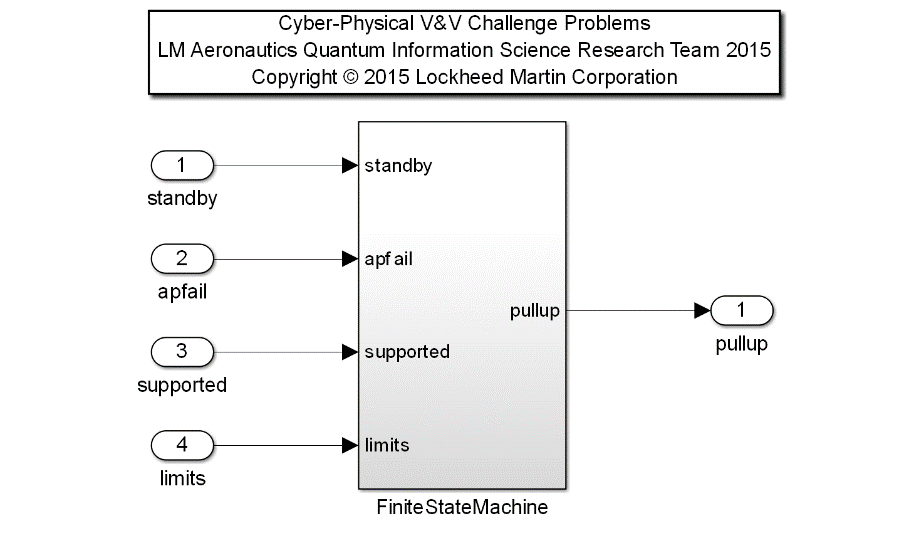
# 1) Finite State Machine

Model: ‘fsm\_12B.mdl’

Description: this model represents an abstraction of detailed design requirements for an Advanced Autopilot System interacting with an independent sensor platform. The Finite State Machine (FSM) represents a cyber-physical system with two independent components executing in real time for the purpose of ensuring a safe automatic operation in the vicinity of hazardous obstacles. The autopilot system, tightly integrated with the vehicle flight control computer, is responsible for commanding a safety maneuver in the event of a hazard. The sensor is the reporting agent to the autopilot with observability on imminent danger. When the conditions are met to allow an autopilot operation (supported and no failures) and the pilot is not manually controlling the vehicle (standby is false), the autopilot will behave normally until a maneuver is required in the event of a hazard (sensor is not good).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Input Scope** | **Name** | **#** | **Type** | **Description** |
| Global | standby | 1 | Boolean | True when the pilot is in control of the vehicle |
| Global | apfail | 2 | Boolean | Failure indication from an external source |
| Global | supported | 3 | Boolean | Indication of general health of system, must be True to enable operation |
| Global | limits | 4 | Boolean | External indication to sensor on faulty condition impeding safe operation. |
|  |  |  |  |  |
| **Output Scope** | **Name** | **#** | **Type** | **Description** |
| Global | pullup | 1 | Boolean | True when the autopilot is in the MANEUVER state |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Input Scope** | **Name** | **#** | **Type** | **Description** |
| Autopilot | standby | 1 | Boolean | True when the pilot is in control of the vehicle |
| Autopilot | apfail | 2 | Boolean | Failure indication from an external source |
| Autopilot | supported | 3 | Boolean | Indication of general health of system, must be True to enable operation |
| Autopilot | good | 4 | Boolean | Prior sensor output. When false indicates a detected fault. |
| Autopilot | state | 5 | Double | Autopilot State variable, Indication of prior value. |
|  |  |  |  |  |
| **Output Scope** | **Name** | **#** | **Type** | **Description** |
| Autopilot | MODE | 1 | Boolean | Autopilot internal moding discrete indicating not in transition state |
| Autopilot | REQUEST | 2 | Boolean | Autopilot internal moding discrete indicating transition to a nominal operation |
| Autopilot | PULL | 3 | Boolean | True when the autopilot is in the MANEUVER state |
| Autopilot | STATE | 4 | Integer | Autopilot State |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Input Scope** | **Name** | **#** | **Type** | **Description** |
| Sensor | mode | 1 | Boolean | Indication from autopilot on current mode of operation. |
| Sensor | request | 2 | Boolean | Secondary indication from autopilot on current mode of operation. |
| Sensor | limits | 3 | Boolean | External indication to sensor on faulty condition impeding safe operation. |
| Sensor | senstate | 4 | Double | Sensor State variable, Indication of prior value. |
| **Output Scope** | **Name** | **#** | **Type** | **Description** |
| Sensor | good | 1 | Boolean | False indicates an unsafe situation where a hazard may exist |
| Sensor | SENSTATE | 2 | Integer | Sensor State |

Requirements:

1. Exceeding sensor limits shall latch an autopilot pullup when the pilot is not in control (not standby) and the system is supported without failures (not apfail).
2. The autopilot shall change states from TRANSITION to STANDBY when the pilot is in control (standby).
3. The autopilot shall change states from TRANSITION to NOMINAL when the system is supported and sensor data is good.
4. The autopilot shall change states from NOMINAL to MANEUVER when the sensor data is not good.
5. The autopilot shall change states from NOMINAL to STANDBY when the pilot is in control (standby).
6. The autopilot shall change states from MANEUVER to STANDBY when the pilot is in control (standby) and sensor data is good.
7. The autopilot shall change states from PULLUP to TRANSITION when the system is supported and sensor data is good.
8. The autopilot shall change states from STANDBY to TRANSITION when the pilot is not in control (not standby).
9. The autopilot shall change states from STANDBY to MANEUVER when a failure occurs (apfail).
10. The sensor shall change states from NOMINAL to FAULT when limits are exceeded.
11. The sensor shall change states from NOMINAL to TRANSITION when the autopilot is not requesting support (not request).
12. The sensor shall change states from FAULT to TRANSITION when the autopilot is not requesting support (not request) and limits are not exceeded (not limits).
13. The sensor shall change states from TRANSITION to NOMINAL when the autopilot is requesting support (request) and the autopilot reports the correct active mode (mode).