Appendix 5 – Example of limit latency and residual probability analysis

ED Decision 2021/015/R

The following example illustrates how the quantitative criteria of CS 25.1309(b)(5) are to be implemented together with CS 25.1309(b)(1). The methodology used is based on the identification of the minimal cut sets associated with the catastrophic top event of the generic system level fault tree provided in Figure A5-1.

The term 'minimal cut set' refers to the smallest set of primary events whose occurrence is sufficient to cause a system failure or, in this case, the failure condition of concern.

(1) The list of minimal cut sets should be produced by cut set order. This will group all dual-order cut sets or failure combinations. The entire list of minimal cut sets of the fault tree in Figure A5-1 is provided in Table A5-1.

(2) The dual-order minimal cut sets that contain a primary event that is latent for more than one flight are then identified from the list in Table A5-1.

(3) Then group those dual-order minimal cut sets:

(3.1) that contain the same active primary event. For each group, sum the remaining latent failure probabilities. For each group, the sum of the latent primary events should be less than 1/1 000.

(3.2) that contain the same latent primary event. For each group, assume that the latent primary event has failed and sum the remaining active primary event probabilities. For each group, the sum of the primary event probabilities should be less than 1×10^{-5}/FH.

(4) The sum of all minimal cut sets should be in the order of 1×10^{-9}/FH.

An alternative method to perform step (3.2) would be to rerun the fault-tree-probability calculation assuming for each model rerun that a different latent primary event has occurred and then verify that the average probability per flight hour of the top event is of the order of 1×10^{-5}/FH or less.

The results of the limit latency and residual probability analysis are provided in Table A5-1.

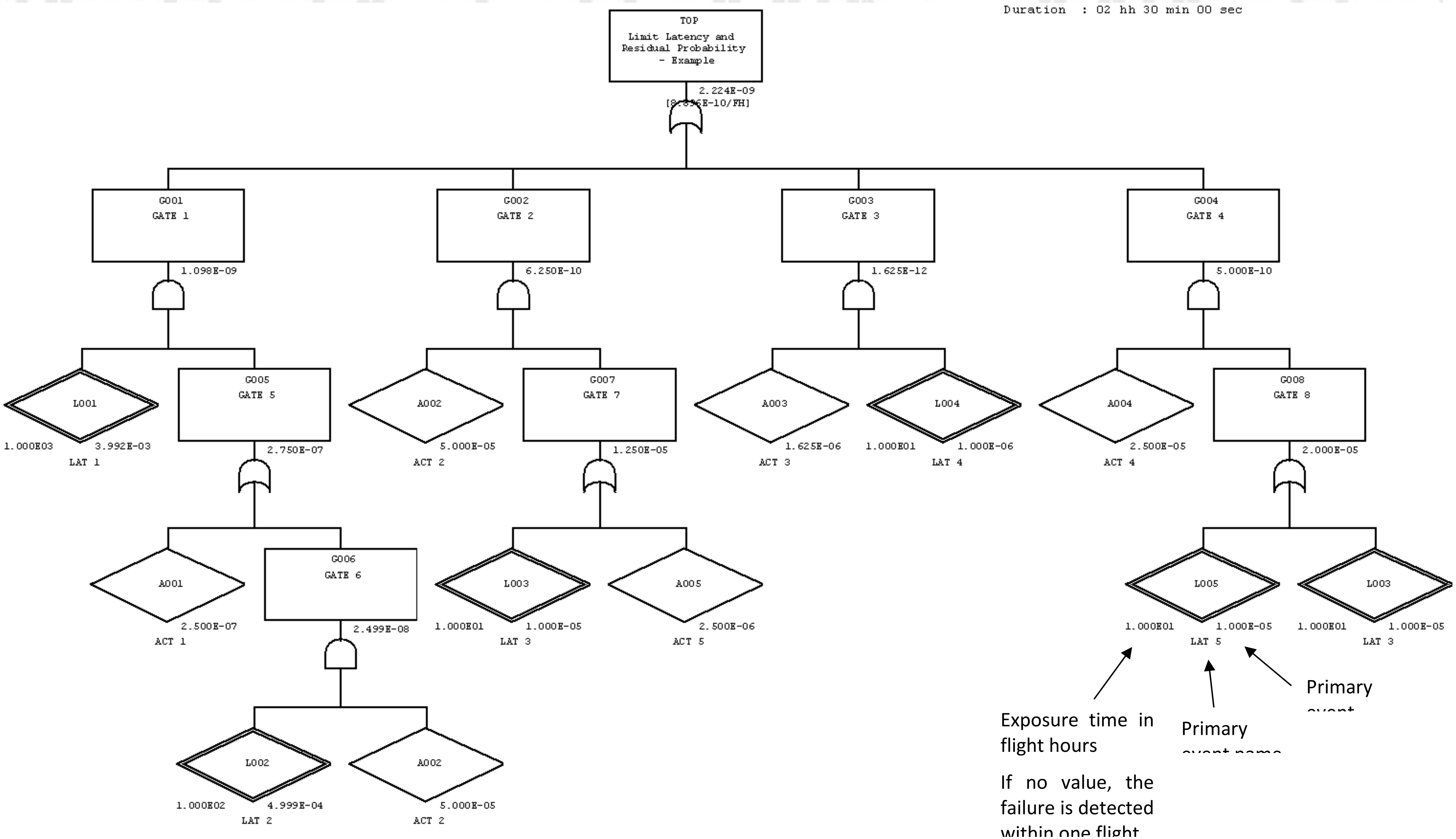

Figure A5-1: Fault Tree

#	Probability (per flight hour)	Event name	Event description	Failure rate (constant, unless noted)	Exposure time	Event probability (per flight)	CS 25.1309(b)(5) Applicability/ compliance
1	3.992E-10	A001	ACT 1	1.000E-07	2.5 h	2.500E-07	Not compliant with the limit latency criterion [L001 probability is more frequent than 1.000E-03].
		L001	LAT 1	4.000E-06	1 000.0 h	3.992E-03	
2	2.000E-10	A002	ACT 2	2.000E-05	2.5 h	5.000E-05	Not compliant with the residual probability criterion [A002 probability per flight hour (2.000E-05/FH) is more frequent than 1.000E-05/FH].
		L003	LAT 3	1.000E-06	10.0 h	1.000E-05	
3	1.000E-10	A004	ACT 4	1.000E-05	2.5 h	2.500E-05	Not compliant with the residual probability criterion [while A004 probability per flight hour is equal to 1.000E-05/FH, the combined probability per flight hour of A004 and A002 (1.000E-05/FH + 2.000E-05/FH) is more frequent than 1.000E-05/FH. *Note: Dual-order minimal cut sets #2 and #3 are grouped due to same event L003 appearing under G002 and G004.*
		L003	LAT 3	1.000E-06	10.0 h	1.000E-05	
4	1.000E-10	A004	ACT 4	1.000E-05	2.5 h	2.500E-05	Compliant with both limit latency and residual probability criteria [A004 probability per flight hour is equal to 1.000E-05/FH and combined probability of L005 and L003 (1.000E-05 + 1.000E-05) is less frequent than 1.000E-03].
		L005	LAT 5	1.000E-06	10.0 h	1.000E-05	
5	5.000E-11	A002	ACT 2	2.000E-05	2.5 h	5.000E-05	This dual-order minimal cut set does not contain any basic event being latent for more than one flight. Therefore, CS 25.1309(b)(5) is not applicable to this minimal cut set.
		A005	ACT 5	1.000E-06	2.5 h	2.500E-06	
6	6.500E-13	A003	ACT 3	6.500E-07	2.5 h	1.625E-06	Compliant with both limit latency and residual probability criteria [A003 probability per flight hour (6.500E-07/FH) is less frequent than 1.000E-05/FH and L004 probability is less frequent than 1.000E-03]
		L004	LAT 4	1.000E-07	10.0 h	1.000E-06	
7	3.991E-11	A002	ACT 2	2.000E-05	2.5 h	5.000E-05	This minimal cut set is more than a dual failure combination. Therefore, CS 25.1309(b)(5) is not applicable to this minimal cut set.
		L001	LAT 1	4.000E-06	1 000.0 h	3.992E-03	
		L002	LAT 2	5.000E-06	100.0 h	4.999E-04	
Flight time = 2.5 hours P[LAT i] ~ FR * T							

Table A5-1: Minimal Cut Sets

[Amdt 25/24]
[Amdt 25/27]

CS 25.1310 Power source capacity and distribution

ED Decision 2016/010/R

(See AMC 25.1310)

(a) Each installation whose functioning is required for type certification or by operating rules and that requires a power supply is an "essential load" on the power supply. The power sources and the system must be able to supply the following power loads in probable operating combinations and for probable durations (see AMC 25.1310(a)):

(1) Loads connected to the system with the system functioning normally.

(2) Essential loads, after failure of any one prime mover, power converter, or energy storage device.

(3) Essential loads after failure of -

(i) Any one engine on two-engine aeroplanes; and

(ii) Any two engines on three-or-more engine aeroplanes.

(4) Essential loads for which an alternate source of power is required, after any failure or malfunction in any one-power supply system, distribution system, or other utilisation system.

(b) In determining compliance with sub-paragraphs (a)(2) and (3) of this paragraph, the power loads may be assumed to be reduced under a monitoring procedure consistent with safety in the kinds of operation authorised. Loads not required in controlled flight need not be considered for the two-engine-inoperative condition on aeroplanes with three or more engines.

[Amdt 25/18]

AMC 25.1310(a) Power source capacity and distribution

ED Decision 2003/2/RM

When alternative or multiplication of systems and equipment is provided to meet the requirements of CS 25.1310(a), the segregation between circuits should be such as to minimise the risk of a single occurrence causing multiple failures of circuits or power supplies of the system concerned. For example, electrical cable bundles or groups of hydraulic pipes should be so segregated as to prevent damage to the main and alternative systems and power supplies.

CS 25.1315 Negative acceleration

ED Decision 2016/010/R

(See AMC 25.1315)

No hazardous malfunction may occur as a result of the aeroplane being operated at the negative accelerations within the flight envelopes prescribed in CS 25.333. This must be shown for the greatest duration expected for the acceleration.

[Amdt 25/18]

AMC 25.1315 Negative accelerations

ED Decision 2003/2/RM

1 Demonstration of compliance with CS 25.1315 should be made by analysis and/or ground tests, and should be supported by flight tests.

2 *Analysis and/or Ground Tests.* Appropriate analysis and/or ground tests should be made on components of essential fluid systems and such other components as are likely to be adversely affected by negative acceleration to demonstrate that they will not produce a hazardous malfunction.

3 *Flight Tests*

3.1 The aeroplane should be subjected to –

a. One continuous period of at least five seconds at less than zero g, and, separately,

b. A period containing at least two excursions to less than zero g in rapid succession, in which the total time at less than zero g is at least five seconds.

3.2 The tests should be made at the most critical condition from the fuel flow standpoint, e.g. with fuel flow corresponding to maximum continuous power and with the fuel representing a typical operational low fuel condition as for a missed approach.

CS 25.1316 Electrical and electronic system lightning protection

ED Decision 2015/019/R

(See AMC 20-136)

(a) Each electrical and electronic system that performs a function whose failure would prevent the continued safe flight and landing of the aeroplane must be designed and installed so that:

(1) the function is not adversely affected during and after the time the aeroplane is exposed to lightning; and

(2) the system automatically recovers normal operation of that function, in a timely manner, after the aeroplane is exposed to lightning, unless the system's recovery conflicts with other operational or functional requirements of the system that would prevent continued safe flight and landing of the aeroplane.

(b) Each electrical and electronic system that performs a function whose failure would reduce the capability of the aeroplane or the ability of the flight crew to respond to an adverse operating condition must be designed and installed so that the function recovers normal operation in a timely manner after the aeroplane is exposed to lightning.

[Amdt 25/17]

CS 25.1317 High-Intensity Radiated Fields (HIRF) protection

ED Decision 2015/019/R

(See AMC 20-158)

(a) Each electrical and electronic system that performs a function whose failure would prevent the continued safe flight and landing of the aeroplane must be designed and installed so that:

(1) The function is not adversely affected during and after the time the aeroplane is exposed to HIRF environment I, as described in Appendix R;

(2) The system automatically recovers normal operation of that function, in a timely manner, after the aeroplane is exposed to HIRF environment I, as described in Appendix R, unless the system's recovery conflicts with other operational or functional requirements of the system that would prevent continued safe flight and landing of the aeroplane; and

(3) The system is not adversely affected during and after the time the aeroplane is exposed to HIRF environment II, as described in Appendix R.

(b) Each electrical and electronic system that performs a function whose failure would significantly reduce the capability of the aeroplane or the ability of the flight crew to respond to an adverse operating condition must be designed and installed so that the system is not adversely affected when the equipment providing the function is exposed to equipment HIRF test level 1 or 2, as described in Appendix R.

(c) Each electrical and electronic system that performs a function whose failure would reduce the capability of the aeroplane or the ability of the flight crew to respond to an adverse operating condition must be designed and installed so that the system is not adversely affected when the equipment providing the function is exposed to equipment HIRF test level 3, as described in Appendix R.

[Amdt 25/17]

CS 25.1319 Equipment, systems and network information protection

ED Decision 2020/006/R

(a) Aeroplane equipment, systems and networks, considered separately and in relation to other systems, must be protected from intentional unauthorised electronic interactions (IUEIs) that may result in adverse effects on the safety of the aeroplane. Protection must be ensured by showing that the security risks have been identified, assessed and mitigated as necessary.

(b) When required by paragraph (a), the applicant must make procedures and Instructions for Continued Airworthiness (ICA) available that ensure that the security protections of the aeroplane's equipment, systems and networks are maintained.

[Amdt 25/25]

AMC to CS 25.1319 Equipment, systems and network information security protection

ED Decision 2020/006/R

In showing compliance with CS 25.1319, the applicant may consider AMC 20-42, which provides acceptable means, guidance and methods to perform security risk assessments and mitigation for aircraft information systems.

The term 'adverse effects on the safety of the aeroplane' limits the scope of this provision to security breaches that impact on the safety and airworthiness of the aeroplane and its operation, rather than security breaches that may impact on the systems that have no safety effect on the aeroplane. For example, while the manufacturer and the air operator may have real concerns about protecting a device that is used to process passenger credit cards and securing passenger information, EASA does not regard this as being subject to review and approval as part of the certification of the system, but instead as something that the air operator or manufacturer would address as part of their business practices and responsibilities to the customer.

The term 'mitigated as necessary' clarifies that the applicant has the discretion to establish appropriate means of mitigation against security risks.

The term 'procedures and Instructions for Continued Airworthiness (ICA)' clarifies that, while the ICA may be one mechanism for providing the necessary instructions to maintain airworthiness, the security protections may go beyond traditional ICA material, and also include other procedures provided to the air operator. This aligns with the existing practices among those applicants for which special conditions (SCs) have been issued to address the protection of the aircraft information systems' security.

[Amdt 25/25]

INSTRUMENTS: INSTALLATION

CS 25.1321 Arrangement and visibility

ED Decision 2003/2/RM

(a) Each flight, navigation, and powerplant instrument for use by any pilot must be plainly visible to him from his station with the minimum practicable deviation from his normal position and line of vision when he is looking forward along the flight path.

(b) The flight instruments required by CS 25.1303 must be grouped on the instrument panel and centred as nearly as practicable about the vertical plane of the pilot's forward vision. In addition –

(1) The instrument that most effectively indicates attitude must be on the panel in the top centre position;

(2) The instrument that most effectively indicates airspeed must be adjacent to and directly to the left of the instrument in the top centre position;

(3) The instrument that most effectively indicates altitude must be adjacent to and directly to the right of the instrument in the top centre position; and

(4) The instrument that most effectively indicates direction of flight must be adjacent to and directly below the instrument in the top centre position.

(c) Required powerplant instruments must be closely grouped on the instrument panel. In addition –

(1) The location of identical powerplant instruments for the engines must prevent confusion as to which engine each instrument relates; and

(2) Powerplant instruments vital to the safe operation of the aeroplane must be plainly visible to the appropriate crewmembers.

(d) Instrument panel vibration may not damage or impair the accuracy of any instrument.

(e) If a visual indicator is provided to indicate malfunction of an instrument, it must be effective under all probable cockpit lighting conditions.

CS 25.1322 Flight Crew Alerting

ED Decision 2011/004/R

(See AMC 25.1322)

(a) Flight crew alerts must:

(1) provide the flight crew with the information needed to:

(i) identify non-normal operation or aeroplane system conditions, and

(ii) determine the appropriate actions, if any;

(2) be readily and easily detectable and intelligible by the flight crew under all foreseeable operating conditions, including conditions where multiple alerts are provided;

(3) be removed when the alerting condition no longer exists.

(b) Alerts must conform to the following prioritisation hierarchy based on the urgency of flight crew awareness and response:

(1) Warning: For conditions that require immediate flight crew awareness and immediate flight crew response.

(2) Caution: For conditions that require immediate flight crew awareness and subsequent flight crew response.

(3) Advisory: For conditions that require flight crew awareness and may require subsequent flight crew response.

(c) Warning and Caution alerts must:

(1) be prioritised within each category, when necessary;

(2) provide timely attention-getting cues through at least two different senses by a combination of aural, visual, or tactile indications;

(3) permit each occurrence of the attention-getting cues required by sub-paragraph (c)(2) to be acknowledged and suppressed, unless they are required to be continuous.

(d) The alert function must be designed to minimise the effects of false and nuisance alerts. In particular, it must be designed to:

(1) prevent the presentation of an alert when it is inappropriate or unnecessary;

(2) provide a means to suppress an attention-getting component of an alert caused by a failure of the alerting function that interferes with the flight crew's ability to safely operate the aeroplane. This means must not be readily available to the flight crew so that it could be operated inadvertently or by habitual reflexive action. When an alert is suppressed, there must be a clear and unmistakable annunciation to the flight crew that the alert has been suppressed.

(e) Visual alert indications must:

(1) conform to the following colour convention:

(i) Red for Warning alert indications.

(ii) Amber or yellow for Caution alert indications.

(iii) Any colour except red or green for Advisory alert indications.

(2) use visual coding techniques, together with other alerting function elements on the flight deck, to distinguish between Warning, Caution and Advisory alert indications, if they are presented on monochromatic displays that are incapable of conforming to the colour convention in paragraph (e)(1).

(f) Use of the colours red, amber and yellow on the flight deck for functions other than flight crew alerting must be limited and must not adversely affect flight crew alerting.

[Amdt 25/11]

AMC 25.1322 Alerting Systems

ED Decision 2011/004/R

Paragraph

1. Purpose

This AMC provides an acceptable means of compliance and guidance material for showing compliance with certain requirements of CS-25, for the design approval of flight crew alerting functions. This AMC addresses the type of alert function elements that should be considered (including visual, aural, and tactile or haptic elements), alert management, interface or integration of alerts with other systems, and colour standardisation. The appendices to this AMC also provide examples for including visual and aural system elements in an alerting system.

2. Scope

a. This AMC is applicable to aeroplane manufacturers, modifiers, avionics manufacturers, EASA type-certification engineers, human factor specialists and test pilots.