UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería del Diseño

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Aeroespacial y Diseño Industrial

Análisis del impacto de los COTS en la Industria Aeroespacial

Trabajo Fin de Máster

Máster Universitario en Ingeniería Aeronáutica

AUTOR/A: Calvo Cendán, Xabier

Tutor/a: Tiseira Izaguirre, Andrés Omar

CURSO ACADÉMICO: 2022/2023

Máster en Ingeniería Aeronáutica

Análisis del impacto de los COTS en la Industria Aeroespacial

Trabajo Final de Máster

Autor: Xabier Calvo Cendán – xcalcen@etsid.upv.es

Tutor: Andrés Omar Tiseira Izaguirre – anti1@mot.upv.es

15 de septiembre de 2023

Resumen

El presente trabajo comenzará repasando qué es la seguridad e introduciendo conceptos relacionados, como el nivel de seguridad o la cultura de la seguridad. También se hablará de los requisitos críticos de seguridad y su relación con los COTS, definiendo este último concepto y presentando las ventajas e inconvenientes que ofrecen este tipo de componentes.

A continuación, se analizará el uso de COTS dentro de la Industria Nuclear, incidiendo sobre las propuestas adoptadas para dar solución a los problemas que se presentan. La metodología empleada será tratada a fondo, haciendo un repaso de los elementos principales que forman parte del Proceso de Dedicación.

Por último, se estudiará la posibilidad de utilizar esta tecnología dentro de la Industria Aeroespacial, haciendo una revisión de la normativa aplicable. Para ello, se expondrán los requisitos existentes en los documentos emitidos por las entidades reguladoras, se analizarán las semejanzas y las diferencias con el Proceso de Dedicación y se propondrá un formulario básico que sirva de ayuda para la certificación de este tipo de componentes.

Palabras clave: COTS, seguridad, hardware, función, calidad

Abstract

This paper will begin by reviewing what safety is and introducing related concepts such as safety level and safety culture. It will also discuss safety critical requirements and their relationship with COTS, defining the last concept and presenting the advantages and disadvantages offered by this type of components.

The use of COTS in the Nuclear Industry will then be analysed, with emphasis on the proposals adopted to solve the problems that arise. The methodology used will be discussed in depth, reviewing the main elements that form part of the Dedication Process.

Finally, the possibility of using this technology in the Aerospace Industry will be studied, reviewing the applicable regulations. In order to do this, the existing requirements in the documents issued by the regulatory agencies will be presented, the similarities and differences with the Dedication Process will be analysed and a basic form will be proposed to help in the certification of this type of components.

Key words: COTS, safety, hardware, function, quality

Resum

El present treball començarà repassant què és la seguretat i introduint conceptes relacionats, com el nivell de seguretat o la cultura de la seguretat. També es parlarà dels requisits crítics de seguretat i la seua relació amb els COTS, definint aquest últim concepte i presentant els avantatges i inconvenients que ofereixen aquest tipus de components.

A continuació, s'analitzarà l'ús de COTS dins de la Indústria Nuclear, incidint sobre les propostes adoptades per a donar solució als problemes que es presenten. La metodologia emprada serà tractada a fons, fent un repàs dels elements principals que formen part del Procés de Dedicació.

Finalment, s'estudiarà la possibilitat d'utilitzar aquesta tecnologia dins de la Indústria Aeroespacial, fent una revisió de la normativa aplicable. Per a això, s'exposaran els requisits existents en els documents emesos per les entitats reguladores, s'analitzaran les semblances i les diferències amb el Procés de Dedicació i es proposarà un formulari bàsic que servisca d'ajuda per a la certificació d'aquesta mena de components.

Paraules clau: COTS, seguretat, hardware, funció, qualitat

Índice

Relación de figuras

Relación de tablas

Nomenclatura

Siglas

AEH	Airborne Electronic Hardware
ASIC	Application-Specific Integrated Circuit
ASME	American Society of Mechanical Engineers
CBA	Circuit Board Assembly
CFR	Code of Federal Regulations
CGI	Commercial Grade Item
CGID	Commercial Grade Item Dedication
CM	Certification Memorandum
COTS	Commercial Off-The-Shelf
CS	Certification Specification
DAL	Development Assurance Level
EASA	European Aviation Safety Agency
ECMP	Electronic Component Management Process
EEE	Electrical, Electronic, and Electromechanical
EPRI	Electric Power Research Institute
EUROCAE	European Organization for Civil Aviation Equipment
LRU	Line Replaceable Unit
NQA	Nuclear Quality Assurance
OACI	Organización de Aviación Civil Internacional
PLD	Programmable Logic Device
QA	Quality Assurance
RCA	Root Cause Analysis
RTCA	Radio Technical Commission for Aeronautics
SPC	Statistical Process Control
TR	Technical Report

Capítulo 1

Introducción

1.1. ¿Qué son los COTS?

La palabra COTS es una sigla que proviene de la expresión inglesa *Commercial Off-The-Shelf*, que traducido literalmente significa Componente Comercial Salido del Estante. Este término hace referencia a aquellos componentes disponibles en el mercado general que no han sido diseñados para una aplicación en concreto. Esta clasificación engloba a una amplia gama de productos, desde componentes mecánicos hasta eléctricos o electrónicos, incluyendo también hardware y software.

Los COTS son componentes destinados al público general, por lo que en un contexto de libre mercado la competencia entre las empresas es elevada. Esto provoca que los fabricantes continuamente estén tratando de optimizar sus procesos de producción, con el objetivo de reducir costes y bajar los precios. Para ello, los componentes son producidos en grandes cantidades y su diseño cambia rápidamente, buscando adaptarse siempre a la última tecnología disponible en el mercado.

Para industrias como la aeroespacial, estos componentes son muy atractivos por su bajo coste y su rápida disponibilidad, además de estar muy avanzados tecnológicamente. No obstante, los altos requisitos de seguridad de la industria suponen, a priori, una barrera de entrada difícil de superar para este tipo de productos. Además, la continua evolución a la que están sometidos puede suponer un problema de obsolescencia, ya que la nueva versión del componente puede ser mejor, pero en todo caso será diferente.

1.2. Justificación del trabajo

Nucleonova es una empresa de ingeniería ubicada en Valencia, focalizada en la aportación de valor a la Industria Nuclear, dando soluciones a los distintos retos a los que se enfrentan sus Clientes.

Nucleonova está especializada en la Ingeniería de Aprovisionamiento, donde se da respuesta a las distintas situaciones planteadas en la gestión de repuestos, obsolescencia y adquisición de equipos, componentes y repuestos. Para ello, ofrece servicios tales como la búsqueda y análisis de equipos equivalentes, gestión de compras, definición de especificaciones técnicas de compra, análisis e interpretación de los requisitos o Calificación de Equipos [1].

Durante mi estancia en Nucleonova, he adquirido conocimientos en varios campos, desde el funcionamiento de los sistemas de calidad de la Industria Nuclear hasta las labores de un agente de compras o la metodología del Proceso de Dedicación de Componentes de Grado Comercial.

Dentro de la Industria Nuclear, la obsolescencia de los equipos es un problema que está a la orden del día. Una de las soluciones más extendidas dentro de la industria consiste en la Dedicación de Componentes de Grado Comercial. A través del Proceso de Dedicación, se abre la posibilidad de utilizar Componentes de Grado Comercial en aplicaciones relacionadas con la seguridad, como si se tratara de Componentes Básicos.

La justificación de este trabajo pasa por analizar el concepto de COTS, la metodología empleada dentro de la Industria Nuclear para ponerlo en práctica a cabo y la posibilidad de adaptar esta metodología a los procesos de la Industria Aeroespacial.

1.3. Objetivos

Los COTS presentan una serie de ventajas que hacen atractivo su uso dentro de industrias como la aeroespacial. Sin embargo, para poder aprovechar todas estas ventajas es necesario darle solución a los inconvenientes asociados a este tipo de componentes.

Este trabajo tiene por objetivo general analizar los problemas que entrañan los COTS y proporcionar las soluciones necesarias que permitan implantar esta tecnología dentro de la Industria Aeroespacial. Para cumplir este objetivo, se han de cumplir una serie de objetivos específicos, presentados a continuación:

- Definir el concepto de seguridad y los conceptos asociados (cultura de la seguridad, *safety critical requirements* o nivel de seguridad) y ver qué implicaciones tienen dentro de la Industria Aeroespacial.
- Definir el concepto *Commercial Off-The-Shelf* y analizar la relación que tiene con la seguridad y los conceptos asociados.
- Estudiar la forma que tienen otras industrias con altos requisitos de seguridad (como la Industria Nuclear) de incorporar componentes comerciales en aplicaciones relacionadas con la seguridad, analizando las normas que regulan esta práctica y la metodología empleada.
- Analizar la normativa existente dentro de la Industria Aeroespacial encargada de regular el uso de componentes COTS en aplicaciones relacionadas con la seguridad.
- Comparar las metodologías existentes en las distintas industrias, estudiando los puntos comunes y las diferencias existentes entre ambos planteamientos.
- Plantear un procedimiento para la certificación de componentes COTS, apoyándose en las guías existentes en la bibliografía y dando solución a los puntos que queden en el aire.

Capítulo 2

Seguridad

2.1. ¿Qué es la seguridad?

La Real Academia Española define el término seguridad como *"cualidad de seguro"* [2]. Por otra parte, el término seguro se define como *"libre y exento de riesgo"* [3]. Es decir, que la seguridad es la cualidad de algo libre y exento de riesgo. Esta definición es coherente con el concepto que tienen las personas sobre la seguridad, y en teoría es correcto. Sin embargo, en la práctica, esta definición del concepto de seguridad no es del todo precisa.

En el mundo de la ingeniería, es imposible asegurar que algo está libre y exento de riesgo. Por muy pequeña que sea, siempre existe la posibilidad que que un sistema falle. Es decir, siempre va a haber riesgos. En la práctica, no todos los riesgos tienen la misma importancia, y los esfuerzos por mitigarlos han de centrarse en aquellos que tengan las consecuencias más graves. De todas formas, por muy grande que sea el esfuerzo realizado, siempre va a existir una posibilidad de que el riesgo se materialice, por lo que habrá que estar preparado para asumir sus consecuencias.

Teniendo en cuenta esto, es necesario definir un concepto relacionado con la seguridad y muy extendido dentro de la Industria Aeroespacial: la seguridad operacional o *safety*. La Organización de Aviación Civil Internacional (OACI) define el término seguridad operacional (de aquí en adelante seguridad) como el *"estado en el que los riesgos asociados a las actividades relacionadas con la operación de aeronaves son reducidos y controlados hasta un nivel aceptable"* [4]. Esta definición, a diferencia de la primera, no habla de libre y exento de riesgo, sino que habla de controlar y reducir el riesgo hasta un nivel aceptable. Pero, ¿qué es un nivel aceptable de seguridad?

2.2. El nivel de seguridad

El nivel de seguridad es un concepto fundamental en relación al cumplimiento de las normas. Es necesario establecer un equilibrio entre los requisitos exigidos y las posibilidades reales de garantizar su cumplimiento. La emisión de normas muy restrictivas puede parecer tentador a ojos de los organismos reguladores, pero esto podría hacer que la certificación de una aeronave se volviera imposible, técnica o económicamente hablando.

El aumento de la seguridad está relacionado con un aumento de los costes, que a su vez están relacionados con la severidad de las normas. No obstante, la relación existente entre el nivel de seguridad y los costes sigue una tendencia exponencial: llegados a cierto punto, un ligero aumento de la seguridad supone un aumento de los costes tan grande que no es rentable llevarlo a cabo.

Como regla general, a la hora de establecer los requisitos de aeronavegabilidad, una propuesta debe ser económicamente razonable, tecnológicamente factible y adecuada para el tipo de aeronave en cuestión. No se pueden exigir los mismos requisitos a una aeronave de recreo que a una gran aeronave de transporte de pasajeros [5].

En la Figura 2.1 se muestra una gráfica que relaciona el aumento de seguridad con los costes asociados a la severidad de las normas. Existen dos zonas claramente diferenciadas: la zona practicable, en la que el aumento de la seguridad no supone un gran coste; y la zona no practicable, en la que una gran inversión económica apenas supone un ligero aumento de la seguridad.

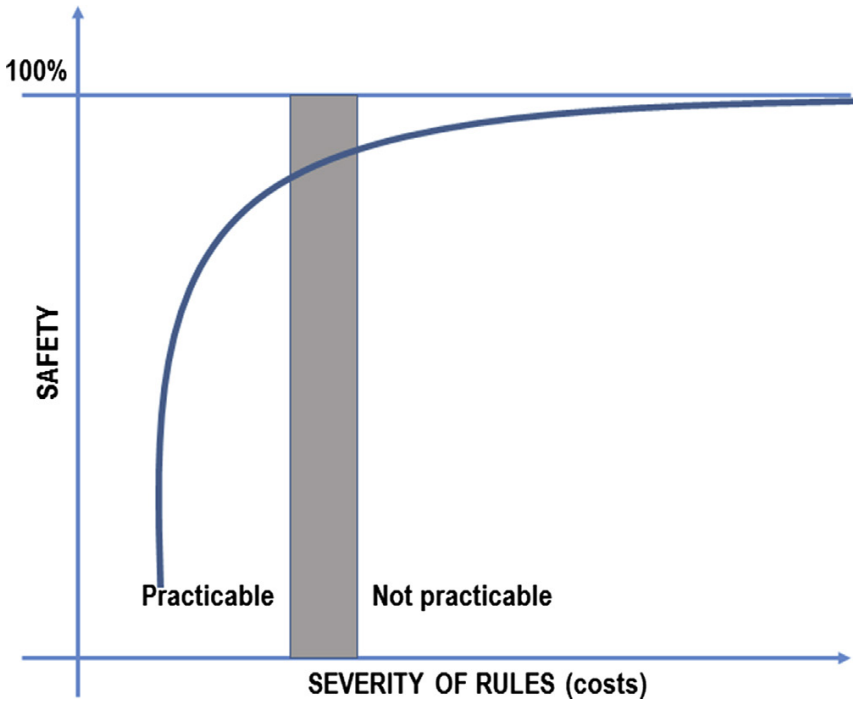

Figura 2.1: Seguridad frente a coste (severidad de las normas) [5]

En las industrias con altos requisitos de seguridad, como la Industria Aeroespacial, las condiciones de fallo de un componente o sistema se clasifican por rangos, de más leve a más grave, mientras que las probabilidades de que un componente o sistema falle se clasifican de igual manera, de probable a extremadamente improbable. Dentro de la bibliografía existen múltiples definiciones y clasificaciones, pero el concepto siempre es el mismo.

Un nivel de seguridad aceptable trata de buscar un punto de equilibro, en el que la gravedad de los fallos se compense con la probabilidad de que estos se produzcan. De esta forma, un fallo sin consecuencias graves para la aeronavegabilidad podrá ser tolerable, y su probabilidad de ocurrencia moderada. Mientras tanto, la probabilidad de que un fallo de consecuencias catastróficas se produzca debe ser reducida al mínimo. Adicionalmente, para este tipo de fallos se han de desarrollar estrategias de mitigación de tal forma que, aunque el fallo se produzca, las consecuencias sean minimizadas.

En la Figura 2.2 se muestra una gráfica que relaciona la gravedad de los fallos con la probabilidad de ocurrencia de cada uno. En el eje horizontal se representa la gravedad de los fallos (de menor a catastrófico), mientras que en el eje vertical se representa la probabilidad de ocurrencia de cada uno de ellos (de probable a extremadamente improbable).

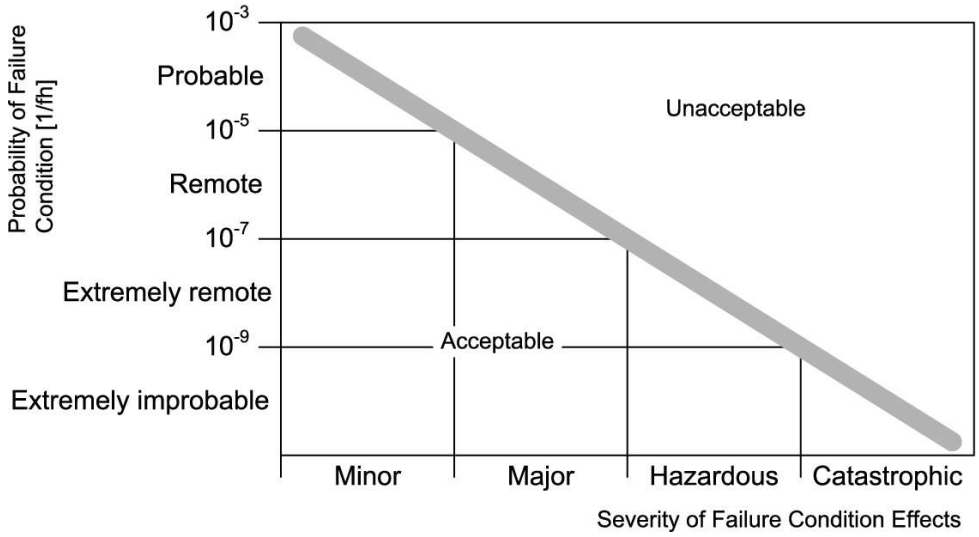

Figura 2.2: Probabilidad frente a gravedad de los fallos [6]

2.3. La cultura de la seguridad

En las industrias en las que la seguridad es crucial (Aeroespacial, Nuclear, Automoción, etcétera) es necesario que todos los miembros de la cadena productiva sean conscientes de ello y se impliquen activamente para lograrlo. Es por ello que en todas estas industrias existe un concepto muy importante relacionado con la seguridad y fundamental para su cumplimiento: la cultura de la seguridad.

La cultura de la seguridad se define como un *"conjunto de valores, conductas y actitudes prolongadas en el tiempo, relativas a los asuntos de seguridad y compartidas por los miembros de una organización a todos los niveles"* [7].

Una cultura de la seguridad positiva implica que:

- Cada individuo es consciente de los peligros y riesgos que suponen las actividades que desarrolla.
- Al ser conscientes de los riesgos, los individuos velan por preservar y mejorar la seguridad.
- Para ello, los individuos emplean todos los recursos a su alcance para llevar a cabo las actividades relacionadas con la seguridad.
- Con la formación adecuada, los individuos son capaces de adaptarse cuando se enfrentan a cuestiones de seguridad.
- Los individuos tienen la capacidad suficiente para comunicar la información relacionada con la seguridad.
- Los individuos evalúan consistentemente el comportamiento y el funcionamiento de la organización en temas de seguridad.

Un aspecto clave para alcanzar y mantener una cultura de seguridad positiva reside en la confianza entre todos los estamentos de la organización. Esta confianza ha de ser establecida y fomentada desde los niveles más altos. Es necesario recalcar que la cultura de seguridad no es algo rígido, sino que puede evolucionar y adaptarse al entorno.

2.4. Los requisitos críticos de seguridad y su relación con los COTS

Los requisitos críticos de seguridad (*safety critical requirements*) son un conjunto de normas y requisitos propios de las industrias con altos estándares de seguridad. Estos requisitos tienen el objetivo de que los sistemas críticos de la aeronave funcionen de forma adecuada incluso en condiciones de fallo, y que permitan a la aeronave volver a una condición de operación normal cuando se produce un fallo.

Estos requisitos están relacionados con algunos conceptos ya mencionados y muy extendidos dentro de la Industria Aeroespacial, como normativa de seguridad, certificación, redundancia de equipos y sistemas, diseño seguro, seguridad operacional o mantenimiento continuado. Los sistemas que cuentan con este tipo de requisitos son aquellos relacionados con la seguridad, y la mayor parte de la normativa en materia de aeronavegabilidad se centra en garantizar el buen funcionamiento de estos sistemas.

Cuando se habla de requisitos críticos de seguridad, el primer impulso es pensar componentes o sistemas muy sofisticados, con un proceso de diseño muy complejo, que han sido sometidos a rigurosas pruebas y controles de calidad para certificar su validez y garantizar la operación segura de la aeronave. Sin embargo, la experiencia ha demostrado que es posible satisfacer estos requisitos utilizando componentes que no han sido diseñados específicamente para ello.

Como se ha mencionado en el Capítulo 1, el término COTS hace referencia a aquellos componentes disponibles en el mercado general que no han sido diseñados para una aplicación en concreto. Este concepto tiene mucho sentido y se utiliza en industrias con altos requisitos de seguridad, como la Industria Aeroespacial, la Industria Nuclear o la Industria Militar.

El uso de componentes comerciales en la Industria Militar se remonta al año 1994, cuando el Secretario de Defensa de los Estados Unidos, William James Perry, introdujo este concepto con la publicación de un Memorando en el que se autoriza e incentiva el uso de componentes comerciales Eléctricos, Electrónicos y Electromecánicos (EEE) en aplicaciones militares [8].

Los componentes utilizados en aplicaciones militares han de cumplir con los requisitos críticos de seguridad. Por este motivo, estos componentes son diseñados con el objetivo de riesgo cero. Para ello, son sometidos a pruebas exhaustivas para garantizar la calidad de las piezas fabricadas. Debido a esto, el volumen de producción es reducido, ya que la totalidad del proceso implica costes muy elevados [9].

Por el contrario, los componentes comerciales cuentan con menos requisitos a la hora del diseño. Es por ello que esta metodología destina más recursos en gestionar los riesgos potenciales, en lugar de centrarse en que estos desaparezcan por completo. Para ello, emplea el Control Estadístico de Procesos (SPC), con el objetivo de obtener una alta fiabilidad en los componentes fabricados. Para que esta metodología alcance buenos

resultados, es necesario tener un volumen de producción elevado. La suma de estos aspectos hace que el coste del proceso de producción se reduzca, por lo que el precio de estos componentes es menor [9].

En la Tabla 2.1 se muestran las principales diferencias entre los componentes diseñados para la Industria Militar y los componentes comerciales.

Componentes militares	**Componentes comerciales**
Riesgo cero	Gestión del riesgo
Pruebas exhaustivas	Control Estadístico de Procesos
Volumen reducido	Alto volumen

Tabla 2.1: Componentes militares frente a componentes comerciales

El uso de componentes COTS en la Industria Aeroespacial es muy atractivo, principalmente por dos motivos: el bajo coste que estos componentes suponen y su rápida disponibilidad. En primer lugar, el gran volumen de producción permite una reducción del precio de los componentes, tal y como se ha comentado en los párrafos anteriores. En segundo lugar, el hecho de que se puedan adquirir los componentes en el mercado general, elimina la necesidad de diseñarlos, por lo que el proceso de diseño desaparece y es sustituido por un proceso de aprovisionamiento, ahorrando grandes intervalos de tiempo. Adicionalmente, otra gran ventaja que puede no ser evidente a primera vista, es que estos componentes cuentan con la tecnología más avanzada en el momento de salir al mercado, tratando siempre de ser la opción más puntera para afrontar la pugna con la competencia.

Sin embargo, no son todo ventajas a la hora de utilizar componentes comerciales en aplicaciones relacionadas con la seguridad. Siguiendo la línea de lo comentado anteriormente, estos componentes no han sido diseñados específicamente para una aplicación en concreto, por lo que lo normal es que durante el proceso de diseño no se hayan tenido en cuenta los requisitos requeridos. Por este motivo, es necesario realizar actividades adicionales de verificación para certificar que los componentes adquiridos cumplen con los requisitos que se les exigen.

Por otra parte, el hecho de que haya una gran competencia en el mercado hace que estos componentes estén en continuo desarrollo, evolucionando e introduciendo mejoras constantemente. Esto supone un problema con el que hay que lidiar, ya que son componentes técnicamente mejores pero en el fondo distintos.

Por último, a diferencia de los componentes que son diseñados específicamente para una aplicación en concreto, para introducir componentes comerciales en un diseño hay que adaptarse a ellos, utilizándolos tal y como son.

En la Tabla 2.2 se muestra un resumen de las ventajas e inconvenientes que presenta el uso de componentes comerciales en aplicaciones relacionadas con la seguridad.

Ventajas	**Inconvenientes**
Bajo coste	Diseño no específico
Rápida disponibilidad	Continuo cambio
Tecnología punta	Necesidad de adaptación

Tabla 2.2: Ventajas e inconvenientes que presenta el uso de COTS

Para poder poner en práctica este concepto es necesario dar solución a todos los problemas que se plantean. Afortunadamente, la mayoría de las industrias han ido planteando soluciones a estos problemas. Estas soluciones suelen ser convergentes, ya que unas aprenden de los errores de las otras y el proceso es realimentado de forma continua. En los siguientes Capítulos se hará un repaso de las formas que han encontrado las diferentes industrias de dar solución a estos problemas, presentando la metodología empleada por cada una de ellas.

Capítulo 3

El uso de COTS en la Industria Nuclear

3.1. Introducción

La Industria Nuclear es una de las más estrictas en lo que a temas de seguridad se refiere. Los sistemas que intervienen en la generación de energía en las centrales nucleares están sometidos a condiciones extremas, en las cuales el mínimo fallo puede desencadenar consecuencias catastróficas. En el ámbito regulador, existe una extensa colección de normas y procedimientos desarrollados para garantizar la operación segura de las centrales nucleares durante toda su vida útil.

A pesar de ello, la Industria Nuclear ha incluido el uso de COTS dentro de sus actividades de diseño y mantenimiento. En este caso, el Instituto de Investigación de la Energía Eléctrica (EPRI) es la organización encargada de regular y asegurar un uso seguro de esta tecnología. Dentro de la Industria Nuclear, se utiliza el término *Commercial Grade Item* (CGI) para referirse a los componentes comerciales.

EPRI define el término Componente de Grado Comercial como una *"estructura, sistema o componente que afecta a una función de seguridad, que no ha sido diseñado como componente básico nuclear"* [10]. Estos artículos no incluyen aquellos cuyo diseño o proceso de fabricación ha requerido inspecciones o verificaciones para garantizar la no presencia de defectos o incumplimientos durante el proceso. A la hora de poner en práctica el concepto, un Componente de Grado Comercial es todo aquel que no ha sido diseñado como Componente Básico.

En los siguientes apartados se hará una revisión del Proceso de Dedicación definido en la EPRI NP-5652 & TR-102260 Rev. 1, "Ingeniería de Planta: Directrices para la Aceptación de Componentes de Grado Comercial en Aplicaciones Nucleares Relacionadas con la Seguridad" [10].

3.2. El Proceso de Dedicación

Tras la puesta en marcha de los primeros reactores nucleares en Estados Unidos, muchos proveedores abandonaron su programa de Garantía de Calidad (QA), a medida que la Industria Nuclear pasaba de grandes compras de equipos con la construcción de las nuevas centrales a compras mucho más pequeñas de repuestos para prestar apoyo a las operaciones y el mantenimiento. Dentro de este contexto, surge la necesidad de dar solución a la baja disponibilidad de componentes de clase nuclear y a la obsolescencia de los equipos.

El Proceso de Dedicación fue desarrollado originalmente como medio alternativo para aceptar componentes de proveedores nucleares que abandonaron su programa de Garantía de Calidad. Actualmente, el Proceso de Dedicación es utilizado en cada vez más aplicaciones, desde la operación y mantenimiento de los reactores en funcionamiento hasta la construcción de nuevas centrales nucleares. Tanto es así, que esta metodología ha sido incorporada en algunos estándares de calidad, como el NQA-1 de la Sociedad Americana de Ingenieros Mecánicos (ASME) [11].

La Dedicación de Componentes de Grado Comercial (CGID) es un proceso de aceptación diseñado con el objetivo de aportar garantías razonables de que los componentes de grado comercial pueden ser utilizados en aplicaciones relacionadas con la seguridad, y que estos cumplirán los mismos estándares de calidad y fiabilidad que los componentes básicos nucleares desarrollados según CFR10 [12].

Para poder comprender el proceso de Dedicación, es necesario definir una serie de conceptos básicos que son fundamentales para entender esta metodología: las características críticas y las garantías razonables.

Una característica crítica es *"cualquier característica importante relacionada con el diseño, el material o el funcionamiento de un Componente de Grado Comercial que, una vez verificada, proporcionará una garantía razonable de que el componente desempeñará correctamente su función de seguridad"* [10].

En el contexto de la aceptación de Componentes de Grado Comercial, una garantía razonable es una *"determinación técnica basada en un nivel de confianza justificable a partir de hechos medibles, acciones u observaciones objetivas de los que se puede inferir la idoneidad del componente para la función prevista"* [10].

El Proceso de Dedicación involucra dos elementos clave, la Evaluación Técnica y el Proceso de Aceptación. Técnicamente, un Componente de Grado Comercial Dedicado es equivalente a un Componente Básico según 10CFR50 Apéndice B. En la Figura 3.1 se muestran los elementos clave involucrados en el Proceso de Dedicación.

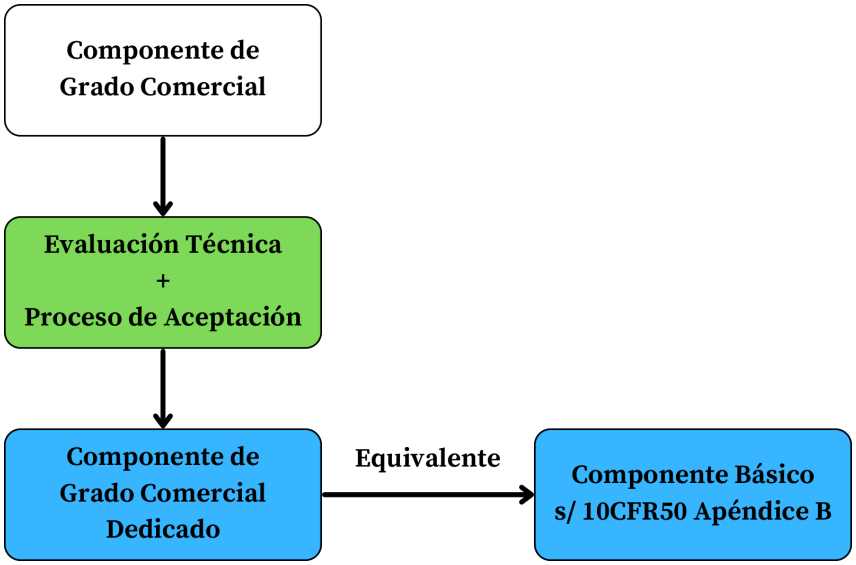

Figura 3.1: Elementos clave del Proceso de Dedicación

La primera parte del Proceso de Dedicación consiste en la Evaluación Técnica. La Evaluación Técnica generalmente está formada por los siguientes puntos:

- Clasificación de seguridad. En función de su relación con la seguridad, un componente puede ser relacionado con la seguridad, no relacionado con la seguridad o no relacionado con la seguridad pero de calidad aumentada.
- Evaluación de equivalencia. Será necesaria para garantizar la idoneidad de un componente alternativo.
- Identificación de los requisitos técnicos y de calidad.
- Identificación de las Características Críticas, Criterios de Aceptación y Métodos de Aceptación, y elaboración de un Plan de Aceptación para el uso de Componentes de Grado Comercial en aplicaciones relacionadas con la seguridad.

La segunda parte del Proceso de Dedicación es el Proceso de Aceptación. La función del Proceso de Aceptación es consiste en proporcionar una garantía razonable de que el componente suministrado cumple con los requisitos especificados y es capaz de realizar su función de seguridad de forma correcta. La verificación de las Características Críticas ha de ser realizada utilizando uno de los siguientes Métodos de Aceptación:

- Método 1: Pruebas e inspecciones.
- Método 2: Inspección de grado comercial.
- Método 3: Verificación de la fuente.
- Método 4: Historial del proveedor/componente.

Previamente a la adquisición de un Componente de Grado Comercial, es necesario realizar una evaluación del componente en cuestión, siguiendo el esquema mostrado en la Figura 3.2.

En primer lugar, hay que analizar si la función que realiza el componente está o no relacionada con la seguridad. Si la respuesta es afirmativa, es necesario comprobar si el componente puede ser adquirido como Componente Básico según 10CFR50 Apéndice B. Por último, si esto no es posible se han de activar los mecanismos necesarios para adquirir el Componente en Grado Comercial. Todo este proceso forma parte de la Evaluación Técnica y por tanto está incluido dentro del Proceso de Dedicación.

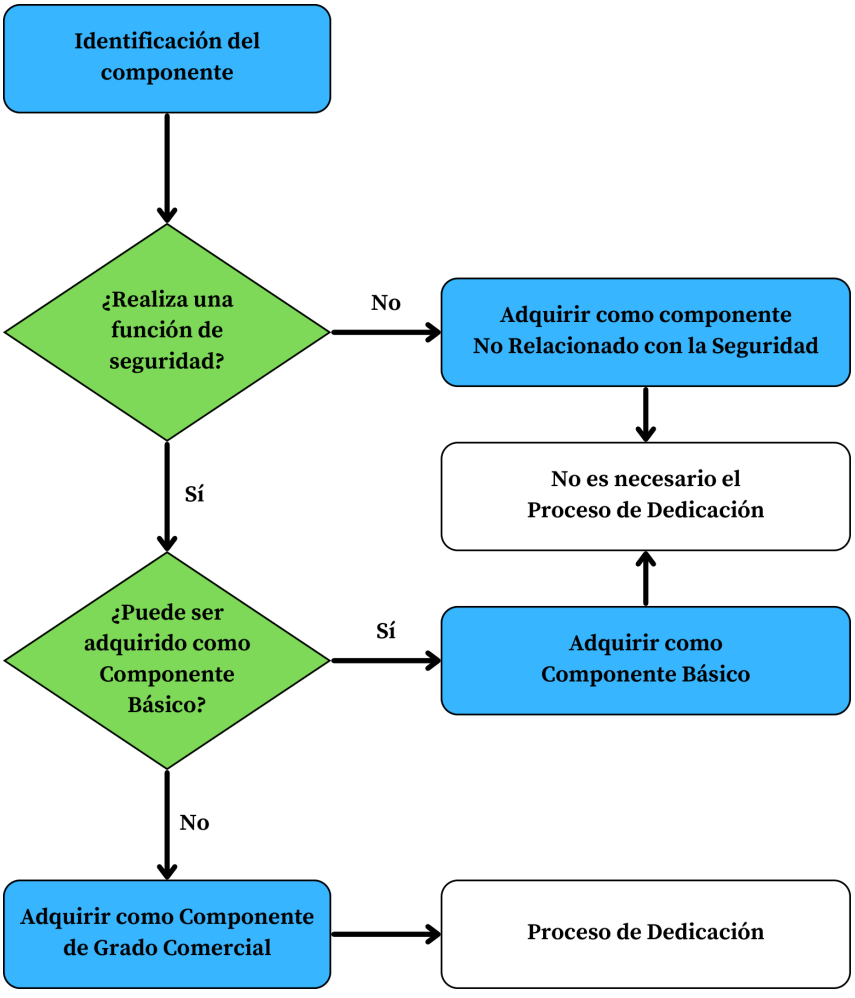

Figura 3.2: Esquema de un Proceso de Dedicación

En los siguientes apartados se tratarán en profundidad los pasos a seguir para llevar a cabo el Proceso de Dedicación. En el Apartado 3.3 se hablará sobre los pasos que involucra la Evaluación Técnica. En el Apartado 3.4 se hablará sobre los pasos que forman parte del Proceso de Aceptación. Por último, en el Apartado 3.5 se analizarán los diferentes Métodos de Aceptación existentes.

3.3. Evaluación Técnica

El Proceso de Dedicación está compuesto de una Evaluación Técnica y un Proceso de Aceptación, tal y como se ha introducido en el Apartado 3.2. En función del componente a dedicar, los pasos a seguir pueden variar, pero la metodología sigue siendo la misma.

El Proceso de Dedicación contiene algunos pasos que son comunes a la Evaluación Técnica y al Proceso de Aceptación. Sin embargo, para simplificar su comprensión, las dos partes serán tratadas en apartados diferentes.

En la Figura 3.3 se muestra un esquema con los pasos a seguir para llevar a cabo la Evaluación Técnica. Estos serán tratados en profundidad a lo largo de este apartado.

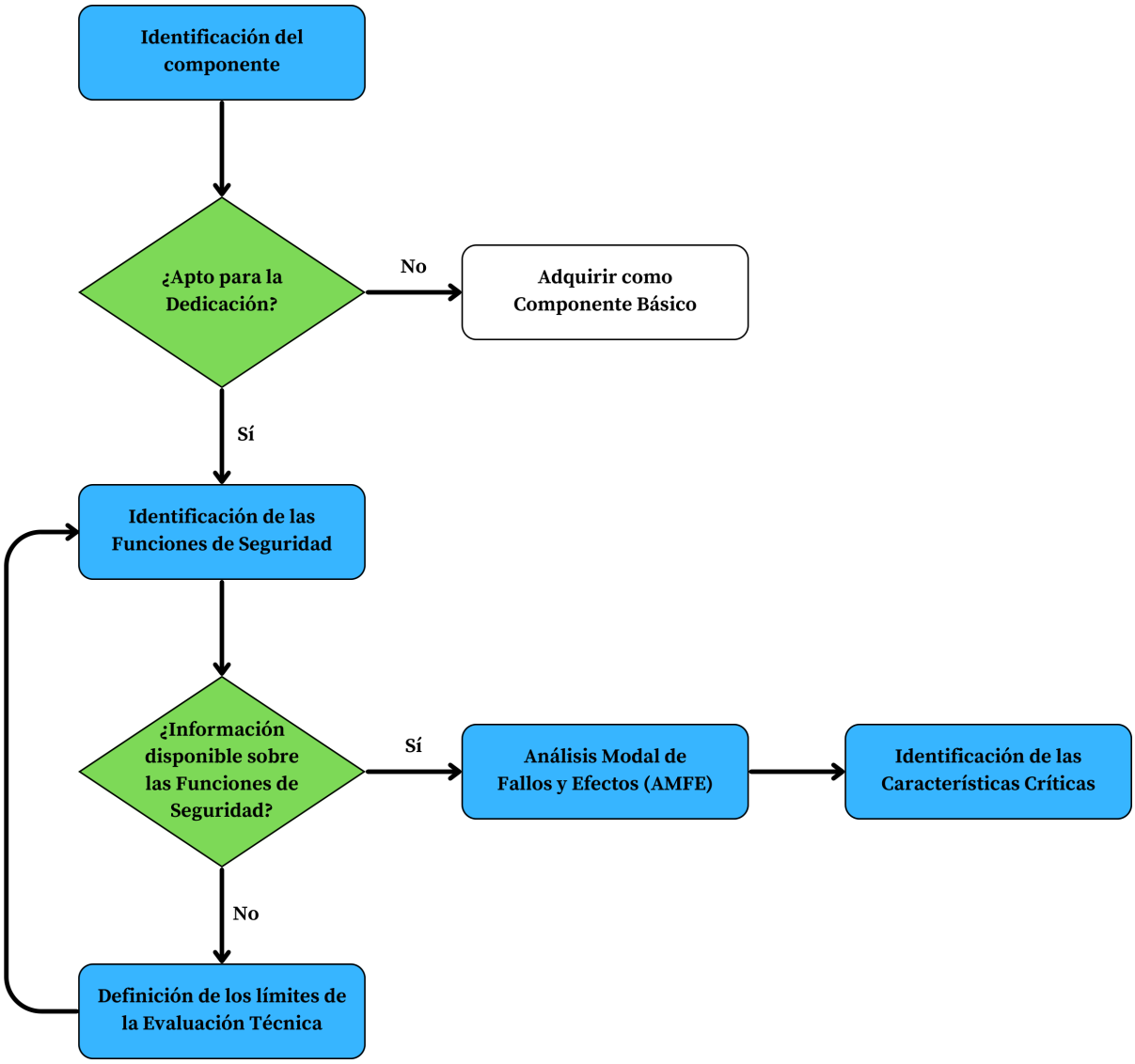

Figura 3.3: Evaluación Técnica

3.3.1. Identificar el componente para su adquisición

Los componentes candidatos han de ser componentes relacionados con la seguridad destinados a ser utilizados como Componentes Básicos. Este proceso puede realizarse durante la revisión de nuevas solicitudes de compra o solicitudes de repuesto.

La identificación de componentes normalmente implica una búsqueda para determinar si el componente puede ser suministrado como componente básico por un proveedor con un programa de garantía de calidad que cumpla los requisitos del Apéndice B de 10CFR50 [12]. Cuando un componente destinado a ser utilizado como tal no está disponible como Componente Básico, inmediatamente pasa a ser candidato para su adquisición como Componente de Grado Comercial.

3.3.2. Determinar si el componente es apto para la Dedicación

Existen ciertas normativas y requisitos que impiden que ciertos componentes sean aceptados mediante el Proceso de Dedicación. Si el componente no es apto, deberá ser adquirido como Componente Básico controlado de acuerdo al programa de garantía de calidad recogido en el Apéndice B de 10CFR50 [12].

Si el componente **NO** se diseña como componente básico exclusivo para centrales nucleares, **NO** se fabrica como componente básico exclusivo de instalaciones nucleares y **NO** se requieren inspecciones y verificaciones en el proceso de diseño y fabricación para detectar fallos y defectos que impidan al elemento realizar la función de seguridad, el componente es apto para el proceso de Dedicación. Si alguna de las sentencias anteriores no se cumple, el componente no es apto para el proceso de Dedicación.

3.3.3. Identificar las Funciones de Seguridad

Este paso es fundamental para la selección de las Características Críticas del componente. Para ello, es necesario identificar la aplicación de destino del componente y las funciones de seguridad asociadas, y documentar todo ello durante la Evaluación Técnica.

Si la aplicación de destino del componente es conocida, entonces se deben determinar las funciones de seguridad del componente. Si el componente no tiene funciones de seguridad, este deberá ser adquirido en grado comercial. Si tiene funciones de seguridad, estas han de ser documentadas correctamente. Si la aplicación de destino del componente es desconocida, han de definirse claramente los límites de la Evaluación Técnica.

3.3.4. Realizar un Análisis Modal de Fallos y Efectos

A partir de las funciones de seguridad, documentadas en el punto anterior, se obtienen los modos de fallo del componente. Los efectos de los modos de fallo son utilizados para seleccionar las Características Críticas del componente a verificar.

El Análisis Modal de Fallos y Efectos puede ser usado para identificar algunas Características Críticas, sobre todo en aquellos casos en los que la información de diseño del componente no está disponible. Tras determinar los modos de fallo, las Características Críticas a verificar quedan determinadas.

3.3.5. Identificar las Características Críticas

Para ello, se ha de recurrir a la información de diseño del componente y a las conclusiones obtenidas del Análisis Modal de Fallos y Efectos. Con esta información, se han de identificar aquellas características que, una vez verificadas, aporten garantías razonables de que el componente en cuestión realizará de forma correcta su función de seguridad.

La metodología utilizada para identificar las Características Críticas puede variar en función de la información disponible. Se pueden utilizar dos métodos básicos: el primero tiene en cuenta las aplicaciones de destino de los componentes, sus funciones de seguridad y el Análisis Modal de Fallos y Efectos para identificar las Características Críticas cuando no está disponible la información de diseño; el segundo método puede utilizarse cuando la información de diseño es suficiente para identificar y utilizar los requisitos de diseño como base para identificar las Características Críticas.

3.3.6. Definir los límites de la Evaluación Técnica

En aquellos casos en los que no se disponga de información suficiente sobre la aplicación de destino o las funciones de seguridad del componente, se han de definir los límites de la Evaluación Técnica. Estos límites tienen como objetivo establecer claramente el alcance de la Evaluación Técnica, identificando las aplicaciones de destino del componente y las funciones de seguridad aplicables. Este enfoque es válido tanto para aplicaciones genéricas como específicas.

En primer lugar, es necesario recopilar toda la información de diseño y los requisitos disponibles. A continuación, se realiza un análisis de la información obtenida con el objetivo de determinar todas las posibles aplicaciones de destino y funciones de seguridad del componente. Cuando la información recopilada es insuficiente, será necesario solicitar al proveedor los datos necesarios para completar la Evaluación Técnica. Si no es posible determinar las aplicaciones de destino y las funciones de seguridad, estas han de quedar definidas, determinando así el alcance real de la Dedicación.

3.4. Proceso de Aceptación

En la Figura 3.4 se muestra un esquema con los pasos a seguir para llevar a cabo el Proceso de Aceptación. Estos serán tratados en profundidad a lo largo de este apartado.

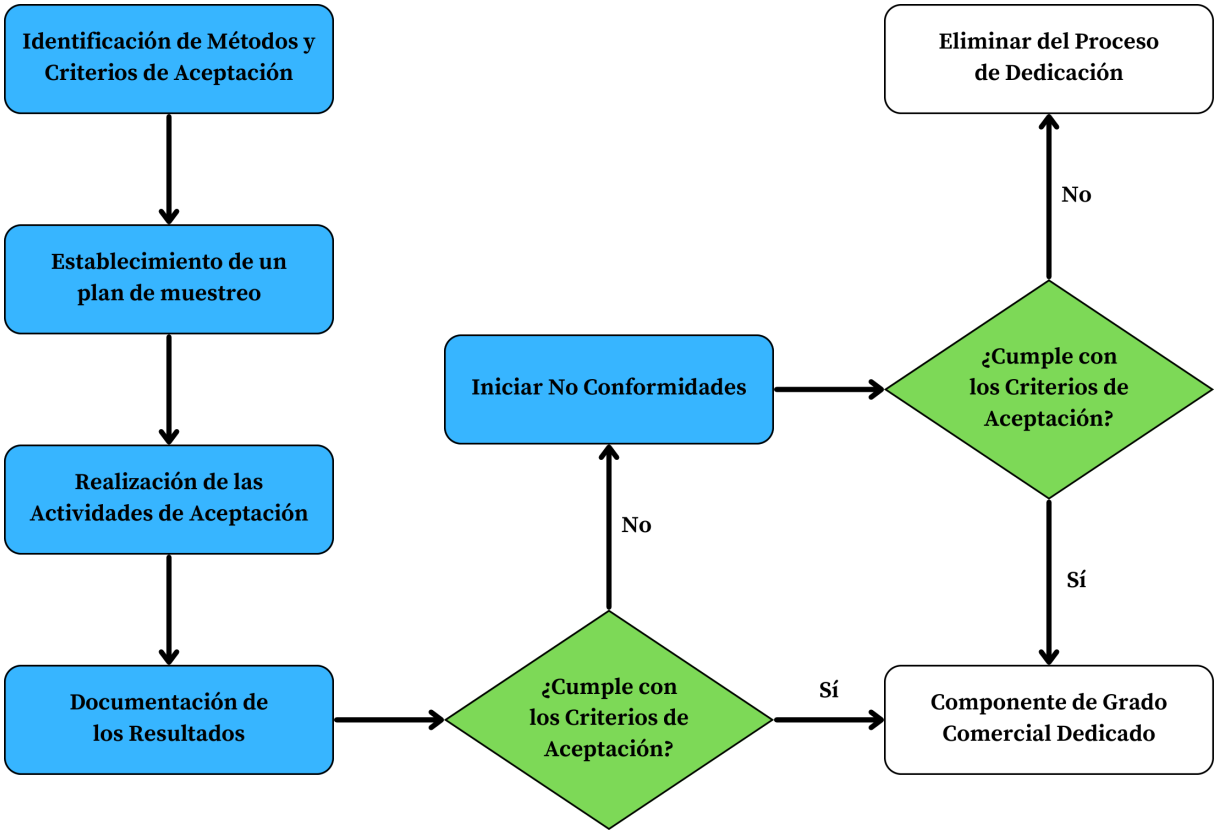

Figura 3.4: Proceso de Aceptación

3.4.1. Identificar los Métodos y Criterios de Aceptación

El siguiente paso consiste en identificar los Métodos y Criterios de Aceptación que serán utilizados para verificar las Características Críticas identificadas durante la Evaluación Técnica. En el Apartado 3.5 se analizan en profundidad cada uno de los Métodos de Aceptación existentes.

Normalmente, las Características Críticas se recogen en una lista o tabla junto con los Métodos y Criterios de Aceptación, de forma que se facilite su identificación. En función del Método de Aceptación elegido, las Características Críticas serán verificadas tras la recepción del componente (Método 1) o antes de esta (Métodos 2, 3 y 4).

3.4.2. Establecer un plan de muestreo

Se ha de establecer un plan de muestreo, siempre que sea posible. El muestreo es especialmente útil cuando se utiliza el Método 1 de Aceptación. De esta forma, puede evitarse el tener que realizar pruebas o inspecciones sobre la totalidad de los componentes.

Para aplicar un plan de muestreo a una Característica Crítica en concreto es necesario definir el lote de componentes que se va a considerar, determinar la homogeneidad del mismo y seleccionar un plan de muestreo coherente. La justificación de la aplicación de un plan de muestreo ha de ser documentada de forma precisa durante la Evaluación Técnica.

3.4.3. Realizar las Actividades de Aceptación

Se han de realizar las Actividades de Aceptación necesarias para verificar las Características Críticas del componente. En el Apartado 3.5 se analizan las actividades correspondientes a cada uno de los Métodos de Aceptación existentes.

Las Actividades de Aceptación no tienen por qué ser desarrolladas en su totalidad por la entidad solicitante. De hecho, esta puede subcontratar a una segunda entidad una parte de las actividades a realizar sobre un componente.

3.4.4. Documentar los resultados del Proceso de Aceptación

Una vez finalizadas las Actividades de Aceptación, se han de documentar los resultados obtenidos, proporcionando pruebas objetivas de las actividades realizadas. La documentación debe ser lo suficientemente completa como para que una persona que no haya participado en dichas actividades pueda verificar los resultados.

Los resultados suelen documentarse en un informe redactado por la entidad encargada de realizar las actividades. En dicho informe, han de aparecer los resultados de las actividades realizadas junto con los Criterios de Aceptación. Las resultados de las actividades que requieran el uso de equipos de medida calibrados han de reflejar el valor real de la medida tomada. Además, se ha de registrar la identificación del equipo de medida utilizado y la fecha de la próxima calibración.

Para poder aceptar un componente, todas las Actividades de Aceptación especificadas durante la Evaluación Técnica han de ser completadas de forma satisfactoria y los resultados de las actividades han de estar claramente identificados como aceptables o no aceptables.

3.4.5. Evaluar las posibles discrepancias existentes

Cuando un componente no cumple con alguno de los Criterios de Aceptación definidos durante la Evaluación Técnica, se han de evaluar las discrepancias existentes entre los resultados esperados y los resultados obtenidos. La causa de las discrepancias debe ser documentada con el objetivo de determinar si más componentes presentarán discrepancias similares en un futuro. Por norma general, esto no supone un problema cuando otros Componentes de Grado Comercial similares han sido sometidos a las mismas evaluaciones con anterioridad.

3.4.6. Iniciar No Conformidades

Cuando surge una discrepancia con algún componente, esta debe ser documentada. Los documentos en los que se recoge esta información se conocen como documentos de No Conformidad. Las causas de las No Conformidades pueden ser muy diversas y cada caso particular ha de ser analizado de forma independiente.

En algunos casos, las discrepancias existentes no son significativas y el componente puede ser aceptado tal y como está. En otros casos, se han de iniciar las acciones correctivas necesarias para garantizar que el componente cumple con los requisitos exigidos. Si con esto no es suficiente, se ha de solicitar la devolución del componente y su sustitución por otro nuevo.

En cualquier caso, la decisión tomada ha de ser justificable de forma objetiva y cualquier acción realizada ha de quedar debidamente documentada.

3.4.7. Eliminar del Proceso de Dedicación

Por último, en aquellos casos en los que el componente no pueda ser aceptado, este ha de ser eliminado del Proceso de Dedicación. En esta situación, se ha de iniciar de nuevo todo el proceso para poder ofrecer una alternativa al Cliente final.

3.5. Métodos de aceptación

3.5.1. Método 1: Pruebas e inspecciones

El primer Método de Aceptación consiste en la realización de pruebas e inspecciones durante la recepción del material (o después de esta) para verificar las Características Críticas del componente. Las inspecciones realizadas en planta una vez ha sido instalado el componente también forman parte de este Método de Aceptación.

Es necesario hacer una distinción entre las actividades realizadas durante la recepción del material y las llevadas a cabo para verificar las Características Críticas del componente. Por un lado, las inspecciones preliminares llevadas a cabo durante la recepción tienen como objetivo verificar atributos tales como el número de componentes recibidos, la ausencia de daños, la configuración general de los componentes, el número de serie, el modelo o la documentación entregada por el proveedor. Por otro lado, las pruebas e inspecciones son actividades adicionales cuyo objetivo es verificar que las Características Críticas del componente cumplen con los Criterios de Aceptación definidos durante la Evaluación Técnica.

Cuando hay suficiente información disponible (a través de fichas técnicas, catálogos, etcétera) y las Características Críticas del componente se pueden verificar mediante pruebas e inspecciones, el Método 1 de aceptación es susceptible de ser usado. Cuando no hay suficiente información disponible será necesario contactar con el suministrador para obtener información adicional, y si esto no es suficiente se ha de recurrir a otros Métodos de Aceptación.

A continuación se muestran una serie de supuestos en los que el Método 1 de aceptación sería el más apropiado:

- Los componentes no son suministrados por un único proveedor.
- Los componentes son relativamente sencillos.
- Los componentes pueden ser sometidos a pruebas o ensayos una vez han sido instalados.
- No hay evidencias de que las organizaciones participantes en la cadena de suministro tengan un sistema de calidad implantado, o este no aporta la confianza suficiente.
- Se han detectado incidencias durante la aplicación del Método 2, por lo que se recurre al Método 1 para despejar cualquier duda.
- Los componentes son adquiridos con frecuencia y en grandes cantidades.

Para poder utilizar el Método 1 de Aceptación se ha de elaborar previamente un documento donde se recojan los siguientes puntos:

- Las pruebas e inspecciones a realizar.
- Los métodos de ensayo y las técnicas de inspección, junto a los procedimientos de ensayo y las normas aplicables cuando así se requiera.
- Los Criterios de Aceptación definidos durante la Evaluación Técnica.
- La documentación requerida para la inspección y los resultados de los ensayos.

En la medida de lo posible, las pruebas e inspecciones serán realizadas siguiendo un plan de muestreo, que ha de ser justificado y documentado de forma correcta.

En la Figura 3.5 se muestra un diagrama de flujo, a modo de resumen, con los pasos a seguir a la hora de poner en práctica el Método 1 durante el Proceso de Aceptación.

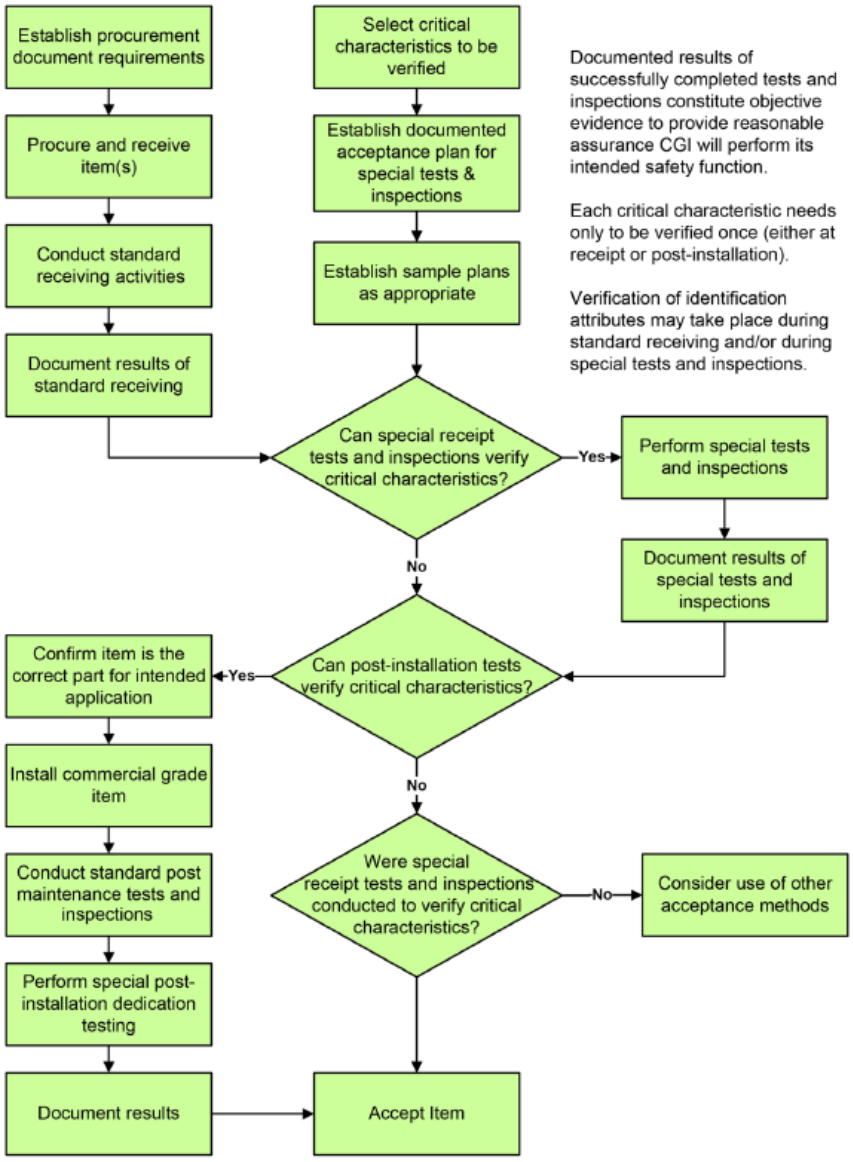

Figura 3.5: Método 1: Pruebas e inspecciones [10]

3.5.2. Método 2: Inspección de grado comercial

El segundo Método de Aceptación consiste en determinar si el suministrador lleva a cabo controles de calidad documentados sobre los Componentes de Grado Comercial, de tal forma que las Características Críticas definidas durante la Evaluación Técnica sean verificadas correctamente. Además, se ha de determinar si dichos controles son implementados de forma eficaz por el proveedor. Para llevar a cabo este Método de Aceptación se han de realizar inspecciones o auditorías.

Cuando el suministrador permite inspeccionar o auditar su sistema de calidad y este a su vez permite verificar las Características Críticas del componente, el Método 2 de Aceptación es susceptible de ser usado. Si mediante este método no es posible verificar una o más Características Críticas del componente, será necesario aplicar otro método para verificar las Características Críticas restantes.

A continuación se muestran una serie de supuestos en los que el Método 2 de Aceptación sería el más apropiado:

- Los componentes son suministrados por un único proveedor.
- La información técnica necesaria para la evaluación técnica y el plan de aceptación no puede ser facilitada por el suministrador.
- Un grupo de componentes es suministrado sistemáticamente por el mismo proveedor.
- El componente constituye un ensamblaje de muchas piezas.
- No es posible verificar las Características Críticas del componente mediante pruebas o inspecciones.

Para poder utilizar el Método 2 de Aceptación se han de cumplir dos requisitos básicos:

- Los controles de calidad del suministrador están correctamente documentados.
- Las Características Críticas del componente son controladas de forma adecuada.

Las inspecciones o auditorías han de ser adaptadas a cada caso particular, siendo el alcance de estas específico para cada Componente de Grado Comercial a suministrar.

En la Figura 3.6 se muestra un diagrama de flujo, a modo de resumen, con los pasos a seguir a la hora de poner en práctica el Método 2 durante el Proceso de Aceptación.

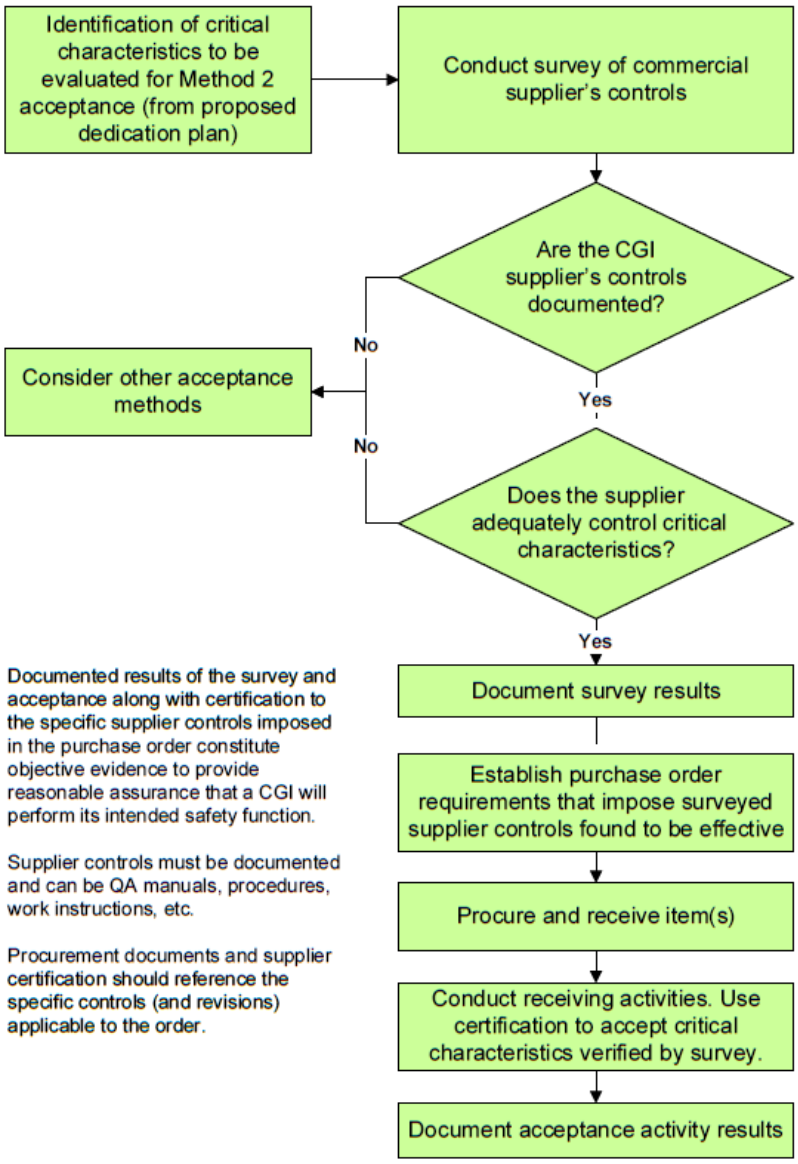

Figura 3.6: Método 2: Inspección de grado comercial [10]

3.5.3. Método 3: Verificación de la fuente

El tercer Método de Aceptación consiste en verificar las Características Críticas del componente de grado comercial en las instalaciones del fabricante. Este método incluye actividades tales como supervisar del proceso de fabricación, supervisar los controles de calidad, realizar pruebas e inspecciones o revisar la documentación del componente, entre otras.

A diferencia del Método 2, pensado para certificar a un proveedor para varios componentes o pedidos, el Método 3 de Aceptación es susceptible de ser usado sólo en aquellos casos en los que se requiere la aceptación de un único componente o pedido.

A continuación se muestran una serie de supuestos en los que el Método 3 de aceptación sería el más apropiado:

- El suministrador no tiene un programa de garantía de calidad documentado que permita controlar las Características Críticas del componente de grado comercial.
- Se requiere dedicar un componente o un lote de componentes que no suelen ser adquiridos con frecuencia.
- El proceso de fabricación es complejo, por lo que las verificaciones posteriores no pueden proporcionar garantías razonables.

Para poder utilizar el Método 3 se ha de elaborar un plan en el que se identifiquen de forma clara las Características Críticas y los Criterios de Aceptación del Componente de Grado Comercial a verificar. Este plan se ha de elaborar durante la Evaluación Técnica y ha de contener, por lo menos, los siguientes puntos:

- El alcance del Método de Aceptación, en el que se identifiquen los componentes y las actividades a realizar para verificar cada una de las Características Críticas.
- Los equipos de medida, el personal o cualquier otro medio para realizar la verificación.
- Los Criterios de Aceptación de las actividades a realizar.
- Los puntos de parada en el proceso del fabricante.
- El orden en el que las actividades deben ser realizadas.

Las actividades de verificación han de ser discutidas con el fabricante durante la planificación para que confirme su disponibilidad para llevarlas a cabo.

En la Figura 3.7 se muestra un diagrama de flujo, a modo de resumen, con los pasos a seguir a la hora de poner en práctica el Método 3 durante el Proceso de Aceptación.

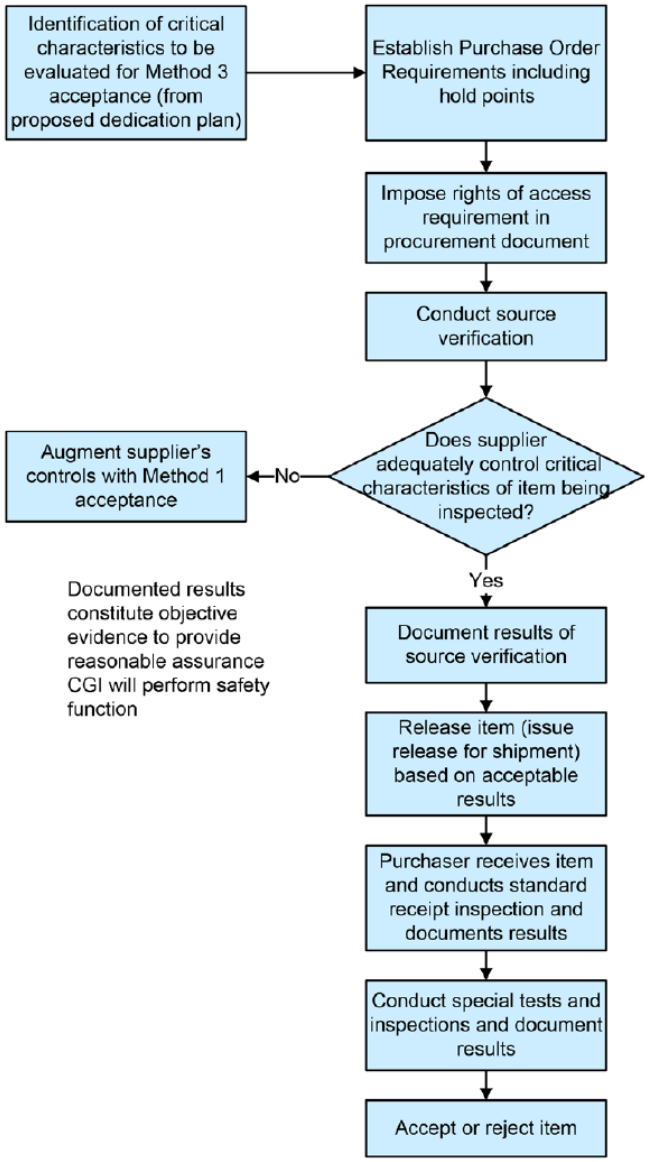

Figura 3.7: Método 3: Verificación de la fuente [10]

3.5.4. Método 4: Historial del proveedor/componente

El cuarto Método de Aceptación consiste en utilizar el desempeño histórico documentado de un proveedor para verificar las Características Críticas de un componente. Para ello, es necesario evaluar el historial del proveedor con componentes idénticos o similares.

Aunque inicialmente el Método 4 fue concebido para ser utilizado en solitario, la experiencia ha determinado que es mejor aplicarlo en dos situaciones: para reducir el plan de muestreo de una o más Características Críticas; o como Método de Aceptación para una característica crítica en particular.

A continuación se muestran una serie de supuestos en los que el Método 4 de aceptación sería el más apropiado:

- El desempeño histórico del proveedor está basado en datos que son aplicables directamente a las Características Críticas del componente relacionado con la seguridad.
- Los cambios realizados por el fabricante en el diseño, proceso de fabricación o similares han sido verificados por una auditoría.

En la Figura 3.8 se muestra un diagrama de flujo, a modo de resumen, con los pasos a seguir a la hora de poner en práctica el Método 4 durante el Proceso de Aceptación.

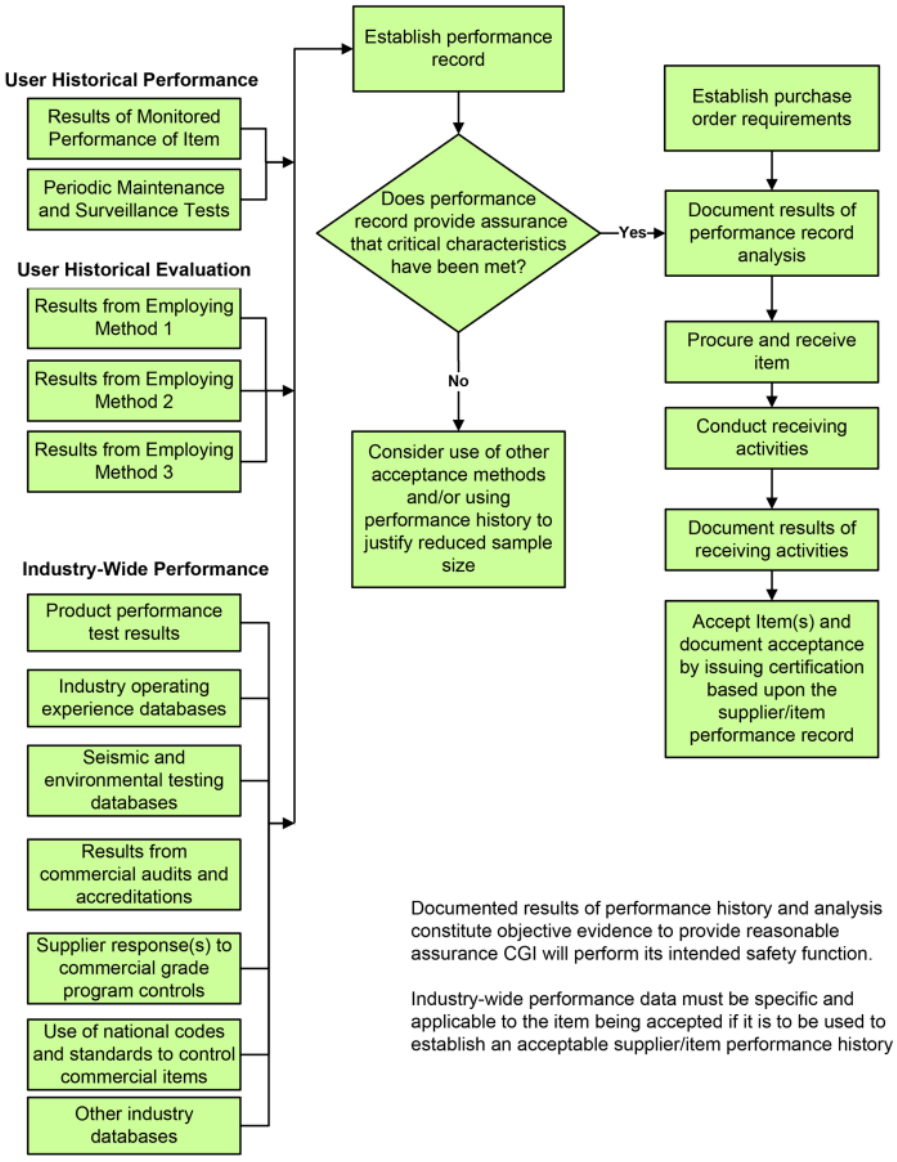

Figura 3.8: Método 4: Historial del proveedor/componente [10]

Capítulo 4

El uso de COTS en la Industria Aeroespacial

4.1. Introducción

La Industria Aeroespacial también ha introducido el uso de COTS dentro del proceso de diseño de las aeronaves. Sin embargo, este no se limita únicamente a componentes electromecánicos, sino que incorpora también el uso de hardware y software comercial. Dentro del marco normativo existente, el uso de COTS dentro de la Industria Aeroespacial está incluido en las normas RTCA DO-254 y RTCA DO-178 C, aplicables a hardware y software de los sistemas de a bordo de la aeronave, respectivamente.

Por un lado, la norma RTCA DO-254 establece las directrices a seguir para el diseño de hardware electrónico de a bordo, de manera que los componentes diseñados cumplan con los estándares de seguridad establecidos por las entidades reguladoras. Uno de los objetivos de este documento es proporcionar la información necesaria para incorporar hardware comercial en el diseño de los sistemas de a bordo de la aeronave [13].

Por otro lado, la norma RTCA DO-178 C establece consideraciones sobre software en la certificación de sistemas y equipos de a bordo de la aeronave, pero no aborda directamente el uso de software comercial, pasando muy por encima de este tema [14].

Por este motivo, este Capítulo se centrará en analizar las principales normativas aplicables en relación al uso de hardware comercial en el diseño de los sistemas de a bordo de las aeronaves. En particular, se analizará la información proporcionada en la RTCA DO-254 y las consideraciones al respecto de la Agencia Europea de Seguridad Aérea (EASA).

4.2. Normativa aplicable: DO-254 / ED-80

4.2.1. Introducción

Con el paso de los años y el desarrollo de la tecnología, las funciones de seguridad de la aeronave son realizadas por componentes cada vez más complejos. Este hecho supone todo un desafío para el diseño y la certificación, que tienen que lidiar con aeronaves cada vez más vulnerables a los posibles fallos que se puedan producir. Para controlar esta situación, es necesario asegurar que los potenciales fallos serán detectados y corregidos a tiempo durante los procesos de diseño y certificación.

Este documento, preparado por el RTCA SC-180 y aprobado el 19 de abril del 2000, proporciona las directrices necesarias para el diseño de hardware electrónico de los sistemas de a bordo de la aeronave [13]. Para ello, se definen una serie de objetivos, cuyo cumplimiento ayudará a que el componente en cuestión desempeñe su función de seguridad de forma correcta. Además, se proporcionan una serie de medios y actividades a realizar para asegurar el cumplimiento de todos los objetivos. No obstante, existe cierta flexibilidad a la hora de definir el procedimiento a seguir, teniendo en cuenta las nuevas tecnologías disponibles.

En cuanto al alcance del documento, esta guía es aplicable a elementos tales como LRUs, CBAs, ASICs, PLDs o COTS. Los componentes comerciales, por su propia tipología, no tienen por qué estar diseñados bajo esta norma, por lo que las consideraciones específicas para este tipo de componentes se tratan en una sección a parte.

4.2.2. Complejidad

En cuanto a la complejidad de un componente, las diferencias entre componentes simples, complejos y muy complejos no están definidas de forma rigurosa. El principal criterio para clasificar un componente en función de su complejidad se basa en la posibilidad (o no) de verificar el dispositivo mediante medios deterministas, y la dificultad del proceso de verificación. Los elementos hardware han de ser examinados de forma jerárquica a todos los niveles, incluyendo las funciones de direccionamiento que puedan no ser comprobables, como los modos no utilizados en dispositivos multifunción o potenciales estados ocultos en máquinas secuenciales.

Un elemento de hardware se identifica como simple sólo si una combinación completa de pruebas deterministas y análisis apropiados para el Nivel de Garantía de Desarrollo puede asegurar un rendimiento funcional correcto en todas las condiciones de funcionamiento posibles sin comportamiento anómalo. Cuando un componente no puede ser clasificado como simple, debe ser clasificado como complejo. Para los elementos complejos, los medios propuestos para proporcionar la garantía del diseño deben ser acordados por la autoridad de certificación al principio del ciclo de vida del diseño del hardware para mitigar el riesgo del programa.

La clasificación de un componente en función de su complejidad debe ser el primer paso a la hora de seleccionar un componente hardware. Mediante este estudio, es posible obtener una idea inicial de las pruebas y análisis que se tendrán que realizar para verificar su idoneidad para la aplicación propuesta. De esta manera, también se puede predecir si la certificación del componente será viable o no.

4.2.3. Funciones del sistema

Una única función del sistema puede estar asignada a un elemento hardware, software o a una combinación de ambos. Los requisitos de seguridad asociados a una función determinada han de ser abordados desde una perspectiva de sistema, de software y de hardware para determinar los niveles de fiabilidad y de garantía necesarios para satisfacer dichos requisitos. En la Figura 4.1 se muestran las relaciones entre las funciones de los sistemas y equipos de a bordo y los procesos de evaluación de la seguridad y de desarrollo de hardware y software.

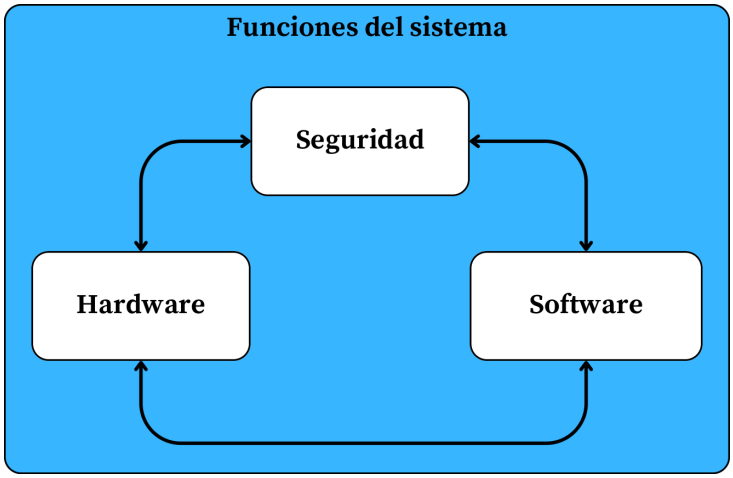

Figura 4.1: Funciones del sistema, seguridad, hardware y software

4.2.4. Niveles de Garantía de Desarrollo

Existen cinco Niveles de Garantía de Desarrollo (DAL) del sistema: A, B, C, D y E. Cada uno de los niveles está asociado a una condición de fallo del sistema. A continuación, se definen cada uno de los niveles mencionados:

- **Nivel A**: Funciones de hardware cuyo fallo o comportamiento anómalo, según se desprende de la evaluación de seguridad del hardware, provocaría un fallo de funcionamiento del sistema que daría lugar a una condición de **fallo catastrófico** para la aeronave.

- **Nivel B**: Funciones de hardware cuyo fallo o comportamiento anómalo, según se desprende de la evaluación de seguridad del hardware, provocaría un fallo de funcionamiento del sistema que daría lugar a una condición de **fallo peligroso/grave** para la aeronave.

- **Nivel C**: Funciones de hardware cuyo fallo o comportamiento anómalo, según se desprende de la evaluación de seguridad del hardware, provocaría un fallo de funcionamiento del sistema que daría lugar a una condición de **fallo grave** para la aeronave.

- **Nivel D**: Funciones de hardware cuyo fallo o comportamiento anómalo, según muestra la evaluación de seguridad del hardware, causaría un fallo de funcionamiento del sistema que daría lugar a una condición de **fallo menor** para la aeronave.

- **Nivel E**: Funciones de hardware cuyo fallo o comportamiento anómalo, según se desprende de la evaluación de seguridad del hardware, causaría el fallo de una función del sistema **sin afectar** a la capacidad operativa de la aeronave ni a la carga de trabajo de la tripulación de vuelo. Si se determina que una función es de Nivel E, no es necesario aplicar ninguna otra orientación de este documento; sin embargo, puede utilizarse como referencia.

Existen cinco clases de condiciones de fallo del sistema: catastrófico, peligroso / grave-mayor, mayor, menor y sin efecto. A continuación, se proporciona una descripción de cada una de ellas:

- **Catastrófico**: Condiciones de fallo que impedirían continuar el vuelo y el aterrizaje con seguridad.

- **Peligroso / Grave-Mayor**: Condiciones de fallo que reducirían la capacidad de la aeronave o la capacidad de la tripulación de vuelo para hacer frente a condiciones operativas adversas hasta el punto de que se produciría: una gran reducción de los márgenes de seguridad o de las capacidades funcionales, una angustia física o una mayor carga de trabajo de tal forma que no se podría confiar en que la tripulación de vuelo realizara sus tareas de forma precisa o completa, o efectos adversos en los ocupantes, incluidas lesiones graves o potencialmente mortales en un pequeño número de dichos ocupantes.

- **Grave**: Condiciones de fallo que reducirían la capacidad de la aeronave o la capacidad de la tripulación de vuelo para hacer frente a condiciones operativas adversas hasta el punto de que se produciría: una reducción significativa de los márgenes de seguridad o de las capacidades funcionales, un aumento significativo de la carga de trabajo de la tripulación de vuelo o de las condiciones que perjudican la eficiencia de la tripulación de vuelo, o molestias para los ocupantes, posiblemente incluyendo lesiones.

- **Menor**: Condiciones de fallo que no reducirían significativamente la seguridad de la aeronave, y que implicarían acciones de la tripulación de vuelo que están bien dentro de sus capacidades. Las condiciones de fallo menores pueden incluir: una ligera reducción de los márgenes de seguridad o de las capacidades funcionales, un ligero aumento de la carga de trabajo de la tripulación de vuelo, como cambios rutinarios del plan de vuelo, o alguna molestia para los ocupantes.

- **Sin efecto**: Condiciones de fallo que no afectan a la capacidad operativa de la aeronave ni aumentan la carga de trabajo de la tripulación de vuelo.

En la Tabla 4.1 se muestra una tabla que relaciona los Niveles de Garantía de Desarrollo del sistema con las condiciones de fallo.

Nivel de Garantía de Desarrollo	Condición de fallo
A	Catastrófico
B	Peligroso / Grave-Mayor
C	Mayor
D	Menor
E	Sin efecto

Tabla 4.1: Niveles de Garantía de Desarrollo y condiciones de fallo

La clasificación de un componente en función de su Nivel de Garantía de Desarrollo debe ser el segundo paso a la hora de seleccionar un componente hardware. De esta forma, es posible visualizar los análisis o ensayos a los que deberá ser sometido el componente, en función de la gravedad de las consecuencias de un potencial fallo.

4.2.5. Uso de componentes COTS

Los COTS son ampliamente utilizados a la hora de diseñar componentes hardware, pero los datos de diseño de estos componentes no suelen estar disponibles. Como se ha comentado anteriormente, el proceso de certificación se centra principalmente en el conjunto de la aeronave, y no tanto en certificar todos los componentes de forma individual. Siguiendo esta metodología, el uso de COTS quedará verificado mediante un Proceso de Gestión de Componentes Electrónicos (ECMP) junto con el proceso de diseño.

La gestión de componentes electrónicos es un proceso de gran importancia para el diseño y desarrollo del hardware. Este proceso, aplicable también a componentes comerciales, permite obtener el crédito de la certificación verificando los siguientes puntos:

1. El fabricante puede demostrar que posee un historial de producción de componentes de alta calidad.

2. El fabricante ha establecido procedimientos de control de calidad.

3. Existe una experiencia operativa que avala el buen funcionamiento del componente.

4. El componente ha sido cualificado por el fabricante o mediante ensayos que demuestran su fiabilidad.

5. El fabricante tiene un control de la calidad de los componentes o puede asegurarlo mediante ensayos adicionales.

6. Los componentes se han seleccionado sobre la base de su idoneidad técnica para la aplicación prevista (rango de temperatura, potencia, tensión, etcétera).

7. El rendimiento y fiabilidad de los componentes es controlado de forma continua y se mantiene una comunicación fluida con el fabricante para implementar mejoras continuas.

El aprovisionamiento de componentes comerciales entraña ciertas dificultades que se deben tener en cuenta para minimizar su impacto en el diseño de componentes hardware. Las principales preocupaciones son las siguientes:

1. La disponibilidad real de los datos de diseño de componentes comerciales.

2. Las variaciones dependientes de los lotes de producción que puedan no ser identificadas.

3. La evolución de la tecnología.

4. La obsolescencia de los componentes comerciales.

4.2.6. Experiencia operativa

La experiencia operativa puede utilizarse para justificar la garantía en el diseño de hardware desarrollado previamente. Esta abarca cualquier dato recogido durante un uso anterior o actual del componente en cuestión, incluidos los datos de componentes utilizados en aplicaciones pertenecientes a otros sectores o campos de aplicación. Una experiencia operativa amplia y satisfactoria de un componente es un buen indicador de la madurez de la tecnología y la calidad de los procesos relacionados con su desarrollo.

Cuando la experiencia operativa es utilizada para garantizar el diseño, que sea válida o no y su importancia dependerá de los siguientes puntos:

1. La similitud de los componentes en relación a la aplicación, la función, el entorno operativo y el Nivel de Garantía de Desarrollo.
2. El grado en el que los datos de diseño están basados en la configuración actual del componente.
3. La medida en la que se han detectado, mitigado y corregido los fallos de diseño durante la operación del componente y la repercusión que han tenido en la seguridad.
4. El índice real de fallos durante la operación del componente.

En los siguientes apartados se abordará la forma que tiene la Agencia Europea de Seguridad Aérea (EASA) de introducir las consideraciones proporcionadas en este documento dentro de su propio marco regulador. En este caso, en las Especificaciones de Certificación (CS) no se aborda este tema directamente, por lo que la postura de la Agencia está recogida en los Medios Aceptables de Cumplimiento AMC 20-152A, correspondiente al Apartado 4.3, y en el Memorando de Certificación CM-SWECH-001, correspondiente al Apartado 4.4.

4.3. Medios Aceptables de Cumplimiento: AMC 20-152A

4.3.1. Introducción

Los Medios Aceptables de Cumplimiento (AMC) son unos estándares no vinculantes adoptados por la Agencia Europea de Seguridad Aérea (EASA) con el objetivo de mostrar medios para establecer el cumplimiento de la normativa básica y las normas de aplicación.

Estos documentos no tienen carácter legislativo, por lo que su cumplimiento no es obligatorio y las entidades solicitantes pueden mostrar el cumplimiento de los requisitos aplicables por medios distintos. No obstante, estos documentos se presuponen conformes con las normas para aportar seguridad jurídica y contribuir a una aplicación uniforme de las mismas. De esta forma, las autoridades competentes están obligadas a reconocer a las entidades reguladas que muestren cumplimiento con estos documentos como conformes con la ley.

El AMC 20-152A describe unos medios aceptables, pero no los únicos, para mostrar cumplimiento con las normativas de aeronavegabilidad aplicables para los elementos electrónicos hardware de los sistemas de a bordo [15]. Este documento reconoce la normativa RTCA DO-254 / ED-80, describe cuando usarla y la complementa con directrices adicionales y aclaraciones, como el uso de dispositivos COTS. El contenido de este documento es aplicable a componentes hardware con un Nivel de Garantía de Desarrollo A, B o C.

4.3.2. Objetivos

Las directrices adicionales y aclaraciones son proporcionadas en forma de objetivos. De este modo, se espera que la entidad solicitante se centre en describir los procesos y actividades necesarios para dar cumplimiento a dichos objetivos. A continuación se muestran los aplicables a los dispositivos COTS.

1. La entidad solicitante ha de **evaluar la complejidad del dispositivo** atendiendo al criterio mostrado a continuación:

    - Si el dispositivo tiene múltiples elementos funcionales que interactúan entre sí, un número significativo de modos funcionales y funciones configurables que permiten diferentes flujos de datos y repartos de recursos en su interior, el dispositivo es complejo.
    - Si el dispositivo contiene procesamiento avanzado de datos, conmutación avanzada o elementos de procesamiento múltiples, el dispositivo es complejo.
    - Si no se cumple ninguno de los criterios anteriores, el dispositivo es simple.

Además, se ha de documentar en una lista aquellos dispositivos relevantes para la clasificación, incluyendo los que se encuentran en el límite entre simples y complejos, para los que será necesario una justificación de su clasificación.

2. La entidad solicitante ha de garantizar que existe un **Proceso de Gestión de Componentes Electrónicos (ECMP)** para abordar la selección, clasificación y gestión de la configuración del dispositivo. Además, el ECMP debe abordar el acceso a la documentación técnica del componente (manual de usuario, ficha técnica, fe de erratas, manual de instalación y cambios realizados por el fabricante).

   Como se mencionó en el Apartado 4.2, el uso de componentes COTS quedará verificado durante el proceso de diseño general, siendo el Proceso de Gestión de Componentes Electrónicos la base para la certificación, utilizado en conjunción con el proceso de diseño.

   En cuanto a la documentación técnica, la disponibilidad de los datos de diseño es un punto importante a tener en cuenta durante el aprovisionamiento de componentes comerciales.

3. La entidad solicitante ha de **determinar la fiabilidad y la idoneidad del dispositivo para la aplicación prevista**, cuando este opere fuera de los límites de funcionamiento establecidos por el fabricante.

   Los dispositivos son seleccionados en función de su idoneidad para realizar la función requerida. No obstante, en ocasiones es necesario que estos trabajen en un rango de funcionamiento el cual no ha sido verificado por el fabricante. En estos casos, se han de aportar las garantías suficientes de que el dispositivo cumplirá con los requisitos exigidos.

4. La entidad solicitante ha de **establecer los medios de cumplimiento necesarios para el microcódigo integrado**, cuando este no está cualificado por el fabricante o ha sido modificado por la propia entidad solicitante.

5. La entidad solicitante ha de **evaluar las erratas existentes en el dispositivo y su relevancia para la aplicación prevista**, además de identificar y verificar los medios necesarios para mitigar estas erratas (hardware, software, sistema, etcétera).

6. La entidad solicitante ha de **identificar los modos de fallo del dispositivo asociados a las funciones utilizadas** y los posibles modos comunes asociados. El sistema de evaluación de la seguridad debe ser retro alimentado con ambos modos.

   Para garantizar el cumplimiento de este objetivo, puede ser interesante realizar un Análisis Modal de Fallos y Efectos, como el realizado durante el Proceso de Dedicación. Una vez identificados los modos de fallo de las funciones del dispositivo, se podría realizar un Análisis de Causa Raíz para tratar de identificar alguna causa común a varios modos de fallo.

7. La entidad solicitante ha de **asegurar que el uso del dispositivo ha sido definido y verificado de acuerdo a la función prevista** del hardware, incluyendo las interfaces hardware-software y hardware-hardware.

Cuando se trata de dispositivos con un Nivel de Garantía de Desarrollo A o B, la entidad solicitante ha de garantizar que las funciones no utilizadas del dispositivo no comprometen la integridad y la disponibilidad de las funciones utilizadas.

8. Cuando se trata de dispositivos con un Nivel de Garantía de Desarrollo A o B, la entidad solicitante ha de **desarrollar y verificar los medios necesarios** (a nivel hardware, software, sistema o una combinación de ellos) **para mitigar cualquier alteración inesperada** de los ajustes de configuración críticos del sistema.

4.4. Memorando de Certificación: CM-SWCEH-001

Un Memorando de Certificación (CM) es un documento elaborado por la Agencia Europea de Seguridad Aérea (EASA), de carácter no vinculante, y que tiene por objetivo aclarar la línea general de actuación de la Agencia sobre un tema específico de certificación. Estos documentos ofrecen orientación sobre un tema concreto y pueden proporcionar información y orientación complementarias para la demostración del cumplimiento de las normas vigentes.

Como se ha mencionado al final del Apartado 4.2, en las Especificaciones de Certificación (CS) no hay ningún requisito específico para la certificación de Hardware Electrónico de A Bordo (AEH). El objetivo de este Memorando es proporcionar material específico que sirva de guía para los aspectos de la certificación asociados con el uso de esta clase de dispositivos [16].

Basado en los puntos expuestos en el Apartado 4.2, este documento discute cómo la norma RTCA DO-254 ha de ser aplicada en el diseño y desarrollo de Hardware Electrónico de A Bordo. Adicionalmente, complementa la aplicabilidad de la norma en relación a los Componentes Comerciales Salidos del Estante (COTS) y proporciona las directrices necesarias para el desarrollo de un Proceso de Gestión de Componentes Electrónicos (ECMP).

El alcance del documento está definido para componentes con un Nivel de Garantía de Desarrollo (DAL) A, B y C. En concreto, la sección dedicada al uso de COTS es aplicable a los siguientes componentes:

- Circuitos integrados.
- Microcontroladores.

Un **circuito integrado** es cualquier dispositivo electrónico (digital o híbrido) que no ejecuta software en un núcleo específico. Los circuitos integrados pueden ser controladores de bus, *flip-flops*, multiplexores, convertidores, memorias, etcétera. Las funciones hardware implementadas en estos componentes pueden ser simples o complejas.

Un **microcontrolador** es cualquier circuito integrado que ejecuta software en un núcleo específico e implementa elementos periféricos de hardware, como controladores de bus, entradas y salidas, etcétera. Dichos elementos periféricos pueden ser simples o complejos.

En este apartado se abordarán los puntos necesarios para la elaboración de un Proceso de Gestión de Componentes Electrónicos, siguiendo la estructura establecida en el Memorando de Certificación. Adicionalmente, se hará un análisis de la relación de cada uno de los puntos con los conceptos desarrollados durante los Apartados 4.2 y 4.3, y su relación con el proceso de Dedicación de Componentes de Grado Comercial en la Industria Nuclear, abordado en el Capítulo 3.

4.4.1. Clasificación del dispositivo

Se han de determinar las características del dispositivo y clasificar a este último en función de las primeras, atendiendo a los criterios mostrados a continuación:

- El Nivel de Garantía de Desarrollo: A, B, C, D o E.
- El tipo de dispositivo: circuito integrado o microcontrolador.
- La complejidad del dispositivo: simple, complejo o muy complejo.

Los Niveles de Garantía de Desarrollo de hardware fueron introducidos en el Apartado 4.2. El dispositivo ha de tener asignado uno de los cinco niveles de la Tabla 4.1.

En cuanto al tipo de dispositivo, el alcance del documento se reduce a circuitos integrados o microcontroladores. La definición de estas dos clases de dispositivos ha sido proporcionada al inicio del apartado.

El criterio para determinar la complejidad de un dispositivo fue introducido en el Apartado 4.2. En el **Objetivo 1** del Apartado 4.3 se define un criterio más específico para la complejidad.

En función del tipo de dispositivo y de su complejidad, este puede pertenecer a cinco categorías diferentes, indicadas en la Tabla 4.2.

	Simple	**Complejo**	**Muy complejo**
Circuito Integrado	✓	✓	–
Microcontrolador	✓	✓	✓

Tabla 4.2: Clasificación en función del tipo de dispositivo y su complejidad

Para determinar que un dispositivo es **simple**, es esencial comprobar la posibilidad de verificar todos los requisitos en todas las configuraciones posibles, mediante pruebas sobre el propio dispositivo. Si el dispositivo no cumple con estos requisitos, entonces es **complejo**.

Cuando un microcontrolador tiene varias CPU (y usan el mismo bus), varios periféricos complejos dependientes entre sí y que intercambian datos o varios buses integrados y utilizados de forma dinámica, el dispositivo es **muy complejo**.

En la Tabla 4.3 se muestra una tabla, a modo de resumen, para la clasificación del dispositivo atendiendo a los criterios expuestos en los párrafos anteriores.

PARTE A: CLASIFICACIÓN DEL DISPOSITIVO

SECCIÓN A.1: NIVEL DE GARANTÍA DE DESARROLLO

○ Nivel A	○ Nivel B	○ Nivel C	○ Nivel D	○ Nivel E

Notas:

A: Catastrófico; **B**: Peligroso / Grave-Mayor; **C**: Mayor; **D**: Menor; **E**: Sin efecto

SECCIÓN A.2: TIPO DE DISPOSITIVO

○ Circuito integrado	○ Microcontrolador

SECCIÓN A.3: DETERMINACIÓN DE LA COMPLEJIDAD

		Sí	No
1	¿Es posible verificar todos los requisitos en todas las configuraciones posibles mediante pruebas sobre el propio dispositivo?	○	○
2	¿El componente es un microcontrolador con varias CPU que usan el mismo bus, varios periféricos complejos dependientes entre sí que intercambian datos o varios buses integrados utilizados de forma dinámica?	○	○
–	**SÍ** a la pregunta 1 → **SIMPLE**	○	○
–	**NO** a la pregunta 1 y **NO** a la pregunta 2 → **COMPLEJO**	○	○
–	**NO** a la pregunta 1 y **SÍ** a la pregunta 2 → **MUY COMPLEJO**	○	○

Tabla 4.3: Clasificación del dispositivo

El primer paso es clasificar el dispositivo que se quiere certificar. En función de sus características, complejidad y Nivel de Garantía de Desarrollo, los requisitos necesarios para la certificación del dispositivo y las actividades de verificación (pruebas o análisis) serán más o menos exigentes. Este punto presenta similitudes con el Proceso de Dedicación descrito en el Apartado 3.2. En el Proceso de Dedicación, el primer paso también consiste en identificar el componente y clasificarlo atendiendo a los criterios correspondientes.

En la Industria Nuclear se habla de componentes Relacionados con la Seguridad (*Safety-Related*) o No Relacionados con la Seguridad (*Non-Safety-Related*), mientras que en la Industria Aeroespacial se habla de componentes con un Nivel de Garantía de Desarrollo A, B, C, D o E. En el segundo caso, los componentes con un nivel de seguridad más elevado son los tres primeros (A, B y C), por lo que los requisitos para la certificación serán más exhaustivos. Los componentes con un nivel de seguridad menor (D y E) están fuera del alcance de este documento, por lo que podría decirse que son el equivalente a los componentes No Relacionados con la Seguridad en la Industria Nuclear.

Industria Nuclear	Industria Aeroespacial
Relacionados con la Seguridad	Niveles A, B y C
No Relacionados con la Seguridad	Niveles D y E

Tabla 4.4: Nivel de Garantía de Desarrollo y su relación con la Seguridad

En cuanto a la complejidad de un dispositivo, en el Proceso de Dedicación no se aborda este aspecto, al menos no de forma directa. Sin embargo, uno de los criterios utilizados para determinar el Método de Aceptación a utilizar se basa en la sencillez del componente: los componentes relativamente sencillos son susceptibles de ser verificados mediante pruebas e inspecciones (Método 1), mientras que aquellos que constituyen un ensamblaje de muchas piezas (Método 2) o cuyo proceso de fabricación es complejo (Método 3) tendrán que ser verificados utilizando otros Métodos de Aceptación.

Industria Nuclear	Industria Aeroespacial
Método 1	Simples
Métodos 2, 3 o 4 (o combinación)	Complejos o Muy Complejos

Tabla 4.5: Complejidad y su relación con los Métodos de Aceptación

4.4.2. Datos del dispositivo

Se ha de identificar y guardar la documentación específica de cada dispositivo. Dentro de este apartado se ha de incluir, por lo menos, el manual de usuario, la ficha técnica, la fe de erratas, el manual de usuario de erratas y el manual de instalación.

Esto se encuentra en consonancia con el **Objetivo 2** del Apartado 4.3, en el que se menciona que el Proceso de Gestión de Componentes Electrónicos deberá abordar el acceso a la documentación técnica del componente.

Cuando los datos de diseño están disponibles, se ha de verificar que estos son consistentes con los requisitos del dispositivo. Cuando no están disponibles, se ha de documentar el siguiente proceso:

- Verificar que el fabricante tiene un sistema de calidad implantado, y que este es aplicado al dispositivo en cuestión.
- Verificar que el fabricante tiene un proceso de fabricación determinista y repetible.
- Verificar que el fabricante realiza un proceso de aprobación interno y cuenta con procedimientos de prueba y criterios de aceptación documentados.

En el caso de microcontroladores muy complejos, si la documentación pública del fabricante no es suficiente se ha de acceder a la documentación privada.

En la Tabla 4.6 se muestra una tabla, a modo de resumen.

PARTE B: DATOS DEL DISPOSITIVO

SECCIÓN B.1: REVISIÓN DOCUMENTAL

○	Ficha técnica: _____	○	Manual de usuario: _____
○	Fe de erratas: _____	○	Manual de erratas: _____
○	Otros: _____	○	Manual de instalación: _____

SECCIÓN B.2: DATOS DE DISEÑO

		Sí	No
1	¿Los datos del dispositivo están disponibles y son consistentes con los requisitos del dispositivo?	○	○
–	**SÍ** a la pregunta 1 → **Parte C**	○	○
–	**NO** a la pregunta 1 → **Preguntas 2, 3 y 4**	○	○
2	¿El fabricante tiene un sistema de calidad implantado y este es aplicado al dispositivo en cuestión?	○	○
3	¿El fabricante tiene un proceso de fabricación determinista y repetible?	○	○
4	¿El fabricante realiza un proceso de aprobación interno y cuenta con procedimientos de prueba y criterios de aceptación documentados?	○	○

Notas: Si el dispositivo es un microcontrolador muy complejo y la documentación pública del fabricante no es suficiente se ha de acceder a la documentación privada.

Tabla 4.6: Datos del dispositivo

Cuando se quiere certificar un componente comercial para su uso en aplicaciones relacionadas con la seguridad, es necesario recopilar toda la información disponible y verificar que es coherente con los requisitos de diseño.

Cuando la información disponible es consistente con los requisitos del dispositivo, los componentes son susceptibles de ser verificados mediante pruebas e inspecciones (Método 1). Cuando la información disponible no es suficiente y no es posible obtener información adicional del suministrador se deberá optar por otros Métodos de Aceptación.

Cuando el fabricante cuenta con un sistema de calidad implantado, un proceso de fabricación determinista y repetible y realiza un proceso de aprobación interno el componente es susceptible de ser verificado mediante el Método 2. Si no se cumple ninguno de estos criterios será necesario recurrir a otros Métodos de Aceptación.

Industria Nuclear	Industria Aeroespacial
Método 1	Datos disponibles
Método 2	Sistema de calidad, proceso de fabricación determinista y repetible y proceso de aprobación interno

Tabla 4.7: Datos disponibles y su relación con los Métodos de Aceptación

4.4.3. Dominio de uso del dispositivo

Se ha de determinar el dominio del dispositivo, asociado a la aplicación en la que va a ser utilizado, y demostrar que el componente opera dentro de los límites establecidos por el fabricante. El dominio del dispositivo puede contener los siguientes aspectos:

- Las funciones utilizadas.
- Las funciones no utilizadas.
- Los medios para desactivar cada una de las funciones.
- Los medios externos para controlar cualquier activación inesperada de las funciones no utilizadas o cualquier desactivación inesperada de las funciones utilizadas.
- Los medios para controlar el reinicio de los dispositivos.
- La configuración de encendido.
- La configuración de reloj.
- Las condiciones de uso.

En el **Objetivo 7** del Apartado 4.3 se menciona que es necesario asegurarse de que las funciones no utilizadas no comprometen la integridad y disponibilidad de las funciones utilizadas del dispositivo. La idoneidad del dispositivo para la aplicación prevista mencionada en el **Objetivo 3** del Apartado 4.3 se asegura determinando las funciones del dispositivo y las condiciones de uso.

PARTE C: DOMINIO DE USO DEL DISPOSITIVO

SECCIÓN C.1: FUNCIONES DEL DISPOSITIVO

	U	N/U
1	○	○
2	○	○
3	○	○

Notas:

U: Utilizada; **N/U**: No Utilizada

SECCIÓN C.2: MEDIOS PARA DESACTIVAR LAS FUNCIONES

1
2
3

SECCIÓN C.3: MEDIOS EXTERNOS PARA CONTROLAR LAS FUNCIONES

1
2
3

Notas: Los medios externos han de controlar cualquier activación inesperada de las funciones no utilizadas o cualquier desactivación inesperada de las funciones utilizadas.

SECCIÓN C.4: MEDIOS EXTERNOS PARA CONTROLAR EL REINICIO

1
2
3

SECCIÓN C.5: CONFIGURACIÓN DE ENCENDIDO

SECCIÓN C.6: CONFIGURACIÓN DE RELOJ

SECCIÓN C.7: CONDICIONES DE USO

Tabla 4.8: Dominio de uso del dispositivo

Este punto también guarda cierta relación con el Proceso de Dedicación descrito en el Apartado 3.2. Durante la Evaluación Técnica del Proceso de Dedicación es necesario identificar las funciones del componente para la aplicación prevista y determinar cuáles están relacionadas con la seguridad y cuáles no.

El proceso descrito en este punto guarda ciertas similitudes. En primer lugar, es necesario identificar las funciones del dispositivo (las utilizadas y las no utilizadas) y centrarse en aquellas que van a ser utilizadas. En este caso, podría decirse que las funciones utilizadas serían equivalentes a las funciones relacionadas con la seguridad y las no utilizadas a las no relacionadas con la seguridad.

Sin embargo, a diferencia del Proceso de Dedicación, centrado únicamente en las funciones relacionadas con la seguridad, en este documento se va más allá, analizando también las funciones no utilizadas. El planteamiento en este caso está claramente definido: no basta solamente con analizar las funciones utilizadas, si no que hay que determinar la influencia de las no utilizadas sobre las primeras, y garantizar que las últimas no intervienen en el funcionamiento del dispositivo.

Además, será necesario evaluar otros aspectos relacionados con el dominio del dispositivo, como la configuración de encendido, los medios para controlar el reinicio de los dispositivos, la configuración de reloj o las condiciones de uso.

4.4.4. Actividades de verificación

Se ha de validar el dominio del dispositivo respecto a las especificaciones de seguridad del sistema. El uso de cada una de las funciones del dispositivo debe estar justificado y ser coherente con los requisitos de seguridad del sistema, especialmente cuando las funciones internas del dispositivo se utilizan para asegurar el cumplimiento de los requisitos de seguridad.

Se ha de asegurar la validez del dominio mediante una serie de actividades de verificación, que han de estar basadas principalmente en:

- Pruebas. Se han de realizar pruebas para, entre otras actividades, comprobar el correcto funcionamiento de las funciones utilizadas, verificar la tolerancia a fallos, verificar la efectividad de los medios para desactivar las funciones no utilizadas, verificar la corrección de las erratas o validar las condiciones de uso definidas por el fabricante.

- Análisis. Se han de llevar a cabo análisis para, entre otras actividades, verificar que el diseño del componente tienen en cuenta la variabilidad de las características, cuando el componente ha sido aprobado previamente, comparar las características y el uso e identificar las diferencias, analizarlas y justificarlas, o analizar el potencial impacto de la activación inesperada de las funciones no utilizadas.

El determinismo del dispositivo (rendimiento, latencia de datos, etcétera) debe ser garantizado para el dominio de uso y las características del dispositivo. Puede ser necesaria una evaluación adicional para el caso de arquitecturas complejas.

En el caso del uso de procesadores con varios núcleos, ha de realizarse una evaluación de todas las funciones que involucren varios núcleos o de las funciones habituales de la CPU que utilicen varios núcleos en su diseño.

PARTE D: ACTIVIDADES DE VERIFICACIÓN
SECCIÓN D.1: PRUEBAS
SECCIÓN D.2: ANÁLISIS

Tabla 4.9: Actividades de verificación

Este punto se corresponde con las actividades desarrolladas durante el Proceso de Aceptación. Al igual que en el Proceso de Dedicación, se han de llevar a cabo una serie de pruebas y análisis para verificar que los dispositivos seleccionados cumplen con los requisitos previamente establecidos.

4.4.5. Análisis de las erratas del dispositivo

Se han de documentar las evidencias que muestren cómo el fabricante recopila, actualiza y publica la fe de erratas y cómo la probabilidad de ocurrencia de nuevas erratas disminuye en función del tiempo, siendo esta característica un indicador de la madurez del componente.

Se han de recopilar todas las erratas del fabricante para mitigar efectos potenciales adversos relacionados con la seguridad. Para ello, se han de documentar los siguientes puntos:

- Justificación de qué erratas son aplicables al dispositivo.
- Justificación de qué erratas no son aplicables al dispositivo.
- Descripción de las acciones necesarias para mitigar las erratas aplicables al dispositivo.

- Evidencia de que las acciones tomadas para mitigar las erratas están cubiertas por los requisitos principales y los datos de diseño.

En el **Objetivo 5** del Apartado 4.3 se menciona que se han de evaluar las erratas del dispositivo y analizar su relevancia en relación a la aplicación prevista.

PARTE E: ANÁLISIS DE LAS ERRATAS DEL DISPOSITIVO		
SECCIÓN E.1: RECOPILACIÓN DE ERRATAS		
	A	N/A
1	○	○
2	○	○
3	○	○
Notas:		
A: Aplicable; **N/A**: No Aplicable		
SECCIÓN E.2: MEDIOS PARA MITIGAR LAS ERRATAS APLICABLES		

Tabla 4.10: Análisis de las erratas del dispositivo

En este caso, no hay un punto en concreto dentro del Proceso de Dedicación que se refiera a las erratas de un dispositivo. Sin embargo, dentro de la guía analizada en el Capítulo 3, se menciona que la confianza en la información técnica proporcionada por el proveedor ha de ser determinada mediante el juicio ingenieril. Si la experiencia demuestra que la información era incorrecta, se deberán tomar las acciones que sean necesarias para determinar la causa del error.

4.4.6. Gestión de la configuración del dispositivo

Se ha de verificar que el fabricante identifica y documenta la configuración del dispositivo, garantiza que puede replicar de forma adecuada y consistente la configuración del dispositivo, controla y documenta los cambios realizados en el dispositivo y proporciona una descripción adecuada de los cambios realizados.

Cuando se realiza un cambio en el componente, se ha de llevar a cabo un análisis del impacto que supone dicho cambio para determinar si es necesario realizar actividades adicionales de verificación.

PARTE F: GESTIÓN DE LA CONFIGURACIÓN DEL DISPOSITIVO			
SECCIÓN F.1: CONFIGURACIÓN DEL DISPOSITIVO			
		Sí	No
1	¿El fabricante identifica y documenta la configuración del dispositivo?	○	○
2	¿El fabricante garantiza que puede replicar de forma adecuada y consistente la configuración del dispositivo?	○	○
3	¿El fabricante controla y documenta los cambios realizados en el dispositivo?	○	○
4	¿El fabricante proporciona una descripción adecuada de los cambios realizados?	○	○
SECCIÓN F.2: CONTROL DE CAMBIOS			
1			
2			
3			

Tabla 4.11: Gestión de la configuración del dispositivo

Este apartado tiene que ver con la evaluación de equivalencia del dispositivo. Cualquier cambio realizado en el dispositivo debe ser tenido en cuenta. Al igual que en el Proceso de Dedicación, los cambios introducidos por el fabricante suponen una dificultad añadida: aunque las prestaciones sean iguales o superiores, el componente ha de ser clasificado como un componente alternativo o incluso nuevo.

4.4.7. Análisis Modal de Fallos y Efectos

Se ha de realizar un análisis a nivel de dispositivo con el fin de refinar los modos de fallo y reducir la probabilidad de que estos se produzcan. Se ha de garantizar que la evaluación del rendimiento y el análisis de la seguridad funcional del dispositivo tengan en cuenta la configuración del dispositivo. Cuando el dispositivo pueda ser configurado se ha de asegurar que la configuración programada configura el dispositivo según lo esperado.

La filosofía en la que se basa el proceso de certificación está centrada en la aplicación final del dispositivo. Las pruebas y análisis realizadas han de demostrar el correcto funcionamiento del dispositivo para la aplicación prevista. El Proceso de Dedicación sigue la misma filosofía. Una forma práctica de analizar las funciones del dispositivo y los posibles modos de fallos asociados es llevar a cabo un Análisis Modal de Fallos y Efectos (AMFE). Aunque en este documento no se mencione, es una buena forma de indagar en el comportamiento del dispositivo y la información resultante es muy útil.

PARTE G: ANÁLISIS MODAL DE FALLOS Y EFECTOS				
Función	Modo de fallo	Efecto	Causa	Característica

Tabla 4.12: Análisis modal de fallos y efectos

4.4.8. Experiencia operativa

Se ha de documentar:

- El mercado objetivo del dispositivo.
- El ambiente en el que ha sido adquirida la experiencia operativa del dispositivo (aviación civil, aviación militar, espacio, telecomunicaciones, automoción, etcétera) y el número de horas de funcionamiento.
- La criticidad de uso del dispositivo.
- El orden de magnitud de tiempo que ha estado en uso el dispositivo.
- Para dispositivos con un Nivel de Garantía de Desarrollo A, B o C, la experiencia operativa será clasificada como suficiente cuando se cumplan los criterios definidos a continuación:
    - Para componentes Nivel A:
        - Al menos dos años de uso con más de 10^6 horas de servicio, sumando horas de aplicaciones aeronáuticas y horas de aplicaciones relacionadas con la seguridad.
        - Al menos dos años de uso con más de 10^5 horas de servicio, sumando horas de aplicaciones aeronáuticas y horas de aplicaciones relacionadas con la seguridad, y más de 10^7 horas de servicio en otras aplicaciones.
    - Para componentes Nivel B:
        - Al menos dos años de uso con más de 10^5 horas de servicio, sumando horas de aplicaciones aeronáuticas y horas de aplicaciones relacionadas con la seguridad.
        - Al menos dos años de uso con más de 10^4 horas de servicio, sumando horas de aplicaciones aeronáuticas y horas de aplicaciones relacionadas con la seguridad, y más de 10^7 horas de servicio en otras aplicaciones.

- Para componentes Nivel C: Más de 10^5 horas de servicio, sumando horas de aplicaciones aeronáuticas, horas de aplicaciones relacionadas con la seguridad, y horas de otras aplicaciones.

Se han de aportar evidencias de la madurez del componente, teniendo en cuenta el número de modificaciones, la naturaleza de estas y la tasa de ocurrencia de erratas asociada a las diferentes versiones.

PARTE H: EXPERIENCIA OPERATIVA DEL PRODUCTO

	Sí	No
¿La experiencia operativa puede ser clasificada como suficiente atendiendo a los criterios descritos en CM-SWCEH-001 Issue 1 Rev. 2?	○	○

Tabla 4.13: Experiencia operativa del producto

Como se ha mencionado anteriormente, es importante documentar la experiencia operativa del dispositivo. Una experiencia operativa amplia y con resultados positivos hace que buena parte de los requisitos exigidos queden verificados, por lo que muchas actividades son prescindibles y el tiempo de desarrollo y los recursos destinados en el proceso son menores.

En la Industria Nuclear, la experiencia operativa puede ser utilizada para validar alguna de las Características Críticas mediante el Método 4, como se ha expuesto en el Apartado 3.5. En la Industria Aeroespacial, la experiencia operativa es muy importante para determinar la madurez del componente, ya que el disponer de una mayor experiencia operativa implica que algunos de los requisitos necesarios para la certificación queden cubiertos.

4.4.9. Mitigación de fallos del dispositivo

En los casos en los que el componente pueda causar un fallo catastrófico por sí solo, sin necesidad de que se produzcan otros fallos simultáneamente, será necesario implementar una arquitectura que permita mitigar dichos efectos.

Para poder identificar esta situación, es necesario llevar a cabo un Análisis de Causas Comunes. Este análisis, realizado a nivel de la aeronave, puede revelar condiciones de fallo peligrosas de otros sistemas que produzcan un fallo catastrófico.

En el **Objetivo 6** del Apartado 4.3 se menciona que han de identificarse los modos de fallo y determinar las posibles causas comunes, dos actividades que van en consonancia

con lo descrito en este punto. Además, el **Objetivo 8** se refiere específicamente a los medios para mitigar cualquier alteración de la configuración crítica del dispositivo.

PARTE I: ESTRATEGIAS DE MITIGACIÓN				
SECCIÓN I.1: ANÁLISIS DE CAUSA RAÍZ				
Problema	Síntoma	Posible causa raíz	Causa raíz real	Solución
SECCIÓN I.2: MÉTODOS DE MITIGACIÓN				

Tabla 4.14: Mitigación de fallos del dispositivo

En Análisis de Causas Comunes o Análisis de Causa Raíz (RCA) es muy interesante porque puede ayudar a identificar una causa que sea común para varios fallos del sistema. Identificar estas causas y corregirlas o mitigarlas a tiempo es fundamental para asegurar el correcto funcionamiento del dispositivo. A partir del Análisis Modal de Fallos y Efectos realizado anteriormente es más sencillo determinar las posibles causas comunes de varios modos de fallo.

En cuanto a la mitigación de fallos, aunque no se trate de forma directa en el Proceso de Dedicación, un Componente de Grado Comercial Dedicado es equivalente a un Componente Básico que, entre otros aspectos, tiene la capacidad de prevenir o mitigar las consecuencias de los accidentes que pudieran dar lugar a exposiciones potenciales fuera del emplazamiento de la central, según 10CFR50 Apéndice B [12].

4.4.10. Partición del dispositivo

Se ha de llevar a cabo un Análisis de Partición para determinar que el componente puede garantizar una partición robusta del sistema, asegurando la independencia entre sistema, hardware y software, cuando sea necesario.

La partición del hardware se define en la RTCA DO-254 como un método implementado para mejorar la fiabilidad y la seguridad mediante la separación física y el aislamiento del hardware que implementa las funciones, incluida la redundancia, para evitar los efectos de los fallos comunes [13].

Este punto, por tanto, es una continuación del anterior. Tras haber realizado un Análisis de las Causas Comunes y describir las estrategias de mitigación, el siguiente paso será realizar el Análisis de Partición para completar la sección.

SECCIÓN I.3: ANÁLISIS DE PARTICIÓN

Tabla 4.15: Análisis de partición

4.4.11. Métodos alternativos

En caso de que se utilicen métodos alternativos a los anteriormente descritos, se ha de proponer a las autoridades componentes la justificación de equivalencia con la DO-254 y el Memorando de Certificación.

Capítulo 5

Conclusiones

Como se ha tratado a lo largo de los Capítulos 1 y 2, los COTS presentan ciertas ventajas que hacen atractivo su uso en industrias con altos requisitos de seguridad, como la Industria Nuclear o la Industria Aeroespacial.

Sin embargo, para poder utilizarlos en aplicaciones relacionadas con la seguridad, es necesario dar solución a los problemas que presentan este tipo de componentes, asegurando que cumplen con los requisitos de seguridad establecidos por los organismos reguladores, pese a no haber sido específicamente diseñados para ello.

Inicialmente, el uso de componentes comerciales en la Industria Nuclear estuvo motivado por la necesidad de dar solución a un problema de obsolescencia. Los fabricantes de componentes de clase nuclear habían abandonado su programa de garantía de calidad o directamente habían desaparecido. En este contexto, surge la metodología del Proceso de Dedicación para ofrecer una alternativa, asegurando que los Componentes de Grado Comercial pueden realizar su función de seguridad y son técnicamente equivalentes a los desarrollados bajo un programa de garantía de calidad nuclear.

Con el paso de los años, en base a la experiencia adquirida y los buenos resultados obtenidos, esta metodología ha demostrado ser efectiva y su uso se ha extendido rápidamente. Los procesos implicados han ido evolucionando y mejorando, hasta tal punto que la metodología del Proceso de Dedicación ha sido incluida en algunos estándares de calidad nuclear, como el NQA-1.

A diferencia de la Industria Nuclear, en la Industria Aeroespacial no existe una necesidad como tal que justifique de primeras el uso de componentes COTS. Sin embargo, como se ha comentado anteriormente, las ventajas que estos componentes presentan, como su bajo coste, su rápida disponibilidad o su avanzada tecnología, hacen atractivo su uso en aplicaciones relacionadas con la seguridad.

Es por este motivo que, aunque no existan unas directrices concretas y unos procesos bien definidos como los de la Industria Nuclear, las normativas que regulan los temas de certificación sí que contemplan la utilización de componentes comerciales.

El uso de COTS en la Industria Aeroespacial no está en un punto de madurez tan elevado como el de la Industria Nuclear. Esto es normal, puesto que en la Industria Nuclear la metodología del Proceso de Dedicación lleva mucho más tiempo implantada y todos los elementos de la cadena de suministro están familiarizados con los conceptos asociados.

Por estos motivos, está claro que hace falta tiempo para que el uso de componentes COTS en la Industria Aeroespacial se convierta en una práctica habitual. Para ello, es fundamental tomar la iniciativa y tratar de desarrollar los mecanismos necesarios para agilizar el proceso de certificación de este tipo de componentes.

Sin embargo, dejar la responsabilidad a los organismos reguladores no suele ser la mejor idea cuando se busca un cambio de paradigma de estas características. Para que esto pueda funcionar, no sólo es necesario que las empresas interesadas pongan de su parte, sino que también se necesita el tiempo suficiente para que la idea se implante.

Para finalizar, aclarar que los cambios en una industria como la Aeroespacial nunca resultan sencillos, pero el hecho de que otras industrias como la Nuclear hayan implantado con éxito esta metodología es un cabo al que aferrarse para continuar trabajando sobre esta premisa en el futuro.

Bibliografía

[1] Nucleonova. *Quiénes somos*. 2023. URL: https://www.nucleonova.es/compania/quienes-somos/ (vid. pág. 2).

[2] Real Academia Española. *seguridad*. 2023. URL: https://dle.rae.es/seguridad (vid. pág. 5).

[3] Real Academia Española. *seguro*. 2023. URL: https://dle.rae.es/seguridad (vid. pág. 5).

[4] Organización de Aviación Civil Internacional. *Anexo 19 al Convenio sobre Aviación Civil Internacional: Gestión de la seguridad operacional*. 2.ª ed. Jul. de 2016 (vid. pág. 5).

[5] Filippo De Florio. *Airworthiness: An Introduction to Aircraft Certification and Operations*. 3.ª ed. 2016 (vid. pág. 6).

[6] Schallert, Christian. «Integrated safety and reliability analysis methods for aircraft system development using multi-domain object-oriented models». Tesis doct. Ene. de 2016. DOI: 10.14279/depositonce-4930 (vid. pág. 7).

[7] Agencia Estatal de Seguridad Aérea. *Libro blanco de cultura de seguridad para operadores aéreos*. 1.ª ed. 2022 (vid. pág. 8).

[8] William J. Perry. *Specifications & Standards - A New Way of Doing Business*. Memorandum for Secretaries of the Military Departments. Washington, jun. de 1994 (vid. pág. 9).

[9] Dan Friedlander. *COTS EEE parts in space applications: evolution overview*. 2016. URL: https://wpo-altertechnology.com/cots-eee-parts-in-space-applications-evolution-overview/ (vid. págs. 9, 10).

[10] Electric Power Research Institute. *Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications - Revision 1 to EPRI NP-5652 and TR-102260*. Technical Report 3002002982. Electric Power Research Institute, sep. de 2014, pág. 378. URL: https://www.epri.com/research/products/000000003002002982 (vid. págs. 13, 14, 24, 26, 28, 29, 69-74).

[11] American Society of Mechanical Engineers. *Quality Assurance Requirements for Nuclear Facility Applications*. Technical Report. American Society of Mechanical Engineers, 2022, pág. 368. URL: https://www.asme.org/codes-standards/find-codes-standards/nqa-1-quality-assurance-requirements-nuclear-facility-applications (vid. pág. 14).

[12] Nuclear Regulatory Commission. *NRC Regulations Title 10, Code of Federal Regulations*. Technical Report. Nuclear Regulatory Commission, ago. de 2023. URL: https://www.nrc.gov/reading-rm/doc-collections/cfr/index.html (vid. págs. 14, 18, 54).

[13] EUROCAE & RTCA. *ED-80/DO-254: Design Assurance Guidance for Airborne Electronic Hardware*. Standard ED-80/DO-254. EUROCAE & RTCA, abr. de 2000 (vid. págs. 31, 32, 54).

[14] EUROCAE & RTCA. *ED-12C/DO-178C: Software Considerations in Airborne Systems and Equipment Certification*. Standard ED-12C/DO-178C. EUROCAE & RTCA, dic. de 2011 (vid. pág. 31).

[15] European Union Aviation Safety Agency. *AMC 20-152A: Development Assurance for Airborne Electronic Hardware (AEH)*. Acceptable Means of Compliance AMC 20-152A. European Union Aviation Safety Agency, mar. de 2021 (vid. pág. 38).

[16] European Union Aviation Safety Agency. *EASA CM-SWCEH-001: Development Assurance of Airborne Electronic Hardware*. Certification Memoranda CM-SWCEH-001. European Union Aviation Safety Agency, ene. de 2018 (vid. pág. 41).

[17] Naciones Unidas. *Objetivos de Desarrollo Sostenible*. 2023. URL: https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/ (vid. pág. 61).

Apéndice A

Objetivos de Desarrollo Sostenible

El 25 de septiembre de 2015, los líderes mundiales adoptaron un conjunto de objetivos globales para erradicar la pobreza, proteger el planeta y asegurar la prosperidad para todos como parte de una nueva agenda de desarrollo sostenible. Cada objetivo tiene metas específicas que deben alcanzarse en los próximos 15 años [17].

Para alcanzar estas metas, todo el mundo tiene que hacer su parte: los gobiernos, el sector privado y los individuos de la sociedad civil. En la Figura A.1 se muestran los diecisiete Objetivos de Desarrollo Sostenible de la Agenda 2030.

Figura A.1: Objetivos de Desarrollo Sostenible [17]

En la Tabla A.1 se muestra el grado de implicación del presente trabajo con cada uno de los Objetivos de Desarrollo Sostenible.

Objetivos	**Alto**	**Medio**	**Bajo**	**No procede**
1. Fin de la pobreza				✓
2. Hambre cero				✓
3. Salud y bienestar				✓
4. Educación de calidad				✓
5. Igualdad de género				✓
6. Agua limpia y saneamiento				✓
7. Energía asequible y no contaminante		✓		
8. Trabajo decente y crecimiento económico				✓
9. Industria, innovación e infraestructura	✓			
10. Reducción de las desigualdades				✓
11. Ciudades y comunidades sostenibles			✓	
12. Producción y consumo responsables		✓		
13. Acción por el clima			✓	
14. Vida submarina				✓
15. Vida de ecosistemas terrestres				✓
16. Paz, justicia e instituciones sólidas				✓
17. Alianzas para lograr los objetivos	✓			

Tabla A.1: Objetivos de Desarrollo Sostenible

En particular, es necesario destacar la implicación del trabajo con los siguientes Objetivos de Desarrollo Sostenible, ordenados de mayor a menor importancia:

- **Industria, innovación e infraestructura** (alto): El contenido de este trabajo está relacionado intrínsecamente con la industria y la innovación, ya que propone una metodología diferente para afrontar los procesos de diseño y desarrollo de los sistemas de la aeronave.
- **Alianzas para lograr los objetivos** (alto): Dado que la metodología descrita en este trabajo se centra en la utilización de componentes comerciales en la Industria Aeroespacial, es necesario desarrollar alianzas entre las empresas del sector, los organismos reguladores y los fabricantes comerciales para lograr el cumplimiento de los objetivos.
- **Energía asequible y no contaminante** (medio): Los componentes comerciales cuentan con la última tecnología disponible y son desarrollados con el objetivo de garantizar una energía asequible y libre de contaminación.
- **Producción y consumo responsables** (medio): La evolución de los componentes comerciales sigue una línea orientada a la producción y el consumo responsable.
- **Ciudades y comunidades sostenibles** (bajo): Los objetivos anteriores ayudan a crear y sostener ciudades y comunidades sostenibles.
- **Acción por el clima** (bajo): La evolución de la tecnología permite la producción de componentes más eficientes y respetuosos con el medio ambiente.

Apéndice B

Pliego de condiciones

B.1. Hardware

El presente trabajo ha sido elaborado en su totalidad a través de medios electrónicos. No se ha utilizado ni tinta ni papel para la realización del mismo. En su lugar, se ha utilizado un ordenador portátil con las siguientes características técnicas:

- **Modelo:** Acer Aspire 5 A515-51G-8151
- **Sistema Operativo:** Windows 11
- **Procesador:** Intel© Core™ i7-8550U 1.8 GHz with Turbo Boost up to 4.0 GHz
- **Tarjeta gráfica:** NVIDIA© GeForce© MX130 with 2 GB VRAM
- **Memoria:** 8 GB DDR4 Memory
- **Almacenamiento:** 1000 GB HDD + 500 GB SSD

B.2. Software

Para la elaboración del trabajo se han utilizado los siguientes programas:

- Adobe Acrobat Reader: gratuito.
- Inkscape: gratuito.
- Canva: gratuito.
- Overleaf: gratuito.
- Libre Office: gratuito.

B.3. Presupuesto

Para la elaboración del trabajo se han empleado un total de 350 horas. Este tiempo cubre los 13,5 créditos asignados al Trabajo Final de Máster.

El trabajo se ha realizado durante la estancia en una empresa, primero con un contrato de prácticas y posteriormente con un contrato de formación. El sueldo medio durante este periodo asciende aproximadamente a 1.000,00 €/mes.

Teniendo en cuenta que este sueldo corresponde a una jornada laboral de 8 horas/día con 20 días laborables al mes, el sueldo por hora es de 6,25 €/hora. En total, el coste de las horas empleadas en la realización del trabajo asciende a 2.187,5 €.

En cuanto al coste del hardware, el ordenador portátil fue adquirido en el año 2018, por lo que se considera amortizado en su totalidad. No obstante, se imputará una cantidad estimada de 500 €, suficiente para adquirir un ordenador de características similares.

Como se ha mencionado en el apartado anterior, el software utilizado en la realización del trabajo es completamente gratuito, por lo que no se le imputa coste alguno.

En cuanto al material bibliográfico consultado, todas las normas están disponibles de manera gratuita salvo una, la RTCA DO-254, que tiene un coste de 295,00 $, que son aproximadamente 275,00 € al cambio.

El la Tabla B.1 se muestra un desglose con todos los costes asociados al trabajo.

Partidas	**Importe**
Horas	2.187,50 €
Hardware	500, 00 €
Software	0,00 €
Normativa	275,00 €
Total	2.962,00 €

Tabla B.1: Presupuesto del trabajo

El presupuesto total del trabajo asciende a un total de **DOS MIL NOVECIENTOS SESENTA Y DOS EUROS**.

B.4. Normativa

La redacción del trabajo ha sido realizada teniendo en cuenta los aspectos indicados en la **NORMATIVA DE TRABAJOS DE FIN DE GRADO Y TRABAJOS DE FIN DE MÁSTER DE LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA**, aprobada por el Consejo de Gobierno en sesión de 21 de julio de 2022 y publicada en el Butlletí Oficial de la Universitat Politècnica de València Núm. 118/2022, con fecha del 27 de julio de 2022.

Apéndice C

Form CGI1 Rev. 0

A la hora de documentar la Evaluación Técnica de un Proceso de Dedicación de Componentes de Grado Comercial no existe un único formato estandarizado. Lo más común es que cada organización tenga su propio formato para documentar la Evaluación Técnica y que estos presenten diferencias entre sí. En algunos casos, los distintos elementos que forman parte de la Evaluación Técnica no tienen por qué estar recogidos en un mismo documento.

En la EPRI NP-5652 & TR-102260 Rev. 1 se proporciona un formato básico de ejemplo para que pueda ser tomado por las distintas organizaciones como referencia para documentar la Evaluación Técnica de un Componente de Grado Comercial [10]. Sin embargo, este formulario no incluye ciertos aspectos a tener en cuenta para llevar a cabo una Evaluación Técnica completa, como la clasificación de seguridad o la evaluación de equivalencia.

En las Figuras C.1 a C.5 se muestra el formato básico de ejemplo incluido en la EPRI NP-5652 & TR-102260 Rev. 1 [10].

Commercial Grade Item Dedication Technical Evaluation

EPRI Joint Utility Task Group
Form CGI1, Rev. 0

Evaluation Number _____ **Revision** _____

SECTION A ITEM DESCRIPTION

INVENTORY CONTROL NO:	
NOUN IDENTIFIER:	
MANUFACTURER NAME:	MANUFACTURER MODEL / PART / CATALOG NUMBER(S)

SECTION B END USE / PARENT / HOST EQUIPMENT INFORMATION

Note: If the specific end-use(s) / plant applications are not known, complete Section C of this form in lieu of Section B prior to proceeding.

☐ Not Applicable (Section C Completed Below)

EQUIPMENT ID (TAG) NUMBERS OR DESCRIPTION OF ITEM USAGE:	
PARENT COMPONENT/HOST DESCRIPTION:	
FUNCTIONAL SAFETY CLASS OF COMPONENT / HOST:	BASIS / SOURCE:
☒ Safety-Related ☐ Non-Safety Related (If non-safety, item is not a candidate for dedication)	

IDENTIFICATION OF PARENT COMPONENT/HOST EQUIPMENT FUNCTION(S)		
FUNCTIONAL MODE	BASIC SAFETY FUNCTION(S)	DESCRIBE (AS REQUIRED)
☐ Active ☐ Passive		
☐ Active ☐ Passive		
☐ Active ☐ Passive		
☐ Active ☐ Passive		

PARENT COMPONENT/HOST EQUIPMENT IS (CHECK ALL THAT APPLY):

☐ EQ	☐ ASME SECTION III
☐ CLASS 1E	☐ CONTAINMENT PRESSURE BOUNDARY
☒ SEISMIC CLASS 1	☐ SERVICE LEVEL 1 COATING
☐ OTHER: (see below)	

Figura C.1: Form CGI1 Rev. 0, Secciones A y B [10]

Commercial Grade Item Dedication Technical Evaluation | **EPRI Joint Utility Task Group** Form CGI1, Rev. 0

Evaluation Number _____ **Revision** _____

SECTION C BOUNDED SCOPE OF USE

Only complete Section C when specific end-use of the item being dedicated unknown.

☐ Not Applicable (Section B Completed Above)

Is the item being dedicated a commodity or standard item designed and constructed in accordance with an industry standard?	☐ Yes ☐ No
IF "YES", LIST THE STANDARD(S) BELOW	
LIST FUNCTIONS AND/OR APPLICATIONS CONSIDERED WHEN COMPLETING THIS EVALUATION	
EQUIPMENT QUALIFICATION CONSIDERATIONS / LIMITATIONS (CHECK ALL THAT APPLY):	
CONSIDERATION ☐ ENVIRONMENTAL QUALIFICATION ☐ SEISMIC QUALIFICATION ☐ OTHER: (see below)	**QUALIFICATION BASIS / LIMITATIONS OF USE:**

SECTION D ITEM INFORMATION

ITEM DESCRIPTION:	
FUNCTIONAL SAFETY CLASS OF ITEM: ☐ Safety-Related ☐ Non-Safety Related (If non-safety, item is not a candidate for dedication)	**BASIS / SOURCE:**

IDENTIFICATION OF ITEM FUNCTION(S)

FUNCTIONAL MODE	BASIC SAFETY FUNCTION(S)	DESCRIBE (AS REQUIRED)
☐ Active ☐ Passive		
☐ Active ☐ Passive		
☐ Active ☐ Passive		

Figura C.2: Form CGI1 Rev. 0, Secciones C y D [10]

Commercial Grade Item Dedication Technical Evaluation | **EPRI Joint Utility Task Group** Form CGI1, Rev. 0

Evaluation Number _____ **Revision** _____

ITEM IS (CHECK ALL THAT APPLY):	
☐ EQ	☐ ASME SECTION III
☐ CLASS 1E	☐ CONTAINMENT PRESSURE BOUNDARY
☐ SEISMIC CLASS 1	☐ SERVICE LEVEL 1 COATING
☐ OTHER: (see below)	
Click here to enter text.	

SECTION E ELIGIBLITY FOR DEDICATION

Is the item eligible for dedication in accordance with 10CFR, Part 21? **If the answer is no, this item cannot be dedicated.**	☒ Yes ☐ No

SECTION F FAILURE MODES / MECHANISMS AND EFFECTS ANALYSIS

CREDIBLE FAILURE MODE/MECHANISM	EFFECTS ON SYSTEM/COMPONENT FUNCTION
BASIS FOR SELECTION OF CREDIBLE FAILURE MODE(S)/MECHANISM(S)	

SECTION G OPERATING EXPERIENCE / HISTORICAL PERFORMANCE INFORMATION

SOURCES REVIEWED AND RESULTS

Figura C.3: Form CGI1 Rev. 0, Secciones E a G [10]

Commercial Grade Item Dedication
Technical Evaluation

EPRI Joint Utility Task Group
Revision 0

Evaluation Number _____ Revision _____

SECTION H IDENTIFICATION ATTRIBUTES

IDENTIFICATION ATTRIBUTES	DESCRIPTION OF INSPECTION	ACCEPTANCE CRITERIA
Manufacturer	Visual	
Identification Number	Visual	

SECTION I CRITICAL CHARACTERISTICS

CRITICAL CHARACTERISTICS	ACCEPTANCE METHOD	DESCRIPTION OF ACCEPTANCE ACTIVITY	SAMPLING PLAN	ACCEPTANCE CRITERIA (INCLUDING TOLERANCES)
DESCRIPTION OF SAMPLING PLANS (if "see below" is selected in the sampling plan column above)				
SAFETY FUNCTION(S) SUPPORTED / BASIS FOR SELECTION OF CRITICAL CHARACTERISTICS / ACCEPTANCE CRITERIA INCLUDING MAINTAINING SEISMIC AND ENVIRONMENTAL QUALIFICATION				

Page 4 of 5

Figura C.4: Form CGI1 Rev. 0, Secciones H e I [10]

Commercial Grade Item Dedication
Technical Evaluation

EPRI Joint Utility Task Group
Revision 0

Evaluation Number _____ **Revision** _____

BASIS FOR SELECTION OF SAMPLING PLANS (IF SAMPLING PLANS ARE USED)

SECTION J REFERENCES

DOCUMENT / SOURCE	REVISION / DATE	COMMENTS

SECTION K REVIEW AND APPROVAL

Prepared by: _____ Date: _____

Reviewed by: _____ Date: _____

Figura C.5: Form CGI1 Rev. 0, Secciones J y K [10]

Apéndice D

Formulario ECMP Rev. 0

A la hora de documentar el Proceso de Gestión de Componentes Electrónicos no existe un formato estandarizado. A lo largo del Apartado 4.4 se han ido introduciendo varias tablas, a modo de resumen, con los puntos más importantes a tener en cuenta en este aspecto.

La idea de este apartado es la de proporcionar un formulario de ejemplo, similar al mostrado en el Apéndice C para el desarrollo de la Evaluación Técnica, que sirva como herramienta para el desarrollo de un Proceso de Gestión de Componentes Electrónicos y de esta manera permita obtener la certificación deseada. Para lograr este objetivo, se han utilizado las tablas mencionadas en el párrafo anterior.

En las Figuras C.1 a C.5 se muestra el formato final del formulario desarrollado durante el Capítulo 4.

Proceso de Gestión de Componentes Electrónicos — Formulario ECMP Rev. 0
Referencia:

PARTE A: CLASIFICACIÓN DEL DISPOSITIVO

SECCIÓN A.1: NIVEL DE GARANTÍA DE DESARROLLO

○ Nivel A ○ Nivel B ○ Nivel C ○ Nivel D ○ Nivel E

Notas:

A: Catastrófico; **B**: Peligroso / Grave-Mayor; **C**: Mayor; **D**: Menor; **E**: Sin efecto

SECCIÓN A.2: TIPO DE DISPOSITIVO

○ Circuito integrado ○ Microcontrolador

SECCIÓN A.3: DETERMINACIÓN DE LA COMPLEJIDAD

		Sí	No
1	¿Es posible verificar todos los requisitos en todas las configuraciones posibles mediante pruebas sobre el propio dispositivo?	○	○
2	¿El componente es un microcontrolador con varias CPU que usan el mismo bus, varios periféricos complejos dependientes entre sí que intercambian datos o varios buses integrados utilizados de forma dinámica?	○	○
–	**SÍ** a la pregunta 1 → **SIMPLE**	○	○
–	**NO** a la pregunta 1 y **NO** a la pregunta 2 → **COMPLEJO**	○	○
–	**NO** a la pregunta 1 y **SÍ** a la pregunta 2 → **MUY COMPLEJO**	○	○

Tabla D.1: Formulario ECMP Rev. 0, Parte A

Proceso de Gestión de Componentes Electrónicos — Formulario ECMP Rev. 0
Referencia:

PARTE B: DATOS DEL DISPOSITIVO

SECCIÓN B.1: REVISIÓN DOCUMENTAL

○	Ficha técnica: _____	○	Manual de usuario: _____
○	Fe de erratas: _____	○	Manual de erratas: _____
○	Otros: _____	○	Manual de instalación: _____

SECCIÓN B.2: DATOS DE DISEÑO

		Sí	No
1	¿Los datos del dispositivo están disponibles y son consistentes con los requisitos del dispositivo?	○	○
–	**SÍ** a la pregunta 1 → **Parte C**	○	○
–	**NO** a la pregunta 1 → **Preguntas 2, 3 y 4**	○	○
2	¿El fabricante tiene un sistema de calidad implantado y este es aplicado al dispositivo en cuestión?	○	○
3	¿El fabricante tiene un proceso de fabricación determinista y repetible?	○	○
4	¿El fabricante realiza un proceso de aprobación interno y cuenta con procedimientos de prueba y criterios de aceptación documentados?	○	○

Notas: Si el dispositivo es un microcontrolador muy complejo y la documentación pública del fabricante no es suficiente se ha de acceder a la documentación privada.

Página 2 de 7

Tabla D.2: Formulario ECMP Rev. 0, Parte B

Proceso de Gestión de Componentes Electrónicos Formulario ECMP Rev. 0
Referencia:

PARTE C: DOMINIO DE USO DEL DISPOSITIVO

SECCIÓN C.1: FUNCIONES DEL DISPOSITIVO

	U	N/U
1	○	○
2	○	○
3	○	○

Notas:

U: Utilizada; **N/U**: No Utilizada

SECCIÓN C.2: MEDIOS PARA DESACTIVAR LAS FUNCIONES

1
2
3

SECCIÓN C.3: MEDIOS EXTERNOS PARA CONTROLAR LAS FUNCIONES

1
2
3

Notas: Los medios externos han de controlar cualquier activación inesperada de las funciones no utilizadas o cualquier desactivación inesperada de las funciones utilizadas.

Tabla D.3: Formulario ECMP Rev. 0, Parte C

Proceso de Gestión de Componentes Electrónicos — Formulario ECMP Rev. 0
Referencia:

PARTE C: DOMINIO DE USO DEL DISPOSITIVO (CONT.)

SECCIÓN C.4: MEDIOS EXTERNOS PARA CONTROLAR EL REINICIO
1
2
3
SECCIÓN C.5: CONFIGURACIÓN DE ENCENDIDO
SECCIÓN C.6: CONFIGURACIÓN DE RELOJ
SECCIÓN C.7: CONDICIONES DE USO

Tabla D.4: Formulario ECMP Rev. 0, Parte C (Cont.)

Proceso de Gestión de Componentes Electrónicos — Formulario ECMP Rev. 0
Referencia:

PARTE D: ACTIVIDADES DE VERIFICACIÓN

SECCIÓN D.1: PRUEBAS

SECCIÓN D.2: ANÁLISIS

PARTE E: ANÁLISIS DE LAS ERRATAS DEL DISPOSITIVO

SECCIÓN E.1: RECOPILACIÓN DE ERRATAS

	A	N/A
1	○	○
2	○	○
3	○	○

Notas:

A: Aplicable; **N/A**: No Aplicable

SECCIÓN E.2: MEDIOS PARA MITIGAR LAS ERRATAS APLICABLES

Tabla D.5: Formulario ECMP Rev. 0, Partes D y E

Proceso de Gestión de Componentes Electrónicos — Formulario ECMP Rev. 0
Referencia:

PARTE F: GESTIÓN DE LA CONFIGURACIÓN DEL DISPOSITIVO

SECCIÓN F.1: CONFIGURACIÓN DEL DISPOSITIVO

		Sí	No
1	¿El fabricante identifica y documenta la configuración del dispositivo?	○	○
2	¿El fabricante garantiza que puede replicar de forma adecuada y consistente la configuración del dispositivo?	○	○
3	¿El fabricante controla y documenta los cambios realizados en el dispositivo?	○	○
4	¿El fabricante proporciona una descripción adecuada de los cambios realizados?	○	○

SECCIÓN F.2: CONTROL DE CAMBIOS

1	
2	
3	

PARTE G: ANÁLISIS MODAL DE FALLOS Y EFECTOS

Función	Modo de fallo	Efecto	Causa	Característica

Tabla D.6: Formulario ECMP Rev. 0, Partes F y G

Proceso de Gestión de Componentes Electrónicos — Formulario ECMP Rev. 0
Referencia:

PARTE H: EXPERIENCIA OPERATIVA DEL PRODUCTO

	Sí	No
¿La experiencia operativa puede ser clasificada como suficiente atendiendo a los criterios descritos en CM-SWCEH-001 Issue 1 Rev. 2?	○	○

PARTE I: ESTRATEGIAS DE MITIGACIÓN

SECCIÓN I.1: ANÁLISIS DE CAUSA RAÍZ

Problema	Síntoma	Posible causa raíz	Causa raíz real	Solución

SECCIÓN I.2: MÉTODOS DE MITIGACIÓN

SECCIÓN I.3: ANÁLISIS DE PARTICIÓN

Tabla D.7: Formulario ECMP Rev. 0, Partes H e I