|  |
| --- |
| Development Plan |
| Doc. Number: <<>>Issue: 1.0 |
| **Compiled** | **Checked** | **Office of Airworthiness** | **Date** |
| NAME:James Lawson | SIGNED: | SIGNED: |   |

# Issue Record

|  |  |  |
| --- | --- | --- |
| **Issue** | **Reason for Change** | **Date** |
| 1.0 | Initial Issue. | dd/mm/yyyy |
|  |  |  |

**Note:** This document is updated as a complete document and not as individual pages.

# Contents

[Issue Record 2](#_Toc102241841)

[Contents 3](#_Toc102241842)

[Abbreviations 4](#_Toc102241843)

[References 4](#_Toc102241844)

[1 Introduction 5](#_Toc102241845)

[2 Scope 5](#_Toc102241846)

[3 Program Organization 5](#_Toc102241847)

[3.1 Schedule 5](#_Toc102241848)

[3.2 Airworthiness Certification 5](#_Toc102241849)

[3.3 Location 5](#_Toc102241850)

[3.4 Personnel and Responsibilities 5](#_Toc102241851)

[3.5 Engineering Review Board (ERB) 8](#_Toc102241852)

[4 System Development Lifecycle 9](#_Toc102241853)

[4.1 System & Safety Development Process 9](#_Toc102241854)

[4.2 System Requirements Capture 1](#_Toc102241855)

[4.3 Requirements Traceability 2](#_Toc102241856)

[4.4 System V&V 3](#_Toc102241857)

[4.5 Requirements Tool 4](#_Toc102241858)

[4.6 Technical Reviews 4](#_Toc102241859)

[5 Configuration Management 5](#_Toc102241860)

[6 Process Assurance 6](#_Toc102241861)

[7 Development Objectives 6](#_Toc102241862)

# Abbreviations

|  |  |
| --- | --- |
| AGS | Aircraft General Spares |
| CAA | Civil Aviation Authority |
| DO | Design Organisation |
| DOA | Design Organisation Approval |
| DOP | Design Organisation Procedure |
| ECR | Engineering Change Request |
| TC | Type Certificate |
| STC | Supplemental Type Certificate |
| C | <<company>> |

# References

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref.** | **Document Number and Title** | **Issue** | **Date** |
|  |  |  | dd/mm/yyyy |
|  |  |  | dd/mm/yyyy |
|  |  |  | dd/mm/yyyy |

# Introduction

The development effort is a process consisting of many multidisciplinary stages. It is paramount to implement a well-defined design assurance process to ensure the integrity of the design. AC 25.174 recognizes SAE ARP4754A as an acceptable practice for a design assurance process for civil certified aircraft.

# Scope

This document describes the development effort to be completed by <<company>>. The safety artifacts for civil certified aircraft are generated in accordance with SAE ARP4761. The development effort of suppliers should be conducted as a direct result of the development effort of <<company>>.

# Program Organization

## Schedule

For detailed program schedule and milestones, refer to the Program Plan.

## Airworthiness Certification

<<company>> will be the applicant for the Supplemental Type Certificate (STC), Type Certificate (TC) for the modified aircraft with the product under development installed. It is the responsibility of systems engineering team to ensure compliance with the regulations and special conditions identified by the Certification Plan(s).

## Location

The development effort of this program will occur at TBD. Ground test activities will occur at TBD. Flight test activities will occur at TBD.

## Personnel and Responsibilities

Personnel resource allocation is defined by the Program Plan. At a minimum, the following <<company>> departments with a breakdown of their responsibilities will be involved in this program execution:

* Engineering
	+ System engineering
	+ Reliability, maintainability and safety
	+ Structural
	+ Electrical
	+ Mechanical
* Certification engineering
	+ Airworthiness, certification planning
* Flight sciences
	+ Flight analysis
* Test engineering
* Aircraft modification
* Flight operations
	+ Ground test
	+ Flight test
* Configuration management
* Quality assurance
* Supply chain management
* Program management

### System Engineering Team Roles and Responsibilities

The system engineering team is responsible for the requirements centric development effort, including but not limited to the following:

* understanding customer requirements/ key performance parameters
* system level requirements
* sub-system level requirements
* allocating the requirements to engineering disciplines to implement
* validation of requirements
* verification of requirements
* system integration

### Systems IPT Lead

The systems IPT lead is responsible for managing the system engineering team throughout the lifecycle of the product under development, including but not limited to the following:

* Ensure program goals are achieved by the system engineering team
* Work with the program managers to manage program cost, schedule and resources
* Prepare formal and informal presentations of progress with respect to plans, costs, schedules
* Provide adequate support to other engineering disciplines

### System Requirements Lead

The systems requirements lead is responsible for overseeing the requirements decomposition, capture and validation process. In this role he/she will act as a liaison with functional leads of these efforts throughout the engineering lifecycle of the product under development, including but not limited to the following:

* Interact with customers for customer technical specification decomposition/ capture, validation and negotiation
* Enforce requirements decomposition/ capture and validation process within this document
* Collect and ensure compliance statements are correct/ complete
* Collect and ensure system and sub-system requirements are correct/ complete
* Ensure all mandatory fields per requirement are complete: V&V methods, safety tag
* All system/ sub-system requirements must either have a parent or be derived with a written rationale giving the reason for their existence
* Ensure system/ sub-system requirements have validation data aligned with designated method(s)
* Ensure requirement decomposition/ capture and validation open issues/ problem reports are dispositioned by specific milestones
* Liaison between system teams and subsystem teams
* Organize and moderate system/ sub-system ERBs and peer reviews
* Generate system requirements documentation, including validation matrix
* Generate system traceability report
* Support subsystem design and installation peer reviews
* Assist system integration, problem report investigation and requirements verification process
* Ensure requirements affected by system integration are dispositioned via ERBs
* Drive day-to-day requirements and validation tasks
* Support non-requirements-centric program milestones (Conformity Reviews, Ground Test, SOF, Flight Test)
* Organize requirements-centric program milestones (SRR, PDR, CDR, Audits)

### System Verification Lead

The systems verification lead is responsible for overseeing the requirements verification process. In this role he/she will act as a liaison with functional leads of these efforts throughout the engineering lifecycle of the product under development, including but not limited to the following:

* Interact with customers for customer technical specification verification and negotiation.
* Enforce requirements verification processes within this document
* Ensure system/ sub-system requirements have verification data aligned with designated method(s)
* Ensure open verification open issues/ problem reports are dispositioned by specific milestones
* Liaison among system/ sub-system teams and test engineering
* Support system/ sub-system ERBs and peer reviews
* Generate system verification matrix
* Generate system verification test reports
* Support subsystem design and installation peer reviews
* Drive day-to-day verification tasks
* Support non verification-centric program milestones (Conformity Reviews, SRR, PDR, CDR, Audits)
* Organize verification-centric program milestones (Ground Test, SOF, Flight Test)
* Participate in the ERBs

### Configuration Management Lead

The configuration management lead is responsible for configuration management related to the product under development. In this role he/she will act as a liaison with functional leads of these efforts throughout the engineering lifecycle of the product under development, including but not limited to the following:

* Overall configuration identification responsibility
* Overall configuration baseline establishment responsibility
* Managing problem reporting tools/ processes
* Managing change control tools/ processes
* Overall configuration index establishment responsibility
* Managing the archive and retrieval of configuration items

### Process Assurance Lead

The process assurance lead is responsible for process assurance of plans and procedures related to the product under development. In this role he/she will manage these efforts throughout the engineering lifecycle of the product under development, including but not limited to the following:

* Manage definition of applicable plans and procedures
* Organise process assurance audits of plans and procedures
* Track and control plan and procedure updates
* Ensure that affected engineering disciplines are aware of plan and procedure updates
* Manage plan and procedure non-compliance and deviations
* Manage process assurance checklists
* Collect evidence of conformance to plans and procedures
	+ Approved plans and procedures
	+ Summary of audits
	+ Controlled/ approved design and development data
	+ Validation artefacts
	+ Verification artifacts
	+ Controlled/ approved certification data
	+ Completed checklists

## Engineering Review Board (ERB)

ERB is a group of engineers composed of representatives from all engineering disciplines who determine scope and ensure complete implementation. Depending on the change, it will consist of the systems IPT lead, the subject matter experts and the engineers responsible for the change and be chaired by a designated ERB chair.

# System Development Lifecycle

## System & Safety Development Process

The <<company>> product engineering development process complies with the intent of SAE ARP4754A, Guidelines for Development of Civil Aircraft and Systems. Figure 4‑1 shows the V development process which applies to all system/ sub-system development effort.

Starting from left to right, Figure 4‑1 illustrates the following:

* The requirements, design/ validation and verification phases of the engineering lifecycle
* The development of a system/ sub-system architecture
* The decomposition and allocation of functions/ requirements to systems and sub-systems
* The technical review milestones throughout the engineering lifecycle
* System artifacts produced throughout the engineering lifecycle
* Safety artifacts produced throughout the engineering lifecycle
* Corresponding major program milestones.



Figure 4‑1: System & Safety Development Process

The system and safety development process will be used to derive the safety requirements for each system/ sub-system, as well as the Design Assurance Level (DAL) and probability/ failure rate budgets. The DAL is to be assigned by the <<company>> product Functional Hazard Assessments (FHA). Any complex hardware or software, including COTS, will satisfy RTCA DO-254 and RTCA DO-178 objectives at their assigned DAL.

Safety requirements exist at the system and sub-system (or item per SAE ARP4754A) level, and are decomposed/ captured top down at each tier, hence the V development process shape. At the system level, the safety requirements are mainly generated from and align with the FHA for the <<company>> product but can also come from the Common Cause Analyses (CCA). At the sub-system level, safety requirements are mainly generated from and align with the Preliminary System Safety Assessment (PSSA). There is traceability between the FHA failure conditions and the PSSA fault tree analysis and events. A top-down fault tree analysis is completed as part of the PSSA followed by a bottom-up fault tree analysis as part of the System Safety Assessment (SSA).

The top-down fault tree is used for the following purposes:

* Capture failure rate requirements for system and sub-system and equipment
* Capture independence requirements

The bottom-up fault tree is used for the following purposes:

* Verify failure rate requirements for system and sub-system equipment
* Verify independence requirements

The bottom-up fault tree analysis is populated by the results of the Failure Mode Effects Analysis (FMEA) and Failure Mode Effects Analysis (FMES). Also, it includes the results of the Single Event Effect (SEE) analysis. A reliability prediction is used to determine component failure rates. The reliability prediction can be a parts count analysis when component junction temperatures are available and a parts stress analysis when they are not available.

## System Requirements Capture

The System Engineering team, will be responsible for decomposing, capturing, implementing, and validating the system and sub-system level requirements. Generally, the requirement types decomposed and captured are as follows:

* Performance
* Functional including human factors
* Physical e.g. size and weight
* Interfaces
* Environmental
* Reliability
* Maintainability
* Safety including FDAL/ IDAL and probability or failure rate budget and cycle time
* Security
* Installation

Each system/ sub-systems level requirement is written with the verb “shall” and has the following required fields:

* All system/ sub-system requirements must either have a parent or be derived with a written rationale giving the reason for their existence
* Validation Method
* Validation Evidence
* Verification Method
* Verification Evidence
* Assumptions (if any)
* Safety Tag (yes or no)

 The following subsections will discuss these fields.

Table 4‑1 defines the <<company>> parallel hybrid-electric powertrain requirements management tool hierarchy.

|  |  |
| --- | --- |
| Requirement Section | Description |
| TBD | TBD |

Table 4‑1: <<company>> Parallel Hybrid-Electric Powertrain Requirements Management Tool Hierarchy

## Requirements Traceability

A child requirement that is linked via a parent/ child relationship must be consistent with the intent of the parent requirement. Requirements that have no parent requirements are considered “derived”. All system/ sub-system requirements must either have a parent or be derived with a written rationale giving the reason for their existence. All derived requirements must be reviewed for safety impact.

A compliance matrix will be created for all regulations, special conditions and standards that have been selected for the program by the Certification Plan(s).

The following report will be generated to ensure requirements traceability:

Compliance matrix for regulations, special conditions and standards showing methods of compliance and the associated evidence.

Validation matrix for system and sub-system requirements showing validation methods and associated evidence.

Verification matrix for system and sub-system requirements showing verification methods and associated evidence.

The following section will describe <<company>> product V&V.

## System V&V



Figure 4‑2: Purpose of V&V

V&V is an iterative process that reduces design and development risk throughout the engineering lifecycle. As illustrated by Figure 4‑2, the purpose of V&V is to ensure the requirements are correct and complete and that the implemented design matches the intended design as specified by the system and sub-system requirements.

### System Requirements Validation

System requirements are validated throughout the top-down phases as shown in Figure 4‑1. The validation process is to ensure that they are correct, complete and unambiguous with respect to the customer requirements and design decisions. A validation matrix is created for all system and subsystem requirements.

The process starts by assigning validation method to each system and sub-system requirement with written assumptions if any. Then, each requirement is substantiated by validation evidence matching the method.

The validation method will be selected from the following:

* Calculations/ Analysis
* Certification
* Design/ Data Review
* Safety Analysis
* Similarity of Service Experience (from previously certified systems)
* Simulation
* Test

NOTE: All system/ sub-system requirements must either have a parent or be derived with a written rationale giving the reason for their existence.

### System Requirements Verification

System requirements are verified throughout the top-down phases as shown in Figure 4‑1. The verification process is to ensure that the implemented design matches the intended design as specified by the system and sub-system requirements. A verification matrix is created for all system and subsystem requirements.

The process starts by assigning verification method to each system and sub-system requirement with written assumptions if any. Then, each requirement is substantiated by verification evidence matching the method.

The verification method will be selected from the following:

* Calculations/ Analysis
* Design/ Data Review
* Equipment Qualification
* Flight Test
* Ground Test
* Laboratory Test
* Functional Test
* Physical Inspection
* Safety Analysis
* Similarity of Service Experience
* Simulation

## Requirements Tool

The decomposing, capturing, tracking and organizing of system and sub-system requirements data and traceability is necessary for the success of the program.

Polarion has been selected as the engineering requirements management tool database. The <<company>> product requirements management tool hierarchy will be fully implemented in Polarion. Each requirement item in Polarion has associated required fields specified by Section 4.2 and can have attachments and internal/ external database reference links.

Peer reviews will be conducted using Polarion for comments, disposition and notes capture. Checklists will be used. A system and sub-system requirements change process will be implemented using Polarion workflow features to prevent unauthorized changes. Polarion can show redline comparison between any two versions of the same requirement item.

Problem reports and V&V evidence will be captured by Polarion. Also, test cases, plans, procedures and test reports will be captured by Polarion as will the Certification Plan(s).

Documents created within Polarion will exported as required for major and minor program milestones.

## Technical Reviews

<<company>> will organize ERBs as required and for major and minor program milestones.

Technical reviews at a minimum will be completed at the following major program milestones:

1. Concept Design Review (CoDR)
2. System Requirements Review (SRR)
3. Preliminary Design Review (PDR)
4. Critical Design Review (CDR)
5. Test Readiness Review(s) (TRR)
6. First Flight Readiness Review (FFRR)
7. Type Inspection Review (TIR)
8. Production Readiness Review (PRR)

Product maturity at technical reviews will be equal to or greater than the following

* 10% design maturity required at Concept Design Review (CoDR)
* 40% design maturity required at Preliminary Design Review (PDR)
* 80% design maturity required at Critical Design Review (CDR)
* 100% Required by Production Readiness Review

Refer to the following <<company>> procedures for technical reviews;

* Preliminary Design Review Exit Criteria
* Critical Design Review Exit Criteria

Checklists for each technical review will be generated prior to the technical review. The results of each technical review will be recorded and archived in the configuration management tool in accordance with the Configuration Management Plan.

The categorization of technical review action items is as follows:

Category 1 action This is an outstanding mandatory action item that is required to be closed in order to successfully exit the technical review milestone. Successful closure of such an item will require mutually agreed data to be provided for approval in order to facilitate technical review milestone closure.

Category 2 action This is an outstanding non-mandatory action item that is not required to be closed in order to successfully exit the technical review milestone but is required to be closed prior to the next major technical review milestone.

If either a category 1 or category 2 action necessitates a problem report and/ or a change request, in accordance with the Configuration Management Plan, these processes should be invoked.

# Configuration Management

<<company>> ensures that the necessary plans are developed and maintained for all aspects of the <<company>> product airworthiness certification by means of an overall commitment to configuration management. The Configuration Management Plan defines the said configuration management activities and processes.

The purpose of the configuration management process can be summarized as follows:

1. to properly identify the functional and physical characteristics of the configuration items,
2. to control changes to those characteristics, and
3. to record and report change processing and implementation status.

A Configuration Index will be created to identify all the items that comprise the <<company>> product under development. This Configuration Index will be maintained throughout the project lifecycle. The Configuration Index should contain at least the following:

* Configuration identification of each <<company>> product system and sub-system item
	+ Associated part numbers/ versions
	+ Associated complex hardware part numbers/ versions
	+ Associated software part numbers/ versions
* Interconnection of items
* Required interface with other systems/ sub-systems and with the aircraft

# Process Assurance

<<company>> ensures that the necessary plans are developed and maintained for all aspects of the <<company>> product airworthiness certification by means of an overall commitment to process assurance. The Process Assurance Plan defines the said development activities and processes.

# Development Objectives

Table 7‑1 shows the development objectives.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Objective | Objective description (from ARP 4754A) | Output | FDAL A | FDAL B | FDAL C | FDAL D | FDAL E |
| 1 Planning process |
| 1.1 | System development andintegral processes activities are defined | Certification Plan | Y | Y | Y | Y | Y |
| Safety Program Plan | Y | Y | Y | Y | N |
| Development Plan | Y | Y | Y | Y | N |
| Validation and Verification Plan | Y | Y | Y | Y | N |
| ConfigurationManagement Plan | Y | Y | Y | Y | N |
| ProcessAssurance Plan | Y | Y | Y | Y | N |
| 1.2 | Transition criteria and interrelationship among processes are defined | Plans inobjective no. 1 | Y | Y | Y | N | N |
| 2.0 System and sub-system development process and requirements decomposition/ capture |
| 2.1 | Functions, functional interfaces and assumptions are defined | List of aircraft and system level functions | Y | Y | Y | N | N |
| 2.2 | Functions are allocated to systems/ sub-systems | Allocation of functions to systems/ sub-systems | Y | Y | Y | N | N |
| 2.3 | System requirements including assumptions are defined, are traceable or rationales are defined for derived requirements; performance, functional, physical, interfaces and environmental | System Requirements | Y | Y | Y | N | N |
| 2.4 | Sub-system requirements including assumptions are defined, are traceable or rationales are defined for derived requirements; performance, functional, physical, interfaces and environmental | Sub-system Requirements | Y | Y | Y | N | N |
| 2.5 | System architecture is defined | System DesignDescription | Y | Y | Y | N | N |
| 2.6 | Sub-system requirements are broken down into High Level Requirements (HLRs) and Low-Level Requirements (LLRs) for software and complex hardware configuration items | Software HLRs and LLRs | Y | Y | Y | N | N |
| Complex hardware HLRs and LLRs | Y | Y | Y | N | N |
| 2.7 | System and sub-system verification is performed | VerificationArtifacts | Y | Y | Y | N | N |
| 3.0 Safety Assessment Process |
| 3.1 | Functional hazard analysis is performed | FHA | Y\* | Y\* | Y | Y | Y |
| 3.2 | The preliminary system safety assessment isperformed | PSSA | Y\* | Y\* | Y | Y | N |
| Top-Down FTA | Y\* | Y\* | N | N | N |
| 3.3 | Safety requirements including; independence, probability budget and Functional Development Assurance Levels (FDAL) and Item Development Assurance Levels (IDALs) are defined | Safety requirements | Y\* | Y\* | Y | Y | N |
| 3.4 | The common cause analyses are performed | Particular RiskAnalysis | Y | Y | Y | N | N |
| Common ModeAnalysis | Y\* | Y\* | Y | N | N |
| Zonal SafetyAnalysis | Y | Y | Y | N | N |
| 3.5 | The system safety assessment is performed | SSA | Y\* | Y\* | Y | Y | N |
| Bottom-Up FTA | Y\* | Y\* | N | N | N |
| 3.6 | Failure Mode Effect Analysis (FMEA), Failure Mode Effects Summary are performed | FMEA/ FMES | Y\* | Y\* | Y | N | N |
| 3.7 | Reliability Prediction is performed | RP | Y\* | Y\* | Y | N | N |
| 3.8 | Single Event Effect Analysis is performed | SEE | Y\* | Y\* | N | N | N |
| 4.0 Requirements Validation Process |
| 4.1 | System and sub-system requirements are complete and correct | ValidationResults | Y\* | Y\* | Y | Y | N |
| 4.2 | Assumptions are justified and validated | ValidationResults | Y\* | Y | Y | Y | N |
| 4.3 | Derived requirements are justified and validated | ValidationResults | Y\* | Y\* | Y | Y | N |
| 4.4 | Requirements are traceable or rationale is defined for derived requirements | ValidationResults | Y | Y | Y | Y | N |
| 4.5 | Validation compliance substantiation is provided | ValidationMatrix | Y | Y | Y | Y | N |
| Validation Summary | Y | Y | Y | Y | N |
| 5.0 Requirements Verification Process |
| 5.1 | Verification procedures are correct | VerificationProcedures | Y\* | Y | Y | Y | N |
| 5.2 | Verify unintended functions do not impact to safety | VerificationProcedures | Y\* | Y | Y | Y | N |
| VerificationResults | Y\* | Y | Y | Y | N |
| 5.3 | Verify performance requirements | VerificationProcedures | Y\* | Y | Y | Y | N |
| VerificationResults | Y\* | Y | Y | Y | N |
| 5.4 | Verify functional requirements including human factors | VerificationProcedures | Y\* | Y | Y | Y | N |
| VerificationResults | Y\* | Y | Y | Y | N |
| 5.5 | Verify physical requirements | VerificationProcedures | Y\* | Y | Y | Y | N |
| VerificationResults | Y\* | Y | Y | Y | N |
| 5.6 | Verify interfaces | VerificationProcedures | Y\* | Y | Y | Y | N |
| VerificationResults | Y\* | Y | Y | Y | N |
| 5.7 | Verify environmental requirements | QualificationProcedures | Y\* | Y | Y | Y | N |
| QualificationResults | Y\* | Y | Y | Y | N |
| 5.8 | Verify safety requirements | Verification Results | Y\* | Y\* | Y | Y | N |
| 5.9 | Verification compliance substantiation is provided | VerificationMatrix | Y | Y | Y | Y | N |
| VerificationSummary | Y | Y | Y | Y | N |
| 5.10 | Identify Certification Maintenance Requirements (CMRs) and disposition problem reports | CMRs | Y | Y | Y | Y | N |
| ProblemReports | Y | Y | Y | Y | N |
| 6.0 Configuration Management Process |
| 6.1 | Configuration items are identified | Configuration Items | Y | Y | Y | Y | N |
| 6.2 | Incomplete, interim and delivery releases are established | Incomplete Releases | Y | Y | Y | Y | N |
| Interim Releases | Y | Y | Y | Y | N |
| Delivery Releases | Y | Y | Y | Y | N |
| 6.3 | Archive and retrieval are established | Archive and Retrieval Records | Y | Y | Y | Y | N |
| 7.0 Process Assurance Process |
| 7.1 | Assurance is obtained that necessary plans are developed and maintained for all aspects of system certification | Evidence ofProcessAssurance | Y\* | Y\* | Y\* | Y | N |
| 7.2 | Development activities and processes are conducted in accordance with those plans | Evidence ofProcessAssurance | Y\* | Y\* | Y\* | Y | N |
| 8.0 Certification and Regulatory Authority Coordination Process |
| 8.1 | Compliance substantiation is provided. | CertificationSummary | Y | Y | Y | Y | N |
| ConfigurationIndex | Y | Y | Y | Y | N |

Table 7‑1: Development Objectives

NOTE:

Y Required for a particular system/ sub-system as dictated by the FDAL for that system/ sub-system

N Not required for a particular system/ sub-system as dictated by the FDAL for that system/ sub-system

\* Independence is required i.e. the activity is performed by a person(s) other than the developer of the system, sub-system or configuration item.