|  |
| --- |
| Configuration Management 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](#_Toc102241809)

[Contents 3](#_Toc102241810)

[Abbreviations 4](#_Toc102241811)

[References 4](#_Toc102241812)

[1 Introduction 5](#_Toc102241813)

[2 Scope 5](#_Toc102241814)

[3 Configuration Management 5](#_Toc102241815)

[3.1 Configuration Identification 6](#_Toc102241816)

[3.2 Configuration Baseline Establishment 7](#_Toc102241817)

[3.3 Problem Reporting 8](#_Toc102241818)

[3.4 Change Control 8](#_Toc102241819)

[3.5 Configuration Index Establishment 9](#_Toc102241820)

[3.6 Archive and Retrieval 10](#_Toc102241821)

[4 Data Control Categories 10](#_Toc102241822)

[4.1 Configuration Management Environment 14](#_Toc102241823)

[5 Configuation Management Lifeycle 15](#_Toc102241824)

[5.1 General 15](#_Toc102241825)

[5.2 CoDR Deliverables 15](#_Toc102241826)

[5.3 SRR Deliverables 15](#_Toc102241827)

[5.4 PDR Deliverables 15](#_Toc102241828)

[5.5 CDR Deliverables 16](#_Toc102241829)

[5.6 FFRR Deliverables 16](#_Toc102241830)

[5.7 TC Deliverables 16](#_Toc102241831)

[6 Templates and Checklists 17](#_Toc102241832)

[6.1 Change Request Matrix Template 17](#_Toc102241833)

[6.2 Change Request Checklist 17](#_Toc102241834)

# 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 Configuration Management Plan describes the activities that are performed on data related to the product under development to support certification.

The objectives of configuration management are as follows:

* Establish requirements, certification and design data baselines
* Changes to requirements, certification and design data baselines are controlled
* Record data that uniquely identifies system/ sub-system configuration
* Establish system/ sub-system baseline archival/ retrieval process
* Establish a system/ sub-system problem reporting and resolution process

# Scope

This document describes the configuration management effort to be completed by <<company>>. The lower-level configuration management effort (e.g. software and complex hardware etc.), should be conducted concurrently with the system/ sub-system level configuration management effort. The lower-level guidance includes the following standards: RTCA DO-178C and RTCA DO-254. Supplier configuration management effort should be reviewed for equivalence to SAE ARP4761 and/ or this plan.

The personnel involved in the configuration management effort and their roles and responsibilities is described by the Development Plan.

The requirements and validation/ verification deliverables at major program milestones is described by the Validation and Verification Plan. Configuration management specific deliverables are described by this plan.

The sequencing of configuration management activities and assignment of resources is described by the Program Plan.

# Configuration Management

The configuration management process (see Figure 3‑1) includes the following components:

* Configuration identification
* Configuration baseline establishment
* Problem reporting
* Change control
* Configuration index establishment
* Archive and retrieval



Figure 3‑1: Configuration Management Process

## Configuration Identification

The purpose of the configuration identification activity is to uniquely identify configuration items so that a configuration baseline can be established. The different types of configuration items are as follows:

* Software part/ version numbers
* Hardware part/ version numbers
* Component e.g. combined software and hardware part/ version numbers
* Requirements data including traceability and rationales
* Validation data i.e. completeness and correctness checks
* Verification data including test plans, procedures and reports with pass/ fail
* Design data e.g. electrical and mechanical data and drawings including assembly drawings
* Component build standard where applicable including all acceptance test procedures necessary

A master configuration index should be created for each Type Certificate (TC), Supplemental Type Certificate (STC) or Technical Standards Order (TSO) product under development. The format of the master configuration index should be a cascading tree.

Part and version numbers for all <<company>> configuration items should be listed by the master configuration index. Standard parts such as active or passive devices that are identified by the Bill of Material (BoM) of a drawing should not be identified by the master configuration index.

## Configuration Baseline Establishment

The purpose of the configuration baseline establishment activity is to maintain control of configuration items.

The different types of baselines are as follows:

Snapshot Performed at any time. The items are not sufficiently mature for an interim or product release.

Incomplete release The baseline does not have all the items necessary for it to be an interim or delivery release. However, the items are sufficiently mature for an interim or product release.

Interim release The baseline has all the items necessary to satisfy the requirements of a major program milestone, but not a product delivery release or some of the items are not sufficiently mature for a product delivery.

Delivery release The baseline has all the items necessary to satisfy the requirements of a product delivery and all of the items are sufficiently mature for a product delivery.

Incomplete, interim and delivery releases are considered established baselines. Testing for certification credit cannot begin until there is an established baseline which has been inspected by the appropriate regulatory authority for software and hardware part conformity. Testing for certification credit includes ground and/ or flight testing and qualification testing e.g. RTCA DO-160G.

Configuration baseline establishment should ensure the following:

* Change control is followed when transitioning from an established baseline to a derivative
* There is traceability between the established baseline and the derivative. If the derivative meets the criteria for an incomplete, interim or delivery release it is considered an established baseline
* Branching of baselines can occur. However, branching should be minimized to prevent unnecessary configuration management effort
* Artefacts required for requirements compliance substantiation are baselined
* Established baselines are subjected to change control
* Established baselines are subjected to archive retrieval processes and procedures
* A change to an established baseline after it has been inspected for software and hardware part conformity will be subject to an impact assessment to determine compatibility and whether repetition of testing is necessary. The change should be coordinated with the appropriate regulatory authority. This includes a change after an STC, TC or TSO.

## Problem Reporting

The purpose of the problem reporting activity is to track issues related to configuration items. Means should be established to track the problem report and it should be dispositioned prior to a delivery release. An impact assessment should be completed before the problem report is dispositioned. The impact assessment should identify other baselines that the problem report effects. Also, it should identify any safety effects.

If a problem report results in a non-compliance to a requirement, it should be associated with the requirement.

If a problem report invokes a change request, it should be associated with the change request. If there are any safety effects a change request is necessary. A problem report can be associated with one or more change requests and a change request can be associated with one or more problem reports.

## Change Control

The purpose of the change control activity is to maintain control of configuration items.

The change control process of configuration items should at a minimum include the following states:

Requested The change has been requested, but not approved

Approved The change has been approved

Implemented The change has been approved and is part of an established baseline

Obsolete The change is abandoned

NOTE: For some configuration items e.g. requirements, validation and verification artifacts, the change implemented state may not be required as tools such as requirements management tools may automatically implement the change when it is approved.

The change is submitted to the systems engineering IPT lead and configuration management lead. The systems engineering IPT lead will decide whether the systems engineering IPT lead and/ or the configuration management lead is selected as the approver(s).

The approver(s) will review the change request and either approve or reject the request. The systems engineering IPT lead will make the final determination of whether a deviation is rejected or approved. The results of each change request will be recorded and archived in the configuration management tool in accordance with this plan. See Figure 3‑2 for change management states.



Figure 3‑2: Change Management States

Change control should ensure the following:

* Changes to the configuration item are appropriately identified by a change to its configuration identification
* Changes to design data, requirements, validation and verification artefacts associated with the configuration item are appropriately identified by a change to its configuration identification
* The integrity of the configuration item changed is maintained as is its relationship with other configuration items

## Configuration Index Establishment

The purpose of the configuration index establishment activity is to identify the items necessary to deliver the product, test or repeat a test of a particular configuration.

The configuration index includes the following items that comprise a system or sub-system:

* All the requirements
* Software configuration items
* Hardware configuration items
* The interconnection of items
* Interfaces with other systems/ sub-systems
	+ Electrical
	+ Mechanical
	+ Data
* Operating guidelines
* Maintenance procedures
* Associated configuration identification
* Any operating limitations
* Capabilities in excess of those required for certification

## Archive and Retrieval

The purpose of the archive and retrieval activity is the archiving and retrieval of configuration items. All baselines and configuration indexes should be archivable and retrievable.

When archiving and retrieving a configuration item the person that created the configuration item and a date stamp should be associated with it.

If a configuration item is changed, the person that requested, approved and implemented the change should be associated with the configuration item and the change itself.

# Data Control Categories

Table 4‑1 shows configuration management to data control category mapping and Table 4‑2 shows data control categories.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Section | Data control category 1 | Data control category 2 |
| Configuration Identification | 3.1 | X | X |
| Configuration Baseline Establishment | 3.2 | X |  |
| Problem Reporting | 3.3 | X |  |
| Change Control | 3.4 | X | X |
| Configuration Index Establishment | 3.5 | X | X |

Table 4‑1: Configuration Management Activity to Data Control Category Mapping

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | 1 | 1 | 1 | 1 | 1 |
| Safety Program Plan | 2 | 2 | 2 | 2 |  |
| Development Plan | 2 | 2 | 2 | 2 |  |
| Validation and Verification Plan | 2 | 2 | 2 | 2 |  |
| ConfigurationManagement Plan | 2 | 2 | 2 | 2 |  |
| ProcessAssurance Plan | 2 | 2 | 2 | 2 |  |
| 1.2 | Transition criteria and interrelationship among processes are defined | Plans inobjective no. 1 | 2 | 2 | 2 | 2 |  |
| 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 | 1 | 1 | 1 | 2 |  |
| 2.2 | Functions are allocated to systems/ sub-systems | Allocation of functions to systems/ sub-systems | 1 | 1 | 1 | 2 |  |
| 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 | 1 | 1 | 1 | 2 |  |
| 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 | 1 | 1 | 1 | 2 |  |
| 2.5 | System architecture is defined | System DesignDescription | 1 | 1 | 1 | 2 |  |
| 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 | 1 | 1 | 1 |  |  |
| Complex hardware HLRs and LLRs | 1 | 1 | 1 |  |  |
| 2.7 | System and sub-system verification is performed | VerificationArtifacts | 2 | 2 | 2 | 2 |  |
| 3.0 Safety Assessment Process |
| 3.1 | Functional hazard analysis is performed | FHA | 1 | 1 | 1 | 1 | 1 |
| 3.2 | The preliminary system safety assessment isperformed | PSSA | 1 | 1 | 1 | 1 |  |
| Top-Down FTA | 1 | 1 | 1 | 1 |  |
| 3.3 | Safety requirements including; independence, probability budget and Functional Development Assurance Levels (FDAL) and Item Development Assurance Levels (IDALs) are defined | Safety requirements | 1 | 1 | 1 | 2 |  |
| 3.4 | The common cause analyses are performed | Particular RiskAnalysis | 1 | 1 | 1 |  |  |
| Common ModeAnalysis | 1 | 1 | 1 |  |  |
| Zonal SafetyAnalysis | 1 | 1 | 1 |  |  |
| 3.5 | The system safety assessment is performed | SSA | 1 | 1 | 1 | 1 |  |
| Bottom-Up FTA | 1 | 1 | 1 | 1 |  |
| 3.6 | Failure Mode Effect Analysis (FMEA), Failure Mode Effects Summary are performed | FMEA/ FMES | 1 | 1 | 1 | 2 |  |
| 3.7 | Reliability Prediction is performed | RP | 1 | 1 | 1 | 2 |  |
| 3.8 | Single Event Effect Analysis is performed | SEE | 1 | 1 | 1 | 2 |  |
| 4.0 Requirements Validation Process |
| 4.1 | System and sub-system requirements are complete and correct | ValidationResults | 2 | 2 | 2 |  |  |
| 4.2 | Assumptions are justified and validated | ValidationResults | 2 | 2 | 2 |  |  |
| 4.3 | Derived requirements are justified and validated | ValidationResults | 2 | 2 | 2 |  |  |
| 4.4 | Requirements are traceable or rationale is defined for derived requirements | ValidationResults | 2 | 2 | 2 |  |  |
| 4.5 | Validation compliance substantiation is provided | ValidationMatrix | 2 | 2 | 2 |  |  |
| Validation Summary | 2 | 2 | 2 |  |  |
| 5.0 Requirements Verification Process |
| 5.1 | Verification procedures are correct | VerificationProcedures | 1 | 1 | 2 | 2 |  |
| 5.2 | Verify unintended functions do not impact to safety | VerificationProcedures | 1 | 1 | 2 | 2 |  |
| VerificationResults | 2 | 2 | 2 | 2 |  |
| 5.3 | Verify performance requirements | VerificationProcedures | 1 | 1 | 2 | 2 |  |
| VerificationResults | 2 | 2 | 2 | 2 |  |
| 5.4 | Verify functional requirements including human factors | VerificationProcedures | 1 | 1 | 2 | 2 |  |
| VerificationResults | 2 | 2 | 2 | 2 |  |
| 5.5 | Verify physical requirements | VerificationProcedures | 1 | 1 | 2 | 2 |  |
| VerificationResults | 2 | 2 | 2 | 2 |  |
| 5.6 | Verify interfaces | VerificationProcedures | 1 | 1 | 2 | 2 |  |
| VerificationResults | 2 | 2 | 2 | 2 |  |
| 5.7 | Verify environmental requirements | QualificationProcedures | 1 | 1 | 2 | 2 |  |
| QualificationResults | 2 | 2 | 2 | 2 |  |
| 5.8 | Verify safety requirements | Verification Results | 2 | 2 | 2 | 2 |  |
| 5.9 | Verification compliance substantiation is provided | VerificationMatrix | 2 | 2 | 2 | 2 |  |
| VerificationSummary | 2 | 2 | 2 | 2 |  |
| 5.10 | Identify Certification Maintenance Requirements (CMRs) and disposition problem reports | CMRs | 2 | 2 | 2 | 2 |  |
| ProblemReports | 2 | 2 | 2 | 2 |  |
| 6.0 Configuration Management Process |
| 6.1 | Configuration items are identified | Configuration Items | 2 | 2 | 2 | 2 |  |
| 6.2 | Incomplete, interim and delivery releases are established | Incomplete Releases | 2 | 2 | 2 | 2 |  |
| Interim Releases | 2 | 2 | 2 | 2 |  |
| Delivery Releases | 2 | 2 | 2 | 2 |  |
| 6.3 | Archive and retrieval are established | Archive and Retrieval Records | 2 | 2 | 2 | 2 |  |
| 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 | 2 | 2 | 2 | 2 |  |
|  | Development activities and processes are conducted in accordance with those plans | Evidence ofProcessAssurance | 2 | 2 | 2 | 2 |  |
| 8.0 Certification and Regulatory Authority Coordination Process |
| 8.1 | Compliance substantiation is provided. | CertificationSummary | 1 | 1 | 1 | 2 |  |
| ConfigurationIndex | 1 | 1 | 2 | 2 |  |

Table 4‑2: Data Control Categories

## Configuration Management Environment

The configuration management environment for baselines should satisfy the following:

* Zero regeneration errors during archival and retrieval
* Will not deteriorate over time
* Accessible for archival and retrieval
* Physically separate databases and/ or duplicate copies to minimize the risk of loss of data in the event of a disaster
* Minimize the risk of loss of data in the event of an attack, unauthorised changes and accidental authorised changes

# Configuration Management Lifecycle

## General

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)

The PDR and CDR are conducted at system and sub-system levels and by the supplier for the equipment provided.

## CoDR Deliverables

The configuration management deliverables for CoDR are the following:

* CoDR interim release/ records
	+ Draft requirements

## SRR Deliverables

The configuration management deliverables for SRR are the following:

* SRR interim release/ records
	+ Requirements
	+ Validation artifacts
	+ Verification artifacts

## PDR Deliverables

The configuration management deliverables for PDR are the following:

* CDR interim release/ records
	+ Requirements
	+ Validation artifacts
	+ Verification artifacts
	+ Critical design data
	+ Problem reports

## CDR Deliverables

The configuration management deliverables for CDR are the following:

* CDR interim release/ records
	+ Requirements
	+ Validation artifacts
	+ Verification artifacts
	+ Critical design data
	+ Problem reports

## FFRR Deliverables

The configuration management deliverables for FFRR are the following:

* FFRR delivery release/ records
	+ Requirements
	+ Validation artifacts
	+ Verification artifacts
	+ Critical design data
	+ Software configuration index
	+ Hardware configuration index
	+ System/ sub-system/ component configuration index
	+ Problem reports

## TC Deliverables

The configuration management deliverables for TC are the following:

* Final delivery release/ records
	+ Requirements
	+ Validation artifacts
	+ Verification artifacts
	+ Critical design data
	+ Software configuration index
	+ Hardware configuration index
	+ System/ sub-system/ component configuration index
	+ Problem reports

# Templates and Checklists

## Change Request Matrix Template

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Identifier | Description | Reason for Change | Impacted Configuration Items/ Requirements | Impact Details |
|  |  |  |  |  |
|  |  |
|  |  |
|  |  |

Table 6‑1: Change Request Template

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Identifier | Description | Corrective action | Impacted Configuration Items/ Requirements | Impact Details |
|  |  |  |  |  |
|  |  |
|  |  |
|  |  |

Table 6‑2: Problem Report Template

## Change Request Checklist

|  |  |
| --- | --- |
| # | Change Request Check |
| 1 | Impact on equipment/ components that have completed qualification testing? |
| 2 | Impact on equipment/ components that have completed ground or flight testing for certification credit? |
| 3 | Impact on software configuration items? |
| 4 | Impact on hardware configuration items? |
| 5 | Impact on delivered products? |

Table 6‑3: Change Request Checklist

|  |  |
| --- | --- |
| # | Problem Report Check |
| 1 | Impact on requirements? |
| 2 | Impact on safety? |
| 3  | Is a root cause analysis necessary? |
| 4 | Is the defect caused by a hardware, software or manufacturing defect? |

Table 6‑4: Problem Report Checklist