ANAC-EASA-FAA-TCCA

Certification Management Team (CMT) Task Specific Team (TST)

Interpretation harmonization addressing Common Modes Errors in Critical Systems in Large Aircraft

1. Introduction

1.1 Overview

The civil aviation industry has expressed concern about the differences in certification criteria between civil certification authorities regarding common mode errors in critical systems. These differences are leading to inefficient and lengthy project validation efforts between authorities and undermining the drive to harmonize airworthiness requirements, guidance, and interpretation.

In order to address this concern, the Certification Management Team (CMT) created a Task Specific Team (TST), comprising senior-level experts from ANAC, EASA, the FAA and TCCA, to engage in policy discussions and seek harmonization. The TST, herein referred to as CME (Common Mode Error) TST, met between February 2022 and April 2025, both virtually and in person.

Interim policy harmonization results were presented to and endorsed by the Certification Management Team Secretariate (CMTS) in June 2023 and presented to industry at the SAE S-18 meeting in January 2024, and the EUROCAE WG-63 meeting in March 2024. Final policy harmonization results and recommendations were presented to and endorsed by the CMTS.

This report documents the results of the CME TST activities and provides a harmonized framework for evaluating critical systems on large transport aircraft with regard to common mode development errors. It is intended for use by both civil certification authorities and industry.

1.2 CME TST Statement of Issue

Based on the initial tasking by the CMT, the following statement of issue was developed by the CME TST in the initial phase of discussion to scope the activity and focus the harmonization effort:

"It is required by rule (CS 25.1309 [1]) or in advisory material (AC 25.1309-1A [6] /AMC 25.1309 [5]), that "Any catastrophic failure condition does not result from a single failure". Single failures may either be random or result from common failures in similar elements (due to lack of independence). Common cause evaluation techniques are applied to identify and assess the potential consequences of the common failure mechanisms or events to show compliance with the "no single failure" requirement. Since errors may cause failures; errors in development, manufacturing, installation, and maintenance could also result in common cause failures (including common mode failures) and therefore these error sources should also be assessed using the same common-cause and cascading failure consideration techniques.

Industry common mode evaluation techniques are qualitative in nature which has resulted in the difficulty of establishing consistent measure of acceptable failure and error mitigation criteria across authority applications. There have been recurrent discussions related to the question whether development assurance and quality assurance activities are sufficient to limit the likelihood of errors to an acceptable level of safety for the considered failure condition and its associated consequence. This is discussed in parallel, and sometimes in

contrast, to the principle of having designs which are inherently error tolerant by virtue of the design architecture, monitoring or dissimilarity. Guidance material defining acceptable means for addressing common failures and errors to a commonly accepted level is also limited.

The purpose and scope of this task will be to discuss and harmonise a policy which identifies the acceptable means of addressing common mode failure and error for compliance to CS 25.1309 [1] / 14 CFR 25.1309 [2]. This policy may also provide guidance on techniques that applicants can use to describe and facilitate discussions with the authority about the amount of risk or residual error that remain in their design. Any remaining differences in the approach between the participating regulatory agencies will also be identified. The harmonization effort will use flight control system functions as the initial discussion focus, but the resulting policy aims to broadly address all systems having potentially catastrophic failure conditions."

It should be noted that the scope of the task evolved from the above Statement of Issue as the CME TST work progressed. As such it is recognized that the scope of this final report (section 1.3) does not entirely align with the objectives initially laid out in the statement of issue.

1.3 Report Scope

In response to industry concerns and to improve alignment between certification authorities, the CME TST developed a harmonized framework for evaluating flight critical systems on large transport aircraft with regard to common mode development errors, which is presented in this report.

This report:

- Provides confirmation of the applicable regulations and guidance material;
- Provides alignment on terminology;
- Clarifies the compliance intent regarding common mode development errors;
- Describes, at a high level, a methodology for performing Common Mode Error tolerance assessments;
- Discusses various considerations relevant to performing a Common Mode Error tolerance assessment, and evaluating its results for acceptability.

The report addresses CS 25 / 14 CFR Part 25 / RBAC 25 / AWM 525 [1, 2, 3, 4], as the CMT tasking was specifically targeted at large transport airplanes. The CME TST recognizes that other product categories have similar 'no single failure' requirements, and therefore may be subject to similar concerns regarding common mode errors. While the framework presented in this report may be found useful for use on other product categories, the CME TST has no position on its applicability outside of CS 25 / 14 CFR Part 25 / RBAC 25 / AWM 525.

Historically, most difficult compliance discussions regarding common mode errors have focused on electronic flight control systems (i.e. fly-by-wire (FBW)). As a result, FBW systems were often used as practical examples in the CME TST deliberations, but as much as possible the group strived to develop a framework of general applicability, in line with the intent per the Statement of Issue to broadly address all systems having potentially catastrophic failure conditions.

Per AMC 25.1309 [5] guidance, common mode errors to be considered as part of the Common Mode Analysis (CMA) include specification (requirements), design, implementation, installation, maintenance, and

manufacturing errors. The CME TST agreed to limit the scope of the task and focus harmonization efforts on development errors, i.e. requirements, design and implementation errors, which have triggered the most difficulties on certification projects. However, it should not be inferred that other error sources are out of the common mode analysis' scope. In particular, some authorities noted an increasing concern about manufacturing errors. The Conclusions and Recommendations section of this report recommends further activities for harmonization in this area.

1.4 Terminology

The CME TST identified inconsistent terminology and terminology usage, both by industry and different certification authorities, as one of the key areas affecting clear communication when discussing common mode error concepts. Early in the CME TST activities, efforts were made to align the relevant terminology and use it consistently in the group's discussions, in interim communications with industry, and in the development of this report.

In general, the existing terminology and definitions in regulatory guidance [5, 7] and industry-recommended practices [10, 11, 12, 13,] are considered applicable in the context of this report. One important exception is the use of the term 'Common Mode Error' (CME) in this report instead of the term 'Common Cause Error' used in industry practices [10, 11, 12, 13]. The CME TST believes the term 'Common Mode Error' used in this report more directly reflects the concept of interest and also notes that this is the term generally used in discussions with applicants.

Where necessary, the CME TST has also defined additional terms within this report, in the context where the corresponding concepts are discussed. These are summarized in Annex 1.

2. Regulatory Framework and Relevant Guidance

2.1 Comparative review

The CME TST performed a comparative review of the applicable certification requirements and confirmed that all authorities have equivalent requirements, as relevant to common mode error considerations for compliance. To simplify the text of this report, generic references to 25.xxxx will be used to represent the corresponding CS 25 / 14 CFR Part 25 / RBAC 25 / AWM 525 [1, 2, 3, 4] certification requirements.

The CME TST agreed:

- The requirements of 25.671(c) and 25.1309(b) [1, 2, 3, 4] are the primary applicable requirements under which common mode errors are addressed for compliance.
- Other requirements could also be relevant (e.g. 25.601, 25.901, 25.1585), but these would not be driving CME expectations, hence will not be specifically addressed in this report.

It should be noted that in the European regulatory hierarchy, a 'no-single failure' criterion also exists in the Essential requirements for airworthiness [14], which are attached at the highest level of European Union regulations, above the EASA CS 25 [1] requirements. This essential requirement reads, in part: "*... any catastrophic failure condition does not result from a single failure..*".

The CME TST also agreed that the advisory material associated with the primary applicable regulations was also equivalent for the purpose of addressing common mode errors for compliance:

- AMC 25.1309 [5] and ARAC SDHWG Report aka Arsenal Draft AC 25.1309 recommendation [7]
- AMC 25.671 [8] and ARAC FCHWG Report, Draft AC 25.671 recommendations [9]

The FAA safety rulemaking activities (NPRM 23-04) were still ongoing during the CME TST activities, and the FAA completed revisions *during* the finalization of this report. The final FAA rulemaking material issued as 14 CFR Amt. 25-152, including associated guidance, has not been evaluated in the context of the CME TST activity and is not reflected in this report, but the CME TST does not expect it would significantly impact the conclusions. A recommendation has been added in section 6 to identify any impacts of the FAA safety rulemaking of 14 CFR Amt. 25-152 may have on the CME TST harmonization efforts herein.

Industry-recommended practices which are referenced in the above advisory material were used by the CME TST as foundational material:

- SAE ARP4761A / EUROCAE ED-135 [12, 13]
- SAE ARP4754B / EUROCAE ED-79B [10, 11]
- RTCA DO-178C/ED-12C [15, 16]
- RTCA DO-254/ED-80 [17, 18]

All documentation referenced within this report has been captured in Annex 2 – Reference Documents:.

2.2 Overview of applicable requirements and guidance

25.671(c)(1) requires that the airplane be shown capable of continued safe flight and landing following any single failure in the flight control system within the normal flight envelope. A failure condition that would prevent continued safe flight and landing would be classified as catastrophic under 25.1309.

The advisory material for 25.671 [8, 9] states that for compliance with 25.671(c)(1), all single failures must be considered regardless of their probability. This advisory material does not provide detailed guidance on development errors but refers to the guidance for 25.1309 (and associated industry guidelines) to address these aspects.

25.1309(b)(1) requires that single failures do not result in a catastrophic failure condition.

Regarding single failures, the advisory material for 25.1309 [5, 6, 7] indicates that failure containment should be provided by the system design to limit the propagation of the effects of any single failure to preclude catastrophic failure conditions. The guidance also indicates that there must be no common cause failure that could affect both the single component, part or element and its failure containment provisions. Since errors may cause failures, the guidance identifies errors as a potential source of common cause failures and clarifies that in performing common mode analyses the effects of errors – including development errors – should be considered.

3. Compliance intent for Common Mode Development Errors

3.1 Development Errors

Per the AMC 25.1309 [5] guidance material definitions, development errors are mistakes in requirements determination, design, or implementation. Errors are not failures but may lead to failures.

A generalized example of this concept is presented in Figure 1, showing the potential progression of a development error to failure conditions. Development errors are pre-existing in the certified design, but require

specific conditions in order for them to manifest as faults. Such conditions could include state, inputs, operating and environmental conditions, crew actions, etc, or combinations thereof. Such conditions, or combinations of conditions, likely were not explicitly anticipated and therefore not addressed as part of validation and verification during development.

A fault is the manifestation of an error resulting in an undesired behavior or effect at the local level (item). Once a fault occurs, it may result in various outcomes:

- It may be contained at a local level (e.g. item, component), without any detectable or detected effect, i.e. without affecting the intended function.
- It may result in a failure, i.e. affect the operation of the system, equipment or item such that it can no longer function as intended, either due to loss of function or malfunction. Failures may be detected and managed within the system (e.g. monitoring, voting, limiting, etc) without system-level effect, or may result in system or aircraft-level effects.
- The failure is assessed (e.g., FHA, PASA, PSSA, SSA) for its effects at the system and aircraft level, and the resulting failure condition classification is determined. For the purpose of this report, the scope of interest is limited to errors potentially resulting in catastrophic (CAT) failure conditions.

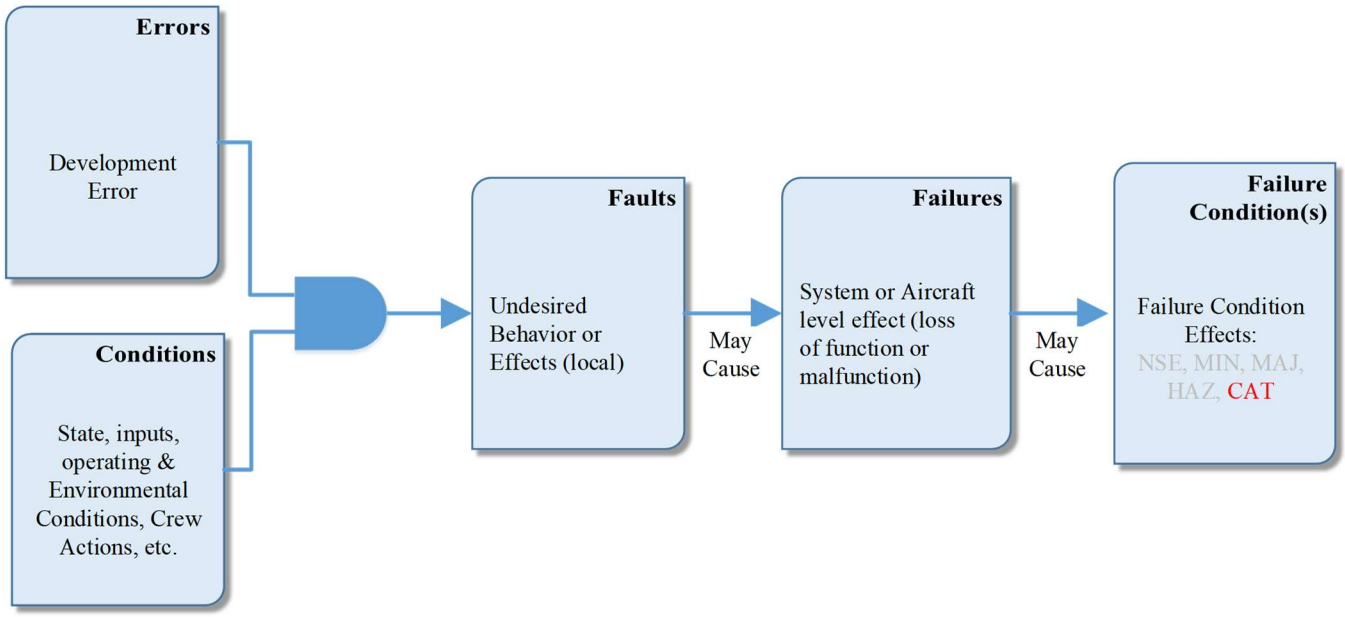

Figure 1 Error to Failure Condition Progression

As described in references [10, 11], the development of aircraft and aircraft systems is a hierarchical and iterative process. Mistakes, i.e. development errors, can be introduced in the requirements, design, or implementation at all levels as shown in Figure 2. Mistakes may occur within a level (i.e aircraft, system (or sub-subsystem), equipment, or item) or between levels. The mistakes may occur in the design formulation, in the capture of requirements for the design, or in the flowdown of the requirements to another layer. For compliance, development errors therefore have to be addressed at all levels.

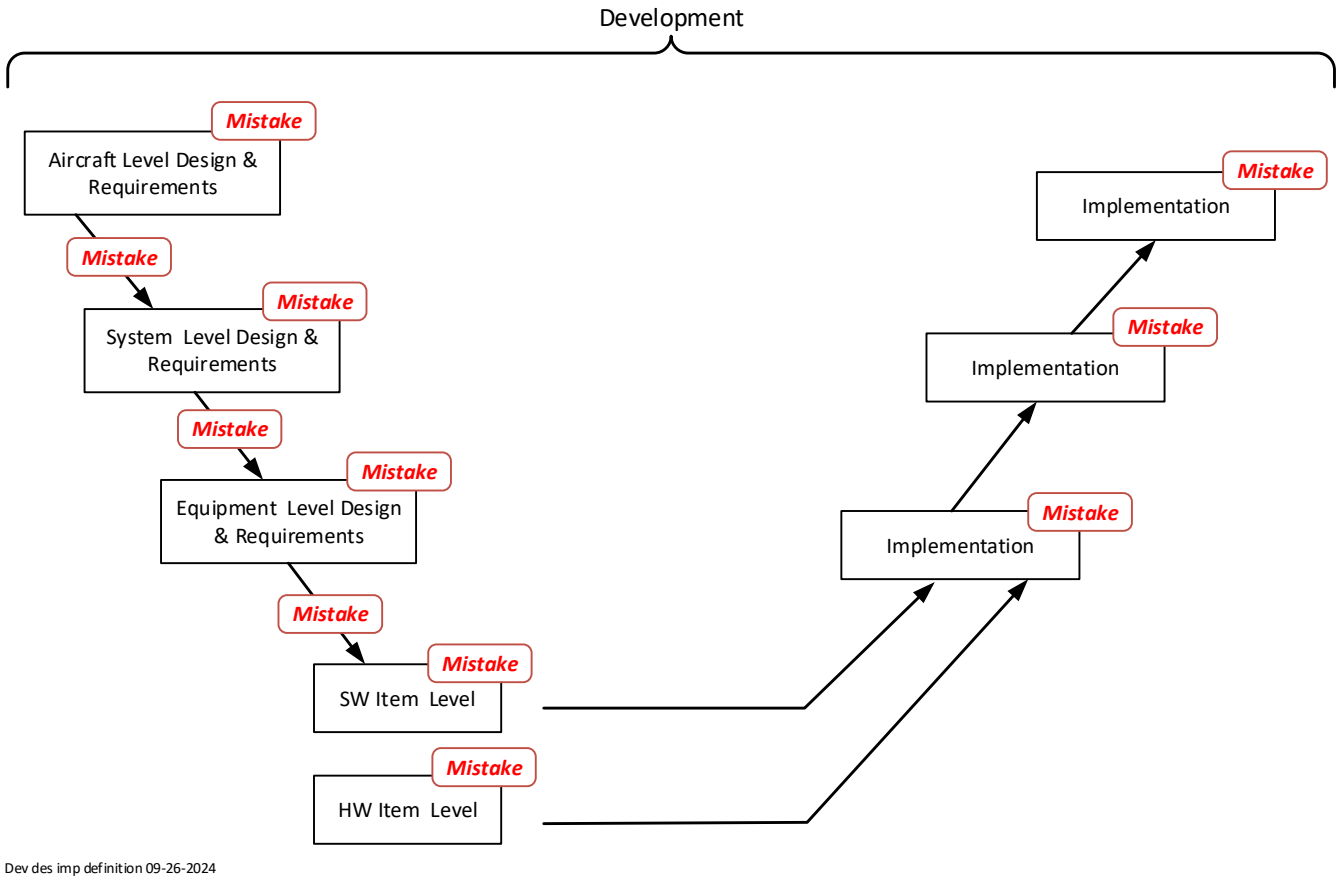

Figure 2 Introduction of Mistakes during Development

3.2 Concepts of minimization and tolerance

As discussed in Section 2, the applicable certification requirements and associated guidance do not allow single failures to result in catastrophic consequences. The guidance is however not explicit regarding the consequences of single development errors. In order to clarify the compliance intent, the CME TST used the concepts of 'minimization' and 'tolerance', which are presented and discussed in this section.

Minimization, as applied to failure and errors, is a **design development objective** intended to reduce the likelihood of failures or errors remaining in the certified design to a level commensurate with the safety consequences of the failure or error.

Tolerance, as applied to failures and errors, is a **design property**, intended to lessen the safety consequences of a failure or error, if it occurs (failure), or manifests itself (error) in service.

3.2.1 Failures, minimization and tolerance

Applying the concepts of minimization and tolerance to **failures** refers to the following:

- Failure **minimization** for compliance refers to achieving a reliable design that limits the occurrence of failures in service. Failure minimization broadly relates to a range of activities performed for compliance with 25.1309(a) [5], such as equipment environmental qualification, endurance testing, use of state-of-the-art design practices, choice of components, materials, etc. This also overlaps with safety compliance under 25.1309(b) [5] since impacting component reliability, and hence failure rates, etc.

- Failure **tolerance** for compliance refers to a range of safety assessment activities performed for compliance with 25.1309(b) [5]. This includes the 'no single failure leading to catastrophic' criterion (fail-safe design principle), including relevant common cause considerations. Design choices such as architecture, layout, redundancy, and system monitors to detect and passivate or reduce the severity of failures would all contribute to failure tolerance regardless of hazard severity.

  Failure minimization and failure tolerance are both necessary to demonstrate compliance. One technique does not replace the other; they are complementary.

  For single failures leading to a catastrophic failure condition, the compliance expectation is to **eliminate** the failure mechanism through the application of the fail-safe design principles (as described in the AC/AMC [5, 7]), resulting in a failure-tolerant design.

3.2.2 Errors, minimization and tolerance

Applying the concepts of minimization and tolerance to **errors** refers to the following:

- Error **minimization** for compliance refers broadly to the development assurance activities at the aircraft and system level (ARP4754 [10, 11]), and to the design assurance activities at the item level (DO-178 [15, 16], DO-254 [17, 18]). The intent of these activities is to provide a level of confidence that the system and items development have been accomplished in a sufficiently disciplined manner to limit the likelihood of development errors that could impact safety. Design simplicity also contributes to error minimization.

- Error **tolerance** for compliance refers to protecting against exposure to a single development error potentially having catastrophic safety effects at the aircraft level. Design choices such as diversity (in requirements, design, implementation), architectural choices, and features such as monitoring which would provide containment or reduce the severity effects of a development error all contribute to error tolerance. Tolerance provides protection for 'unknowns'.

Both error minimization and error tolerance are necessary to adequately address common mode development errors for compliance. One technique does not replace the other, they are complementary.

With respect to error minimization, the CME TST expects consistent application of development assurance methods at aircraft, system, and item levels to minimize the likelihood of development errors that could impact aircraft safety. Error minimization techniques are not developed further in this report. For guidance, the applicant should refer to the relevant industry practices [10, 11, 12, 13].

In assessing development error tolerance, the starting point must be a design and architecture already meeting the fail-safe design principles, i.e. a design that is failure-tolerant. On this basis, a 'single path' design where

single failures could result in catastrophic effects would not be compliant, and should not need to be evaluated for development error tolerance considerations. The methodology and considerations for error tolerance presented in this report are therefore focusing on common mode development errors (CME), where a single development error could affect (negate) the assumed independence of multiple elements.

For critical systems, the applicant is expected to include a CME assessment, addressing error tolerance aspects, as part of the CMA and therefore as part of the overall safety process. CME considerations should be reflected in the safety requirements flow down as necessary, from the aircraft level to the item level.

It is recognized that dependent on the system, full tolerance to common mode development errors – at all levels – may be impractical. The compliance expectation in providing error tolerance is to minimize the exposure of the design to common mode errors leading to a catastrophic aircraft level effect (i.e. minimize areas where the design is not tolerant to such errors). Note: although the term 'minimize' is similar, this should not be confused with the concept of 'error minimization' described earlier in this section.

The methodology and preliminary assessment of a design with respect to CME, including any residual exposure to CME leading to CAT, should be presented to and discussed with the certifying authority early in the development program, utilizing the guidance provided in this document.

Section 3.4, as well as sections 4 and 5 of this report, further discusses the compliance expectations for error tolerance.

3.3 Development errors and independence

The development errors of concern, common mode development errors (CME), are those that would defeat independence claims made in the PSSA or PASA. Industry practices [12, 13] have defined four types of independence: process independence, item development independence, functional independence, and physical independence. Figure 3 depicts the relationship between the concepts of error minimization and error tolerance discussed in Section 3.2.2, and the different types of independence:

- Process independence supports error minimization;
- Item development independence and functional independence both provide error tolerance;
- Physical independence is generally not associated with development errors, and is not addressed in this report.

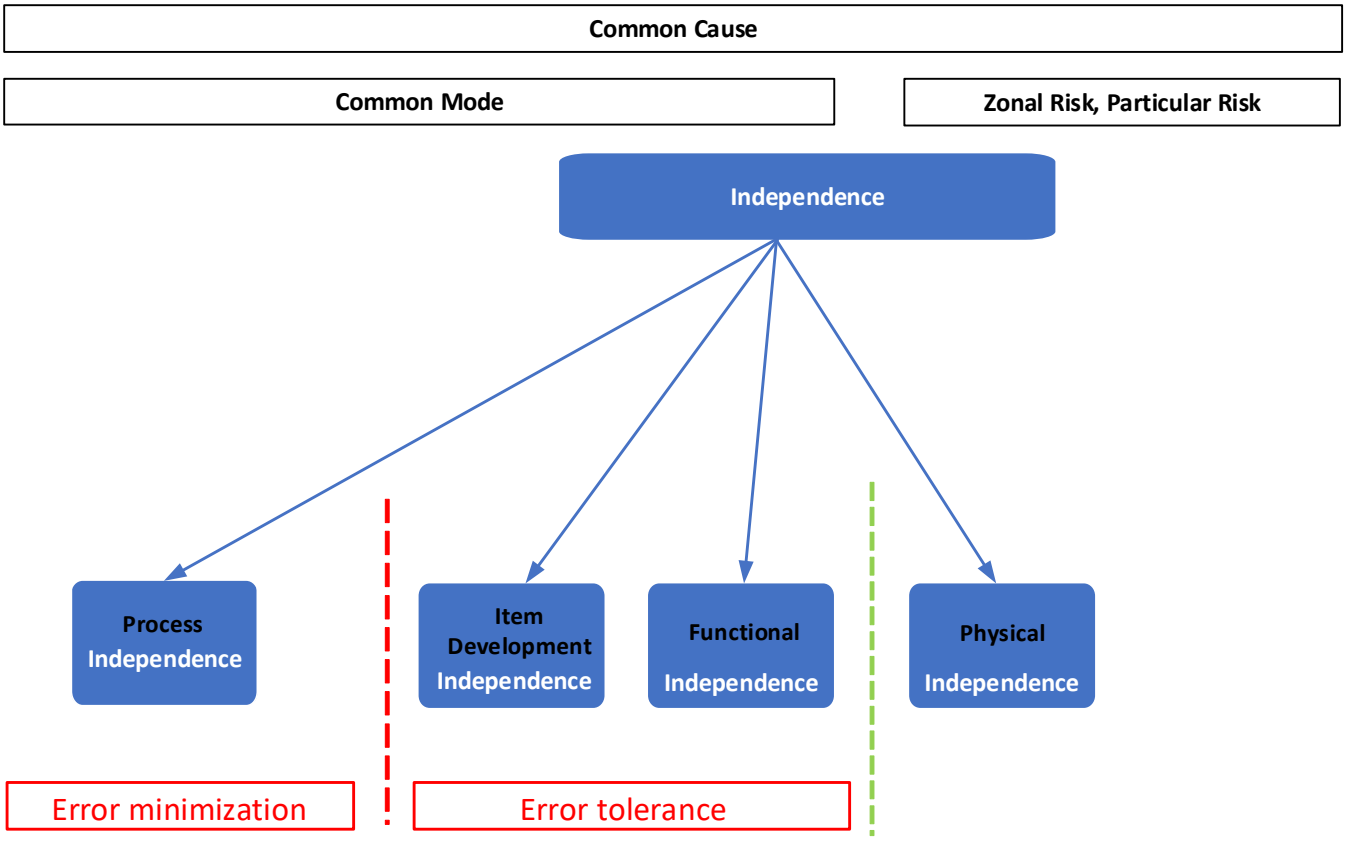

Figure 3 Relationship between Independence Types, error minimization and error tolerance

3.4 Error tolerance – PRA analogy

An analogy with particular risk assessments (PRAs) is helpful to clarify the compliance expectation noted in section 3.2.2 for providing error tolerance, i.e., minimizing the residual exposure in the design to the risk of a CME leading to a CAT.

Particular Risks are also events that can defeat assumed independence, leading to potentially catastrophic effects. In the case of PRAs, the risk comes from internal and external events, such as tire failure, bird strike, or detonation of an explosive device (survivability of systems, 25.795(c)(2)). Showing compliance in these PRAs is typically achieved via redundancy and physical separation of aircraft systems and their associated functions.

However, fully eliminating the potential for catastrophic effects due to such events can sometimes be impractical, for example:

- There may be insufficient space in the envelope of the airframe, to fully separate systems; or
- The aircraft's basic configuration may be such that the exposure is inevitable (e.g. rotor fragment from one engine impacting another engine); or
- Changing the routing of a system to improve separation, to address potential CAT effects under one PRA, would move that system into an area such that it is creating exposure to CAT effects under a different PRA.

The outcome of PRA assessments will be a design that takes into consideration these and other constraints in applying various design precautions and mitigations, such that the risk of Particular Risks defeating the assumed independence and potentially leading to a CAT event is minimized. The final compliance will involve agreement with the regulatory authorities that the design of the system and its installation (routing and separation) implement all practical precautions and indeed reflect such minimization of the risk, including cases where full protection cannot be provided, along with agreed justifications.

4. CME Tolerance Assessment within the Safety Process

4.1 Overview

As discussed in the compliance expectations section 3.2.2, the assessment of common mode development errors (herein referenced as common mode error - CME) must include both error minimization and error tolerance techniques. Both are necessary and complementary, one technique does not replace the other. For guidance on error minimization, the applicant should refer to the relevant industry practices [10, 11, 12, 13]. Error minimization is not further developed in this report**.**

Section 4.3 herein describes the methodology that should be used to address error tolerance for CME. The CME TST expects that a dedicated assessment of CME tolerance be performed as part of the PASA/PSSA process comprising the following essential elements:

- A systematic evaluation of the design to identify susceptibilities to CME leading to catastrophic failure conditions.
- Evaluation of error tolerance and implementation of meaningful mitigations where feasible.
- Documentation of the CME tolerance assessment, including coverage and residual exposure to CME with associated justification.

The CME tolerance assessment should be an integral part of the safety process and must ensure that the design and architecture are thoroughly and systematically evaluated for areas of susceptibility where a CME could have potentially catastrophic effects. The evaluation should address development errors (requirements, design, and implementation) at all levels, i.e. aircraft, system (and subsystem) and item levels. The primary intent of the CME tolerance assessment is to achieve system error tolerance to the maximum practical extent by the implementation of feasible and meaningful mitigations, to either further reduce exposure to CME susceptibility or contain the effects of the identified susceptibilities.

The assessment of common mode error tolerance in system design is inherently subjective and guided by experienced judgment. Considering the criticality of the subject, and to reduce the possibility of late design changes, it is recommended that the applicant perform the CME tolerance assessment early in the development process and ensure early involvement by the certifying authority, and the validating authorities when applicable.

The results of the CME tolerance assessment must be captured in the compliance documentation for certification and maintained under configuration control. Similar to all safety assessment activities, the CME tolerance assessment and its results should be updated in the context of post-TC design changes, as directed by a Change Impact Analysis (CIA).

4.2 Background - Common Mode Analysis

ARP4761A/ED-135 [12, 13] was published in December 2023 during the work of the CME TST, and provides guidance and guidelines for performing the system safety assessment. The CMT Authorities recognize this industry Recommended Practice, and its contents have been used by the CME TST as supporting material.

Appendix M of ARP4761A/ED-135 [12, 13] provides the current common mode analysis (CMA) qualitative analytical method to support the evaluation of independence. Figure 4 summarizes at a high level, the key CMA interfaces when accomplished as part of a PASA or PSSA. The Appendix M method establishes the general framework for systematic evaluation of common failure and error mechanisms within the overall system safety assessment process. Note that the process in Appendix M of ARP4761A applies to a variety of error sources, while the focus of the present report is limited to development errors.

The PASA/PSSA safety processes provide the independence principles of interest. These independence principles are developed in the PASA or PSSA processes using failure condition and severity classification information from the aircraft and system FHAs. The independence principles represent the assumptions of independence supporting hazardous and catastrophic failure conditions. Architecture and implementation characteristics are provided from the aircraft or system development activities and process information is provided from the development plans.

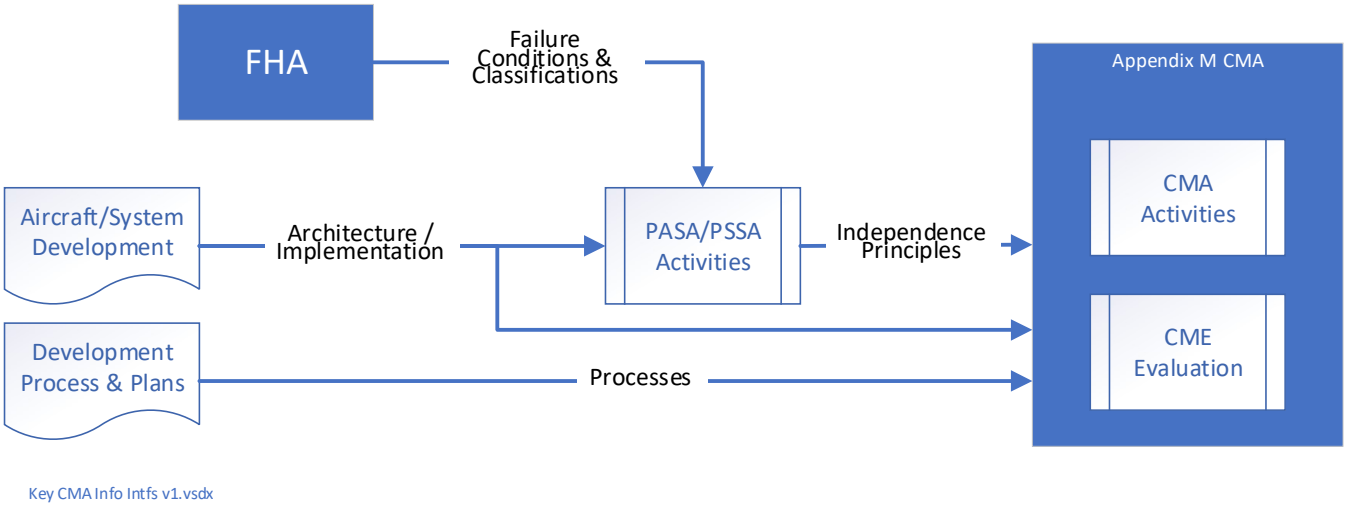

Figure 4 Key CMA Informational Interfaces

As part of the CMA activities, a list of common cause types and sources, including error sources, is developed for a project, by tailoring the general table of concerns found in ARP4761A/ED-135 [12, 13], Table M-1 – CMA Questionnaire Examples. This becomes the project-specific CMA (including CME) questionnaire.

Each independence principle is evaluated using this project-specific questionnaire to capture effects and mitigation in a suggested format, as shown in ARP4761A/ED-135 [12, 13] Table M-2 Example CMA Evaluation Table Format.

The CME Tolerance Assessment methodology described in Section 4.3 is consistent with the overall CMA activities above, and is intended to augment the industry practices with additional content specifically targeted to evaluating common mode errors.

4.3 CME Tolerance Assessment Methodology

The current recommended industry practice for CMA provides limited information on how to address CME, and does not capture and format the analysis results in a manner that optimally presents the error tolerance and residual error potential in the design. The Authorities therefore recommend that a dedicated and more detailed CME tolerance assessment be conducted, separate from the rest of the CMA, providing an analysis that focuses on the design susceptibility to common mode development errors affecting independence principles. The overall CME Tolerance Assessment flow is captured in Figure 5, and is described in the following sub-sections.

The Figure 5 CME tolerance assessment process flow is modeled after Figure M-1 in ARP4761A/ED1-35 [12, 13]. Figure 5 can be understood as enhancing and expanding the "Evaluate Independence Principle" process depicted in Figure M-1 of ARP4761A/ED-135 [12, 13] with the more detailed process flow and activities that address CME Tolerance. The intent is to provide a focused and systematic evaluation of CMEs which may result in a co-dependency between otherwise assumed independent elements.

For completeness, Figure 5 also includes the Development Phase error minimization activities of design and development assurance. The assessment methodology described in section 4 is limited to the CME tolerance aspect.

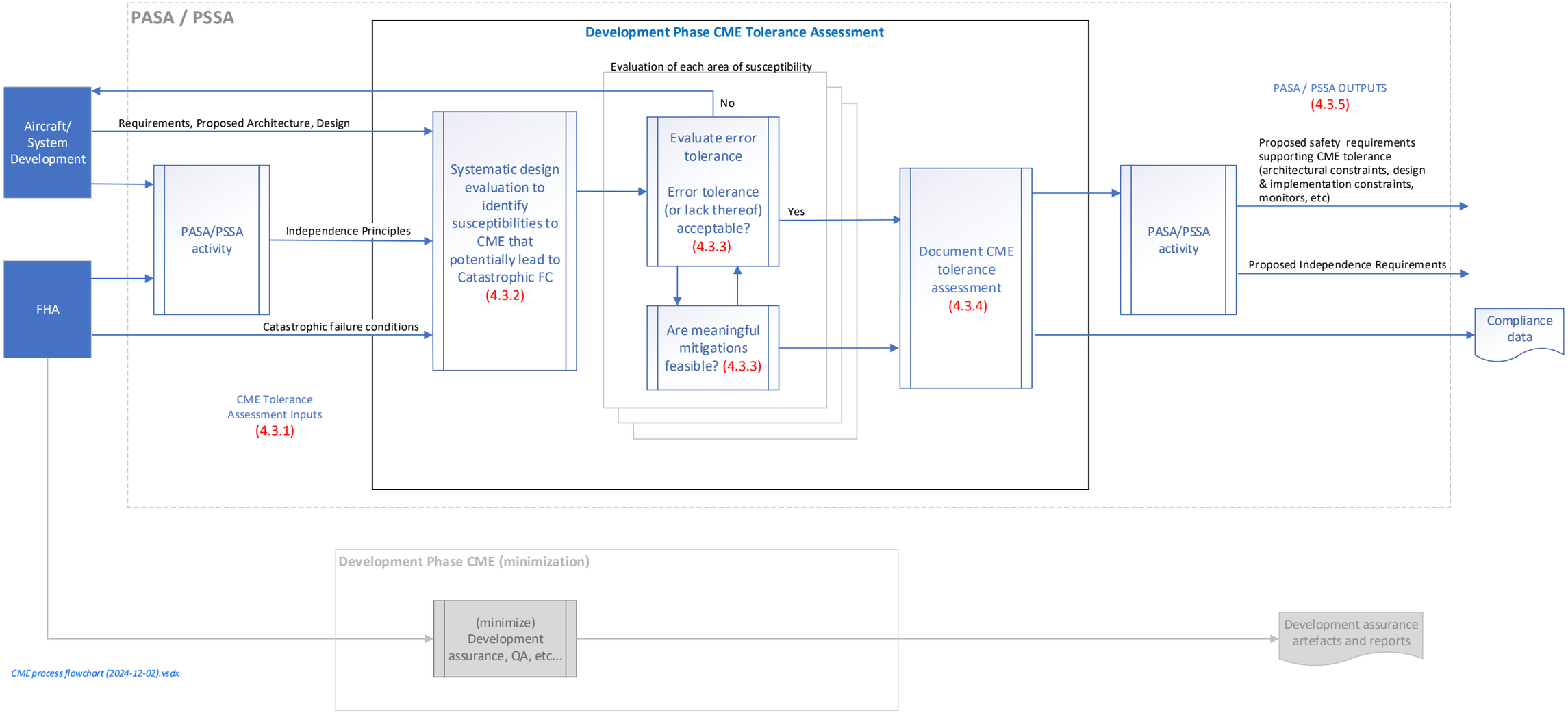

Figure 5 CME Tolerance Assessment Process Flowchart

4.3.1 Inputs to the CME Tolerance Assessment

The inputs needed to perform the CME tolerance assessment include:

a. **Independence principles** and associated rationale, identified in the PASA/PSSA, including any project level independence principles coming from other sources or experience.
Note: Some independence principles will already be known (i.e. those shown as inputs to the process), but it is the task of the CME tolerance assessment to help identify additional independence principles and define all associated independence requirements.

b. **Requirements, proposed architecture and design** information, which include:
   - Detailed architecture and design characteristics pertinent to the level being evaluated and updated incrementally as development progresses, which will serve as the basis for the systematic evaluation of potential susceptibility to CME. This includes but is not limited to:
   - Planned CME tolerance features and mitigations, i.e. characteristics intended to remove or reduce sources of CME, or mitigate their effects (e.g. planned diversity, partitioning, monitoring, etc.).
     Note: Some of these tolerance features and mitigations will already be known or planned (i.e. those shown as inputs to the process), but it is the task of the CME tolerance assessment, during the PASA/PSSA phase, to help define the need for additional tolerance features and mitigations.

c. The **AFHA/SFHA** - extract of catastrophic failure conditions used to narrow the focus of the CME tolerance assessment.

4.3.2 Systematic Design Evaluation to identify CME Susceptibilities

A systematic approach is necessary to evaluate the proposed design and architecture and identify areas which are susceptible to CME defeating the necessary independence and potentially leading to catastrophic effects.

The applicant should propose a suitable methodology that, for catastrophic failure conditions, systematically addresses the contribution of potential development errors to the top event, such as:

a) Using existing preliminary fault trees developed to address failures, and including the contribution of development errors.

   Notes:
   - The inclusion of development errors must be only qualitative and should not include any quantitative numerical probabilities.
   - For complex and highly integrated systems it is likely impractical to include development error considerations in the traditional quantitative fault tree (i.e. the FTAs used for failures).

b) Developing a set of qualitative "error fault trees" (see notes below) to address specifically the contribution of development errors.

Notes:

- ARP4761A/ED-135 [12, 13] Appendix G, section G.10.3 describes the use of fault trees constructed of potential error sources to support FDAL / IDAL assignment. The principle of using error fault trees to support a CME evaluation is similar but would require increased granularity in reflecting error source contribution compared to that necessary for DAL assignment.
- An example using this approach is presented in Annex 3.

c) Developing error-specific dependency diagrams (reference ARP4761A/ED-135 [12, 13] Appendix H).

d) Using another suitable methodology proposed by the applicant.

The methodology proposed must provide a means not only to address the independence principles already identified from other PASA / PSSA activities but also a means to identify additional independence principles that may be specific to development errors.

4.3.2.1 Failure conditions:

All catastrophic failure conditions, including both loss of function and malfunction, need to be addressed by the evaluation. A CME evaluation that covers multiple FHA failure conditions may also be acceptable. For example, in a given design, erroneous commands in the roll or yaw axes may have common potential error source contributors (e.g. same computing paths, inputs, common resources, etc) such that their susceptibility to CME could be evaluated jointly.

A top-down methodology starting from the catastrophic (CAT) top events will most likely need to be complemented by a bottom-up activity, to ensure adequate coverage, particularly for aspects such as common resources.

4.3.2.2 Analysis scope:

To systematically evaluate the proposed design and architecture for its susceptibility to common mode errors, the scope of the assessment should include, at a minimum, all system elements containing either software or Airborne Electronic Hardware (AEH). For more details on the scope of the CME evaluation for AEH, see Section 5.3.

Supporting systems (e.g. hydraulic systems, electrical power systems, avionics, systems providing critical input data, data busses, etc.) should also be included in the assessment for the system being evaluated if development errors in these supporting systems could contribute to a catastrophic failure condition.

In order to ensure completeness of the evaluation and the associated documented traceability, every potential susceptibility to CME in the proposed design and architecture should be identified, regardless of potential existing mitigations. The objective is to be more inclusive at this stage of the evaluation; taking credit for mitigations will be discussed in section 4.3.3 when evaluating tolerance to CME, and subsequently documented per section 4.3.4 for completeness and traceability.

4.3.2.3 Analysis granularity:

Careful consideration should be given to applying an appropriate level of granularity in the systematic design evaluation so that potential susceptibilities to CME are adequately identified and allow for a meaningful evaluation of error tolerance in the next step (per section 4.3.3). Some iterations may be necessary in the analysis for all or part of the design to increase (or decrease) granularity where this is found necessary.

If the design evaluation is performed at too high a level, i.e. with too low granularity, there is concern some areas of susceptibility to CME won't be visible, and therefore won't be identified, affecting completeness of the evaluation This would be mostly a concern when considering functional breakdown. Additionally, if the design evaluation is performed at a level that is too high, the functional interactions may not be adequately considered, which would result in gaps in the CME tolerance assessment. For example, in a FBW flight control system:

- Functions such as Control Laws, air/ground logic, and monitors should be considered separately in the assessment rather than grouped together into a single "FCC computing" function.
- The granularity of functions should be sufficient to identify susceptibilities to CME which potentially defeat the necessary independence between (1) loss of normal mode and (2) loss or malfunction of the function(s) that handle reversion to an alternate/direct mode.
- The granularity of functions should be sufficient to identify susceptibilities to CME which potentially defeat the necessary independence between (1) loss of normal mode and (2) loss or malfunction of the function(s) which provide awareness of mode reversion to the crew.

If the design evaluation is performed at too low level, i.e. with too high granularity, the design would effectively be broken down in a large number of very small 'pieces', which may each look simple and possibly error-free (fully analyzable and testable) on their own. However, this could overlook the concern that the error potential in complex and highly integrated functions and systems lies also, and perhaps mostly, in the interactions and integration between the different small 'pieces'. This could also affect the completeness of the evaluation, and result in gaps in the CME tolerance assessment. For example, an assessment of a FBW flight control system where the 'base events' would be individual filters, gains, limiters, etc in control laws would be at a much too low level to result in a meaningful evaluation.

4.3.3 Evaluation of Error Tolerance and Mitigations

In the previous step, the applicant has identified all areas of susceptibility to CME in the design, i.e. where a CME could affect the independence principles necessary to satisfy the safety objectives associated with catastrophic failure conditions. Each identified area of susceptibility to CME now needs to be systematically evaluated for error tolerance. While the evaluation should address all relevant sources of errors, it would primarily be focused on the potential effects of a CME (derived from the failure conditions and associated independence principles) rather than the error sources themselves.

The evaluation of the proposed design and architecture for error tolerance, performed as part of the PASA/PSSA, needs to address the known specific error tolerance features and mitigations in the design, and identify other (not CME specific) design and architecture features for which credit can be taken in providing error tolerance, and propose / evaluate additional error tolerance features and mitigations, where necessary, in an iterative process.

This section provides an overview of the activity. Relevant considerations on a number of topics are further elaborated in section 5.

4.3.3.1 Error tolerance features, mitigations:

Error tolerance features in the design and architecture, also referred to as mitigations in this report, are those features that address the risk of CME leading to catastrophic effects by either:

- containing the effects of errors, such that they do not propagate to a failure condition (Figure 1); or
- mitigating the effects of errors by reducing the hazard criticality of the resulting failure condition to less than CAT; or
- avoiding by design the potential for CME leading to catastrophic effects.

The following are examples of typical mitigations providing error tolerance, in no particular order of precedence (refer to Section 5 for further details):

- Monitors and alerts,
- Functional independence,
- Architectural, design, and implementation diversity.

Experience has shown that error tolerance implemented at higher levels tends to inherently cover a broader range of potential sources of errors and address multiple areas of susceptibility. Therefore, it is recommended that error tolerance be implemented at a high-level in the system design (e.g. architectural means, broad monitors, high-level functional independence, etc.) where possible, rather than addressing susceptibility to CME via mitigations implemented at lower levels (e.g. source code, software tools, low-level functions, etc.). In order to effectively implement error tolerance at high level in the system design, it should be an explicit consideration in the design choices made in early phases of conceptual development.

Error tolerance at lower levels may also be needed in specific areas, but the benefits in terms of providing error tolerance will be limited to that specific area, i.e. at low level. For example, use of different compiler tools for software executing on two different controller lanes may provide mitigation for compiler errors, but would not address susceptibility to CME due to source code errors or requirement errors.

For each area of susceptibility, the error tolerance evaluation should explicitly identify the extent to which the CME effects (leading to the failure condition) would be addressed by the error tolerance features / mitigation, and for which sources of errors. Conversely, the evaluation should explicitly identify any remaining unmitigated error potential, in terms of effects (or other characteristics as appropriate) and in terms of sources of error. This notion is sometimes referred to as ‘coverage’, but should remain a qualitative evaluation of what is ‘covered’ or ‘not covered’ (in terms of effects and error sources) as part of the common mode assessment; there is no intent to quantify such coverage.

For example:

- A given software function, implemented from different source codes and with different compilers used, may be found to provide adequate tolerance for a number of error sources, but would not provide tolerance for errors in the software requirements (specification).
- A dedicated monitor providing detection of erroneous behavior (due to CME) of a function and reversion to an alternate and independent control path may only be effective in certain phases of flight.

4.3.3.2 Meaningful and feasible additional mitigations:

The evaluation of error tolerance should also evaluate and capture whether there are additional meaningful error mitigations that are feasible to address otherwise unmitigated CME potentially leading to catastrophic effects. Where the evaluation of a given area of susceptibility indicates it would not be tolerant to CME, or where the coverage would be partial (either in terms of effects or error sources), the applicant should investigate whether additional meaningful mitigations are feasible. As shown in Figure 5, this may be an iterative process.

Proposed additional mitigations should be introduced according to the extent and nature of the associated area(s) of susceptibility to CME. The intent of the expression “meaningful mitigations” in this context is to highlight the importance of implementing such mitigations when and where it contributes to improving the overall error tolerance of the design. Potential side effects of proposed additional mitigations must also be considered, including evaluating such mitigations as potential sources of development errors themselves, as part of the CME assessment approach. Section 5.2.5 presents additional considerations on managing complexity when introducing error tolerance mitigations.

The intent of the expression “feasible mitigations” should be understood in the context of the early phases of system development, when the PASA and PSSA activities are performed, and should reflect industry state-of-the-art approaches and techniques.

Potential additional mitigations must be returned to the PASA or PSSA processes and the aircraft/system development process for consideration. Once proposed for implementation, each added mitigation should be captured by means of system and safety requirements in a manner consistent with the applicant’s system development and safety processes, and the CME tolerance assessment revised as necessary.

4.3.3.3 Acceptability of error tolerance and residual exposure to CME:

It is recognized that, depending on the system design, it may not be possible to provide full coverage for all areas of susceptibility to CME, and for all error sources, through the implementation of meaningful and feasible mitigations. For systems performing comparatively simpler functions full, or near full, coverage may be possible for CMEs potentially leading to catastrophic failure conditions. However, this may not be possible at the higher end of systems complexity and integration, such as for FBW flight control systems. As noted in section 3.2.2, the compliance expectation in providing error tolerance is to minimize the residual exposure in the design to the risk of a CME leading to a catastrophic failure condition (i.e. minimize areas where the design is not tolerant to such errors). Therefore, the applicant

should seek to provide coverage for areas of susceptibility to CME to the maximum practical extent, i.e. considering industry state-of-the-art approaches and techniques (see section 5.1.3).

The CME tolerance evaluation should explicitly identify those areas of unmitigated (residual) susceptibility to CME potentially leading to a catastrophic condition, i.e. where there is a lack of CME tolerance, along with supporting justifications. Investigations of potential additional meaningful and feasible mitigations to address unmitigated areas of susceptibility to CME (including where these were not implemented, with rationale) would form part of this supporting justification.

Further measures and considerations, whilst not meant to achieve error tolerance, could be proposed by the applicant as part of this justification, as appropriate and after careful consideration, where meaningful and feasible mitigation was considered impractical to implement. For example (refer to Section 5.4 for further details):

- Service history,
- Design simplicity,
- Additional V&V, extensive testing, or
- Flight crew procedures.

The preliminary assessment of a design with respect to CME, including any residual exposure to CME potentially leading to a catastrophic failure condition, should be presented to and discussed with the certifying authority early in the development program, for concurrence. While it is not possible to propose definite criteria for acceptability, due to so much being dependent on the specific application, section 5 of this report elaborates on a number of elements to be considered.

4.3.4 Documentation of the CME Tolerance Assessment

The CME tolerance assessment should be documented in such a way to provide traceable evidence that the methodology has been systematically applied to all relevant elements of the design and architecture under consideration, and with an appropriate level of granularity. This documentation forms part of the safety compliance demonstration.

The following should be captured as a minimum (refer to sections 4.3.1 through 4.3.3 for details):

- Relevant AFHA / SFHA catastrophic failure conditions, including any additional failure condition that may have been identified from a bottom-up evaluation.
- Evidence of the systematic evaluation of the design and architecture to identify areas of susceptibility, i.e. contribution of potential development errors to the catastrophic top events. The form this takes will depend on the methodology used by the applicant (e.g. qualitative “error fault trees”, dependency diagrams, or other).
- Identified areas of susceptibility to CME, with adequate traceability to the failure condition(s), independence principle(s) and potential error sources and effects.
- For each area of susceptibility, the evaluation of error tolerance including consideration for relevant mitigations.

- Identified areas of residual susceptibility to CME potentially leading to a catastrophic condition (i.e. where there is a lack of CME tolerance), if any, along with supporting justification.

The compliance data related to section 4.3.3 – Evaluation of error tolerance and mitigations – should be captured and presented in a manner that clearly links the independence principle(s) under evaluation, the area(s) of susceptibility to CME, and potential error sources considered, the details associated with the failure condition(s) and potential error effects, all relevant mitigations, and justification for any area of residual susceptibility or partial coverage.

The overall CME tolerance assessment documentation should present a systematic, logical, and convincing narrative supported by justification that the aircraft-level risk has been minimized.

Annex 4 presents an example of a format that could be used to document the results of the CME tolerance evaluation per section 4.3.3. The applicant can propose an alternative format that would meet the expectations noted above. Annex 4 also provides a partially worked example, using the same nominal system example as used in Annex 3.

Note that the proposed format in Annex 4 is not a template to be used in lieu of the systematic design evaluation per section 4.3.2. Rather, it proposes one example of how to document the results of the applicant's systematic tolerance evaluation and provide the information in a manner that satisfies certifying authority expectations.

4.3.5 Outputs of CME Tolerance Assessment

The CME tolerance assessment documentation discussed in section 4.3.4, although mostly pertaining to a development phase activity, should be directly referenced as certification compliance data. The resulting CME tolerance assessment captures sufficient data to identify what is mitigated (i.e. covered) by the planned error tolerance techniques or strategies, as well as capturing any residual development error risks. The initial CME tolerance assessment should be revisited and kept updated with changes in the design.

The CME tolerance assessment documentation and outputs to other PASA and PSSA activities should provide sufficient data from which additional independence requirements and other safety requirements specifically supporting CME tolerance may be developed within the PASA/PSSA processes. Such safety requirements could include for example: architectural constraints, design and implementation constraints, CME specific monitoring, etc.

5. Considerations when Performing the CME Tolerance Assessment

Following the methodology provided in Section 4, this section contains practical considerations for performing the CME tolerance assessment, including guidelines and best practices on the use of mitigations for error tolerance and justifications of residual exposure to CME. Although not establishing

definitive pass/fail criteria, these considerations are intended to provide an aid to engineering judgment when performing and reviewing the CME tolerance assessment.

5.1 General Considerations

5.1.1 Certifying Authorities Involvement

As noted in section 4.1, the subjective nature of the CME tolerance assessment makes it imperative that the applicant involve the certifying authority (CA) as early in the development as practical. The applicant should present to and seek agreement from the CA on their proposed plan for the CME tolerance assessment based on the methodology discussed in section 4 of this report, including how the applicant will document the CME tolerance assessment to facilitate consistent discussions and evaluation of the assessment results.

The applicant's documentation should capture and present a logical and convincing narrative, with justification, that the compliance intent for CME presented in section 3 of this report is successfully achieved.

The consistent application of the CME tolerance assessment methodology and documentation strategies presented in Section 4 will enhance the certifying and validating authorities' ability to achieve consistent engineering decision-making regarding the assessment results and whether the proposed design meets the compliance intent.

5.1.2 Integrity and Availability

The CME tolerance assessment should address equally both integrity (erroneous behavior, malfunction) and availability (loss of function) catastrophic effects of potential error sources. The safety objectives for both types of failure conditions need to be satisfied when providing error tolerance. Safety critical systems such as flight controls would be expected to have catastrophic failure conditions related to both malfunction and loss of function effects. The design of such systems therefore requires a careful evaluation considering both availability and integrity, and care needs to be taken so that one aspect does not come at the expense of the other.

5.1.3 State-of-the-art Techniques

The applicant should be aiming to provide error tolerance to the maximum practical extent for areas of susceptibility to a CME leading to catastrophic failure conditions, for all development error sources, by utilizing current state-of-the-art techniques. Such techniques refer to implementing architectural solutions or features that remove or mitigate the potential susceptibility or provide error effects containment such that it is no longer catastrophic.

For an area of susceptibility that cannot reasonably be fully mitigated (i.e. partial coverage), the applicant should minimize the residual exposure of a CME leading to a catastrophic failure condition, again by utilizing current state-of-the-art error tolerance techniques.

In such a case, the CME tolerance assessment will need to explain why full coverage is not practical and provide a supporting rationale for the acceptability of the residual exposure to CME. The rationale should be based on the proposed design being state-of-the-art, experience, sound engineering judgment, or other arguments, which support the proposal not to implement other potential error tolerance techniques. Section 5.4 presents some considerations related to the justification of residual exposure to CME.

5.2 General Considerations on Error Tolerance

This section presents general considerations on some techniques to provide error tolerance. It describes best practices that the applicant may use to evaluate the effectiveness and coverage of proposed mitigations. Some limitations of each error tolerance technique are also outlined.

5.2.1 Effectiveness of Mitigations

Once a susceptibility to CME has been identified, the goal is to identify and apply the most effective means to mitigate the susceptibility or its effects. Each potential susceptibility to CME leading to a catastrophic outcome should be addressed commensurate with the specificities of the susceptibility. For example, if the susceptibility is related to a function specification, then a mitigation that introduces functional independence could be considered; if the susceptibility is related to item implementation, then potentially add item independence; etc.

The effectiveness of the chosen error tolerance technique, i.e. how the mitigation is appropriate to the susceptibility of concern, should be presented in the CME tolerance assessment. The effectiveness of the mitigation and the coverage it provides in terms of error tolerance will vary depending on the technique being considered (e.g. functional independence, hardware diversity, monitoring, crew mitigation, etc.)

5.2.2 Functional Independence

Functional Independence is a characteristic that minimizes the likelihood of common development errors by using different functions (ARP4754B, section 2.2 [10, 11]). Functional independence is one means of providing tolerance against potential errors in the functional specification(s) (i.e. mistakes in the requirements). References [10, 11] provide additional detail in section 5.2.3.2.1.1.

Functions are considered independent if their intended behavior (with a sufficient level of detail) are sufficiently different. Different ways of writing the same requirement (e.g., textual, graphical, or model formats of the same requirement) do not make them different for claiming functional independence (i.e. for requirement errors). Establishing clear criteria to evaluate how different the behavior of different functions must be in order to cover all potential susceptibilities to CME is difficult. However, some examples of characteristics that may contribute to demonstrating that functions are sufficiently different for providing error tolerance against potential CME include:

- Different intended functional behavior
- Simpler functional behavior,
- Limited sensor usage,

- Alternate signal management structure,

Using different, simpler and/or more limited behaviors for the alternate function(s) is considered an effective best practice to reduce the likelihood of common development errors with the primary function.

Different functions must be defined by different requirement sets; however, the way in which the requirement sets are packaged (e.g. requirement management tool modules vs. section within a single module) isn't directly relevant. It is assumed that there is appropriate configuration control in place and that the applicant's system development process will ensure potential errors in the requirements management tool are adequately accounted for and minimized.

5.2.3 Monitors and Alerts

The fail-safe design concept principles often involve the use of failure detection and annunciation. This is typically accomplished through a combination of monitoring mechanisms introduced in the design. Monitors should trigger an appropriate response so that the effects of the detected failure are contained. Examples of monitor responses include mode reversion, channel switching or isolation, activation of backup functions and protections, etc. along with accompanying alerts and indications for flight crew awareness. Similarly, for development errors, the introduction of monitors in the design may be an effective technique to provide error tolerance by providing detection and containment of their potential effects.

Monitors should be introduced in the design through safety requirements identified in the PASA/PSSA process, including from the CME tolerance assessment. Consideration should be given to ensuring independence between functions and their respective monitors. When evaluating the effectiveness of monitoring to provide error tolerance for an identified area of susceptibility to CME, it is crucial to ensure that the monitor, including its response mechanisms, could not be affected by the same development error.

Coverage is another key aspect to be considered when discussing the effectiveness of monitors for the purpose of CME tolerance. The applicant is expected to detail the coverage provided by the proposed monitors, whether the monitor(s) provides full or partial containment against identified areas of susceptibility to CME, and expand for each monitor on cases that would be covered / not covered if coverage is partial. Assessment of coverage and overall determination of acceptability is usually done for the combination of proposed monitors in a given system. See also the discussion on coverage in section 4.3.3.1. Depending on the nature of the monitor, aspects to be detailed for coverage assessment may involve detection and voting thresholds, timing and rate characteristics of the condition, flight phases, etc.

As discussed in section 4.3.3.1, introducing mitigations such as monitors at higher levels is usually preferable, since they would tend to address inherently more potential areas of susceptibility to CME. One example would be monitors for flight control laws. It is recognized that the use of diversity in the high-level specifications of flight control laws may not be easily implemented. Industry practice has shown that the use of aircraft/system-level monitoring of the flight control laws may be a possible means to introduce CME error tolerance in such cases.

5.2.4 Architectural, Design, and Implementation Diversity

Diversity is the quality or state of being different in nature, i.e. diversity essentially means ‘different’. It provides CME tolerance by introducing independence. Diversity is introduced in the system by the design of functional failure paths that are sufficiently different, at all levels, to minimize the likelihood of a development error in one functional failure path manifesting itself in another functional failure path(s). Therefore, the use of diversity aims essentially to remove the “common mode” aspect of the potential development error, thus reducing the criticality of the development error effect (e.g. by the containment provided by the different functional failure paths).

Diversity can be employed in many ways and at different levels, ranging from functional specifications at aircraft, system, and item levels, down to diverse implementation solutions at item levels. Diversity at architectural and design levels may also overlap with the concepts of functional independence, and the design of monitors and alerts, which are further discussed in sections 5.2.2 and 5.2.3 of this report.

The concept of diversity at an item level, particularly for the software and AEH domains, has often been referred to as dissimilarity. This is one possible means to address implementation co-dependence, such that development errors introduced at the item level may not occur in redundant items performing similar functions. The use of the term ‘diversity’ is preferred in this report. Diversity is a broader concept aimed at providing error tolerance, while dissimilarity is narrower in scope, i.e. one means to introduce diversity specifically at SW/AEH level.

As discussed throughout this report, the higher the level of complexity, the higher the risk of potential development errors, and therefore, the higher the need for providing error tolerance solutions, including diversity. This principle is illustrated for AEH as presented in section 5.3.

Diversity, when used as a means of providing error tolerance, should be specifically targeted to the area(s) of susceptibility of concern. This means that the use of diversity should be meaningful in its intent (i.e. not different just for the sake of being different). The CME tolerance assessment will support identifying where diversity will be the most effective error mitigation strategy.

As for other aspects of the CME tolerance assessment, the appropriate level of diversity in the design to address areas of susceptibility to CME should be agreed upon with the certifying authority early in the project. In this context, the “level of diversity” refers to the extent to which things are different versus what may remain common or similar. As it happens for independence, diversity is not an absolute characteristic. For example, diversity should be targeted to address the specific area(s) susceptibility of concern.

When diversity is proposed as a means to provide error tolerance, the applicant is expected to clearly describe the nature of that diversity (i.e. what is different, what remains the same or similar), and how the proposed diversity provides error tolerance for the areas of susceptibility to CME it is intended to mitigate, and the residual exposure to CME, if any. This should flow naturally from the process methodology described in section 4 and exemplified in Annex 3 and 4 of this report.

5.2.5 Error Tolerance and Complexity

Error tolerance may be achieved via a variety of design and architectural features. Some of these error tolerance features would be inherent to meet the system requirements (e.g., functional, safety, or operational requirements) separate from any CME considerations, whereas other features may be specifically implemented to address CME concerns. The latter case may result in a relative increase in the complexity of the design. While in general increased complexity does carry the risk of increased potential for development errors, this would greatly depend on the specifics of the system architecture design being considered and the complexity involved in the error tolerance technique being added relative to the inherent complexity of the system design.

For example, modern highly integrated and safety critical systems such as full fly-by-wire flight control systems are already inherently complex, so the relative added complexity that may be involved with the addition of error tolerance in a specific area of the system should be considered in the context of the overall system complexity. Although the introduction of error tolerance mitigations might lead to additional potential for development errors in specific areas, each error effect would be expected to be less significant due to the overall increased error tolerance in the system. The applicant's development assurance process should ensure that the addition of error tolerance mitigations would not create unmanaged risk due to increased complexity.

5.3 CME Assessment for Airborne Electronic Hardware (AEH)

As discussed throughout this report, the higher the level of complexity in a given area of the design, the higher the risk of potential development errors, and therefore, the higher the need for providing error tolerance solutions, including diversity, to address the risk of CME leading to a catastrophic event. This section presents examples applied to AEH to illustrate this principle of increasing need for error tolerance commensurate with the complexity of the design (or, in this example, device) under assessment. This section also intended to clarify where simpler electronic components may be considered out of scope of the CME tolerance assessment for Development Errors.

The evaluation of error sources at the item level will consider the error potential associated with the electronic components to be used in the implementation. Figure 6 presents four groupings of AEH components based on their complexity and potential risk of containing common development error sources of concern, along with typical CME tolerance mitigations to consider and/or justification that may be applicable.

- The first two columns (1 and 2) refer to AEH components with perceived very low / low complexity and risk. Such components often have wide industry usage and service experience, and would typically be fully tested as part of verification activities (FAT). As a result, these do not represent a concern of development errors remaining in the certified design, and can be considered out of scope of the associated CME tolerance assessment.

- Column three (3) captures AEH components of gradually increasing complexity and as a result gradually increasing risk due to potential development errors. These components fall within the scope of the CME tolerance assessment and need to be addressed per the methodology discussed in

section 4. With proper justification and subject to the considerations in section 4.3.3.3, some applications could be determined to be 'simple' under DO-254 / ED-80 [17, 18] (i.e. fully analyzable and testable - FAT). Similarly, again with proper justification and subject to the considerations in section 4.3.3.3, components and functions that have extensive service history and are performing simple functions (simple, fully analyzable and testable functionality) could in some cases be found acceptable.

- Column four (4) represents AEH components that have the highest complexity and hence highest risk potential for development errors.

Each specific application and device needs to be reviewed case by case. For example, power supply blocks are shown in Figure 6 spanning Column 2 (low complexity/risk, "Out of Scope") and Column 3 (Increasing complexity / risk, "In Scope"). The relative complexity / risk, and whether in scope or not of the CME tolerance assessment, would depend on whether the power supply block is of simple analogue construction or more custom for the specific design (e.g potentially containing programmable hardware). The determination of whether this type of component would be in or out of scope of the CME tolerance assessment needs to be discussed with the certifying authority.

The named inclusion of specific components in Figure 6 is intended to be for illustrative purposes and not a definitive sorting of these components.

Figure 6Airborne Electronic Hardware (AEH) CME Risk Potential

<table>
<tr><th></th><th>1</th><th>2</th><th>3</th><th>4</th></tr>
<tr><td>Complexity / risk of development errors</td><td>Very Low</td><td>Low</td><td colspan="2">Gradually increasing</td><td>Very High</td></tr>
<tr><td>CME tolerance assessment</td><td colspan="2">Out of Scope</td><td colspan="3">In scope</td></tr>
<tr><td>Examples of typical components</td><td>- Resistors
- Capacitors
- Diodes
- Transistors
- Etc.</td><td>- Linear Integrated Circuits
- Digital Logic Circuits
- Memory RAM
- Memory NV RAM
- A to D converters
- Etc.</td><td colspan="3">Processors
Complex / programmable components, e.g. complex COTS, ASIC, FPGA, PLD, etc. (Including device and logic)
Power Supply Block</td></tr>
<tr><td>Typical CME tolerance features / mitigations</td><td></td><td></td><td colspan="3">Diversity in function
Components diversity</td></tr>
<tr><td>Other justifications</td><td></td><td></td><td>Potential FAT
Simple function</td><td></td><td></td></tr>
</table>

5.4 General Considerations – Justification for Residual Exposure to CME

The measures and considerations discussed in this section do not constitute error tolerance, and as discussed in section 4.3.3.3, could only be proposed by the applicant as part of a justification for residual exposure to CME, as appropriate and after careful consideration, where meaningful and feasible mitigations were considered impractical to implement.

5.4.1 Service History

In some cases, service history could be used as part of a justification for residual exposure to CME at the item or implementation level. Electronic components providing ARINC-429 interfaces are an example of potentially appropriate service history usage. Through appropriate analysis, these devices may be shown to have extensive industry use over a wide variety of applications, such that device implementation errors and ARINC 429 protocol errors have been sufficiently addressed so as not to be of concern.

The applicant should conduct an analysis to substantiate the credit of service history in the target design for development errors. This analysis should cover the extent of the service history (e.g. accumulated flight hours), similarity of applications (e.g. airplane models, systems, intended functions, operational environment, etc.), relevant in-service issues associated with the component/device, and eventual design changes. Substantiating the absence of residual CME via service history is difficult, hence service history may provide justification for a limited range of cases. Also, service history would not typically be applied as a justification at the system level.

5.4.2 Simplicity

Simplicity could be used as part of a justification for residual exposure to CME in some cases. It is important to note that simplicity is a characteristic to be demonstrated, not just an argument to be claimed. A justification based on simplicity would normally only be appropriate when it is possible to define a comprehensive set of tests and analyses to fully ensure correct function under all foreseeable operating conditions and to rule out the possibility of anomalous behaviors. This is sometimes referred to as being Fully Analyzable and Testable (FAT). The combination of tests and analyses is expected to be performed to rule out the possibility of development errors in that system element and to confirm the results of the CME assessment. Such demonstration should account as appropriate for all relevant integration and interaction aspects within the broader system.

The use of simplicity as part of a justification for residual exposure to CME, should be limited to cases where the simplicity of the design can be clearly and easily established. The applicant should avoid cases in which extensive investigation and detailed analyses would be required to justify it, since this would indicate the system element under review is indeed not “simple”. Complexity is inherent to current state-of-the-art safety critical systems. Each system element should be considered complex unless it can be justified and demonstrated as simple to full satisfaction. The applicant should also avoid breaking down the system into too many smaller “simple” pieces for the evaluation. Complexity often results from the integration of, and interactions between, simple elements. Therefore, any discussion of simplicity should be done with an appropriate level of granularity (as discussed in Section 4.3.2.3), with the context of the full system and its integration taken into consideration.

5.4.3 Additional V&V including extensive testing

AMC 25.1309 [5, 7] recognizes that exhaustive testing for more complex or integrated systems may either be impossible because all of the system states cannot be determined, or impractical because of the number of tests that must be accomplished. However, it is also recognized that more extensive testing can be useful to enhance the validation and verification processes to further minimize the possibility of development errors.

The use of comprehensive integrated tests, for example, has proven to be a useful strategy to provide further knowledge of the integrated system behavior to assess common resources and multiuser interfaces such as air/ground logics, air data, and inertial information, etc. These activities not only contribute to enhancing the validation and verification processes for such complex and integrated systems but may help to identify unintended behaviors that could result from development errors.

The extensive testing discussed herein should not be considered as an alternative to other techniques discussed in this document, especially to the error tolerance techniques. Additional V&V usually provides targeted development assurance activities to further minimize potential exposure to development errors. One example of such a targeted application is the additional V&V activities that are covered in specific CRIs / CMs / IPs for the development of flight control laws. In these guidance materials, additional guidance is provided for the V&V of control laws with detailed guidance to address particular control law aspects such as robustness, discontinuities, corner cases, and others.

The extensive testing for V&V discussed in this section should not be confused with the Fully Analyzable and Testable (FAT) technique discussed in the section 5.4.2 Simplicity. Extensive testing can enhance V&V effectiveness for complex and integrated systems, but it is not an alternative to error tolerance techniques, which remain necessary. FAT, when successfully applied, aims to provide full coverage against development errors through exhaustive testing, which is only achievable in combination with the appropriate application of the simplicity argument for the element under analysis.

5.4.4 Flight Crew Intervention

Although it may be used in very specific cases, flight crew intervention has generally limited value as part of a justification for residual exposure to CME. Flight crew action to mitigate the potentially catastrophic effects of a CME would only be effective for cases where the detection of the condition and the corrective action by the crew can both occur appropriately and in a timely manner, and without undue burden or exceptional piloting skills or strength. This will typically require the design of specific alerts, the development of associated flight crew procedures, and possibly dedicated flight crew training. The dynamics of the failure effects may also be an important aspect that limits the effective applicability of this method. For example, many flight control system failure effects could not be counteracted in a timely manner if they occur during flight phases close to the ground or if the failure effects are highly dynamic.

The level of determinism necessary for validating expected flight crew response makes it difficult to take credit for such actions to cover “unknown effects” associated with potential development errors. Validation of such flight crew detection and procedures would be based on well-defined scenarios, which if fully known and established, could be better mitigated by additional tolerance. Considering all

these limitations, flight crew intervention is usually not effective for dealing with development errors, except for very few and thoroughly validated cases.

6. Conclusions and Recommendations

6.1 Conclusions

This report documents the results of the CME TST activities and provides a harmonized framework for evaluating critical systems on large transport aircraft with regard to common mode development errors. Important steps were made toward mutual understanding of each authorities' approaches. The four authorities reached agreement on the applicable regulations and guidance, on the applicable terminology, and on the intent and associated safety objectives. A high-level methodology to evaluate common mode development errors was developed and agreed between the authorities, along with expectations for the associated compliance documentation, and various applicable guidelines and considerations.

The expectations in terms of CME process and documentation of the process outcome are to a large extent harmonized when using the guidance of this report. In addition, the application of the new industry standard ARP4761A/ED-135 [12, 13] (released during the CMT Tasking) contains a dedicated chapter of CMA and will help the industry.

Considering the complex nature of this subject and the variability of the design of such safety critical systems, complete harmonization on the acceptability of the assessment outcomes is not feasible without being overly prescriptive. Given that the rules and compliance objectives are aligned between authorities, if an applicant follows the methodology in Section 4, applies the considerations in Section 5, and engages with their primary authority early, it should facilitate the discussions with validating authorities for this subject. It is therefore expected this harmonization will represent an efficiency gain for both authorities and applicants, in the context of type validation activities.

This harmonization task did not identify a need for new Rulemaking.

6.2 Recommendations

6.2.1 Industry Engagement

Industry has published recommended practices for performing safety assessments of aircraft and aircraft systems (ARP4761A/ED-135 [12, 13]) which are recognized by the four authorities, and provide a basis for harmonization. Appendix M of these recommended practices addresses Common Mode Analysis which encompasses CME. This existing industry standard is complemented and further enhanced specifically in the area of CME by the agreements achieved by the CME TST, and documented in this report.

Since the methodology defined in this report remains at a high level, it is recommended that the industry further develop detailed CME practices and guidelines supporting the implementation of the guidance contained in this report.

6.2.2 Other Sources of Errors

In order to bound the scope of this CMT task, it was agreed to prioritize efforts on addressing Development Errors. However, it should not be inferred that other error sources are not to be considered as part of a CMA. In particular, there is an increasing concern with manufacturing errors, which may not always be detected via typical means of error minimization (e.g. manufacturing quality assurance, product acceptance test, environmental stress screening, highly accelerated life test, etc.)

It is therefore recommended that further work be performed to ensure manufacturing errors are adequately addressed. While other error sources were not considered within this working group, the methodology proposed in this report for CME may in part be relevant to addressing other types of errors, including manufacturing errors.

6.2.3 Continued Authority Harmonization

As noted in section 2.1, the FAA completed a rulemaking activity associated with 14 CFR 25.1309 and its associated advisory material. Due to the timeline of the final issuance under FAR Amendment 25-152, these revisions were not considered by the CME TST. These revisions are not expected to have any significant impact to the content or conclusions of this report. However it is recommended that any future authorities harmonization task to identify impacts of the FAA safety rulemaking of 14 CFR Amt. 25-152 should also consider the content of this report as part of the wider activity.

Annexes

Annex 1 – Definitions & Abbreviations

Definitions for unique terms used in this document:

Term	Definition or Description	Source
Common Mode Error	An error which affects a number of elements otherwise considered to be independent.	ARP 4754A / ED-79
Error tolerance	A design property intended to lessen the safety consequences of a failure or error, if it occurs (failure), or if it manifests itself (error) in service. For more details, see section 3.2.2.	CME TST
Error minimization	A design development objective intended to reduce the likelihood of occurrence of failures, or of errors remaining in the certified design to a level commensurate with the safety consequences of the failure or error. For more details, see section 3.2.2.	CME TST

Abbreviations

CM	Certification Memo
CME	Common Mode Error
COTS	Commercial Off The Shelf
CRI	Certification Review Item
IP	Issue Paper

Annex 2 – Reference Documents:

Ref No	Document	Title
1.	CS 25 Amdt 27 Book 1	EASA – Certification Specifications – Large Aeroplanes https://www.easa.europa.eu/en/document-library/certification-specifications/cs-25-amendment-27
2.	14 CFR Part 25 Amdt 123	FAA – Airworthiness Standards: Transport Category Airplanes https://www.ecfr.gov/current/title-14/chapter-I/subchapter-C/part-25
3.	RBAC 25 Amdt 146	ANAC - Requisitos de Aeronavegabilidade: Aviões Categoria Transporte https://www.anac.gov.br/assuntos/legislacao/legislacao-1/rbha-e-rbac/rbac/rbac-25
4.	AWM 525 Change 525-30	TCCA – Airworthiness Manual Chapter 525 – Transport Category Airplanes https://tc.canada.ca/en/corporate-services/acts-regulations/list-regulations/canadian-aviation-regulations-sor-96-433/standards/airworthiness-chapter-525-transport-category-aeroplanes-canadian-aviation-regulations-cars
5.	CS 25 Amdt 27 Book 2	Acceptable Means of Compliance - 25.1309 Equipment, systems and installations https://www.easa.europa.eu/en/document-library/certification-specifications/cs-25-amendment-27
6.	AC 25.1309-1A	Advisory Circular - System Design and Analysis https://drs.faa.gov/browse/AC/doctypeDetails?Status=Current&Status=Historical&AC%20Number=AC%2025.1309-1A
7.	TAEsdaT2-5241996	ARAC SDHWG Report aka Arsenal, Draft rule and AC 25.1309 recommendation https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/TAEsdaT2-5241996.pdf
8.	CS 25 Amdt 27 Book 2	Acceptable Means of Compliance - 25.671 Control Systems – General https://www.easa.europa.eu/en/document-library/certification-specifications/cs-25-amendment-27
9.	TAEfch-fcs-8261998	ARAC FCHWG Report, Draft rule and AC 25.671 recommendation https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/taefch-fcs-8261998.pdf
10.	EUROCAE ED-79B	Guidelines for Development of Civil Aircraft and Systems, 2024-1
11.	SAE ARP-4754B	Guidelines for Development of Civil Aircraft and Systems, 2024-1

12.	EUROCAE ED-135	Guidelines for Conducting the Safety Assessment Process on Civil Aircraft, Systems, and Equipment. 2024-1
13.	SAE ARP4761A	Guidelines for Conducting the Safety Assessment Process on Civil Aircraft, Systems, and Equipment. 2024-1
14.	EU 2018/1139	EU Basic Regulations, Essential requirements for airworthiness https://www.easa.europa.eu/en/document-library/regulations/regulation-eu-20181139
15.	RTCA DO-178C	Software Considerations in Airborne Systems and Equipment Certification
16.	EUROCAE ED-12C	Software Considerations in Airborne Systems and Equipment Certification
17.	RTCA DO-254	Design Assurance Guidance for Airborne Electronic Hardware
18.	EUROCAE ED-80	Design Assurance Guidance for Airborne Electronic Hardware
19.	EASA CRI	Consideration of Common Mode Failures and Errors in Flight Control Function
20.	FAA CPP 25.1309-2	Use of Dissimilarity in Critical System Implementations
21.	ANAC FCAR	Development Error Mitigation in Aircraft Systems
22.	TCCA CM	Flight Control System Common Mode Errors

Annex 3 –Systematic Evaluation of Susceptibilities to CME Using Qualitative Error Tree

This appendix presents an example of an approach that could be used to systematically evaluate a proposed design and identify areas of susceptibility to CME potentially causing CAT effects, which is the first step in the CME tolerance assessment. Refer to section 4.3.2 for further details.

The example developed in this appendix is based on a qualitative fault tree ("error tree") approach, which is one of several possible approaches, as mentioned in section 4.3.2.

This example is not intended to suggest a preference for this or any other particular approach, but rather to provide an illustration of how such methodology could achieve the intent of systematically evaluating a design to identify susceptibilities to CME, and how it supports the next steps of the overall CME tolerance methodology described in section 4.

Example background information, ie Not CME specific:

1) The FHA is developed.

2) Preliminary FTAs (quantitative, for random failures) are developed as part of the PSSA / PASA.

3) As part of the PSSA / PASA activities independence principles are identified, including from a preliminary CMA (per ARP4761 App. M).

CME specific:

4) Specifically for catastrophic failure conditions, a separate suite of 'error fault trees' (qualitative only) are developed to reflect development error contributions to that failure condition.

   With the catastrophic failure conditions as top events*, error fault trees are developed to the level of detail (granularity) necessary to support a meaningful identification of the areas of susceptibility and subsequent evaluation of error tolerance. As a minimum, all contributors associated with complex elements in the system need to be included. See additional discussion on these aspects in section 4.3.2.

   * Note: For some systems, it may be possible to simplify the evaluation where multiple FHA cases can be represented by one error fault tree, such that the total number of 'error fault trees' for CAT conditions would be less than the number of conventional FTAs for the same CAT conditions. For example, for a given Flight Control System design if the contributors are the same for different CAT failure conditions, these could be grouped into a single evaluation (e.g. roll control runaway (CAT) and yaw control runaway (CAT) contributors are the same).

See the partial example at the end of this annex.

5) For each 'error fault tree', the FFS (cutsets) which could lead to the CAT top events are identified. There may be single member FFSs and multiple member FFSs. Consolidation / grouping of similar FFS at this stage may be possible (analysis optimization).

   a) **Single member FFSs** (leading directly to a CAT) represent areas of susceptibility to CME, where there is an apparent lack of independence. Each of these cases will be evaluated per section 4.3.3.

   b) **Multiple member FFSs** also represent areas of susceptibility to CME, hence will also be evaluated per section 4.3.3.

      Note 1: Whether a particular area of susceptibility appears in the analysis as single FFS or multiple FFS may depend on the granularity of the analysis, particularly for functional independence. Similar considerations would nevertheless apply in the evaluation performed per section 4.3.3. If the FFS granularity is found too high-level to provide adequate tools to evaluate error tolerance (section 4.3.3), it may be necessary to perform an iteration and increase granularity of the relevant parts of the error fault trees.

      Note 2: In principle, all multiple member FFS should be further evaluated per section 4.3.3. However, it is possible some of the FFS generated would represent combinations where it would be readily obvious that a common mode error affecting the independence of the two members would not be a realistic possibility. For example:
      - Multiple member FFS representing combination of an AEH requirement error AND a software implementation error;
      - Multiple member FFS representing combination of a software requirement error in two different systems performing different functions.

      Such cases once identified may not need to be further evaluated in detail per section 4.3.3.

   See the partial example at the end of this annex.

6) A complementary "bottom up" evaluation of the design is performed to ensure completeness of the evaluation and identification of areas of susceptibility. Any additional areas of susceptibility identified will be evaluated per section 4.3.3.

From the error trees and FFS, new independence principles may be identified in addition to those which had been previously identified (from step 3) and should be captured.

Below is a partial example of error fault tree developed for one failure condition of a high lift flight control system, along with a small subset of associated FFSs. This is intended for illustration purposes only of the approach described in this annex. The hypothetical system used in this example is the same as in Annex 4, and the failure condition partially developed corresponds to FHA F.C. ID 4 (Unannunciated loss of flaps – CAT).

Note only one branch of the FTA was fully developed for the purpose of this example; other branches remain undeveloped and are noted as such (Δ symbol, FTA transfer – incomplete). If completed, each of these branches would be expected to go down to a level similar to that currently shown for the Loss of flaps function / Loss of motor command branch.

Functional failure sets:

A complete assessment of all relevant FFS would be expected, per section 4.3.3. The following are a small subset of FFS that could be extracted from the above FTA example (once completed), for illustrative purposes:

- FFS #30 [Loss of flaps motor function due to requirement error in motor command function] AND [Loss of annunciation due to requirement error in EICAS functions]
- FFS #37 [Loss of brake release command due to SW error in flaps ECU COM] AND [Loss of fault reporting due to SW error in flaps ECU MON]
- FFS #47 [Loss of brake release enable due to AEH (processor) error in flaps ECU MON] AND [Loss of flaps unresponsive monitor due to AEH (processor) error in flaps ECU MON]
- FFS #45 [Loss of motor enable due to SW error in flaps ECU MON] AND [Loss of fault reporting due to AEH error in ECU MON]

Annexe 4 provides examples of how to document the results of the CME tolerance evaluation for the FSS above.

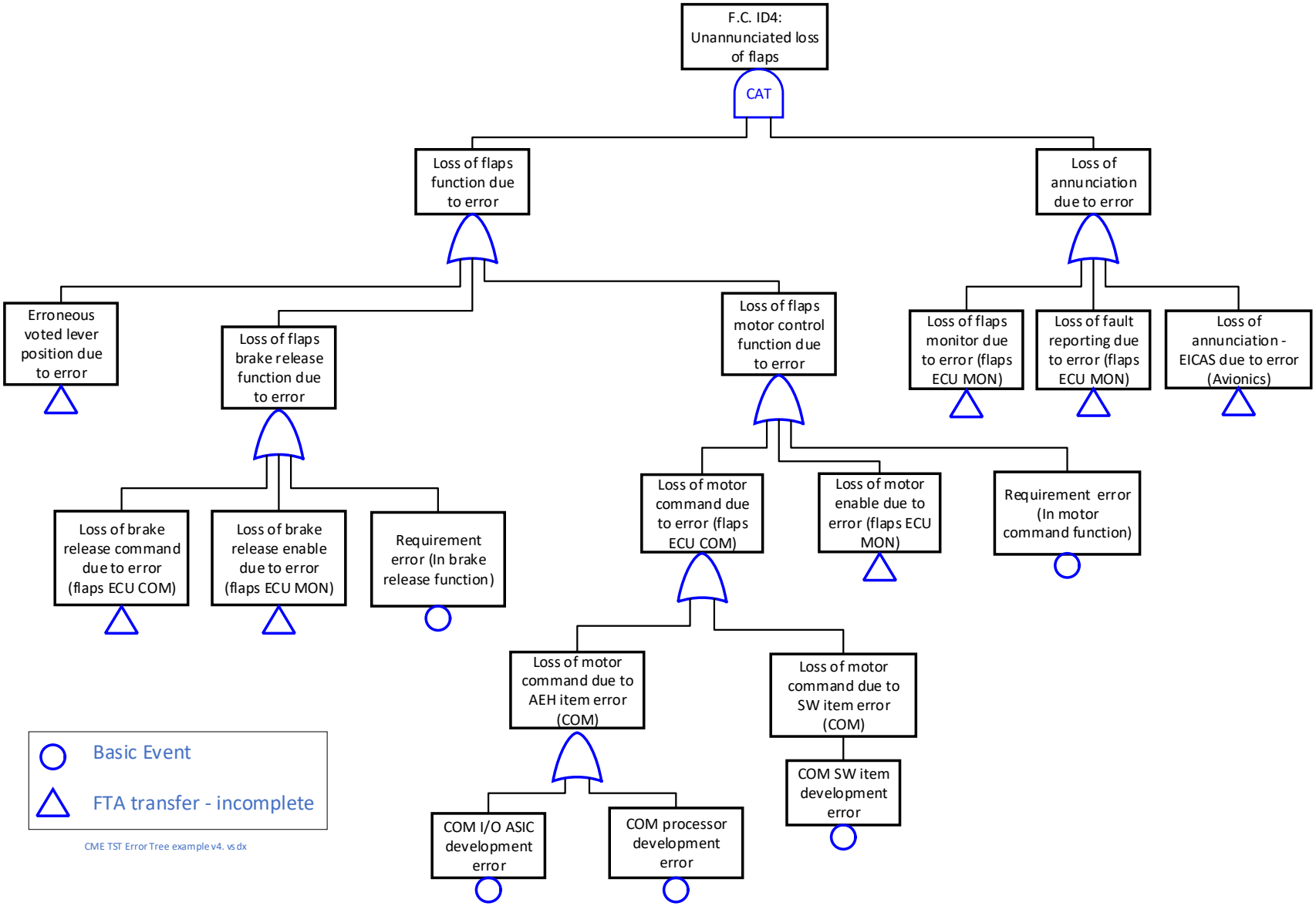

Figure 7 - Error fault tree partial example

Annex 4 – Worked CME Tolerance Evaluation Example

This annex presents a partial example of a CME tolerance evaluation for a hypothetical flap control system, first introduced in Annex 3. It is intended to illustrate one way of recording the results of the applicant's systematic CME tolerance evaluation (section 4.3.3), which is a subset of the necessary compliance documentation of the CME tolerance assessment (section 4.3.4). The format presented in Table 2 of this annex does not reflect a complete CME assessment, and should also not be seen as an analysis template.

The CME tolerance evaluation (section 4.3.3) is directly linked to the CME susceptibilities identified by the systematic process that precedes it (section 4.3.2). To help illustrate this, Annex 4 includes examples of CME tolerance evaluation for the few FFS examples identified based on the partial error fault tree developed in Annex 3.

The partial data entries in Table 2 are illustrative only, and are intended to show the type of information and expected level of detail in recording the tolerance evaluation results. The technical contents of these entries should not be interpreted as certification authorities policy on the acceptability of the hypothetical error tolerance techniques, or residual exposure and justifications that are presented in the example.

The notes included in italics and brackets in this example *[Note: …]* are intended as clarifications for the reader of this report.

System Design and Architecture overview:

[The CME tolerance evaluation documentation should include an appropriate system architecture and design description, including features that may provide mitigation against CME; or reference to the system description report and revision. Most details are omitted in this example for brevity. A subset of design features and operational characteristics is highlighted below to aid in understanding the hypothetical system example used in this Annex.]

- Command (COM) and Monitor (MON) lanes to ensure command integrity against random failures (F.C. ID 1, F.C. ID 3, F.C. ID 4, F.C. ID 5).
- Flap brakes independently signaled from COM and MON lanes
  (F.C. ID 1, F.C. ID 4).
- Flap motor commanded by COM lane and enabled by MON lane
  (F.C. ID 1, F.C. ID 3, F.C. ID 4).
- Mechanical interlocks (gated positions) successfully prevent inadvertent Flap Lever movement (F.C ID 1, F.C. ID 3).
- LH and RH flap surfaces are mechanically interconnected through a flex drive shaft; a development error will not lead to flap asymmetry unless it is combined with the failure of the flap surface flex drive shaft (F.C. ID 2).
- Redundant flap lever LVDT position sensors voted to mitigate erroneous flightcrew command inputs (F.C. ID 1, F.C. ID 3, F.C. ID 4).

- (…)

System FHA CAT failure conditions:

- FHA F.C. ID 1: Uncommanded flap deployment – CAT
- FHA F.C. ID 2: Flap asymmetry – CAT
- FHA F.C. ID 3: Erroneous flap position – CAT
- FHA F.C. ID 4: Unannunciated loss of flaps – CAT *[see Annex 3]*
- FHA F.C. ID 5: Erroneous flap position data output to primary flight controls (CAT)
- (…)

[Note: FC list incomplete in this example, for brevity].

Annex 4 Table 1 - CME Tolerance evaluation worksheet description

Column #	Worksheet Column Explanation
1	Independence principle under evaluation, unique identifier and principle description.
2	Potential areas of Susceptibility identified based on the systematic evaluation of the proposed design, for the error source(s) identified in column 4. FFS or equivalent.
3	Potential effects on item, system, and aircraft for the area of susceptibility identified in column 2, and for the various applicable Failure Conditions. The column 3 entries capture in narrative form how the area(s) of Susceptibility (column 2) to the postulated common mode error source (column 4) could result in catastrophic effects for each failure condition relying on this independence principle.
4	Potential common mode error source being evaluated. In the context of development error tolerance assessment, this entry would be a mistake in requirement specifications, design, or implementation.
5	Evaluation of the error tolerance relevant to the area of susceptibility, for the identified error source(s), and discussion of any residual CME exposure. The narrative should include error tolerance features or mitigations existing or planned to address the common mode development error susceptibility, and their associated coverage. This column also describes any residual exposure to CME affecting the independence principle, for which justification should be included in the final version of the tolerance assessment if deemed acceptable.

Annex 4 Table 2 - CME tolerance evaluation results example

1	2	3	4	5
Independence Principle(s) (IP)	**Potential Areas of Susceptibility** *(Potential **susceptibilities** identified from the systematic design evaluation.)*	**Potential effects** *(How the potential **susceptibility** can result in the CAT F.C.(s) effect)*	**Error source(s)**	**Error Tolerance Evaluation and Results** *(Description of error tolerance features and mitigation, resulting coverage, and overall acceptability of error tolerance. Description of residual exposure to CME if any, and associated justification. For what is mitigated / covered, the outcome should provide sufficient data to define Safety / Independence Requirements)*
1.1: Flap system COM path must be independent from flap system MON path	(…)	F.C. ID 1: (…) F.C. ID 3: (…) F.C. ID 5: (…)	(…)	**Error tolerance**: (…) **Residual exposure to CME, and justification**: (…)
(…)				
1.1: Flap system COM path must be independent from flap system MON path	FFS #105 (Multiple): [Erroneous consolidated flap position output due to error in COM I/O ASIC] and [Erroneous consolidated flap position output due to error in MON I/O ASIC]	F.C. ID 5: A common development error between the COM and MON I/O ASICs (AEH) could result in an erroneous consolidated flap position data to other systems	Requirement Design Implementation	**Error tolerance**: Although this was represented as a multiple member FFS, since the COM and MON I/O ASICs are identical components, the occurrence of a common mode error affecting both COM and MON ASICs – either low level requirements, design or implementation – could affect in the same manner the critical consolidated flap position output to the primary flight control system. These critical data outputs from both flap ECU COM and MON are protected by an application layer CRC. If the output value is affected by the I/O ASICs, the flight control system will detect it, flag the data as invalid, and use a safe default value. Error tolerance acceptable; no additional mitigation required. *[Note: This could have been represented as a single member FFS for "I/O ASIC", i.e. without distinguishing between COM and MON if it is already known the same component will be used. Granularity and breakdown can be subjective, but the end result evaluation would be the same in either case.]*
(…)				

1	2	3	4	5
1.1: Flap system COM path must be independent from flap system MON path	FFS #78 (Single): [Erroneous flap lever position due to LVDT error]	F.C. ID 1: A common development error in the flap lever LVDTs outputs to COM and MON could lead to uncommanded flap deployment. F.C. ID 3: A common development error in the flap lever LVDT outputs to COM and MON could lead to erroneous flap surface position.	Requirement Design Implementation	**Error tolerance**: None **Residual exposure to CME, and justification**: LVDTs are simple, FAT components. Not a concern for development errors. *[Note: Included in this example for illustration purposes. In a "real-world" CME tolerance assessment, such element would be out of scope since LVDTs can be considered simple FAT components. Ref. section 5.3]*
1.1: Flap system COM path must be independent from flap system MON path	FFS #12 (Single): [Erroneous ARINC 429 protocol]	F.C. ID 1: (…) F.C. ID 3: (…) F.C. ID 5: (…)	Requirement Design Implementation	**Error tolerance**: (…) **Residual exposure to CME and justification**: A429 protocol is industry standard, and the same used in airplane XYZ with extensive service history and no significant issues as detailed in report ##. Implementation of A429 protocol in the flap control system follows AC 20-156 guidelines for legacy databus technology.
(…)				
6.2 Flap system alerts must be independent from flap system command function	FFS #30 (Multiple): [Loss of flaps motor function due to requirement error in motor command function] AND [Loss of annunciation due to requirement error in EICAS functions] *[ref. Annex 3]*	F.C. ID 4: Common requirement error in the motor command function and in the EICAS function could lead to loss of flaps motor function that is not annuncated to the flightcrew by the EICAS function.	Requirement Error	**Error tolerance**: This is a multiple member FFS representing the potential occurrence of a common requirement error in the development of two independent systems at aircraft level, performing different functions and developed by different suppliers. Error tolerance acceptable; no additional mitigation required.
(…)				

1	2	3	4	5
6.2 Flap system alerts must be independent from flap system command function	FFS #37 (Multiple): [Loss of brake release command due to SW error in flaps ECU COM] AND [Loss of fault reporting due to SW error in flaps ECU MON] *[ref. Annex 3]*	F.C. ID 4: Common development error between the COM SW item (affecting brake release) and the MON SW item (affecting fault reporting) could lead to loss of flaps command that is not annuncated to the flightcrew	Requirement Design Implementation	**Error tolerance**: This is a multiple member FFS representing the potential occurrence of a common development error in the flap ECU COM SW and the flap ECU MON SW. - Different functions & associated functional requirements at system level* provide extensive error tolerance (i.e. coverage for most CME susceptibilities) at the lower-level item implementation. - The ECU MON and ECU COM softwares are independent items, each with their own DO-178C process and documentation package. - The ECU MON and ECU COM softwares are executed on different processors, one in each lane. Error tolerance acceptable; no additional mitigations necessary. *[Notes:* - **Common specification errors in the related system level functions would be addressed in a separate line of this assessment table.* - *Potential common mode errors resulting from common development tools, libraries, models, etc… should also be considered as necessary but have not been elaborated on in this example.]*
(…)				
6.2 Flap system alerts must be independent from flap system command function	FFS #45 (Multiple): [Loss of motor enable due to SW error in flaps ECU MON] AND [Loss of fault reporting due to AEH error in ECU MON] *[ref. Annex 3]*	F.C. ID 4: Common development error between the MON SW item (affecting motor enable) and MON processor AEH item (affecting reporting function) could lead to loss of flaps command that is not annuncated to the flightcrew		**Error tolerance**: This is a multiple member FFS representing the potential occurrence of a common development error in the flap ECU COM software item and in the flap ECU AEH (processor) item. A common mode error affecting the independence of these two FFS members (i.e. a SW item and an AEH item) is not considered to be a realistic possibility. No further evaluation is required (ref. Annex 3 step 5.b note 2). *[Note: Common specification errors in the related system level functions would be addressed in a separate line of this evaluation table.]*
(…)				
6.2 Flap system alerts must be independent from flap system command function	FFS #47 (Multiple): [Loss of brake release enable due to AEH (processor) error in flaps ECU MON] AND [Loss of flaps unresponsive monitor due to AEH (processor) error in flaps ECU MON] *[ref. Annex 3]*	F.C. ID4: Development error in MON AEH (processor) could result in loss of both brake release enable and loss of flaps unresponsive monitors, resulting in loss of flap actuation that is undetected and not annunciated to the flightcrew.	Requirement Design Implementation	**Error tolerance**: Although this was represented as a multiple member FFS, it represents the occurrence of a (single) error in the AEH (processor) of the ECU MON – either low-level requirements, design or implementation – affecting two different functions implemented in MON. As a common mode error could potentially result in loss of both functions, the necessary independence would not be achieved with the system architecture as presented; the **lack of error tolerance in the proposed system is not acceptable**. *[Note: at this point, this should trigger a loop towards system / architecture re-design, and/or additional error tolerance features and mitigations should be proposed. This example reflects work in progress during development, and the iterative nature of the evaluation.]*

---- End ----