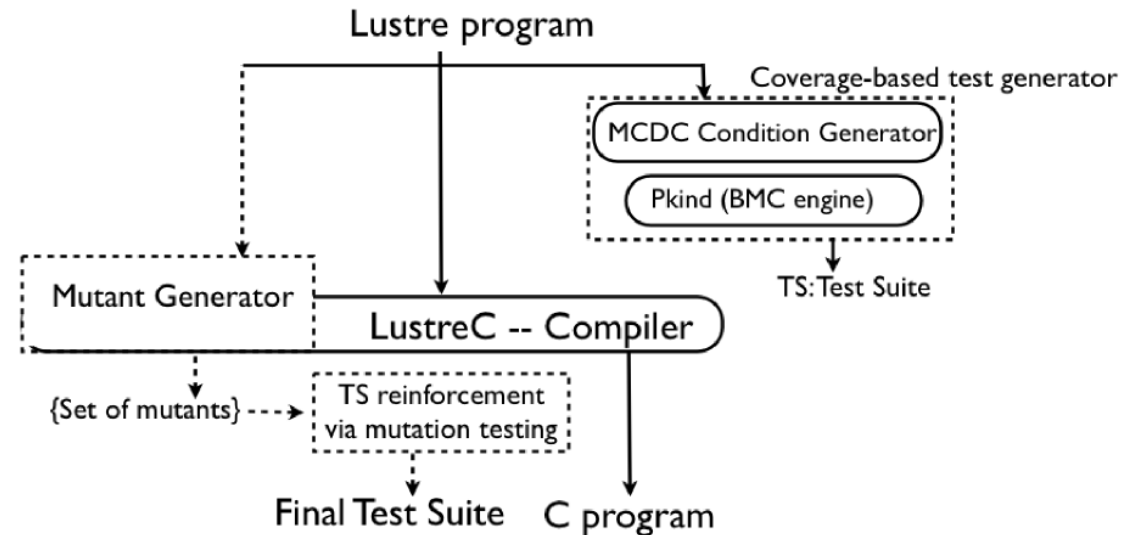
Corresponding Model Component
fsm_12B/FiniteStateMachine IMPORT

FRET Variable Name ↑	Model Variable Name	Variable Type	Data Type	Description
----------------------	---------------------	---------------	-----------	-------------



Test-case generation

- Random test generation (Simulink)
 - MC/DC
 - Mutation-based
- } via LustreC (Work in Progress)



HOME

PLOTS

APPS

New Script

New Live Script

New

Open

Find Files

Compare

Import Data

Save Workspace

New Variable

Open Variable

Clear Workspace

Favorites

Analyze Code

Run and Time

Clear Commands

Simulink

Layout

Preferences

Set Path

Add-Ons

Help

Community

Request Support

Learn MATLAB

Search Documentation

Sign In

FILE

VARIABLE

CODE

SIMULINK

ENVIRONMENT

RESOURCES

Current Folder

Command Window

Workspace

home

akatis

Documents

CoCoSim

demo

Name

cocosim_output

ABC.slx

ABC_PP.slx

absolute.slx

absolute_PP.slx

mcdc_test.slx

Details

New to MATLAB? See resources for [Getting Started](#).

>> clear

>>

Name	Value
------	-------

Library	# supp. Blocks	% supp. Blocks	Unsupported blocks
Discontinuities	11/12	91%	Backlash
Discrete	19/21	90%	Discrete PID Controller, Discrete PID Controller (2DOF)
Logic & Bit Operations.	18/19	95%	Extract Bits
Lookup Tables.	9/9	100%	
Math Operations.	31/37	83%	Algebraic Constraint, Complex to Magnitude-Angle, Complex to Real-Imag, Find, Magnitude-Angle to Complex, Real-Imag to Complex
Model Verification	11/11	100%	
Ports & Subsystems.	29/31	93%	While Iterator Subsystem, While Iterator
Signal Attributes.	13/14	93%	Unit Conversion
Signal Routing.	13/25	52%	Data Store Memory, Data Store Read, Data Store Write, Environment Controller, Goto Tag Visibility, Index Vector, State Reader, State Writer, Variant Source, Variant Sink, Manual Variant Source, Manual Variant Sink
Sinks.	9/9	100%	Visualization blocks are ignored
Sources.	15/26	57%	Band-Limited White Noise, Counter Free-Running, Counter Limited, From File, From Spreadsheet, Repeating Sequence, Repeating Sequence Interpolated, Repeating Sequence Stair, Signal Editor, Signal Generator, Waveform Generator
User-Defined Functions.	2/15	13%	Argument Inport, Argument Outport, Event Listener, Function Caller, Initialize Function, Interpreted MATLAB Function, Level-2 MATLAB S-Function, MATLAB System, Reset Function, S-Function, S-Function Builder, Simulink Function, Terminate Function

Block Name	Unsupported Options
Trigonometry	Operator 'cos + jsin' is not supported.
Switch	Allow different data input sizes option is not supported.
Relational Operator	Operator "isInf", "isNaN", "isFinite" are not supported.
Merge	- Allow unequal port widths is not supported. - We support only Merge blocks that are connected to conditionally-executed subsystem.
Function Call Generator	Number of iterations > 1 is not supported.
For Iterator	- External iteration limit source is not supported. - External increment is not supported. - Action Ports inside a For Iterator block should have "States when execution is resumed" option set to "reset". - Outports in a conditionally executed Subsystem inside a For Iterator block should have "Output when disabled" set to "reset". - Memory blocks are only allowed in the first level of the For Iterator Subsystem.
Discrete Pulse Generator	Option "Use external signal" is not supported.
Demux	Bus selection mode should be off.
Selector	"Starting and ending indices (port)" option is not supported.
Multiport Switch	- "Specify indices" option is not supported. - Allow different data input sizes is not supported.
Lookup Table blocks	- More than 7 dimensions interpolation is not supported. - "Intermediate results Data Type" option should be set to double or single.
From Workspace	"Cyclic repetition" option is not supported.
Delay	When Delay length > 1, the initial condition should be scalar.
Concatenate	Concatenate dimension > 2 is not supported.
Assignment	- OutputInitialize set to 'Specify size for each dimension in table' is not supported, - IndexOptionArray set to 'Starting and ending indices (port)' is not supported.

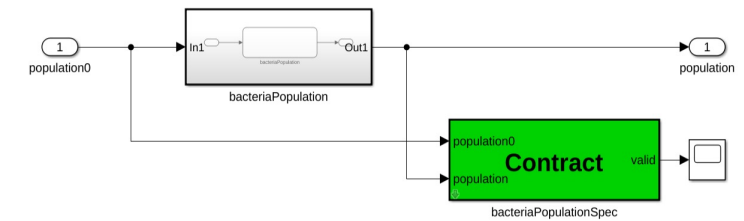
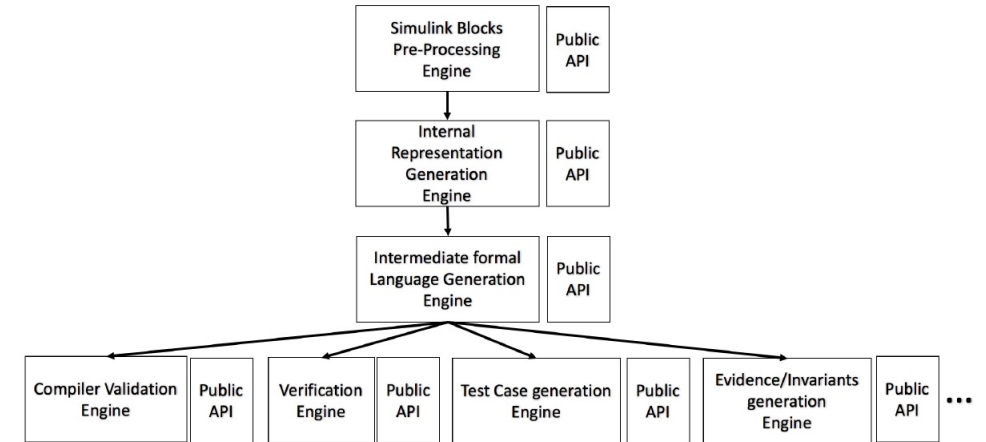
Thank you!

<https://github.com/NASA-SW-VnV/CoCoSim>

Guillaume Brat (guillaume.p.brat@nasa.gov)

Pierre-Loïc Garoche (pierre-loic.garoche@enac.fr)

Andreas Katis (andreas.katis@nasa.gov)



Verification Summary

ABC_PP/S/C__abstracted/C

Result

✓

ABC_PP/S/B__abstracted/B

Result

✓

ABC_PP/S/A__abstracted/A

Result

✗

ABC_PP/S

Abstract C	Abstract B	Abstract A	Abstract C	Result
✓	✓	✓	✓	✗
✓	✗	✓	✓	✓

