

# 2003 FAA National Software Conference

## Software Level Determination

FAA AIRCRAFT CERTIFICATION  
SERVICE NATIONAL SOFTWARE  
CONFERENCE  
Reno, Nevada  
September 16 - 19, 2003

SOFTWARE LEVEL DETERMINATION  
USING SAE ARP 4754  
CERTIFICATION CONSIDERATIONS  
FOR HIGHLY INTEGRATED OR  
COMPLEX AIRCRAFT SYSTEMS

JIM TREACY  
FAA CHIEF SCIENTIST - AVIONICS

## ARP 4754

### Certification Considerations for Highly Integrated or Complex Aircraft Systems

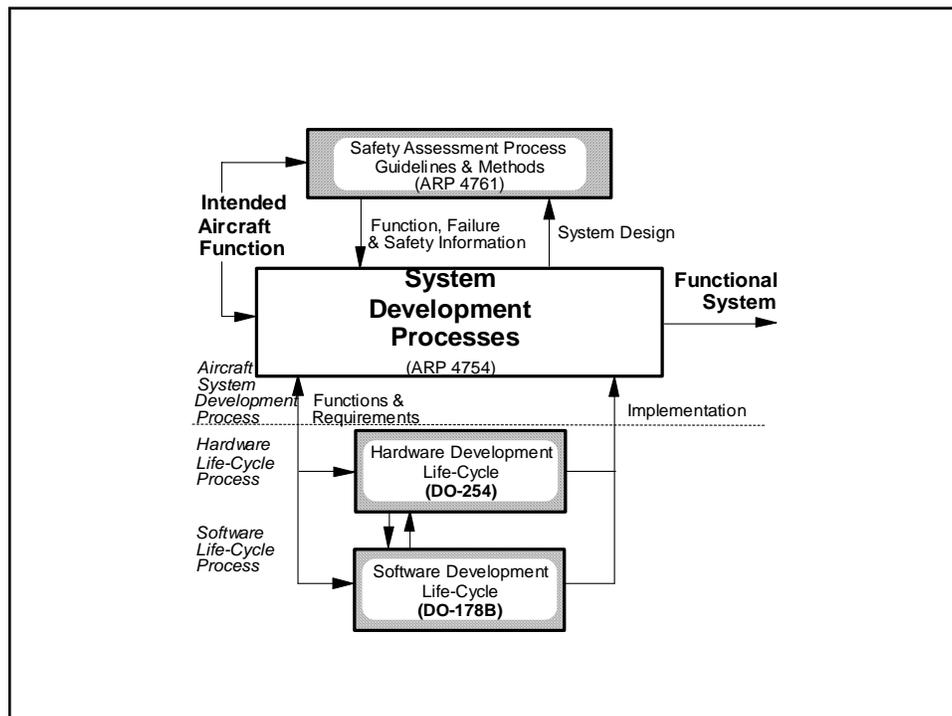
- Describes the Aircraft Systems Engineering Process
  - Requirements Capture
  - Allocation of Requirements
  - Architectural Considerations
  - Software Design Assurance Level Determination
  - Hardware Level Assurance Level Determination
  - Integration

# 2003 FAA National Software Conference

## Software Level Determination

### ARP 4754 (continued)

- Safety Assessment Process (high level)
  - Functional Hazard Assessment (FHA)
  - Preliminary System Safety Assessment
  - System Safety Assessment
- Requirements Validation
- System Verification



# 2003 FAA National Software Conference

## Software Level Determination

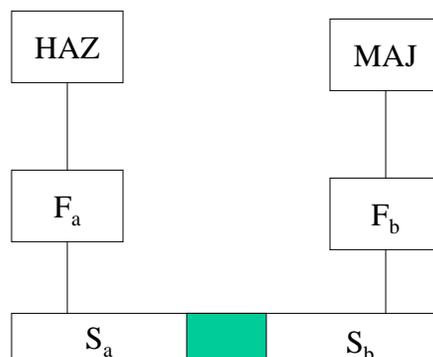
### Development/Design Assurance Determination

- Section 5.4 of SAE ARP 4754
- Sections 2.2 and 2.3 of RTCA/DO-178B
- Draft Policy Memorandum ANM-03-117-09
- Section 9.(b)(4) of draft AC 25.1309-1B

### Development/Design Assurance Determination

#### EXAMPLE 1a:

Partitioned Design (Reference SAE ARP4754, section 5.4.1.1, and RTCA DO-178B, section 2.3.1)



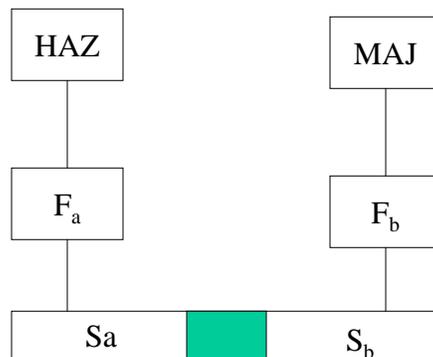
$F_a$  and  $F_b$  are independent functions that are implemented by systems  $S_a$  and  $S_b$ , respectively.  $S_a$  and  $S_b$  are partitioned.

# 2003 FAA National Software Conference

## Software Level Determination

### Development/Design Assurance Determination

#### EXAMPLE 1a: Partitioned Design (Continued)



#### FHA:

- Effects of  $F_a$  alone:  
Hazardous
- Effects of  $F_b$  alone:  
Major
- Both functions fail:  
Hazardous

#### PSSA:

- Failure of one function can not impact the other.
- Dissimilar hardware in  $S_a$  and  $S_b$

### Development/Design Assurance Determination

#### EXAMPLE 1a: Partitioned Design (Continued)

#### SAE ARP4754:

Level B for the overall system including, the partition.

- $S_a$  is Level B associated to its Hazardous effect.
- $S_b$  is Level C corresponding to the Major effect.

#### RTCA DO-178B

If the functions  $F_a$  and  $F_b$  are implemented in software:

- Software in  $S_a$  is Level B
- Software in  $S_b$  is Level C

If the partitioning protection involves software:

Partitioning software is Level B

#### RTCA DO-254

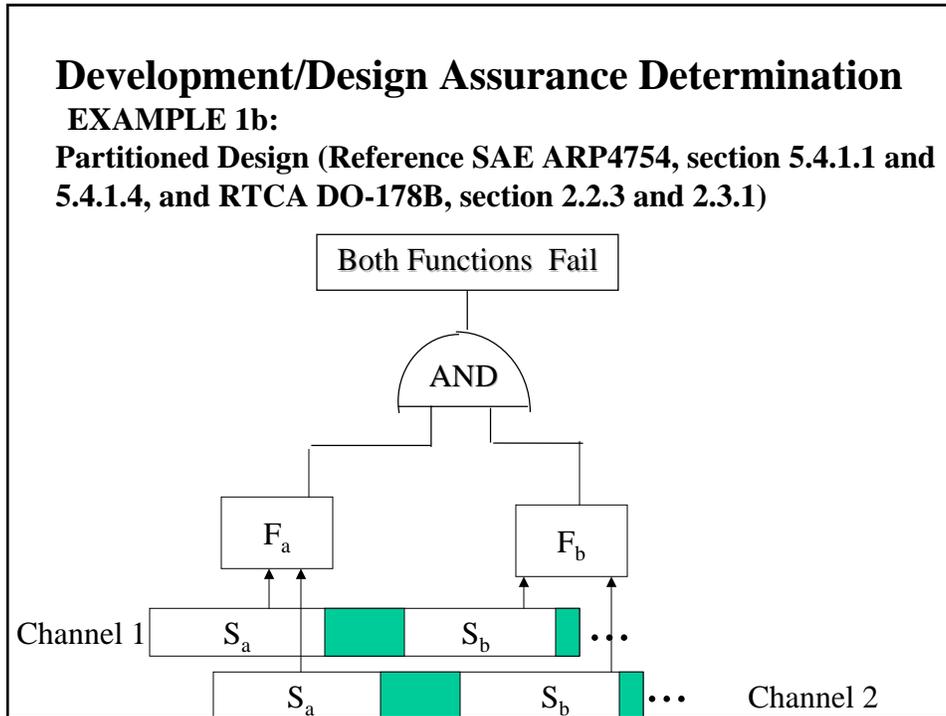
- Function  $F_a$  is at Level B
- Function  $F_b$  is at Level C

•There is no direct guidance for assigning the DAL to the partition.

Based on the FHA and PSSA, the hardware used for partitioning protection would be Level B.

# 2003 FAA National Software Conference

## Software Level Determination



### Development/Design Assurance Determination

#### EXAMPLE 1b:

Partitioned Design (Reference SAE ARP4754, section 5.4.1.1 and 5.4.1.4, and RTCA DO-178B, section 2.2.3 and 2.3.1)

- $F_a$  and  $F_b$  are independent functions representing an active command and a monitor that are implemented by systems  $S_a$  and  $S_b$ , respectively.  $S_a$  and  $S_b$  are integrated in a computer system that provides the multiple functions from two identical channels. The hardware and the software in Channel 1 and Channel 2 are the same.

# 2003 FAA National Software Conference

## Software Level Determination

### Development/Design Assurance Determination

#### EXAMPLE 1b:

Partitioned Design (Reference SAE ARP4754, section 5.4.1.1 and 5.4.1.4, and RTCA DO-178B, section 2.2.3 and 2.3.1)(Continued)

#### FHA:

- Failure (undetected malfunction) of both functions  $F_a$  and  $F_b$  is Catastrophic.
- Failure of  $F_a$  alone (loss of function): Major
- Failure of  $F_b$  alone (loss of function): Major
- Failure of Channel 1: Major
- Failure of Channel 2: Major

#### PSSA:

Design Assurance Level (DAL) for  $S_a$  to be higher than DAL for  $S_b$

### Development/Design Assurance Determination

#### EXAMPLE 1b:

Partitioned Design (Reference SAE ARP4754, section 5.4.1.1 and 5.4.1.4, and RTCA DO-178B, section 2.2.3 and 2.3.1)(Continued)

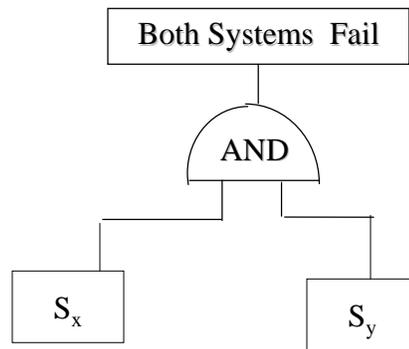
ARP4754	DO178B	DO254
<p>The overall system including the partition is level A.</p> <p>Either <math>S_a</math> or <math>S_b</math> is raised to level A. The PSSA assigned the higher level to <math>S_a</math>. Therefore, <math>S_a</math> is level A and <math>S_b</math> is level C.</p> <p>Note: Switching, voting and fault detection would be level A.</p>	<p>If the functions <math>F_a</math> and <math>F_b</math> are implemented in software, then per section 2.2.3, the software is level A for at least one system.</p> <p>Per section 2.3.1 Software in <math>S_a</math> is level A as assigned by the PSSA. Software in <math>S_b</math> is level C.</p> <p>If the partitioning protection involves software, that software is level A.</p>	<p>Common hardware is used to implement <math>S_a</math> and <math>S_b</math>. The hardware design assurance level is A.</p>

# 2003 FAA National Software Conference

## Software Level Determination

### Development/Design Assurance Determination

**EXAMPLE 2: Parallel Architecture – Dissimilar-and-Independent Designs Implementing an Airplane-Level Function (Reference ARP4754 section 5.4.1.2, and DO178B sections 2.2.3, 2.3.1 and 2.3.2)**



### Development/Design Assurance Determination

**EXAMPLE 2: Parallel Architecture – Dissimilar-and-Independent Designs Implementing an Airplane-Level Function (Reference ARP4754 section 5.4.1.2, and DO178B sections 2.2.3, 2.3.1 and 2.3.2)(Continued)**

Parallel systems  $S_x$  and  $S_y$  provide for the a/c level function and they are dissimilar and independent.

#### FHA:

- Effects of functional failures:
  - Malfunction = Catastrophic
  - Loss = Major
- Effect of loss or malfunction of  $S_x$  alone: Major
- Effect of loss or malfunction of  $S_y$  alone: Major

#### PSSA:

No hardware common mode failures

# 2003 FAA National Software Conference

## Software Level Determination

### Development/Design Assurance Determination

**EXAMPLE 2: Parallel Architecture – Dissimilar-and-Independent Designs Implementing an Airplane-Level Function (Reference ARP4754 section 5.4.1.2, and DO178B sections 2.2.3, 2.3.1 and 2.3.2)(Continued)**

#### ARP4754

Per item 2 in Table 4 of ARP4754, the overall system is level A.  $S_x$  and  $S_y$  are level B

Per Note 2 of table, any switching, voting, fault detection would be level A.

#### DO178B

Per section 2.2.3, if software is used in  $S_x$  and  $S_y$ , at least one is software level A. The other may be level C.

Any switching, voting, fault detection would be level A.

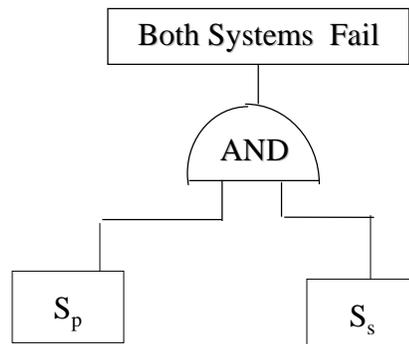
#### DO254

The PSSA uses the strategy contained in ARP4754 for DAL assignment; level B would be assigned to the hardware of  $S_x$  and  $S_y$ .

### Development/Design Assurance Determination

**EXAMPLE 3:**

**Parallel Architecture – Redundant-channel System Design Implementing an Airplane-Level Function (Reference ARP4754 section 5.4.1.3, and DO178B section 2.2.3)**



# 2003 FAA National Software Conference

## Software Level Determination

### Development/Design Assurance Determination

#### EXAMPLE 3: Parallel Architecture – Redundant-channel System Design Implementing an Airplane-Level Function (Reference ARP4754 section 5.4.1.3, and DO178B section 2.2.3)(Continued)

Primary channel  $S_p$  and secondary channel  $S_s$  provide an a/c level function.  $S_p$  is always used unless it has failed.  $S_s$  does not contribute to fault detection of  $S_p$ , and cannot cause  $S_p$  to fail.

#### FHA:

- Effects of combined failure:
  - Malfunction = Catastrophic
  - Loss = Major
- Effect of  $S_p$  alone: Major
- Effect of  $S_s$  alone: Major

#### PSSA:

- $S_p$  is a dissimilar design from  $S_s$
- The failure rate of  $S_p$  must be less than  $1 \times 10^{-5}$

### Development/Design Assurance Determination

#### EXAMPLE 3: Parallel Architecture – Redundant-channel System Design Implementing an Airplane-Level Function (Reference ARP4754 section 5.4.1.3, and DO178B section 2.2.3)(Continued)

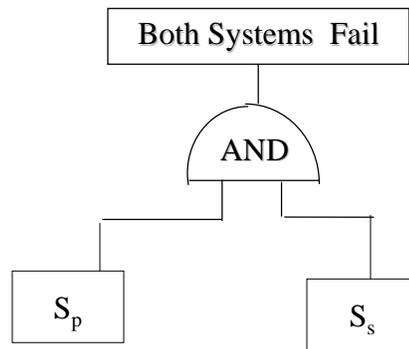
ARP4754	DO178B	DO254
<p>Per item 3 in Table 4:</p> <p>The overall system is level A.</p> <p>The primary portion <math>S_p</math> is level A, and the secondary portion <math>S_s</math> is level B, regardless of their individual failure effect.</p> <p>The failure detection, monitoring and switching logic is level A</p>	<p>Section 2.2.3 recommends the software in either <math>S_p</math> or <math>S_s</math> is at level A, while the other can be level C associated with <u>loss</u> of the aircraft level function.</p> <p>If implemented in software, the failure detection, monitoring and switching logic is level A.</p>	<p>The PSSA uses the strategy as ARP4754 to assign level A to the hardware in <math>S_p</math> and level B to the hardware in <math>S_s</math>.</p>

# 2003 FAA National Software Conference

## Software Level Determination

### Development/Design Assurance Determination

**EXAMPLE 4: Active-Monitor Parallel Architecture (Reference ARP4754 section 5.4.1.4, and DO178B section 2.3.3) with Dissimilar Hardware**



### Development/Design Assurance Determination

**EXAMPLE 4: Active-Monitor Parallel Architecture (Reference ARP4754 section 5.4.1.4, and DO178B section 2.3.3) with Dissimilar Hardware(Continued)**

An a/c level function is implemented in a parallel architecture where a monitor is needed to meet the integrity requirement.  $S_a$  is the active controller and  $S_m$  is the monitor.  $S_m$  and  $S_a$  are independent.

#### FHA:

- Effects of failures:
  - Undetected Malfunction is Catastrophic
  - Loss of function is Major
- Effect of  $S_a$  alone:
  - Malfunction detected by monitor is Hazardous
  - Loss of function is Major
- Effect of  $S_m$  alone:
  - Malfunction (nuisance shutdown) is Major
  - Loss (no monitoring capability) is Minor

# 2003 FAA National Software Conference

## Software Level Determination

### Development/Design Assurance Determination

**EXAMPLE 4: Active-Monitor Parallel Architecture (Reference ARP4754 section 5.4.1.4, and DO178B section 2.3.3) with Dissimilar Hardware(Continued)**

**PSSA:**

- No hardware common mode failures
- The monitor detects all failures (100% coverage)

### Development/Design Assurance Determination

**EXAMPLE 4: Active-Monitor Parallel Architecture (Reference ARP4754 section 5.4.1.4, and DO178B section 2.3.3) with Dissimilar Hardware(Continued)**

ARP4754	DO178B	DO254
Per item 4 in table 4:  The overall system is level A.  Either S <sub>a</sub> or S <sub>m</sub> can be level A. If S <sub>a</sub> is level A, then S <sub>m</sub> can be level C. If S <sub>m</sub> is level A, then S <sub>a</sub> is level B.  The switching, voting, and fault detection is level A.	Per Section 2.3.3 Safety-Monitoring:  The s/w in S <sub>a</sub> can be lowered to the level associated with <u>loss</u> of <b>provided</b> S <sub>m</sub> s/w has the following three attributes: 1) it is developed to level A, 2) it has adequate fault coverage, 3) it is independent from S <sub>a</sub> .  The guidance does not discuss what S <sub>m</sub> software level should be if S <sub>a</sub> is developed to level A.	The strategy of ARP4754 is used to assign level A to the hardware of S <sub>a</sub> and level C to the hardware of S <sub>m</sub> .  Alternatively, level B could be used for S <sub>a</sub> and level A for S <sub>m</sub> .

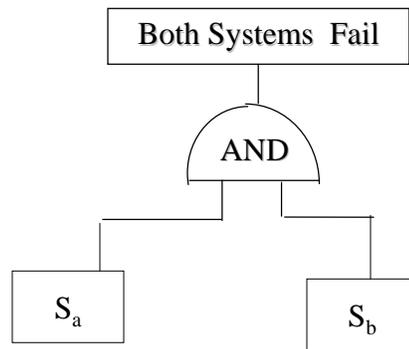
# 2003 FAA National Software Conference

## Software Level Determination

### Development/Design Assurance Determination

#### EXAMPLE 5:

Backup Parallel Architecture (Reference ARP4754 section 5.4.1.5, and DO178B section 2.2.3)



### Development/Design Assurance Determination

#### EXAMPLE 5:

Backup Parallel Architecture (Reference ARP4754 section 5.4.1.5, and DO178B section 2.2.3)

$S_a$  is the primary system.  $S_b$  is the independent backup system.

#### FHA:

- Effects of functional failures:
  - Malfunction = Catastrophic
  - Loss = Major
- Effect of  $S_a$  alone: Hazardous
- Effect of  $S_b$  alone: Minor

#### PSSA:

- $S_a$  must meet integrity requirements without the backup and must have a very low hardware failure rate – less than  $1 \times 10^{-7}$  for loss of function)
- $S_a$  to have higher Design Assurance Level than  $S_b$
- $S_a$  and  $S_b$  have no common hardware failure modes

# 2003 FAA National Software Conference

## Software Level Determination

<b>Development/Design Assurance Determination</b>		
<b>EXAMPLE 5:</b>		
<b>Backup Parallel Architecture (Reference ARP4754 section 5.4.1.5, and DO178B section 2.2.3)</b>		
<b>ARP4754</b>	<b>DO178B</b>	<b>DO254</b>
<p>Per item 5 in Table 4:</p> <p>The overall system is level A.</p> <p>S<sub>a</sub> is level A, regardless of its hazardous effect. S<sub>b</sub> can be level C albeit its effect is Minor.</p> <p>Per Note 2 of the table, the switching, voting, fault detection is level A.</p>	<p>The guidance for parallel architecture section 2.2.3 recommends the software in either to be at level A. The other channel can be level C corresponding to the <u>loss</u> of the aircraft level function (Major.) The software that determines that the primary channel has failed (fault detection or safety monitoring) and switches to the backup channel would be Level A.</p>	<p>Using the strategy as of ARP 4754, the PSSA would assign level A to the hardware of S<sub>a</sub> and level C to S<sub>b</sub>.</p>

<p><b>EXAMPLE 6: A Yaw Damper with a Manual Safety Feature</b></p> <p>Suppose an airplane has inherent lightly damped Dutch roll characteristics. A Yaw Damper (YD) system is provided to arrest the Dutch roll and to improve ride quality. However, the YD system is not critical because without it the Dutch roll will eventually damp itself out. Suppose the airplane safety assessment is as follows:</p> <p><b>Airplane Level FHA:</b></p> <ul style="list-style-type: none"> <li>▪ <i>Sustained</i> oscillation at the dutch roll frequency is Catastrophic.</li> <li>▪ Loss of yaw damping function is at most Major taking into account the inherent dutch roll damping characteristics.</li> <li>▪ YD failed “hardover” is Major.</li> </ul> <p><b>System Architecture:</b></p> <p>There are two <i>identical</i> digital Yaw Damper Modules (YDM) each of which has a failure rate of 10<sup>-5</sup>/flt-hr. Only one module is in control at any given time. The YDMs monitor each other and both shut down if the outputs disagree. System shutdown is annunciated on the flight deck. A manual switch is provided on the flight deck to shut down the YDMs in case of malfunction.</p>
---

# 2003 FAA National Software Conference

## Software Level Determination

### **EXAMPLE 6: A Yaw Damper with a Manual Safety Feature System Level FHA:**

- Yaw Damper Module (YDM):
- Loss of 1 YDM due to hardware failure is Major if it leads to shutdown of the remaining good YDM.
- Loss of 2 YDMs due to hardware failure is Major (loss of YD function).
- Malfunction due to hardware common mode failure in both YDMs causing oscillation at dutch roll frequency is Hazardous (without the manual switch, this failure would be Catastrophic). It is assumed the pilot is trained to compensate by turning the YD switch to “Off”.
- Malfunction due to hardware failure in one YDM is Major.
- Software malfunction causing oscillation at dutch roll frequency is Hazardous (Catastrophic without the manual switch). It is assumed the pilot is trained to compensate by turning the YD switch to “Off”.
- Loss of YD function due to software is Major.

### **EXAMPLE 6: A Yaw Damper with a Manual Safety Feature System Level FHA(Continued):**

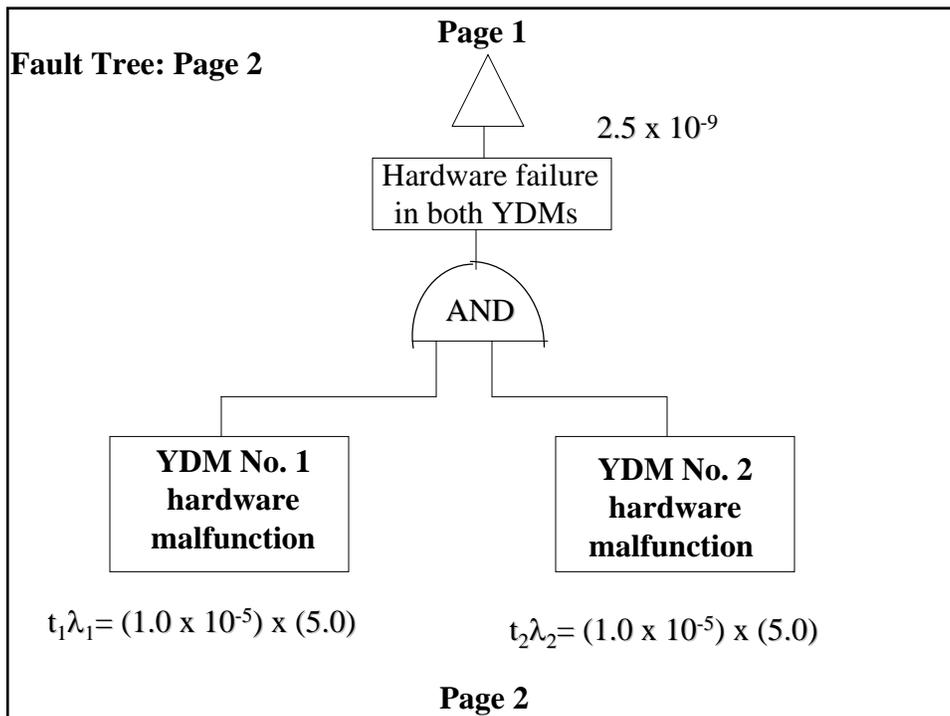
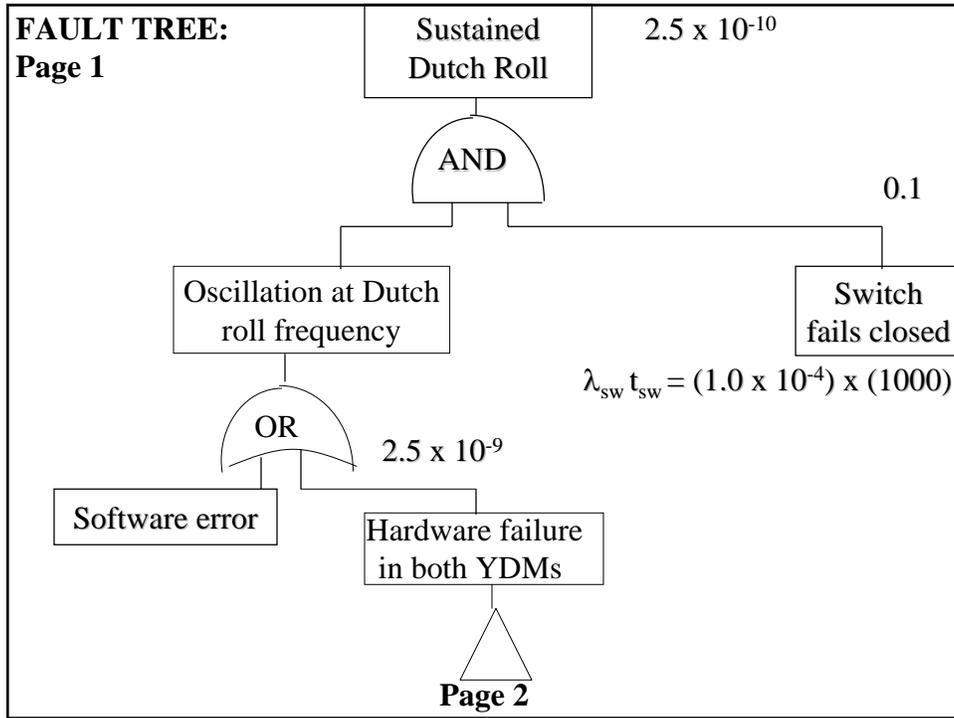
- Manual Switch:
  - Failed open is Major (causes loss of YD function)
  - Failed connected is Minor (slight reduction in system capability – loss of manual shutdown, no immediate safety effect on airplane)
  - The failure rate of the switch to the closed position is  $1.0 \times 10^{-4}$
  - Establish an inspection of the manual switch every 1000 flight hours

#### **PSSA:**

- For the switch failure to be Minor in the failed-connected condition, the two YDMs combined must be sufficiently reliable for the combination of malfunctioning YDM and switch failure to meet the numerical safety objectives (see fault tree below.)
- There are no common mode failures between the switch and the YDMs.
- Assume an average flight time of 5.0 hours

# 2003 FAA National Software Conference

## Software Level Determination



# 2003 FAA National Software Conference

## Software Level Determination

**Development assurance Level Determination:  
Using the ARP4754 guidance :**

- The overall system (YDM and Switch) would be assured to level A because the top hazard category is Catastrophic.
- YDM (as a system of s/w and h/w) is at level B corresponding to the hazardous effect of a malfunction (assumed to occur simultaneously.)
- According to the FHA, the DAL of the switch should be level B per 5.4.1.2. However, since the switch is a simple hardware component, no DAL is necessary and only the reliability requirement needs to be satisfied.

**Development assurance Level Determination  
Software level according to DO-178B alone:**

- Because the top level effect is Catastrophic, the YD software is level A even though the system incorporates the manual safety switch.

# 2003 FAA National Software Conference

## Software Level Determination

### Development assurance Level Determination for Hardware DAL according to DO-254:

- Because the two YDMs have identical hardware, the safety assessment identifies the possibility of common mode failures. The YDM hardware are developed to level B corresponding the Hazardous category due to both YDMs malfunctioning. If there were no common mode failures, the YDM could be level C corresponding to the failure of each module.
- No need for assigning DAL to the switch as it is a “simple” device.