We Cover All Boundaries

Design Verifier Comparison to T-VEC VGS

T-VEC Technologies, Inc

Understanding Value of Tool Chains - Example Thread

Starts with model creation and simulation, and then model transformation enables code generation test vector generation, test driver generation, test execution, and test coverage analysis, with model-to-test traceability

	MS Project	DOORS	TTM/SCR	Simulink	Stateflow	Real Time Workshop	T-VEC Tester for Simulink	T-VEC Vector Generation System	Vectorcast	Design Verifier with Prover	LDRA	Rational Test RT	Reactis
Project planning	H												
Requirement management		H	S/I										
Requirement modeling			H										
Requirement simulation			I					S					
Design modeling				H									
Design simulation				H									S
Concurrent modeling													
Property specification			S				H	H					U
Model transformation			H				H	I					U
Code generation				I	I	H							
Disjointness checking			I					H					
Race condition checking			I					H					
Satisfiability non-linear								H					U
Satisfiability linear								H		L			U
Satisfiability logical								H		S			U
Arithmetic exceptions								H					U
Prove properties			I	I	I			H		S			U
Concurrency analysis				I	I	S							
Test sequence generation							I	H					S
Test vector generation								H					S
Test driver generation								H	I				
Model coverage								H		I			S
Test coverage analysis									H		H	H	
Test execution									H		H	H	
Test results analysis								H	H		H	H	
Model-to-test traceability			I	I				H					
Model standards													
Code standards									H		H	H	
Model management													
Confirmation management													
Test management								A	H		U	U	
Embedded Target Testing									H		U	U	

Key: Categories

- H: High - relatively complete
- S: Some
- L: Low
- U: Unknown - possible
- A: Absorbed - unnecessary
- I: Provided through tight tool integration

What's the value of the capability?

Saves significant human effort, increases consistency, identifies defects, assesses completeness, covers entire life cycle

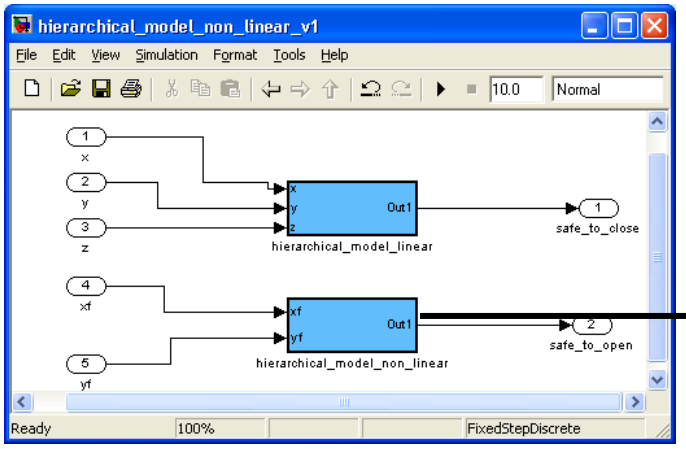
Focus Area of Comparison Related to Analysis

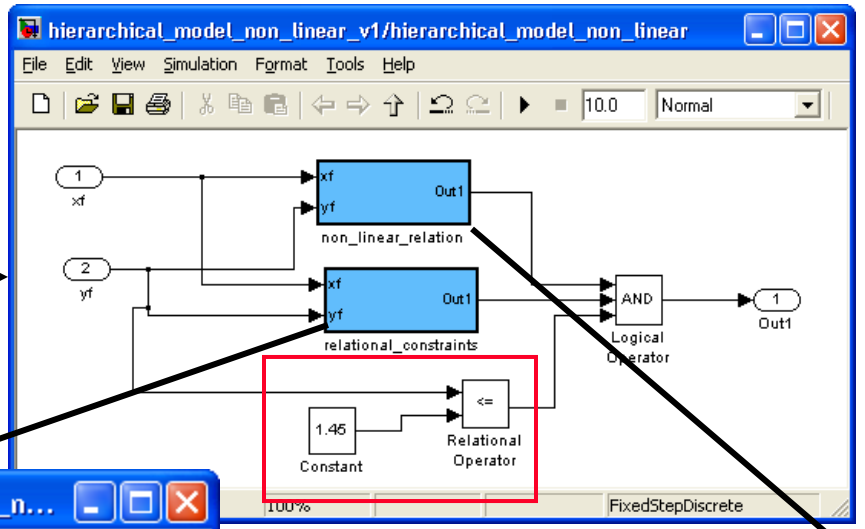
	MS Project	DOORS	TTM/SCR	Simulink	Stateflow	Real Time Workshop	T-VEC Tester for Simulink	T-VEC Vector Generation System	Vectorcast	Design Verifier with Prover	LDRA	Rational Test RT	Reactis
Project planning	H												
Requirement management		H	S/I										
Requirement modeling			H										
Requirement simulation			I					S					
Design modeling				H									
Design simulation				H									S
Concurrent modeling													
Property specification			S				H	H					U
Model transformation			H				H	I					U
Code generation				I	I	H							
Disjointness checking			I					H					
Race condition checking			I					H					
Satisfiability non-linear								H					U
Satisfiability linear								H		L			U
Satisfiability logical								H		S			U
Arithmetic exceptions								H					U
Prove properties			I	I	I			H		S			U
Concurrency analysis				I	I	S							
Test sequence generation							I	H					S
Test vector generation								H					S
Test driver generation								H	I				
Model coverage								H		I			S
Test coverage analysis									H		H	H	
Test execution									H		H	H	
Test results analysis								H	H		H	H	
Model-to-test traceability			|	I				H					
Model standards													
Code standards									H		H	H	
Model management													
Confirmation management													
Test management								A	H		U	U	
Embedded Target Testing									H		U	U	

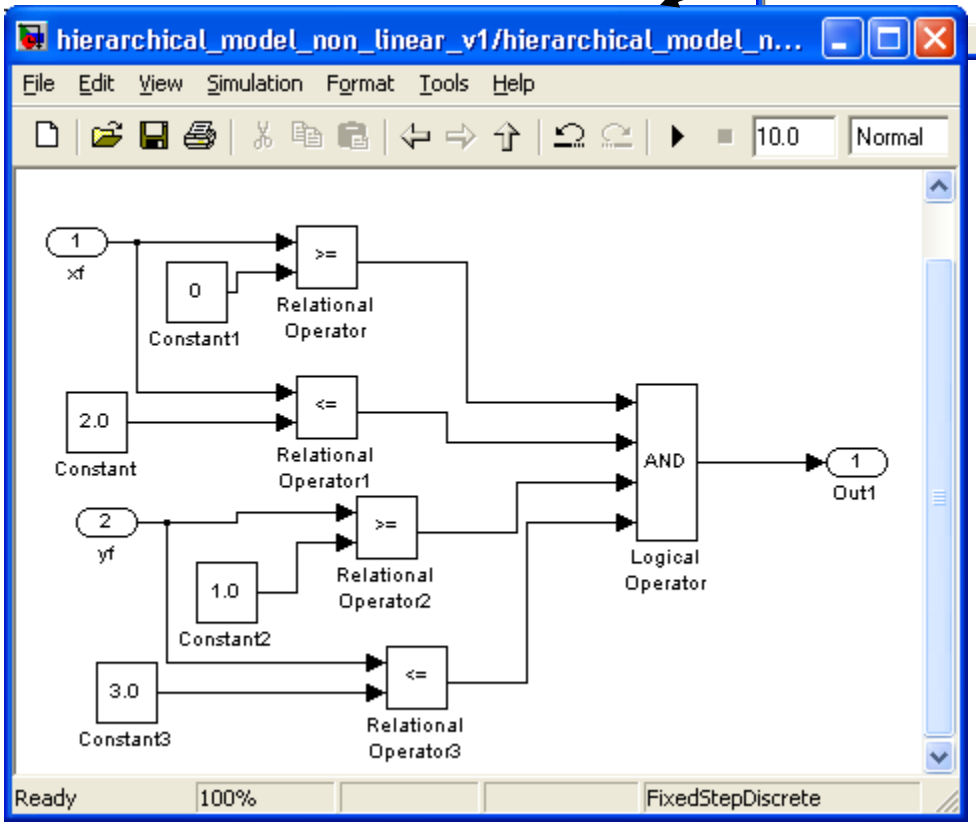
Key: Categories

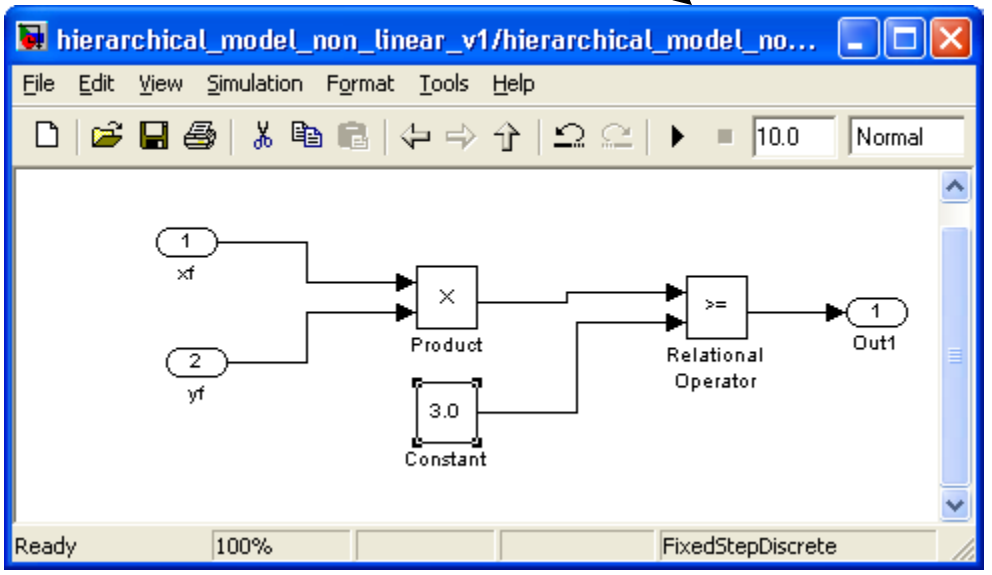
- H: High - relatively complete
- S: Some
- L: Low
- U: Unknown - possible
- A: Absorbed - unnecessary
- I: Provided through tight tool integration

Example: Hierarchical Model with Non-linear Floating Point Operations and Constraints

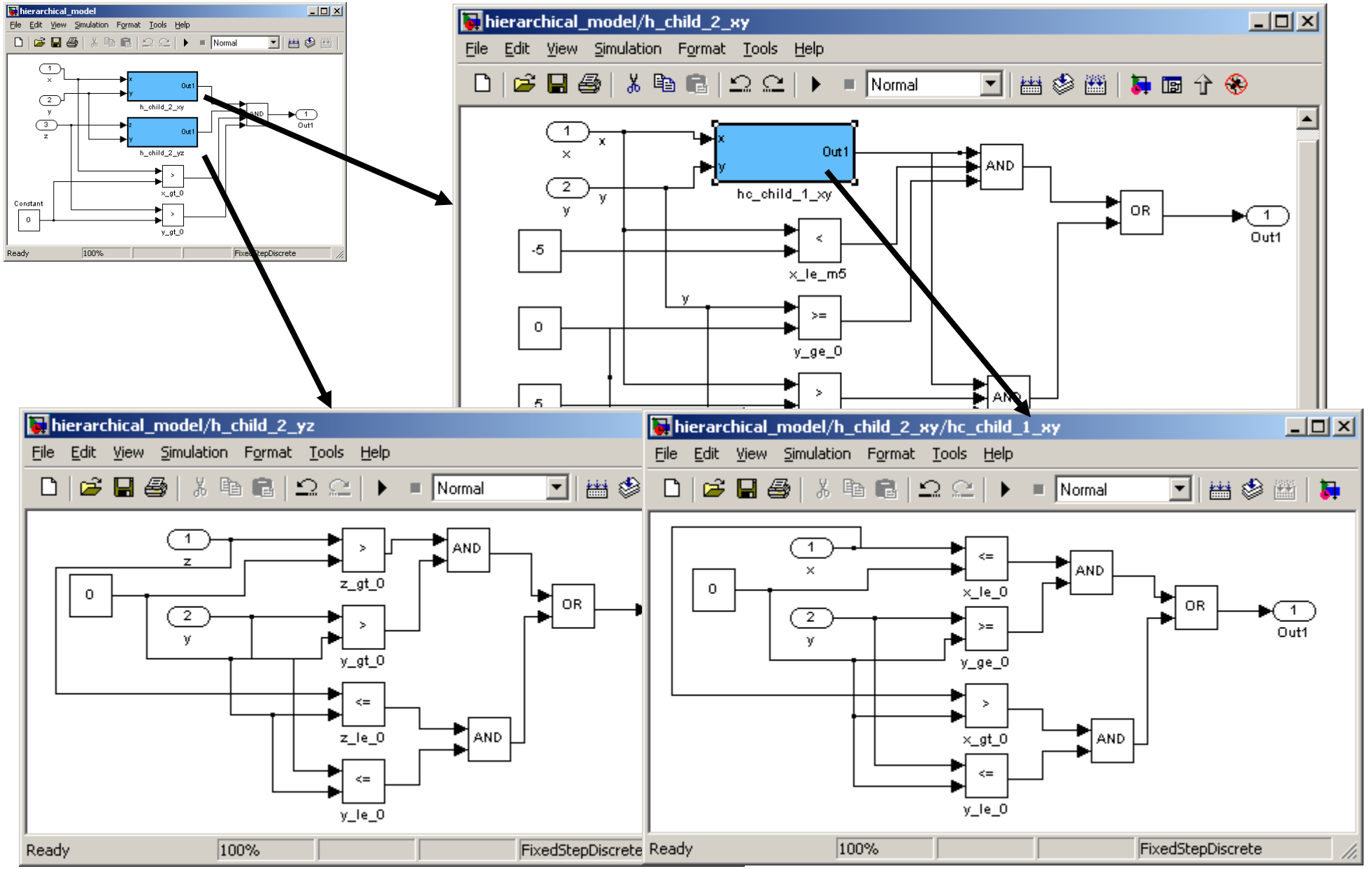








Extends Original Hierarchical Model with Inconsistent Linear Constraints

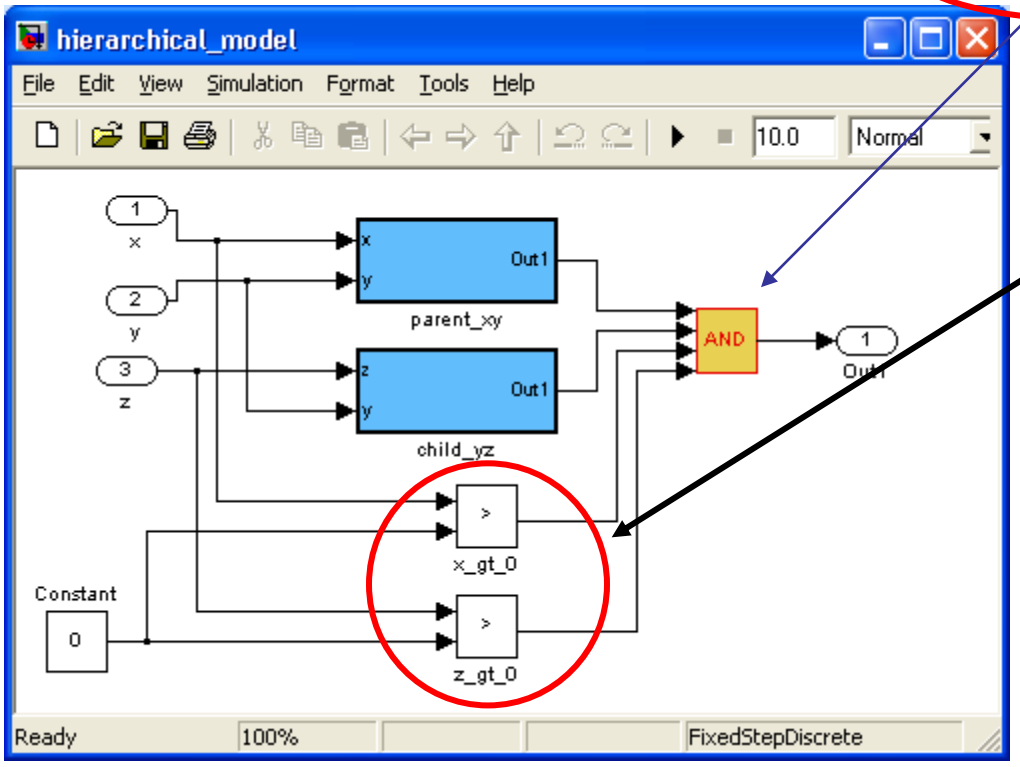


Potential Error Highlighted on Simulink Diagram

- **Constraints introduced at this level of model not satisfiable down through the other hierarchical paths of the lower-level subsystems**

Uncovered DCP Paths

DCP Number	DCP Path	Failure Detection
6	hierarchical_model_root, hierarchical_model_root_FR__1, cv_hierarchical_model_root_RP__1, hierarchical_model_root_RP__1<<2>>, hierarchical_model_root_RP__0, RP1_2, RP1_2_disjunctions<<5>>, COV_Logical_Operator_true (goto model)	Vector Generator



Failure Analysis

All inputs to AND gate must be TRUE

- Requires x > 0, z > 0
- Requires h_child_2_xy and h_child_2_yz be TRUE, which requires y <= 0

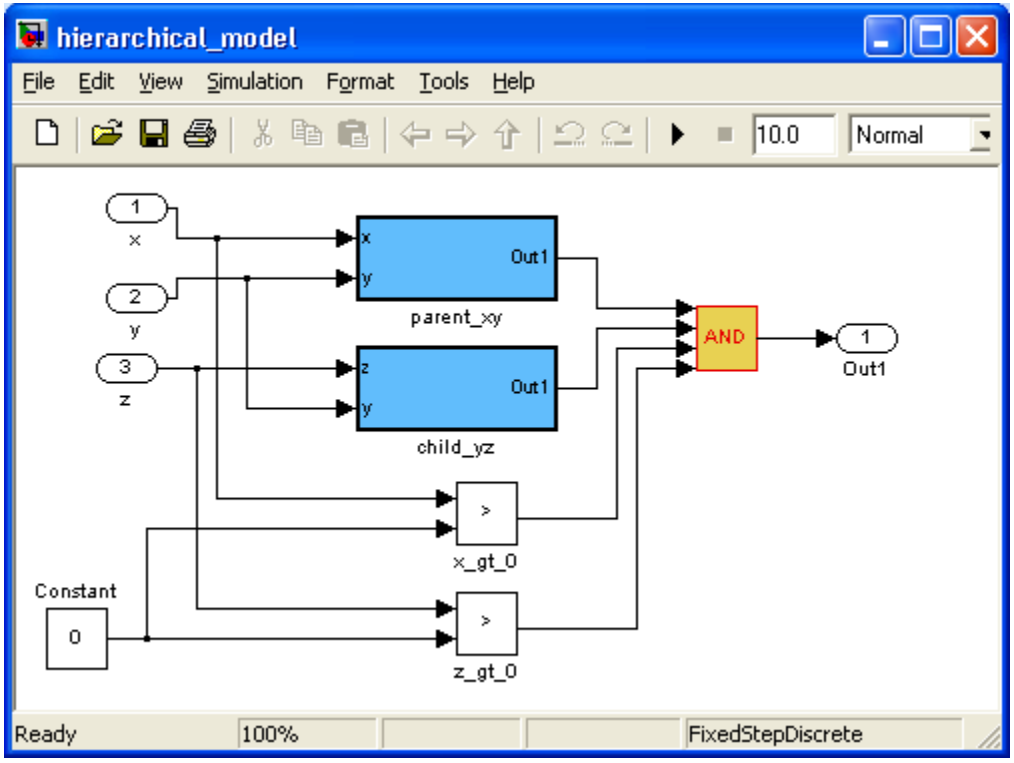
- Resulting in contradiction between top level system logic and logic across 2 subsystems

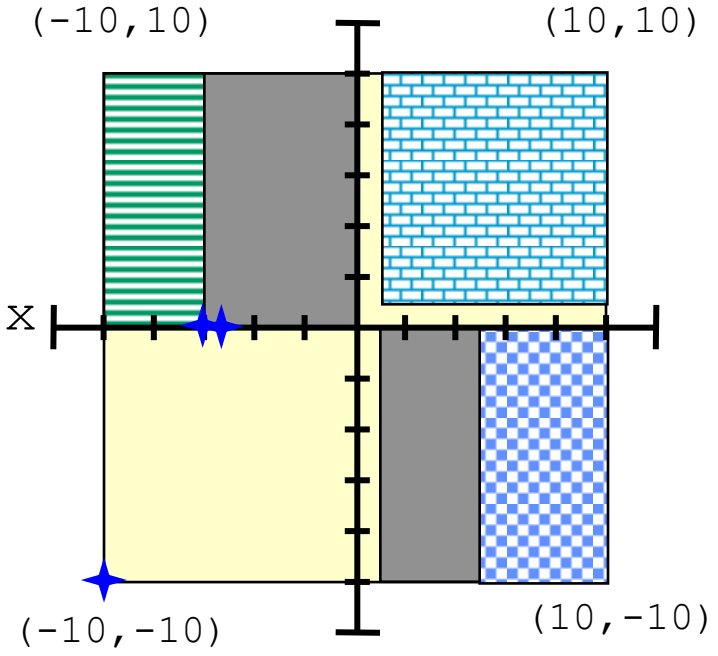
Test Generation Is A Byproduct Of Model Analysis

- **Vectors do not cover all paths when there are inconsistent constraints**

For complete AND coverage there should be at least one output that is "1" (TRUE)

#	__output	x	y	z
1, 5, 7	0	(-10)	(0)	(1)
2, 6, 8	0	(-6)	(0)	(10)
3	0	(-10)	(0)	(-10)
4	0	(-6)	(0)	(0)
9	0	(-5)	(0)	(1)
10	0	(0)	(0)	(10)





Non-linear Non-Satisfiability

Vector Gen Error # 1			
DCP # / Fix Point Location / Fix Order	1	LOW_BOUND	SPEC_SEQUENTIAL
Reason For Error / VG Stage / Time Period	Arithmetic Relation Failure	GROUND_LEVEL_FCP	T > 0
SS File Constraint Name	child_fxy`child_fxy_1__LS		
SS File Constraint Location	child_fxy.SS	Line # 38	Column # 24
SS File Constraint Input Domain	Occurance at UA = 3488 fo:FloatType [3.0e+000 .. 1.0e+001] fx:FloatType [0.0e+000 .. 2.0e+000] fy:FloatType [1.0e+000 .. 1.45e+000]		
Failed Pre-Condition Relation	cv_equal_to		
Exact SS File Location	child_fxy.SS	Line # 19	Column # 22
Input Domain At Error	Occurance at UA = 3488 fo:FloatType [3.0e+000 .. 1.0e+001] INTERM_00954_000:FLOAT32 [0.0e+000 .. 2.9e+000] @ scope = 0x50004		

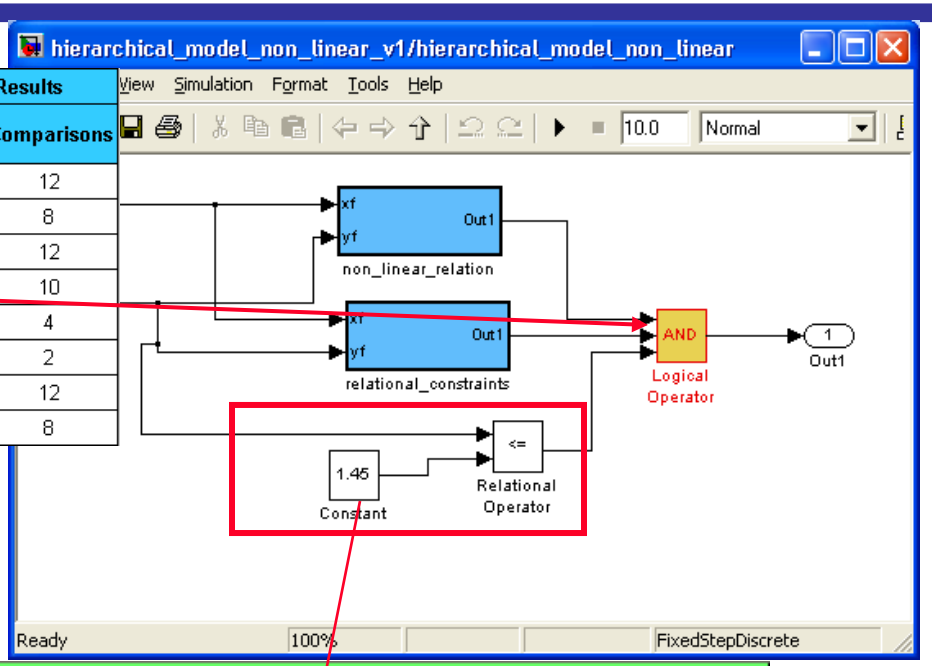
Test #	Ver				
1					
2					
3					
4					
5					
6	6	TRUE = 1	1.0e+001	1.27778e+000	7.82607e+000
7	7	TRUE = 1	3.00001e+000	1.66667e+000	1.8e+000
8	8	TRUE = 1	1.0e+001	1.66667e+000	5.99999e+000
9	9	TRUE = 1	3.00001e+000	2.05556e+000	1.45946e+000
10	10	TRUE = 1	9.99999e+000	2.05556e+000	4.86485e+000
11	11	TRUE = 1	3.00001e+000	2.44444e+000	1.22728e+000
12	12	TRUE = 1	1.0e+001	2.44444e+000	4.09092e+000
13	13	TRUE = 1	2.99999e+000	2.83333e+000	1.05882e+000
14	14	TRUE = 1	1.0e+001	2.83333e+000	3.52942e+000
15	15	TRUE = 1	3.0e+000	3.22222e+000	9.31035e-001
16	16	TRUE = 1	1.0e+001	3.22222e+000	3.10345e+000
17	17	TRUE = 1	3.0e+000	3.61111e+000	8.30769e-001
18	18	TRUE = 1	9.99999e+000	3.61111e+000	2.76923e+000
19	19	TRUE = 1	3.0e+000	4.0e+000	7.5e-001
20	20	TRUE = 1	1.0e+001	4.0e+000	2.5e+000

Behavior: parent_fxy_non_satisfiability

#	Assignment	Condition
1	TRUE	child_fxy AND child_fxy_2 AND (fy <= 1.45 OR fy <= 1.5)

Non-linear Non-Satisfiability

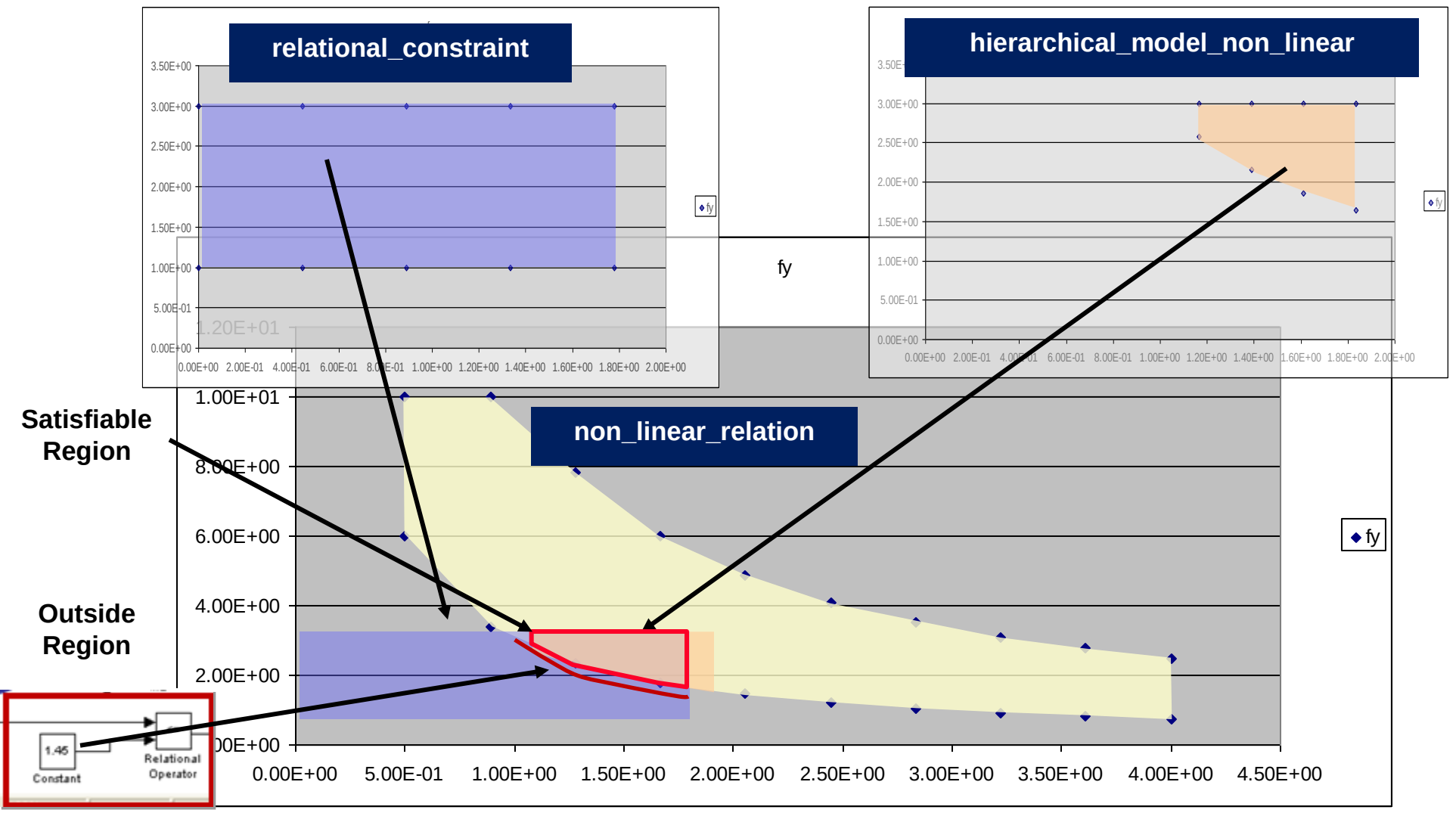
Subsystem	Compilation		Test Vectors		Coverage		Test Results	
	DCPs	Warn/Err	Vectors	Warn/Err	Untested DCPs	Warn/Err	Failures	Comparisons
child_xy	7	0/0	8	0/0	0	0/0	0	12
child_yz	7	0/0	8	0/0	0	0/0	0	8
hierarchical_model_linear	6	0/0	5	0/2	1 of 6	0/3	0	12
hierarchical_model_non_linear	5	0/0	5	0/2	1 of 5	0/3	0	10
hierarchical_model_non_linear_v1_root	1	0/0	2	0/0	0	0/0	0	4
non_linear_relation	1	0/0	2	0/0	0	0/0	0	2
parent_xy	9	0/0	10	0/0	0	0/0	0	12
relational_constraints	6	0/0	8	0/0	0	0/0	0	8



Vector Gen Error # 1			
DCP # / Fix Point Location / Fix Order	5	LOW_BOUND	SPEC_SEQUENTIAL
Reason For Error / VG Stage / Time Period	Arithmetic Operator Failure	GROUND_LEVEL_FCP	T > 0
SS File Constraint Name	non_linear_relation`RP1		
SS File Constraint Location	non_linear_relation.SS	Line # 37	Column # 24
SS File Constraint Input Domain	Occurance at UA = 10429 INTERM_Out1_oPort:booleanUint8 [1 .. 1] @ scope = 0x70002 xf_iPort:FloatType [1.1e-004 .. 2.0e+000] yf_iPort:FloatType [1.0e+000 .. 1.45e+000]		
Failed Pre-Condition Operation	cv_multiplication_of		
Exact SS File Location	non_linear_relation.SS	Line # 17	Column # 43
Input Domain At Error	Occurance at UA = 10429 INTERM_02018_013:FLOAT32 [3.0e+000 .. 1.0e+002] @ scope = 0x70004 xf_iPort:FloatType [1.1e-004 .. 2.0e+000] yf_iPort:FloatType [1.0e+000 .. 1.45e+000]		

Non-linear Satisfiability Example

- **Seeded defect defines a subspace that is not within the subdomain of the other modeled subsystems**



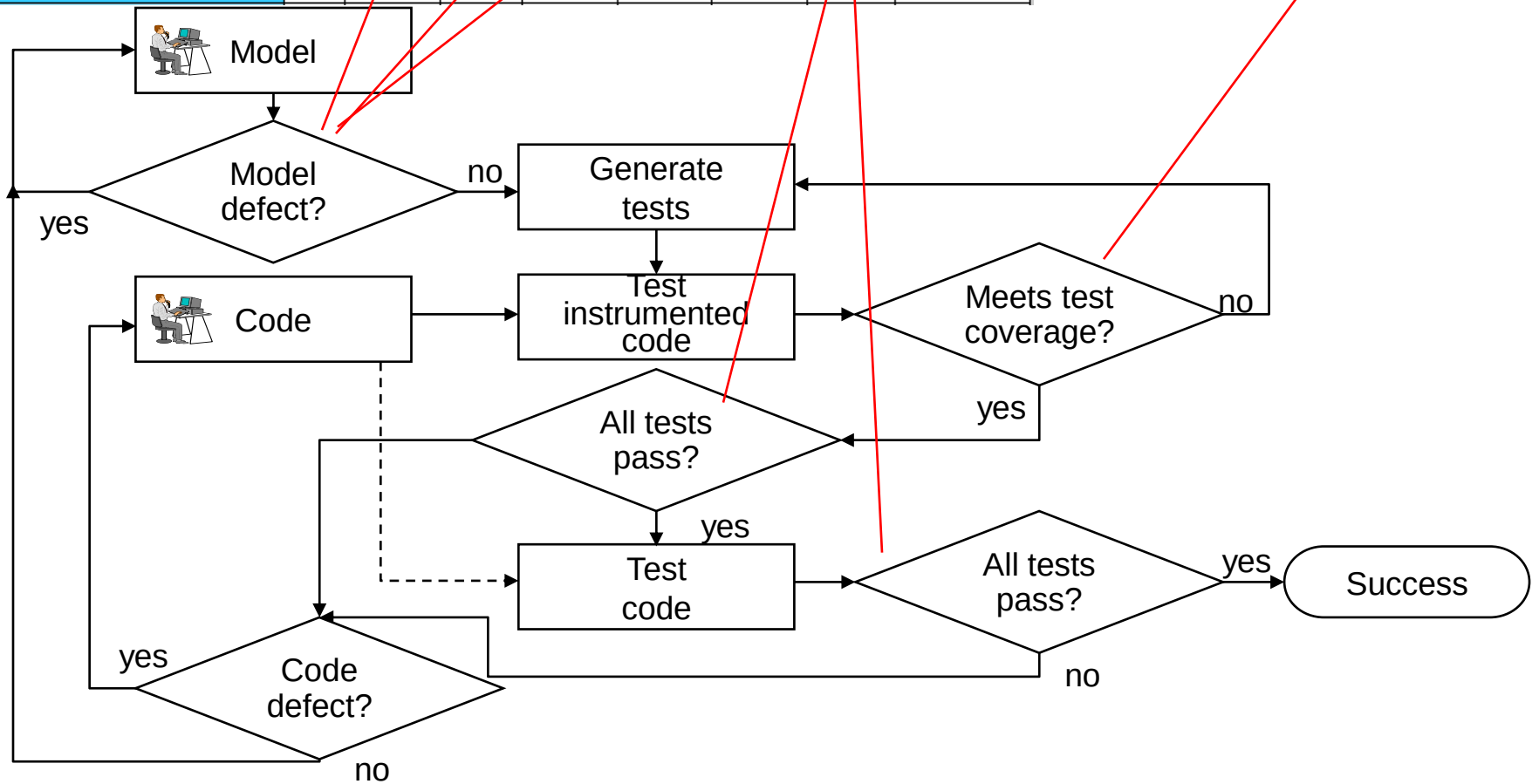
Measurement Data Derived Directly from Models and Associated Automation

Subsystem	Compilation		Test Vectors		Coverage		Test Results	
	DCPs	Warn/Err	Vectors	Warn/Err	Untested DCPs	Warn/Err	Failures	Comparisons
child_xy	7	0/0	8	0/0	0	0/0	0	8
child_yz	7	0/0	8	0/0	0	0/0	0	8
hierarchical_model_linear	6	0/0	5	0/2	1 of 6	0/3	0	5
hierarchical_model_non_linear	5	0/0	5	0/2	1 of 5	0/3	0	5
hierarchical_model_non_linear_v1_root	1	0/0	2	0/0	0	0/0	0	4
non_linear_relation	1	0/0	2	0/0	0	0/0	0	2
parent_xy	9	0/0	10	0/0	0	0/0	0	10
relational_constraints	6	0/0	8	0/0	0	0/0	0	8

VectorCAST

Metrics

Unit	Subprogram	Complexity	MCDC Coverage	MCDC Pairs
hierarchical_model	hierarchical_model_child_yz	1	100% (1 / 1)	
	hierarchical_model_step	1	100% (1 / 1)	
	hierarchical_model_initialize	1	100% (1 / 1)	
	hierarchical_model_terminate	1	100% (1 / 1)	
TOTALS	4	4	100% (4 / 4)	
parent_xy	hierarchical_model_child_xy	1	100% (1 / 1)	
	hierarchical_model_parent_xy	1	100% (1 / 1)	
TOTALS	2	2	100% (2 / 2)	
GRAND TOTALS	6	6	100% (6 / 6)	



Worked with SSCI Member on a Comparison of Design Verifier and T-VEC

	MS Project	DOORS	TTM/SCR	Simulink	Stateflow	Real Time Workshop	T-VEC Tester for Simulink	T-VEC Vector Generation System	Vectorcast	Design Verifier with Prover	LDRA	Rational Test RT	Reactis
Project planning	H												
Requirement management		H	S/I										
Requirement modeling			H										
Requirement simulation			I					S					
Design modeling				H									
Design simulation				H									S
Concurrent modeling													
Property specification			S				H	H					U
Model transformation			H				H	I					U
Code generation				I	I	H							
Disjointness checking			I					H					
Race condition checking			I					H					
Satisfiability non-linear								H					U
Satisfiability linear								H		L			U
Satisfiability logical								H		S			U
Arithmetic exceptions								H					U
Prove properties			I	I	I			H		S			U
Concurrency analysis				I	I	S							
Test sequence generation							I	H					S
Test vector generation								H					S
Test driver generation								H	I				
Model coverage								H		I			S
Test coverage analysis									H		H	H	
Test execution									H		H	H	
Test results analysis								H	H		H	H	
Model-to-test traceability				I				H					
Model standards													
Code standards									H		H	H	
Model management													
Confirmation management													
Test management								A	H		U	U	
Embedded Target Testing									H		U	U	

Key: Categories

- H: High - relatively complete
- S: Some
- L: Low
- U: Unknown - possible
- A: Absorbed - unnecessary
- I: Provided through tight tool integration

Design Verifier Did Not Produce Tests for Some Objectives

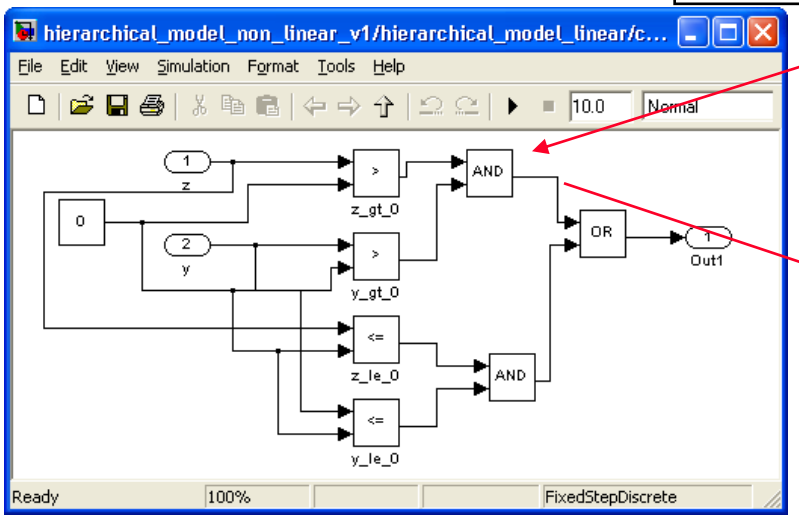
Design Verifier Report

Number of Test Objectives: ……...124
Objectives Satisfied: …….... 73
Objectives Proven Unsatisfiable: …11
Objectives Producing Errors:……...40

hierarchical_model_linear/child_yz/Logical Operator

View

#:	Type	Description	Status	Test Case
1	Condition	Logic: input port 1 T	Satisfied	6
2	Condition	Logic: input port 1 F	Satisfied	1
3	Condition	Logic: input port 2 T	Satisfied	8
4	Condition	Logic: input port 2 F	Satisfied	6
5	Mcdc	Logic: MCDC expression for output with input port 1 T	Satisfied	8
6	Mcdc	Logic: MCDC expression for output with input port 1 F	Produced error	n/a
7	Mcdc	Logic: MCDC expression for output with input port 2 T	Satisfied	8
8	Mcdc	Logic: MCDC expression for output with input port 2 F	Satisfied	6



T-VEC VGS Vectors

Test #	Vector #'s	_output	z_iPort	y_iPort
1	1, 3, 5, 13	1	-32768	-32768
2	2, 8, 10, 12	1	32767	32767
3	4	0	0	32767
4	6	0	32767	0
5	7	1	1	1
6	9	0	-1	-32768
7	11	0	-32768	1
8	14	1	0	0

Comparing Test Vectors

Design Verifier Tests						
Test	output	x	y	z	xf	yf
1	none	-32768	-32768	-32768	0	0
2	none	-32768	-32768	-32768	-1	1
3	none	-32768	-32768	-32768	1	1
4	none	8192	-32768	-32768	3	1
5	none	1	0	-32768	3	1
6	none	-32768	-32768	32767	0	0
7	none	6	-32768	32767	0	0
8	none	-32768	32767	32767	0	0
9	none	32766	32767	32767	0	0

Design Verifier produced only 9 tests

T-VEC VGS – 66 tests

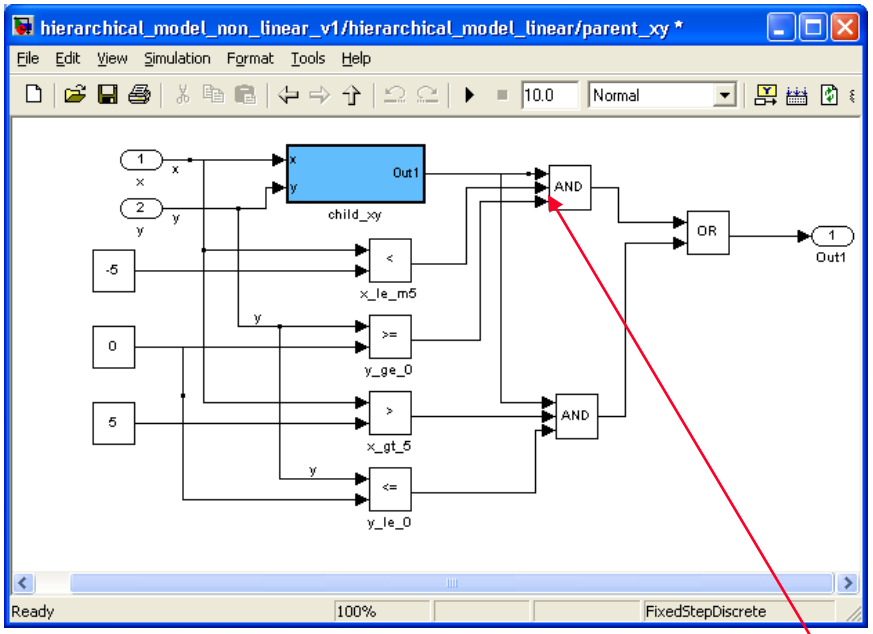
hierarchical_model_non_linear_v1 Project Status

Project Filename: C:\data\blackbur\lm\lm_astro\lm_space_2009\models\hierarchical_model\hierarchical_model_non_linear_v1.prj

Total Test Case Comparisons	68
Total Test Comparison Failures	0
Total Test Vectors	66
Total Test Paths (DCPs)	50
Date Generated	04-08-09 12:57:53

Subsystem	Compilation		Test Vectors		Coverage		Test Results	
	DCPs	Warn/Err	Vectors	Warn/Err	Untested DCPs	Warn/Err	Failures	Comparisons
child_xy	7	0/0	8	0/0	0	0/0	0	8
child_yz	7	0/0	8	0/0	0	0/0	0	8
hierarchical_model_linear	6	0/0	5	0/2	1 of 6	0/3	0	5
hierarchical_model_non_linear	5	0/0	5	0/2	1 of 5	0/3	0	5
hierarchical_model_non_linear_v1_root	1	0/0	2	0/0	0	0/0	0	4
non_linear_relation	1	0/0	20	0/0	0	0/0	0	20
parent_xy	9	0/0	10	0/0	0	0/0	0	10
relational_constraints	6	0/0	8	0/0	0	0/0	0	8

DV Did Not Prove Test Objective for Linear Relationships



Test #	Vector #'s	_output	x	y
1	1, 3, 7, 11, 13	0	(-32768)	(-32768)
2	2, 4, 6, 12, 16	0	(32767)	(32767)
3	5	0	-5	(-32768)
4	8	1	(32767)	-1
5	9	1	-32768	0
6	10	1	-6	32767
7	14	0	5	(32767)
8	15	1	(-32768)	1
9	17	1	6	-32768
10	18	1	32767	0

T-VEC VGS Vectors

Objectives Proven Unsatisfiable

Simulink Design Verifier proved that there does not exist any test case exercising these test objectives. This often indicates the presence of dead-code in the model. Other p model due to parameter configuration or test constraints such as given using Test Condition blocks. In rare cases, the approximations performed by Simulink Design Verifie:

#:	Type	Model Item	Description	Test Case
54	Condition	hierarchical_model_linear/parent_xy/Logical Operator	Logic: input port 3 F	n/a
56	Mcdc	hierarchical_model_linear/parent_xy/Logical Operator	Logic: MCDC expression for output with input port 1 F	n/a
60	Mcdc	hierarchical_model_linear/parent_xy/Logical Operator	Logic: MCDC expression for output with input port 3 F	n/a
66	Condition	hierarchical_model_linear/parent_xy/Logical Operator4	Logic: input port 3 F	n/a
68	Mcdc	hierarchical_model_linear/parent_xy/Logical Operator4	Logic: MCDC expression for output with input port 1 F	n/a
72	Mcdc	hierarchical_model_linear/parent_xy/Logical Operator4	Logic: MCDC expression for output with input port 3 F	n/a
87	Condition	hierarchical_model_linear/Logical Operator	Logic: input port 4 T	n/a
89	Mcdc	hierarchical_model_linear/Logical Operator	Logic: MCDC expression for output with input port 1 T	n/a
91	Mcdc	hierarchical_model_linear/Logical Operator	Logic: MCDC expression for output with input port 2 T	n/a
93	Mcdc	hierarchical_model_linear/Logical Operator	Logic: MCDC expression for output with input port 3 T	n/a
95	Mcdc	hierarchical_model_linear/Logical Operator	Logic: MCDC expression for output with input port 4 T	n/a