

APÉNDICE 2. CONCEPTO DE DISEÑO "FAIL-SAFE" DE LA DNA.

1. CONCEPTO DE DISEÑO "FAIL-SAFE" DE LA DNA

Los estándares de aeronavegabilidad de la DNAR Parte 25 están basados en, e incorporan, los objetivos, y principios o técnicas, del concepto de diseño "fail-safe", que considera los efectos de las fallas y combinaciones de fallas en la definición de un diseño seguro. Al respecto, los siguientes objetivos básicos pertinentes a fallas se aplican:

- a. En cualquier sistema o subsistema, la falla de cualquier elemento único, componente, o conexión durante algún vuelo (desde la liberación de los frenos hasta la desaceleración en tierra para detenerse) debe ser asumida, sin tener en cuenta su probabilidad. Tal falla simple no debe evitar continuar con seguridad el vuelo y aterrizar, o reducir la capacidad del avión o la habilidad de la tripulación para afrontar las condiciones de la falla resultante.
- b. También deben asumirse las fallas subsecuentes durante el mismo vuelo, ya sean detectadas o latentes, y sus combinaciones, a menos que se demuestre que su probabilidad unida con la primera falla es extremadamente improbable.

2. PRINCIPIOS Y/O TÉCNICAS "FAIL SAFE"

El concepto de diseño "fail-safe" utiliza los siguientes principios o técnicas de diseño para garantizar un diseño seguro. El uso de solamente uno de estos principios o técnicas pocas veces resulta adecuado o suficiente. Generalmente es necesario una combinación de dos o más para proporcionar un diseño "fail-safe"; por ejemplo, para garantizar que las condiciones de falla mayores sean improbables y las condiciones de fallas catastróficas sean extremadamente improbables. En tal sentido se puede considerar:

- a. Integridad y Calidad del diseño. Incluyendo los Límites de Vida, para garantizar la función prevista y prevenir fallas.
- b. Sistemas Redundantes ó de Backup. Para garantizar la continuidad del funcionamiento después de cualquier falla simple (o de otro número de fallas); por ejemplo, dos o más sistemas hidráulicos, sistemas de control vuelo, etc.
- c. Aislación de Sistemas, Componentes, y Elementos de tal manera que la falla de uno no provoque la falla del otro. Conceptualmente la aislación es también considerada como un elemento independiente.
- d. Confiabilidad Probada de tal manera que las fallas múltiples, e independientes sean improbables durante el mismo vuelo.
- e. Anuncio o Indicación de Falla, para proporcionar la detección.

- f. Procedimientos de la Tripulación para usar después de la detección de la falla, para que resulte factible continuar con el vuelo en forma segura y aterrizar mediante la acción correctiva específica de la tripulación.
- g. Verificabilidad: la capacidad para verificar una condición de los componentes.
- h. Límites del Efecto de una Falla considerada en el Diseño, incluyendo la capacidad en soportar el daño, para limitar el impacto en la seguridad o los efectos de una falla.
- i. Trayectoria de una Falla considerada en el Diseño, para controlar y dirigir los efectos de una falla en el sentido que limite su impacto en la seguridad.
- j. Márgenes o Factores de Seguridad, para admitir cualquier condición adversa impredecible o no definida.
- k. Tolerancia de Error que considere los efectos adversos de errores impredecibles durante el diseño del avión, ensayo, fabricación, operación, y mantenimiento.