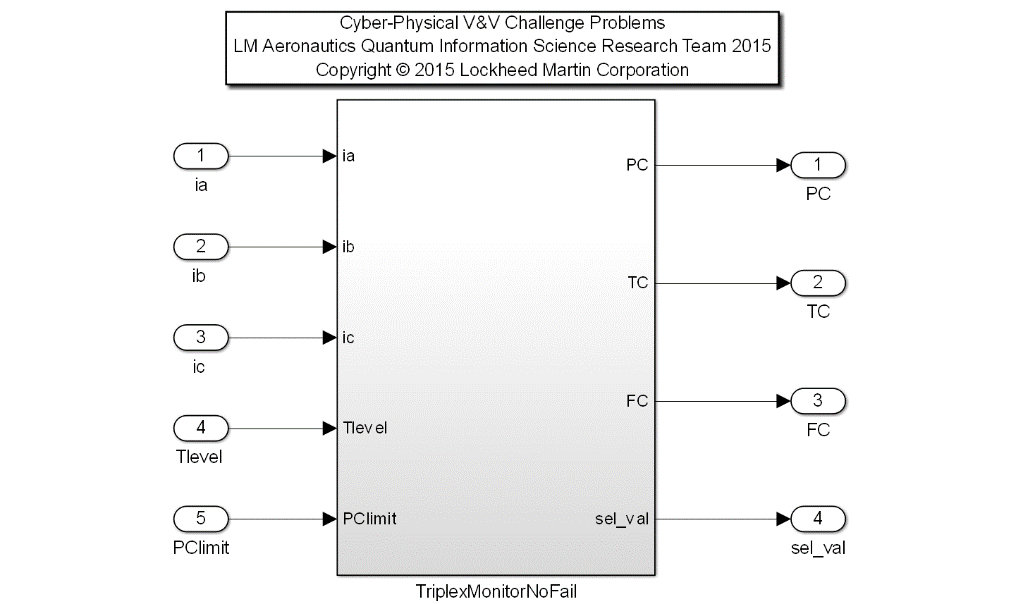
# 0) Triplex Signal Monitor

Model: ‘triplex\_12B.mdl’

Description: this challenge problem involves the verification of a redundancy management system using quantum simulation techniques. The purpose of this redundancy management system is to prevent errors from propagating past the input portion of an airborne application. The assumed platform configuration is a set of three computers which execute identical software applications, and which each take the same set of input values from sensors on the aircraft. For each set of triplex inputs, the redundancy management system must monitor for failures (or imminent failures), report the failure status of the set to the necessary functions, and choose an acceptable signal for computational use. All of the inputs used in redundancy management are triply redundant and have some type of tie-breaking capability.

The redundancy management system operates according to the failure state of the input set it is currently handling. An input set is defined as the triplex signals of a particular input. Each input set has its own failure state which is determined by redundancy management and is generally independent from the failure states of all other input sets. There are three failure states, the no-fail state, single-fail state and dual-fail state. The redundancy management system operates in all three conditions.

In the no-fail and the single-fail case, an error will manifest itself as a difference in the values of the signals of an input set. The difference is referred to as a miscompare until it is latched and reported to redundancy management as a failure. A miscompare that persists but has not yet been declared failed is known as a failure in progress.

In the RM system, an input set is comprised of inputs from three branches: A, B, and C. Three difference equations are formed from each pair combination of the three inputs. The difference equations form the basis for fault detection and isolation and input selection in the ensuing monitor and selector routines. All three inputs are cross-channel monitored and then selected based on results from the input monitor and from other functions within RM. By monitoring prior to selection, failures are detected in a timely manner and are prevented from influencing the selected value during a pending second failure. Failures latched by the monitors are reported to failure processing. A mid-value selection (MVS) algorithm is utilized as the basic selection method for the no-fail case and a good channel average (GCA) for the single fail case. The mid-value selection reduces the transient associated with the first input failure while the good channel average reduces the potential transient associated with a second input failure.

The mid-value is defined as the signal value bound by the remaining two signal values. For example, if ia < ib < ic, the mid-value is selected as the value of ib. In the case where two signal values are identical, e.g. ia < ib < ic, the mid-value equals the bound set by the second signal ic. Finally, in the case where all three signal values are identical, ia = ib = ic, the mid-value is also equivalent.

The good channel average is defined as the numerical median between the two remaining signals after a single fail. For example, if branch B is indicated as failed, the GCA is computed as ½\*(ia+ic).

A pending second failure causes the monitor to execute its tie-break algorithms to determine the remaining good signal. Monitoring is terminated after the second failure in an input set. Totalizer counters (TC) are primarily of use during Operational Flight Program (OFP) testing and are employed to maintain a running log of the total number of miscompares, which have occurred in an input set. Each device has a unique persistence counter (PC) and totalizer counter.

A certain amount of mistracking between inputs in a given input set must be permitted to account for both sensor mistrack and for tolerances on the input sampling hardware for the three vehicle management computer (VMC) branches. The object of an input trip level is to define the total allowable discrepancy between the compared signals in an input set. Whenever the difference between compared signals is greater than the designated trip level, the possibility of an input failure must be considered. The purpose of input failure persistence is to prevent false failure declarations of an input that may be temporarily mistracking for some unknown transitory problem. Input failure persistence (or persistence count, PC) is therefore defined as the total number of iterations that signals are permitted to miscompare outside of their designated trip level before a failure is declared. If the signals miscompare for a single frame longer than the allocated persistence, an input failure will be declared. The term "pending failure" is used to describe the period of time that a signal is out of tolerance but has not reached the persistence count limit. After the persistence has expired, the monitor takes action to operate without the offending input and the failure is referred to as a “latched failure”.

The appropriate case of the RM input monitor for each triplex input device is based on the device’s failure status as recorded in failure management’s Device Status Table (DST). If no failures have been marked in the Monitor State (MS) of the DST entry of a device, the no fail monitor is executed for that triplex input device. If only one branch has been marked as failed in the MS of the DST entry of a device, the single fail monitor is executed for that triplex input device. If more than one branch is marked as failed in the MS of the DST entry of a device, then no monitoring is performed for that triplex input. After a latched first failure of an analog input, the single fail monitor is utilized. After a first failure has been latched, only one difference equation is needed for failure detection. The monitor observes the difference equation containing the inputs of the remaining two inputs. If the absolute value of the difference equation is outside the trip level and the PC is greater than or equal to its limit, the monitor reports the second failure to failure management. Inputs with more than one failure are no longer monitored. The single fail monitor is responsible for fault detection and isolation of a second failure. After the tie-breaking tasks have been accomplished and the DST has been updated to indicate the second failure, the single fail monitor is no longer executed.

This challenge problem models the RM triplex signal input monitor in the setting of the no-fail state and for a portion of the single-fail state. The following natural language requirements shall be met for the given Simulink implementation.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Input Scope** | **Name** | **#** | **Type** | **Description** |
| Global | ia | 1 | Double | Signal to monitor on branch A |
| Global | ib | 2 | Double | Signal to monitor on branch B |
| Global | ic | 3 | Double | Signal to monitor on branch C |
| Global | Tlevel | 4 | Double | Threshold level leading to a miscompare between 2 signals |
| Global | PClimit | 5 | Integer | Persistence Count limit governing duration of miscompare prior to latched fault |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Output Scope** | **Name** | **#** | **Type** | **Description** |
| Global | PC | 1 | Integer | Current Persistence Count in # of frames |
| Global | TC | 2 | Integer | Current Totalizer Count in # of frames |
| Global | FC | 3 | Integer | Latched Fault Code |
| Global | set\_val | 4 | Double | Selected value between the triplex signals |

Requirements:

[RM-001] In the no-fail state, a mis-compare, which shall be characterized by one branch differing with the other two branches by a unique trip level that lasts for more than the persistence limit, shall be reported to failure management as a failure.

[RM-002] In the no-fail state, the mid-value shall be the selected value. **Note:** a first failure in progress will not affect the method for determining the selected value.

[RM-003] In the single fail state, a good channel average of the remaining two good branches shall be used to determine the selected value.

[RM-004] If a second failure is in progress, the selected value shall remain unchanged from the previous selected value.