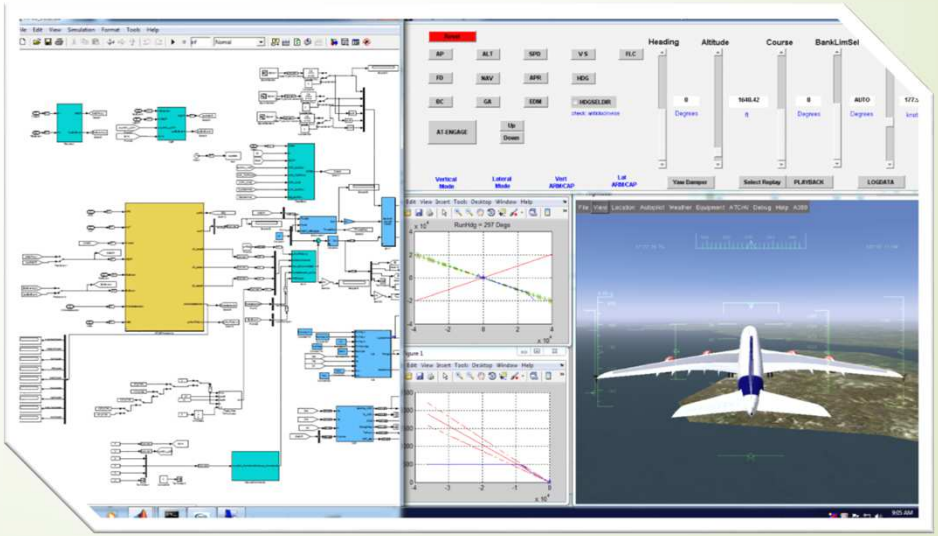
Exploring Simulink Design Verifier - 2

Auto-pilot Mode Transition

Natasha Jeppu, NITK Surathkal

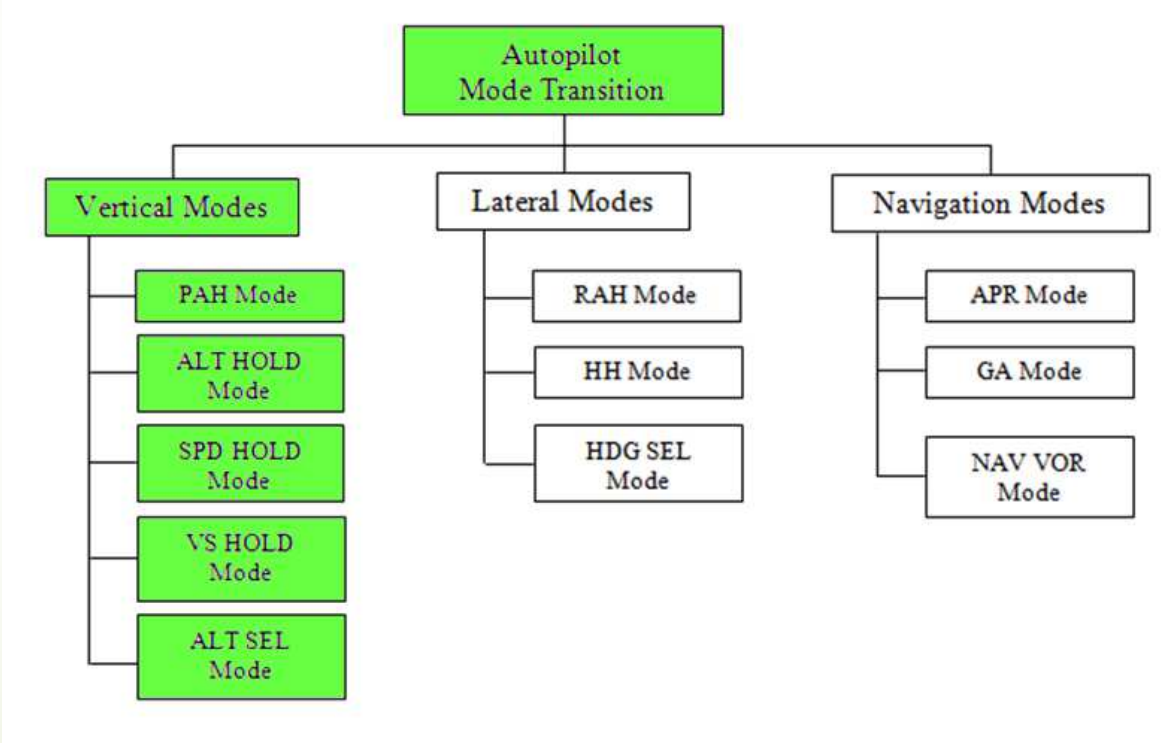
Autopilot

- Autopilot system is a mechanical, electrical or hydraulic system used to guide an airplane with minimal or no assistance from the pilot. It also reduces the fuel consumption and increases flight safety.



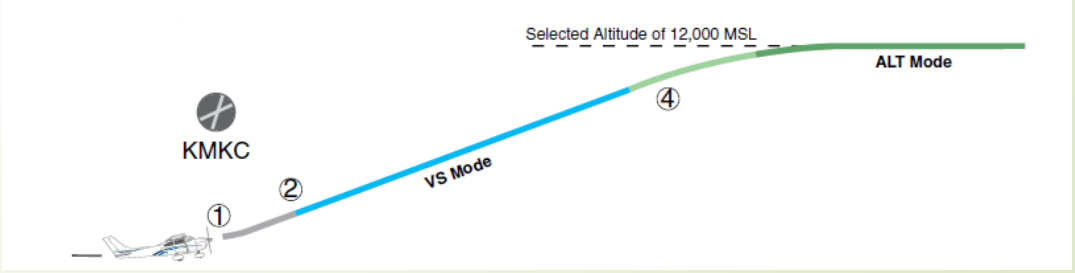
Autopilot Modes

- We consider only the vertical modes for the problem



Vertical Modes

- PAH mode – This is the basic autopilot mode in vertical axis. This mode holds the current pitch angle.
- Altitude Hold mode (ALT) – This mode holds the aircraft at the current altitude reference.
- Speed Hold mode (SPD) – This mode maintains the present airspeed.
- Vertical Speed mode (VS) – This mode is used to automatically maintain the aircraft at a selected vertical speed (climb rate) reference.
- Altitude Select mode (ALT SEL) – This mode captures the Selected Altitude. The 3 phases are, Arming, Capture and Hold



Transition Table

States	Sl. No.	Modes	Buttons				Software Triggers			
			01	02	03	04	05	06	07	08
			AP	SPD	VS	ALT	**ALTS**	**ALTCAP**	**ALTCPDN**	**APFAIL**
Vertical	01	DIS(Vertical)	02	00	00	00	00	00	00	00
	02	PAH	01	03	04	05	00	06	00	01
	03	SPD HOLD	01	02	04	05	00	06	00	01
	04	VS	01	03	02	05	00	06	00	01
	05	ALT HOLD	01	03	04	02	00	00	00	01
	06	ALTS CAP	01	00	00	05	00	00	05	01
AP	01	AP ON	02	00	00	00	00	00	00	02
	02	AP OFF	01	00	00	00	00	00	00	00
ALT SEL	01	ALTS OFF	00	00	00	00	02	00	00	00
	02	ALTS ARM	01	00	00	01	01	03	00	01
	03	ALTSEL CAP	01	00	00	01	00	00	01	01

Condition Table

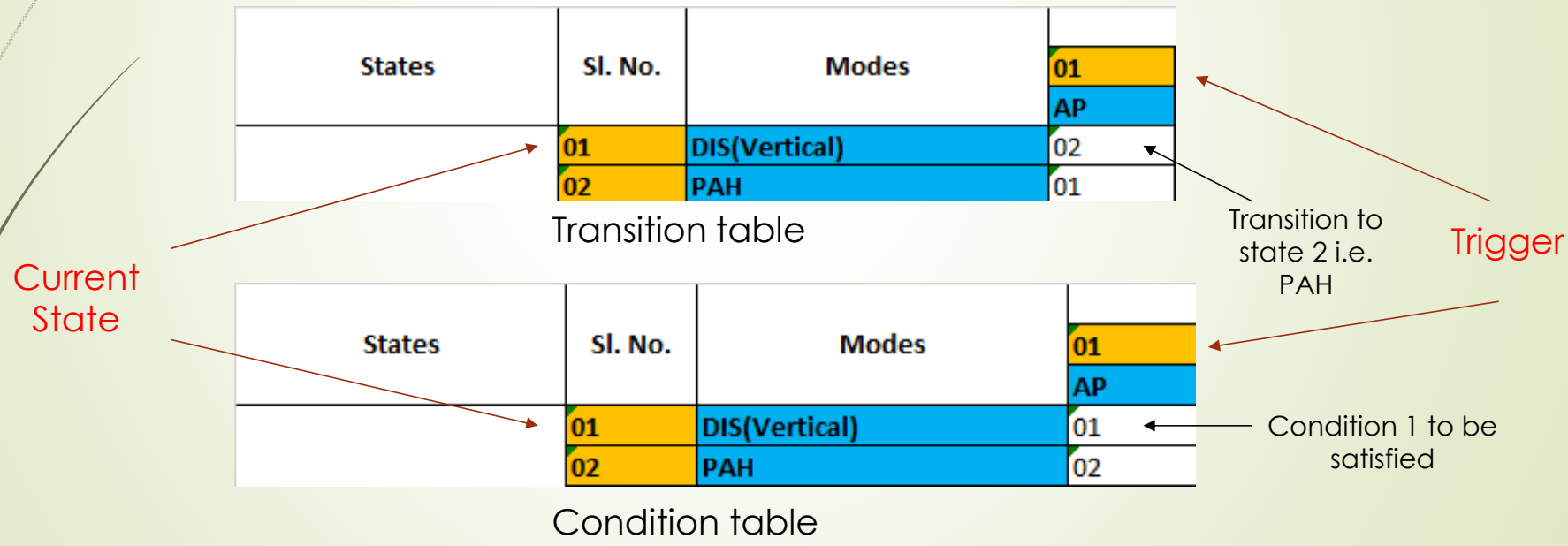
States	Sl. No.	Modes	Buttons				Software Triggers			
			01	02	03	04	05	06	07	08
			AP	SPD	VS	ALT	**ALTS**	**ALTCAP**	**ALTCPDN**	**APFAIL**
Vertical	01	DIS(Vertical)	01	00	00	00	00	00	00	00
	02	PAH	02	03	04	05	00	00	00	02
	03	SPD HOLD	02	00	04	05	00	00	00	02
	04	VS	02	03	00	05	00	00	00	02
	05	ALT HOLD	02	03	04	00	00	00	00	02
	06	ALTS CAP	02	00	00	05	00	00	00	02
AP	01	AP ON	00	00	00	00	00	00	00	00
	02	AP OFF	01	00	00	00	00	00	00	00
ALT SEL	01	ALTS OFF	00	00	00	00	00	00	00	00
	02	ALTS ARM	02	00	00	05	00	00	00	02
	03	ALTSEL CAP	02	00	00	05	00	00	00	02

How to use these tables?

- There are three independent modes
  - Vertical mode
  - AP mode
  - ALTSEL mode
- Each row indicates the current state in each mode.
- The columns indicates the trigger.
- The corresponding cell defined by the state (row) and trigger (col) in the condition table gives the condition to be satisfied for a transition to take place.
- The corresponding cell in the transition table indicates the new state to which the autopilot twill transit if the condition is satisfied.

Example

- Consider DIS state (state 1) in Vertical mode and trigger 1 that is AP trigger.



Example

- First, look at the cell corresponding to vertical state 1 i.e. DIS and trigger AP in the condition table. The value in the cell indicates the condition to be satisfied for the transition to take place (in this case condition 1).

- If this condition is satisfied then the corresponding cell in the transition is looked at. The value in the cell indicates the state of transition within the given mode.
- In this case state 2 indicates PAH state in vertical mode.

Conditions

- C1: No AP inhibit conditions exist.
- C2: AP ON
- C3: CAS is greater than 120 and less than Vmo (knots)
- C4: |VS|>50 ft/min.
- C5: |VS| is less than 500 ft/min

Trigger not possible conditions

- if AP is OFF software triggers ALTS,ALTCAP,ALTCAPDN and APFAIL are not possible
- if ATLSEL mode is not in ARM state then ALTCAP trigger is not possible
- if VERTICAL state not in ALTCAP mode ALTCAPDN trigger is not possible
- if VERTICAL state in ALTHOLD mode then ALTS trigger is not possible

Assertions

- If Vert = ALTCAP then ALTSEL = ALTSEL CAP
- If Vert = ALT HOLD then ALTSEL = OFF
- If Vert = DIS then AP = OFF
- If Vert = DIS then ALTSEL = OFF

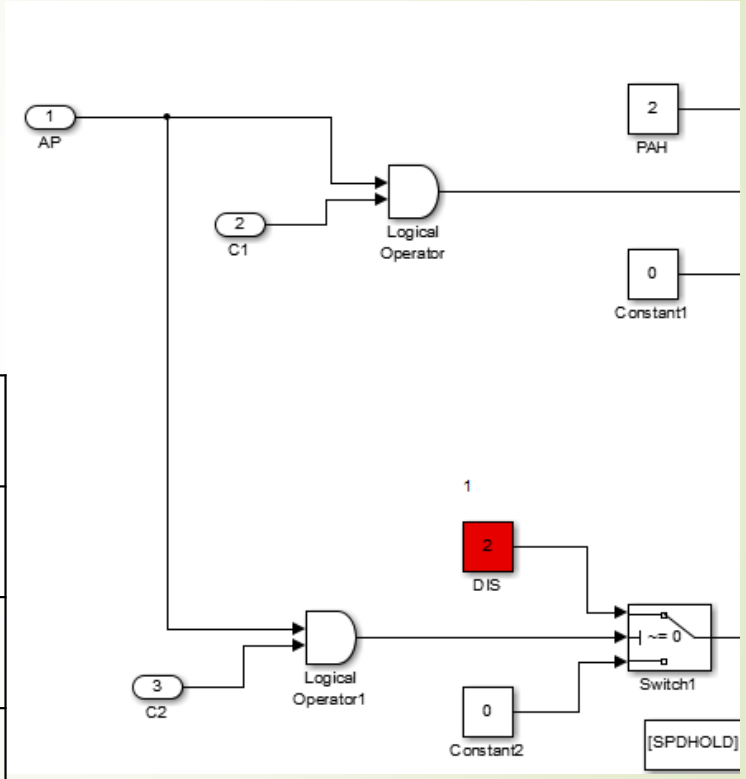
Mutants

- We added some deliberate mutants to our model and used random testing and design verifier to check for errors.
- We did five trials of testing for each mutant and noted the average time taken by each trial to detect the error and the objectives that are falsified.

Mutant 1

- DIS replaced by code 2 instead of 1.

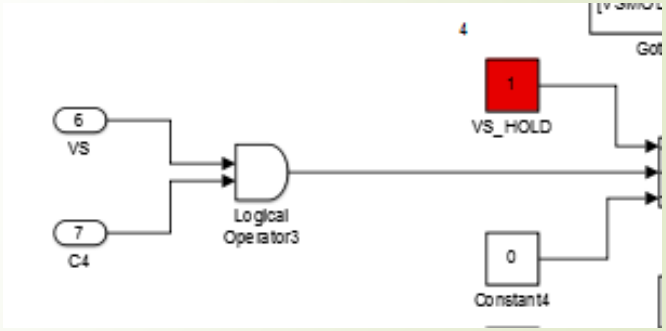
	Design Verifier	Random Testing
Objective falsified	5	5
Average time taken	16.8	1.312
Standard deviation	0.447214	0.798636



Mutant 2

- VS_HOLD replaced by code 1 instead of 4. Indicated in red inside.

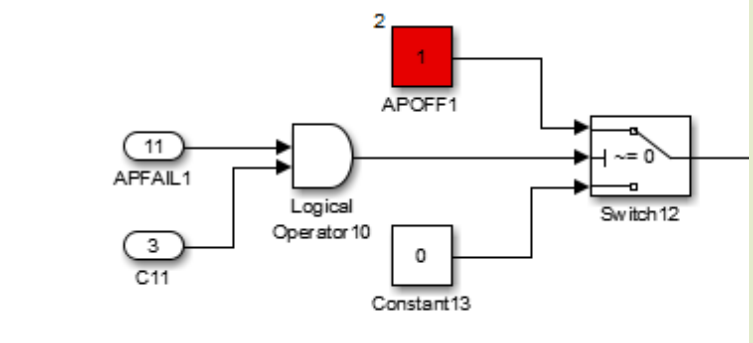
	Design Verifier	Random Testing
Objective falsified	5	5
Average time taken	21.4	64.61
Standard deviation	0.547723	15.17442



Mutant 3

- APOFF made APON in AP mode.

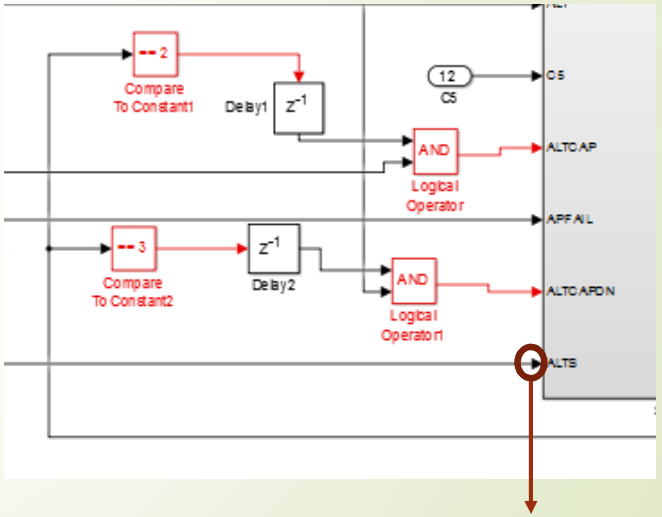
	Design Verifier	Random Testing
Objective falsified	5	5
Average time taken	21.4	4.558
Standard deviation	0.547723	2.743177



Mutant 4

- ALTS trigger connected directly without checking for ALTHOLD.

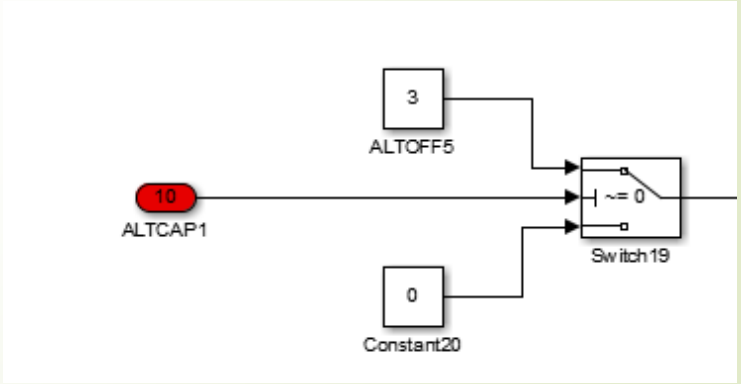
	Design Verifier	Random Testing
Objective falsified	4	5
Average time taken	23.6	7.244
Standard deviation	2.302173	6.524058



Mutant 5

- Condition c2 for ALTCAP trigger removed.

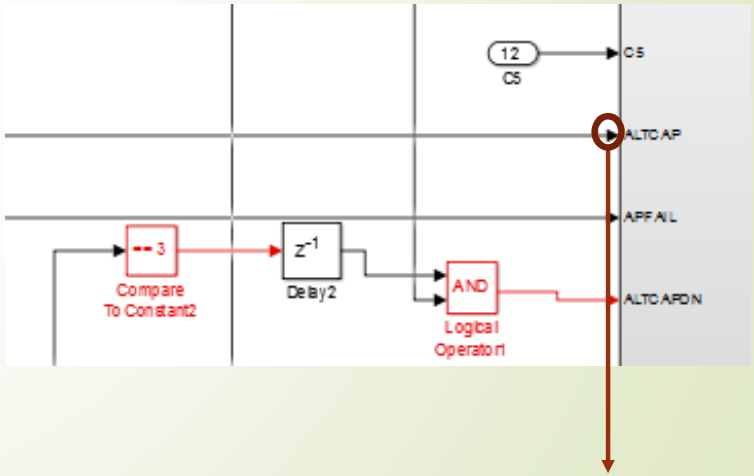
	Design Verifier	Random Testing
Objective falsified	2	2
Average time taken	12.2	5.172
Standard deviation	0.447214	5.46013



Mutant 6

- ATLCAP connected directly without checking for ATLSARM state.

	Design Verifier	Random Testing
Objective falsified	1	1
Average time taken	18.4	25.74
Standard deviation	2.408319	12.10929

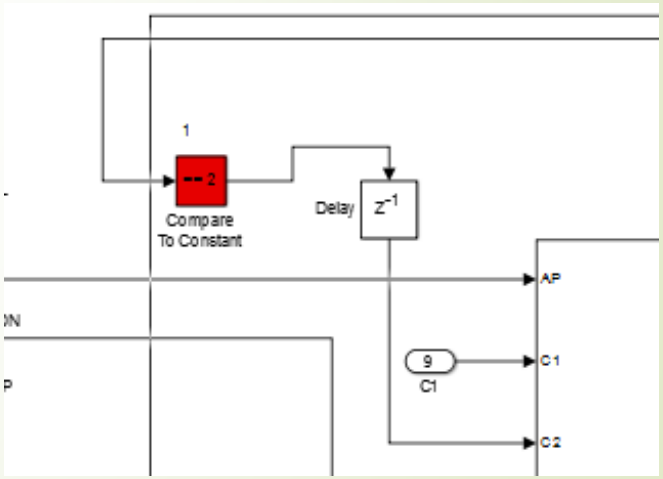


Condition missing

Mutant 7

- Condition C2 changed to APOFF true instead of APON true.

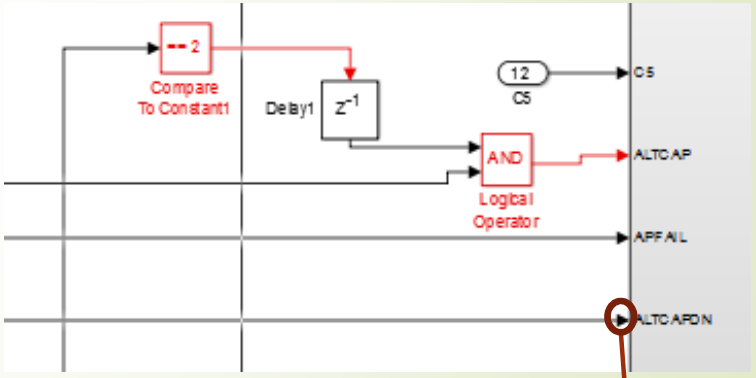
	Design Verifier	Random Testing
Objective falsified	5	5
Average time taken	21.6	1.346
Standard deviation	5.176872	1.077186



Mutant 8

- ALTCPDN connected directly without checking for ALTCAP state.

- This mutant is not detected by random testing or Design verifier because this is already taken care of inside the block.

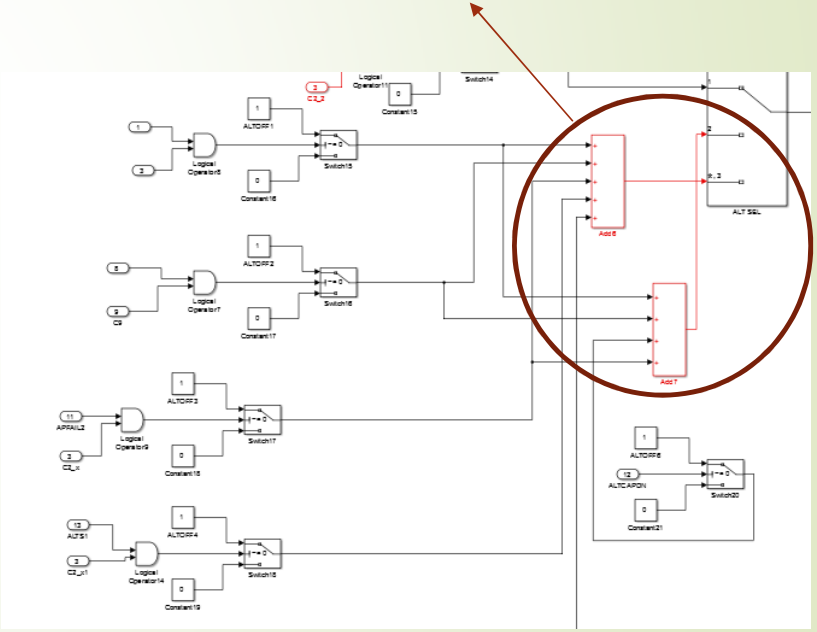


Condition missing

Mutant 9

- Switching transition conditions for ALTSARM and ALTSCAP in ALTSEL mode .

	Design Verifier	Random Testing
Objective falsified	1	1
Average time taken	19.2	91.05
Standard deviation	0.447214	94.75757



- Contact: natasha.jeppu@gmail.com