Exploring Design Verifier

NATASHA Y JEPPU

(STUDENT NITK, SURATHKAL)

Autodestruct

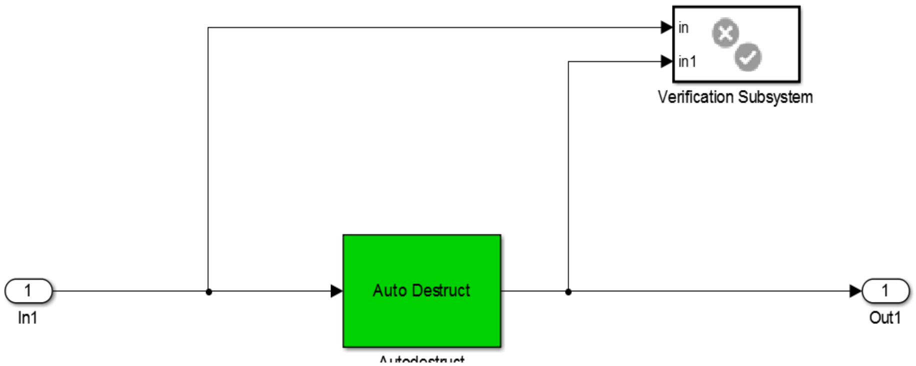
Requirements

A) If the Input <= 25 degrees then Autodestruct = TRUE

B) If the input >= - 25 degrees then Autodestruct = TRUE

ELSE

C) Autodestruct = FALSE



compare_error_prove.slx

Delay OnOff

Requirements

A) If the input is TRUE and holds TRUE for a duration of TON (20) Frames then output = TRUE

B) If the input is FALSE and holds FALSE for a duration of TOFF (40) Frames then the output = FALSE

ELSE

C) The output shall be equal to previous value (NO CHANGE)

delay_on_off_prove.slx
delay_on_off_test.slx

Antiwindup Integrator

Requirements

The output shall be computed as Input * DT (0.01 sec) + Previous Output

- $O_k = O_{k-1} + I_k*(0.01)$
- If $I_k = I_{k-1} = 0$ then $O_k = O_{k-1}$
- If $O_{k-1} >= 0.5$ AND $I_k < 0$ then $O_k < 0.5$
- If $O_{k-1} <= -0.5$ AND $I_k > 0$ then $O_k > -0.5$

Where k is the current frame. O is the output and I the input.

integ_verify_prove.slx

Hysteresis

Requirements

- If I_1 > 65 then O_1 = TRUE
- If I_1 <=65 then O_1 = FALSE

In the first frame

For all k>1

- If I_k < 60 then O_k = FALSE
- If I_k > 70 then O_k = TRUE
- If I_k<=70 AND I_k>=60 then O_k = O_{k-1}

Where k is the current frame, I is the input and O is the output

logical_hystersis_prove.slx

Priority

Requirements

- Priority circuit shall have 8 inputs and 8 outputs.
- Only one output can be TRUE at a time.
- If I_n = TRUE AND (all inputs of higher precedence than I_n) = FALSE then

  O_n = TRUE

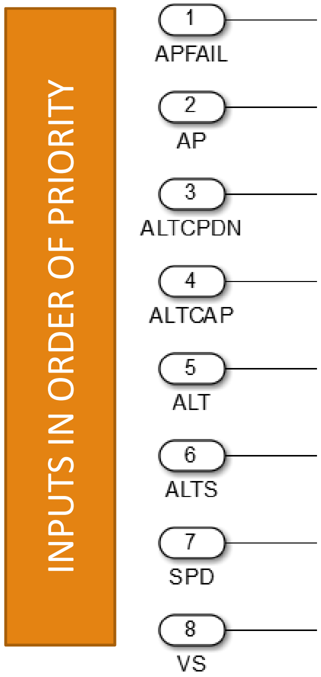
  i.e. I_1,I_2,I_3.....I_{n-1} is FALSE.

Eg: O_1=TRUE implies I_1 = TRUE

O_2=TRUE implies I_1 = FALSE AND I_2 = TRUE

- If sum of inputs >=1 then sum of outputs = 1 taking Booleans 0 and 1 as integers

priority_01_error.slx
priority_01_prove.slx
priority_prove.slx



Rate limiter

Requirements

- $O_1 = I_1$

For all k > 1

- If $\text{abs}\{(O_k-O_{k-1})/DT\} < 1$ then $O_k = I_k$
- $\text{abs}\{(O_k-O_{k-1})/DT\} <= 1$ for all k>1

Where k is the current frame, I is the input and O is the output. DT is the sampling time.

The output rate should be limited to 1

rate_limit_prove.slx

Window counter

Requirements

- If $(I_k + I_{k-1} + \ldots\ldots.+ I_{k-9}) > 3$ then O_k = TRUE

  else

  O_k = FALSE

window_counter_prove.slx
window_counter_test.slx

On ground circuit

Requirements

Weight on wheels

- If any two of (WOWN,WOWL,WOWR) = TRUE then ONGROUND = TRUE

Alternate on ground

- If CAS < 60 AND RADALT < 100 AND for 20 frames then ONGROUND = TRUE
- If CAS > 70 OR RADALT > 150 AND for 40 frames then ONGROUND = FALSE
- If first frame AND CAS <= 65 AND RADALT <= 125 then ONGROUND = TRUE

wow_correct_prove.slx
wow_fail_prove.slx

Transient free switch

Requirements

For input A and B bounded between -1 and 1 the output shall be bounded between -1 and 1.

This block has caused problems in flight controls. In case of the LCA program it caused a slat failure by giving a negative value where the output was to be bounded between 0 and 1. SDV proves this very easily and comes with a test case. The second model used in other flight programs does not have this problem

Refer:

http://www.mathworks.com/matlabcentral/fileexchange/39047-testing-of-safety-critical-control-systems

TFS.slx