Seminário Internacional de VANT - 2010

SI VANT 2010

27 a 29 de outubro de 2010

São José dos Campos - SP

Realização

DCA-BR

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

Apoio

ANAC
Agência Nacional de Aviação Civil - Brasil

CAvEx

NOVOTEL HOTELS

braVoo MONITORAMENTO AÉREO

BRVANT SOLUÇÕES TECNOLÓGICAS

SANTOS LAB

Patrocínio

AEL AEROELETRÔNICA

AGX tecnologia

EMBRAER Defense Systems

eSysTech Embedded Systems Technologies

Gyrofly

KONATUS

PRICE INDUCTION BRASIL

SENTIENT

SOLENTECH

TBX

xmobots

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

Qualificações de Software para VANTs: Visão geral da RTCA DO-178B

Marina Mendonça Natalino Zenun

Motivação

Organização Brasileira
para o Desenvolvimento
da Certificação Aeronáutica

- Uso crescente e Complexidade
- Tecnologia está mudando rapidamente
- Tem sido usado para funções críticas
- **Safety**
- Ariane 5 – European Space Agency (ESA) - 1996

Objetivo:

Apresentar uma Visão geral da RTCA DO-178B

Roteiro

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

1. Introdução
2. Processos da DO-178B
   - Planejamento
   - Desenvolvimento
   - Integração
3. Conclusão
4. Referências

Introdução

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

- Título:
  - "Software considerations in Airborne Systems and Equipment Certification"
- Definição:
  - Conjunto de normas para a produção de software embarcado.
- Desenvolvido:
  - RTCA Special Committee 167 e EUROCAE WG-12.

Introdução

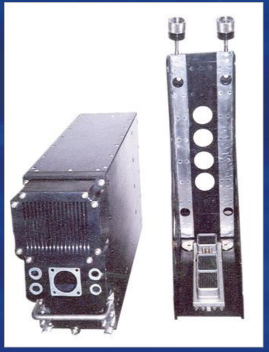
Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

- **Objetivo:**
  - Fornecer à comunidade da aviação um g[illegible]ia para determinar de forma cons[illegible]stente e com [illegible]m nível aceitável de confiança, que [illegible] [illegible]cado cumpre com os requisitos de a[illegible]dade.
- **O que não faz**
  - Não define relação entre req[illegible]necedores.
  - Não define as divisões de [illegible]
  - Não define como fazer.

Como usá-la?

Desenvolvimento Sistemas Complexos

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica



Requisitos Stakeholders (aeronavegabilidade)

↓

Requisitos de Sistema

↓

Requisitos de sub-sistemas

↓

Requisitos de componentes

Software ⇄ Hardware

Importância de bons requisitos

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

Problema

Requisitos de baixo nível

Requisitos corretos	Requisitos errados

Design

Design Correto	Design Errado	Design baseado em especificação errada

Implementação (coding)

Programas Corretos	Programas com erros	Programas baseados em design errado	Programas baseados em especificação errada

Testes

Funções corretas	Erros corrigíveis	Erros incorrigíveis	Erros Escondidos

Programas perfeitos

Programas imperfeitos

Características de bons requisitos

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

- Necessário
- Conciso
- Não ambíguo
- Completo (standalone)
- Consistente
- Livre de implementação
- Factível
- Verificável

Ref.: INCOSE (International Council on Systems Engineering)

Requisitos

- 23.1301

Each item of installed equipment must be:

- Of a kind and design appropriate to its intended function;
- Labeled to its identification, function, or operating limitations;
- Installed according to limitations specified for that equipment; and
- Able to function properly when installed.

Requisitos

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

- 23.1309

- Design ensures it performs intended functions under any foreseeable operating condition;
- Systems and associated components, separately and in relation to other systems, designed so any failure condition that prevents continued flight and landing is extremely improbable;
- Any other failure conditions which reduce the capability of airplane or crew to cope with adverse operating conditions is improbable.

Requisitos

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

- STANAG 4671
  - AMC.1309(b) System Design and Analysis

  (6) Software development assurance levels

  (a) The software integrated in UAV System should perform their intended function with a level of confidence in safety that complies with the requirements set by this paragraph. A software safety program should include identification of the software rigor required for safety criticality elements (e.g., safety integrity level as described in IEC 61805), provide software development assurance evidence of safe software engineering (e.g, RTCA/DO-178B for software and RTCA/DO-254 for firmware)

Requisitos

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

- STANAG 4671 (cont.)
  - AMC.1309(b) System Design and Analysis

(6) Software development assurance levels

(b) The software life cycle assurance process agreed with the Certifying Authority should be demonstrated with the approach defined in RTCA DO- 178B / ED-12B "Software considerations in airborne systems and equipment certification", especially with annex A for the process objectives and outputs by software level. If equivalent standards are provided, a Plan for Software Airworthiness should be provided and agreed with the Certifying Authority in order to present how the quoted standards will be applied.

Software X Safety Assessment

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

- Software não segue as leis da física:
  - Software não quebra;
  - Não falha em modos previsíveis;
  - Quanto mais o software é usado, menos provável será a ocorrência de falhas;
  - Software não é confiável por sua própria natureza. Certamente terá erros.

Software X Safety Assessment

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

- Não se pode usar abordagem de confiabilidade para software.

- Portanto *design assurance* é usado para se adquirir confiança no software.

- A meta do *design assurance* é eliminar quantos erros for possível antes de se carregar o software na aeronave (VANT). A ideia é detectar e corrigir os erros.

- Apenas um sistema simples, onde todas as combinações de entradas podem ser testadas, assegura o cumprimento dos requisitos FAR XX.1301 e 1309 sem a necessidade de se usar DO-178 B ou outro processo de *design assurance.*

- *Assurance levels* são atribuídos no processo de safety assessment.

Assurance levels - aeronave

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

CATEGORY	Meaning	SW Level
Catastrophic	***All failure conditions that prevent continued safe flight and landing***	***A***
Hazardous	***Large reduction in safety margins;*** ***Crew can´t perform tasks;*** ***Adverse impact upon occupants;***	***B***
Major	***Significant reduction in safety;*** ***Increase workload crew is inefficient;*** ***Discomfort to occupants;***	***C***
Minor	***Slight reduction in safety;*** ***Slight increase in crew workload;*** ***Inconvenience to occupants***	***D***
No-Effect	***No effect on the operation of the aircraft***	***E***

Assurance levels - UAV

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

DAL allocation for system and each portion of the system architecture		Degree of redundancy	
		Single failure/errors	Double failure/errors two or more independent/dissimlar portions
Failure Conditions Classification	Catastrophic	DAL B	DAL B for the system and, DAL C for each portion
	Hazardous	DAL C	DAL C for the system and, DAL D for each portion
	Major	DAL D	DAL D for the system and, DAL D for each portion
	Minor	DAL E	DAL E
	No Safety Effect	DAL E	

Ref. STANAG 4671

Objetivos x Assurance levels DO-178B

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

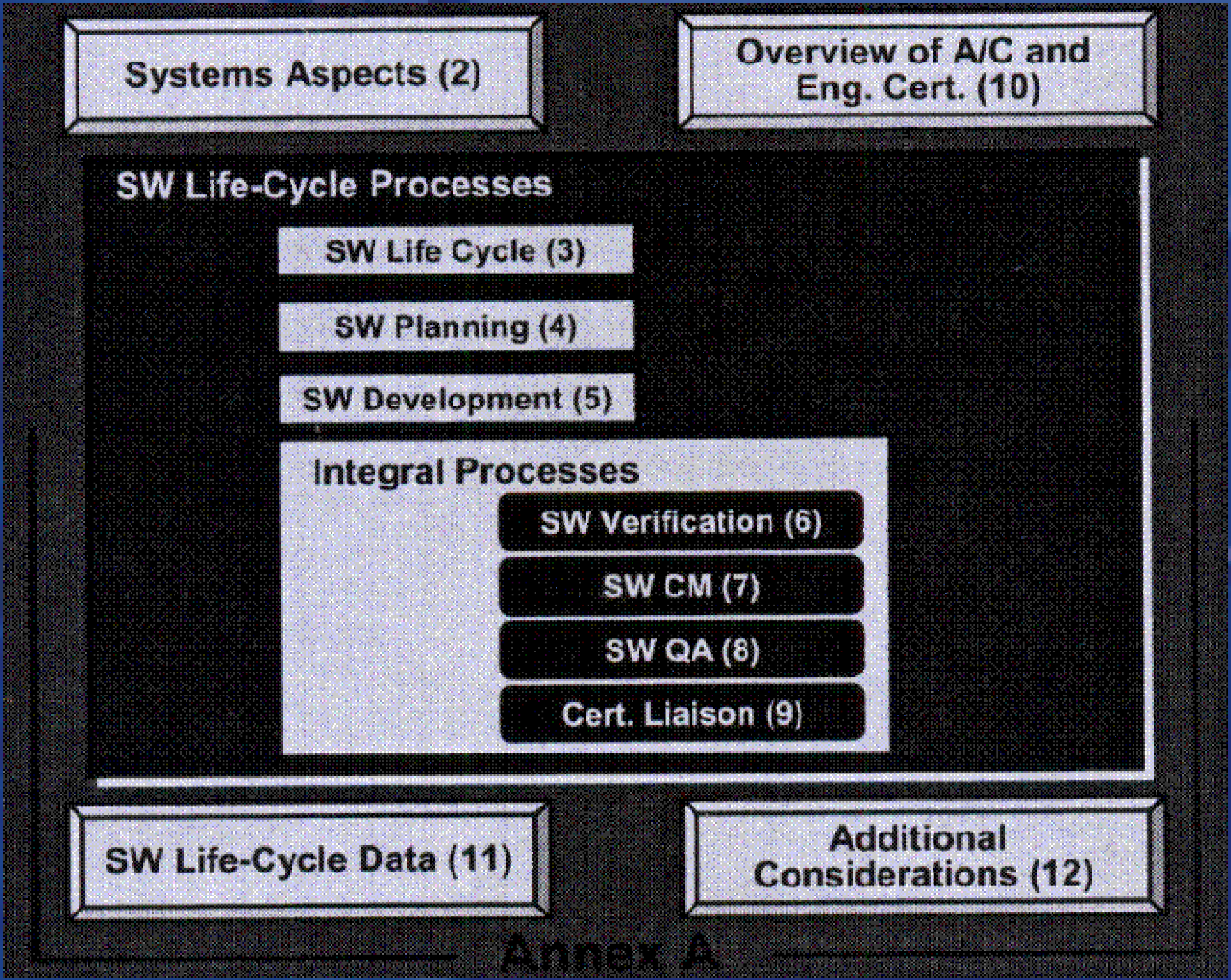
RIGOR

- Level A – 66 objetivos;
- Level B – 65 objetivos;
- Level C – 57 objetivos;
- Level D – 28 objetivos.

Definição dos documentos a serem gerados

Estrutura DO-178B

Organização Brasileira
para o Desenvolvimento
da Certificação Aeronáutica



Anexo A- ex. Tabela A-1

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

Processo Planejamento Software

Independência: Separação de responsabilidades que garantam o cumprimento do objetivo avaliado.

(Outra pessoa)

	Objective Description	Objective Ref.	Applicability by SW Level A	B	C	D	Output Description	Output Ref.	Control Category by SW level A	B	C	D
1	Software development and integral processes activities are defined.	4.1a 4.3	○	○	○	○	Plan for Software Aspects of Certification Software Development Plan Software Verification Plan SCM Plan SQA Plan	11.1 11.2 11.3 11.4 11.5	① ① ① ① ①	① ① ① ① ①	① ② ② ② ②	① ② ② ② ②
2	Transition criteria, inter-relationships and sequencing among processes are defined.	4.1b 4.3	○	○	○							
3	Software life cycle environment is defined.	4.1c	○	○	○							
4	Additional considerations are addressed.	4.1d	○	○	○	○						
5	Software development standards are defined.	4.1e	○	○	○		SW Requirements Standards SW Design Standards SW Code Standards	11.6 11.7 11.8	① ① ①	① ① ①	② ② ②	
6	Software plans comply with this document.	4.1f 4.6	○	○	○		SQA Records Software Verification Results	11.19 11.14	② ②	② ②	② ②	
7	Software plans are coordinated.	4.1g 4.6	○	○	○		SQA Records Software Verification Results	11.19 11.14	② ②	② ②	② ②	

LEGEND:
- ● The objective should be satisfied with independence.
- ○ The objective should be satisfied.
- Blank Satisfaction of objective is at applicant's discretion.
- ① Data satisfies the objectives of Control Category 1 (CC1).
- ② Data satisfies the objectives of Control Category 2 (CC2).

Controle de Configuração

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

- Categorias de controle p/ dados produzidos durante o ciclo de desenv. de software
  - Control Category 1 (CC1) - **Rigoroso**
  - Control Category 2 (CC2) – **Folgado**
- Essas categorias são relacionadas ao controle do gerenciamento da configuração indicados na tabela abaixo:

SCM Process Objective	Reference	CC1	CC2
Configuration Identification	7.2.1	•	•
Baselines	7.2.2a, b, c, d, e	•	
Traceability	7.2.2f, g	•	•
Problem Reporting	7.2.3	•	
Change Control - integrity and identification	7.2.4a, b	•	•
Change Control - tracking	7.2.4c, d, e	•	
Change Review	7.2.5	•	
Configuration Status Accounting	7.2.6	•	
Retrieval	7.2.7a	•	•
Protection against Unauthorized Changes	7.2.5b(1)	•	•
Media Selection, Refreshing, Duplication	7.2.7b(2), (3), (4), c	•	
Release	7.2.7d	•	
Data Retention	7.2.7e	•	•

DO-178B – Anexo A

- Tabela A1 – Software Planning Process
- Tabela A2 – Software Development Process
- Tabela A3 – Verification of Outputs of Requirements Process
- Tabela A4 – Verification of Outputs of Design Process
- Tabela A5 – Verification of Outputs of Coding/ Integration Process
- Tabela A6 – Testing of Outputs of Integration Process
- Tabela A7 – Verification of Verification Process Results
- Tabela A8 – Software Configuration Management Process
- Tabela A9 – Software Quality Assurance Process
- Tabela A10 – Certification Liaison Process

Divisão dos ciclos da DO-178B

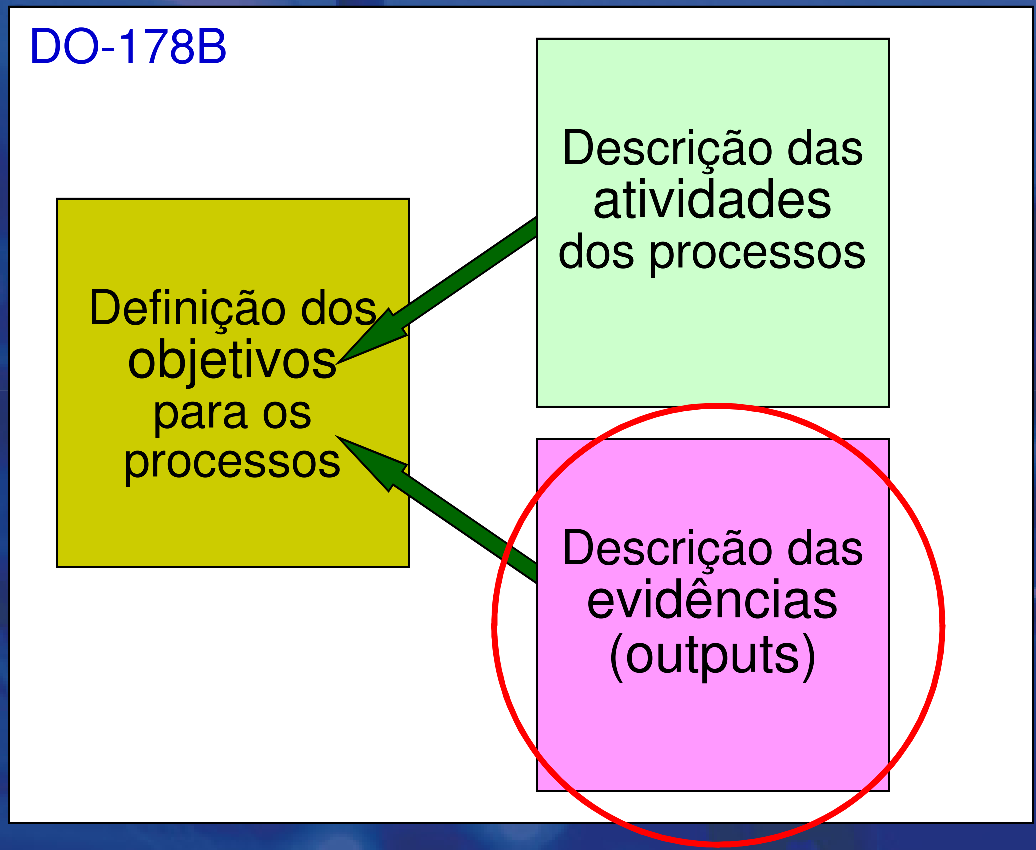
Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

Planejamento	Define e coordena as atividades dos processos de desenvolvimento e integração de software para um projeto.
Desenvolvimento	Produz o produto do software. É dividido em: - Processo de definição de requisitos do software - Processo de projeto do software - Processo de codificação do software - Processo de integração do software.
Integração	Garante correção, controle e confiança nos processos de desenvolvimento do software e nas suas saídas. É dividido em: - Processo de verificação do software - Processo de controle de configuração do software - Processo de garantia da qualidade do software - Processo de interface com a certificação.

DO-178B

Processos da DO-178B

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica



Processo de Planejamento do Software

Planejamento

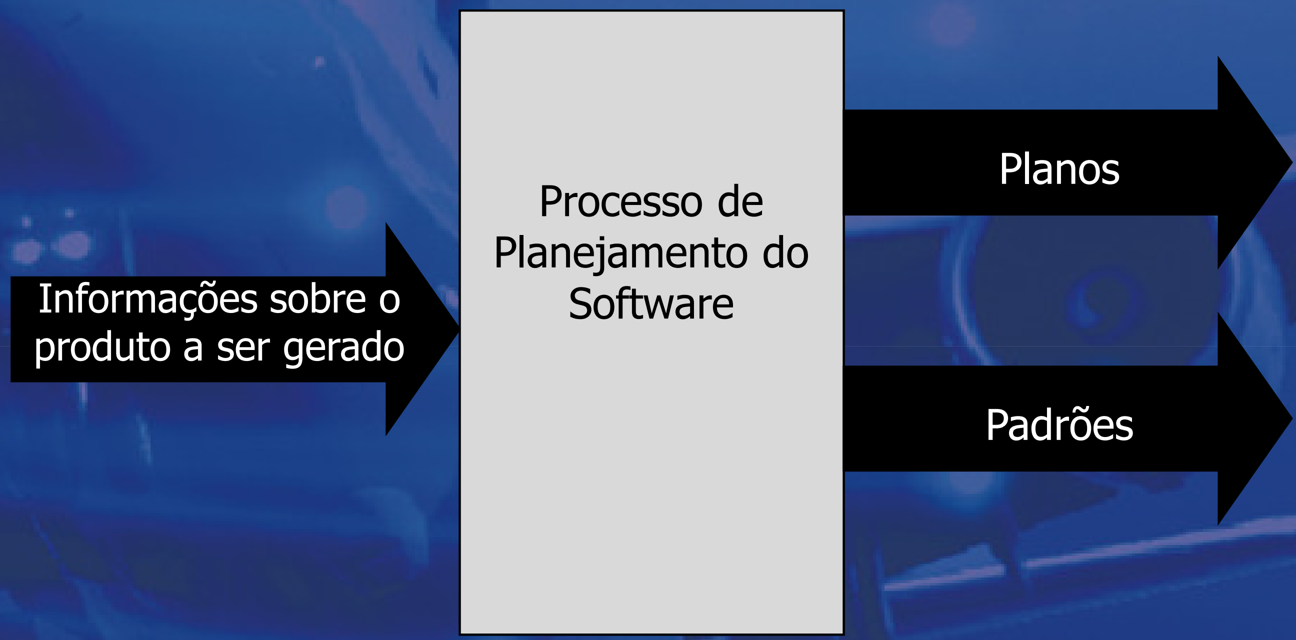
Organização Brasileira
para o Desenvolvimento
da Certificação Aeronáutica

Planejamento	Requisitos	Verificação
	Projeto	Controle de Configuração
	Codificação	Garantia da Qualidade
	Integração	Interface com Autoridade

Planejamento

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

ENTRADA SAÍDAS



Planejamento

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

SAÍDAS

Planos	PSAC - *Plan for Software Aspects of Certification* SDP - *Software Development Plan* SVP - *Software Verification Plan* SCMP - *Software Configuration Management Plan* SQAP - *Software Quality Assurance Plan*
Padrões	SRS - *Software Requirements Standards* SDS - *Software Design Standard* SCS - *Software Code Standard*

Geração dos documentos:
Baseada nos níveis de software

Processo de Desenvolvimento do Software

Desenvolvimento

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

Planejamento	Requisitos	Verificação
	Projeto	Controle de Configuração
	Codificação	Garantia da Qualidade
	Integração	Interface com Autoridade

Desenvolvimento

❑ **Saídas do Processo de Desenvolvimento**

Dados	SRD - *Software Requirements Data*
Descrição	SDD – *Software Design Description*
Código	SC – *Source Code* EOC – *Executable Object Code*

Geração dos documentos:
Baseada nos níveis de software

Desenvolvimento

DCA-BR
Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

- **Tabela A-2**

(Desenv. de software)

	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	High-level requirements are developed.	5.1.1a	○	○	○	○	Software Requirements Data	11.9	①	①	①	①
2	Derived high-level requirements are defined.	5.1.1b	○	○	○	○	Software Requirements Data	11.9	①	①	①	①
3	Software architecture is developed.	5.2.1a	○	○	○	○	Design Description	11.10	①	①	②	②
4	Low-level requirements are developed.	5.2.1a	○	○	○	○	Design Description	11.10	①	①	②	②
5	Derived low-level requirements are defined.	5.2.1b	○	○	○	○	Design Description	11.10	①	①	②	②
6	Source Code is developed.	5.3.1a	○	○	○	○	Source Code	11.11	①	①	①	①
7	Executable Object Code is produced and integrated in the target computer.	5.4.1a	○	○	○	○	Executable Object Code	11.12	①	①	①	①

LEGEND:		
	●	The objective should be satisfied with independence.
	○	The objective should be satisfied.
	Blank	Satisfaction of objective is at applicant's discretion.
	①	Data satisfies the objectives of Control Category 1 (CC1).
	②	Data satisfies the objectives of Control Category 2 (CC2).

Processo de Desenvolvimento

(Definição de Requisitos do Software)

Requisitos

Planejamento	Requisitos	Verificação
	Projeto	Controle de Configuração
	Codificação	Garantia da Qualidade
	Integração	Interface com Autoridade

Requisitos

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

ENTRADAS

- Requisitos do sistema
- Interface de Hardware
- Arquitetura do sistema
- SDP- Software Develop. Plan
- SRS - Software Req. Standards

Processo de Definição de Requisitos do Software

Processo de Projeto do Software

Processo de Codificação do Software

Processo de Integração

Processo de Desenvolvimento

SAÍDA

SRD - Software Requirements Data

(Requisitos de alto nível + derivados):

- Funcionais
- Desempenho
- Interfaces HW e SW
- Segurança

Processo de Desenvolvimento

(Projeto de Software)

Projeto

DCA-BR
Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

Planejamento	Requisitos	Verificação
	Projeto	Controle de Configuração
	Codificação	Garantia da Qualidade
	Integração	Interface com Autoridade

Projeto

DCA-BR
Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

ENTRADAS

SRD - Software Requirements Data

SDP - Software Develop. Plan

SDS - Software Design Standards

Processo de Definição de Requisitos do Software

Processo de Projeto do Software

Processo de Codificação do Software

Processo de Integração

Processo de Desenvolvimento

SAÍDA

SDD – Software Design Description

(Arquitetura do Software e Requisitos de baixo nível)

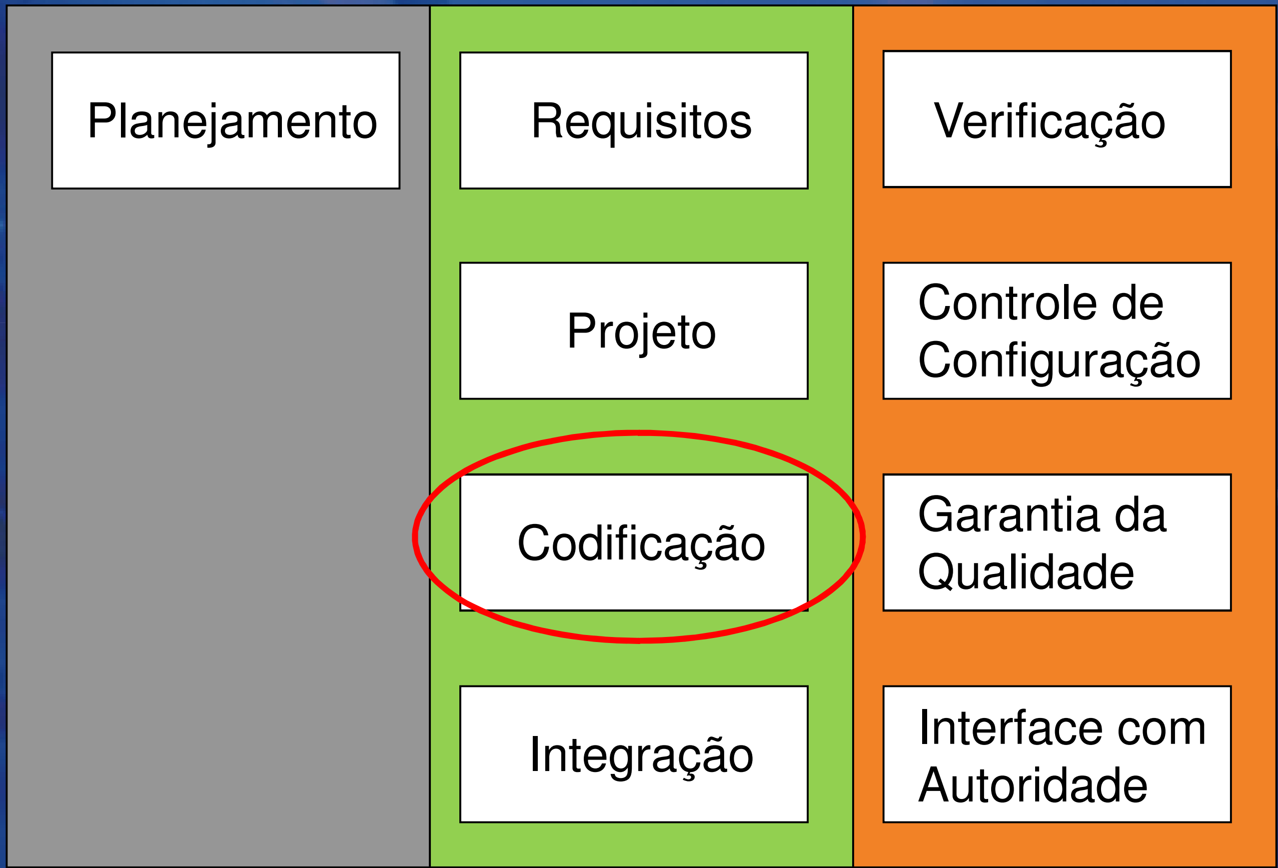
Requisitos de alto nível usados

Processo de Desenvolvimento

(Codificação de Software)

Codificação

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica



Codificação

DCA-BR
Organização Brasileira
para o Desenvolvimento
da Certificação Aeronáutica

ENTRADAS

SDD – Software Design Description

(Arquitetura do Software e Requisitos de baixo nível)

SDP - Software Develop. Plan

SCS - Software Code Standards

Processo de Definição de Requisitos de Software

Processo de Projeto de Software

Processo de Codificação de Software

Processo de Integração

Processo de Desenvolvimento

SAÍDAS

Código Fonte

Código Objeto Executável

Processo de Desenvolvimento

(Integração)

Integração

Planejamento	Requisitos	Verificação
	Projeto	Controle de Configuração
	Codificação	Garantia da Qualidade
	Integração	Interface com Autoridade

Integração

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

Estrutura selecionada para implementar os requisitos

ENTRADAS

Arquitetura do Software

Código Fonte

Código Objeto Executável

SDP - Software Develop. Plan

Computador principal

Processo de Definição de Requisitos de Software

Processo de Projeto de Software

Processo de Codificação de Software

Processo de Integração

Processo de Desenvolvimento

SAÍDA

Código Objeto Executável Final

Processo de Integração

(Processo de Verificação de Software)

"V&V"

Integração

Planejamento	Requisitos	Verificação
	Projeto	Controle de Configuração
	Codificação	Garantia da Qualidade
	Integração	Interface com Autoridade

Verificação

Organização Brasileira
para o Desenvolvimento
da Certificação Aeronáutica

Planejamento	Requisitos	Verificação
	Projeto	Controle de Configuração
	Codificação	Garantia da Qualidade
	Integração	Interface com Autoridade

Verificação

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

- Verificação não é simplesmente teste.
- O processo de verificação de software é uma combinação de:
  - Revisões
  - Análises
  - Desenvolvimento de casos de teste e procedimentos
  - Execução dos procedimentos de teste.

Verificação

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

ENTRADAS

- Requisitos do Sistema
- Requisitos de Software (SRD)
- Arquitetura de Software (SDD)
- Código Fonte
- Código Objeto Executável
- Rastreabildade de dados
- Software Verif. Plan (SVP)

Processo de Verificação de Software

Processo de Revisão e Análise

Saídas dos processos:
- Requisitos
- Projeto
- Codificação
- Integração
- Verificação

Verificação de:
- precisão
- integralidade (perfeição)
- requisitos verificáveis
- Arquitetura do sw
- Código fonte

Processo de Teste do Software

(Desenv. de *test cases* e procedimentos)

Verificação de:
- consistência interna
- perfeição dos requisitos

Execução dos Procedimentos

Demonstração de cumprimento com os requisitos

SAÍDAS

- Software Verification Cases & Procedures
- SVCP
- SVR
- Software Verification Results

Verificação

Organização Brasileira
para o Desenvolvimento
da Certificação Aeronáutica

- Tabela A-3
(Verificação das saídas do processo de definição de requisitos)

.........até

- Tabela A-7
(Verificação dos resultados do processo de verificação)

	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Software high-level requirements comply with system requirements.	6.3.1a	●	●	○	○	Software Verification Results	11.14	②	②	②	②
2	High-level requirements are accurate and consistent.	6.3.1b	●	●	○	○	Software Verification Results	11.14	②	②	②	②
3	High-level requirements are compatible with target computer.	6.3.1c	○	○			Software Verification Results	11.14	②	②		
4	High-level requirements are verifiable.	6.3.1d	○	○	○		Software Verification Results	11.14	②	②	②	
5	High-level requirements conform to standards.	6.3.1e	○	○	○		Software Verification Results	11.14	②	②	②	
6	High-level requirements are traceable to system requirements.	6.3.1f	○	○	○	○	Software Verification Results	11.14	②	②	②	②
7	Algorithms are accurate.	6.3.1g	●	●	○		Software Verification Results	11.14	②	②	②	

LEGEND:		
	●	The objective should be satisfied with independence.
	○	The objective should be satisfied.
	Blank	Satisfaction of objective is at applicant's discretion.
	①	Data satisfies the objectives of Control Category 1 (CC1).
	②	Data satisfies the objectives of Control Category 2 (CC2).

Verificação

DCA-BR
Organização Brasileira para o Desenvolvimento

- **Tabela A-4**

(Verificação das saídas do processo de projeto de software)

	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Low-level requirements comply with high-level requirements.	6.3.2a	●	●	○		Software Verification Results	11.14	②	②	②	
2	Low-level requirements are accurate and consistent.	6.3.2b	●	●	○		Software Verification Results	11.14	②	②	②	
3	Low-level requirements are compatible with target computer.	6.3.2c	○	○			Software Verification Results	11.14	②	②		
4	Low-level requirements are verifiable.	6.3.2d	○	○			Software Verification Results	11.14	②	②		
5	Low-level requirements conform to standards.	6.3.2e	○	○	○		Software Verification Results	11.14	②	②	②	
6	Low-level requirements are traceable to high-level requirements.	6.3.2f	○	○	○		Software Verification Results	11.14	②	②	②	
7	Algorithms are accurate.	6.3.2g	●	●	○		Software Verification Results	11.14	②	②	②	
8	Software architecture is compatible with high-level requirements.	6.3.3a	●	○	○		Software Verification Results	11.14	②	②	②	
9	Software architecture is consistent.	6.3.2b	●	○	○		Software Verification Results	11.14	②	②	②	
10	Software architecture is compatible with target computer.	6.3.3c	○	○			Software Verification Results	11.14	②	②		
11	Software architecture is verifiable.	6.3.3d	○	○			Software Verification Results	11.14	②	②		
12	Software architecture conforms to standards.	6.3.3e	○	○	○		Software Verification Results	11.14	②	②	②	
13	Software partitioning integrity is confirmed.	6.3.3f	●	○	○	○	Software Verification Results	11.14	②	②	②	②

LEGEND:
● The objective should be satisfied with independence.
○ The objective should be satisfied.
Blank Satisfaction of objective is at applicant's discretion.
① Data satisfies the objectives of Control Category 1 (CC1).
② Data satisfies the objectives of Control Category 2 (CC2).

Verificação

Organização Brasileira
para o Desenvolvimento
da Certificação Aeronáutica

- **Tabela A-5**
(Verificação das saídas dos processos de codificação e integração)

	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Source Code complies with low-level requirements.	6.3.4a	●	●	○		Software Verification Results	11.14	②	②	②	
2	Source Code complies with software architecture.	6.3.4b	●	○	○		Software Verification Results	11.14	②	②	②	
3	Source Code is verifiable.	6.3.4c	○	○			Software Verification Results	11.14	②	②		
4	Source Code conforms to standards.	6.3.4d	○	○	○		Software Verification Results	11.14	②	②	②	
5	Source Code is traceable to low-level requirements.	6.3.4e	○	○	○		Software Verification Results	11.14	②	②	②	
6	Source Code is accurate and consistent.	6.3.4f	●	○	○		Software Verification Results	11.14	②	②	②	
7	Output of software integration process is complete and correct.	6.3.5	○	○	○		Software Verification Results	11.14	②	②	②	

LEGEND:
- ● The objective should be satisfied with independence.
- ○ The objective should be satisfied.
- Blank Satisfaction of objective is at applicant's discretion.
- ① Data satisfies the objectives of Control Category 1 (CC1).
- ② Data satisfies the objectives of Control Category 2 (CC2).

Verificação

DCA-BR
Organização Brasileira
para o Desenvolvimento
da Certificação Aeronáutica

- **Tabela A-6 (Teste das saídas do processo de integração)**

	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Executable Object Code complies with high-level requirements.	6.4.2.1 6.4.3	○	○	○	○	Software Verification Cases and Procedures	11.13	①	①	②	②
							Software Verification Results	11.14	②	②	②	②
2	Executable Object Code is robust with high-level requirements.	6.4.2.2 6.4.3	○	○	○	○	Software Verification Cases and Procedures	11.13	①	①	②	②
							Software Verification Results	11.14	②	②	②	②
3	Executable Object Code complies with low-level requirements.	6.4.2.1 6.4.3	●	●	○		Software Verification Cases and Procedures	11.13	①	①	②	
							Software Verification Results	11.14	②	②	②	
4	Executable Object Code is robust with low-level requirements.	6.4.2.2 6.4.3	●	○	○		Software Verification Cases and Procedures	11.13	①	①	②	
							Software Verification Results	11.14	②	②	②	
5	Executable Object Code is compatible with target computer.	6.4.3a	○	○	○	○	Software Verification Cases and Procedures	11.13	①	①	②	②
							Software Verification Results	11.14	②	②	②	②

LEGEND:

●	The objective should be satisfied with independence.
○	The objective should be satisfied.
Blank	Satisfaction of objective is at applicant's discretion.
①	Data satisfies the objectives of Control Category 1 (CC1).
②	Data satisfies the objectives of Control Category 2 (CC2).

Verificação

Organização Brasileira
para o Desenvolvimento
da Certificação Aeronáutica

- **Tabela A-7**

(Verificação dos resultados do processo de verificação)

	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Test procedures are correct.	6.3.6b	●	○	○		Software Verification Cases and Procedures	11.13	②	②	②	
2	Test results are correct and discrepancies explained.	6.3.6c	●	○	○		Software Verification Results	11.14	②	②	②	
3	Test coverage of high-level requirements is achieved.	6.4.4.1	●	○	○	○	Software Verification Results	11.14	②	②	②	②
4	Test coverage of low-level requirements is achieved.	6.4.4.1	●	○	○		Software Verification Results	11.14	②	②	②	
5	Test coverage of software structure (modified condition/decision) is achieved.	6.4.4.2	●				Software Verification Results	11.14	②			
6	Test coverage of software structure (decision coverage) is achieved.	6.4.4.2a 6.4.4.2b	●	●			Software Verification Results	11.14	②	②		
7	Test coverage of software structure (statement coverage) is achieved.	6.4.4.2a 6.4.4.2b	●	●	○		Software Verification Results	11.14	②	②	②	
8	Test coverage of software structure (data coupling and control coupling) is achieved.	6.4.4.2c	●	●	○		Software Verification Results	11.14	②	②	②	

LEGEND:
- ● The objective should be satisfied with independence.
- ○ The objective should be satisfied.
- Blank Satisfaction of objective is at applicant's discretion.
- ① Data satisfies the objectives of Control Category 1 (CC1).
- ② Data satisfies the objectives of Control Category 2 (CC2).

Processo de Integração

(Processo de Controle de Configuração de Software)

Controle de Configuração

Organização Brasileira
para o Desenvolvimento
da Certificação Aeronáutica

Planejamento	Requisitos	Verificação
	Projeto	Controle de Configuração
	Codificação	Garantia da Qualidade
	Integração	Interface com Autoridade

Controle de Configuração

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

- **Categorias de controle p/ dados produzidos durante o ciclo de desenv. de sw**
  - *Control Category 1* (CC1) - Rigoroso
  - *Control Category 2* (CC2) - Folgado

- Essas categorias são relacionadas ao controle do gerenciamento da configuração indicados na tabela abaixo:

SCM Process Objective	Reference	CC1	CC2
Configuration Identification	7.2.1	•	•
Baselines	7.2.2a, b, c, d, e	•	
Traceability	7.2.2f, g	•	•
Problem Reporting	7.2.3	•	
Change Control - integrity and identification	7.2.4a, b	•	•
Change Control - tracking	7.2.4c, d, e	•	
Change Review	7.2.5	•	
Configuration Status Accounting	7.2.6	•	
Retrieval	7.2.7a	•	•
Protection against Unauthorized Changes	7.2.5b(1)	•	•
Media Selection, Refreshing, Duplication	7.2.7b(2), (3), (4), c	•	
Release	7.2.7d	•	
Data Retention	7.2.7e	•	•

Controle de Configuração

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

ENTRADA

SAÍDAS

Software Configuration Management Plan

SCMP

Processo de Controle de Configuração

SCMR

Software Configuration Management Records

SCI – Software Config. Index

PR – Problem Report

SECI

Software life Cycle Environment Config. Index

Controle de Configuração

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

- **Tabela A-8**

(Processo de controle de configuração de software)

	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Configuration items are identified.	7.2.1	○	○	○	○	SCM Records	11.18	②	②	②	②
2	Baselines and traceability are established.	7.2.2	○	○	○	○	Software Configuration Index	11.16	①	①	①	①
							SCM Records	11.18	②	②	②	②
3	Problem reporting, change control, change review, and configuration status accounting are established.	7.2.3 7.2.4 7.2.5 7.2.6	○	○	○	○	Problem Reports	11.17	②	②	②	②
							SCM Records	11.18	②	②	②	②
4	Archive, retrieval, and release are established.	7.2.7	○	○	○	○	SCM Records	11.18	②	②	②	②
5	Software load control is established.	7.2.8	○	○	○	○	SCM Records	11.18	②	②	②	②
6	Software life cycle environment control is established.	7.2.9	○	○	○	○	Software Life Cycle Environment Configuration Index	11.15	①	①	①	②
							SCM Records	11.18	②	②	②	②

LEGEND:		
	●	The objective should be satisfied with independence.
	○	The objective should be satisfied.
	Blank	Satisfaction of objective is at applicant's discretion.
	①	Data satisfies the objectives of Control Category 1 (CC1).
	②	Data satisfies the objectives of Control Category 2 (CC2).

Processo de Integração

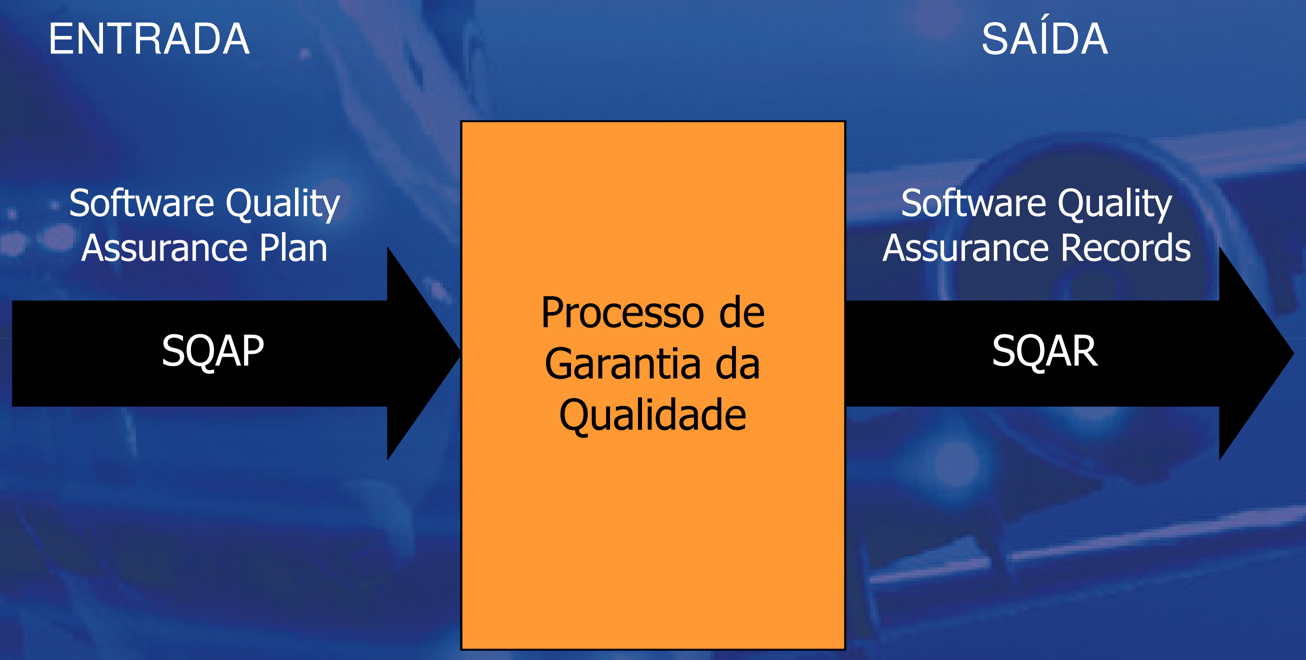
(Processo de Garantia da Qualidade de Software)

Garantia da Qualidade

Organização Brasileira
para o Desenvolvimento
da Certificação Aeronáutica

Planejamento	Requisitos	Verificação
	Projeto	Controle de Configuração
	Codificação	Garantia da Qualidade
	Integração	Interface com Autoridade

Garantia da Qualidade



Garantia da Qualidade

Organização Brasileira
para o Desenvolvimento
da Certificação Aeronáutica

- **Tabela A-9**

(Processo de garantia da qualidade de software)

	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Assurance is obtained that software development and integral processes comply with approved software plans and standards.	8.1a	●	●	●	●	Software Quality Assurance (SQA) Records	11.19	②	②	②	②
2	Assurance is obtained that transition criteria for the software life cycle processes are satisfied.	8.1b	●	●			SQA Records	11.19	②	②		
3	Software conformity review is conducted.	8.1c 8.3	●	●	●	●	SQA Records	11.19	②	②	②	②

LEGEND:		
	●	The objective should be satisfied with independence.
	○	The objective should be satisfied.
	Blank	Satisfaction of objective is at applicant's discretion.
	①	Data satisfies the objectives of Control Category 1 (CC1).
	②	Data satisfies the objectives of Control Category 2 (CC2).

Organização Brasileira
para o Desenvolvimento
da Certificação Aeronáutica

Processo de Integração

(Interface com a Autoridade)

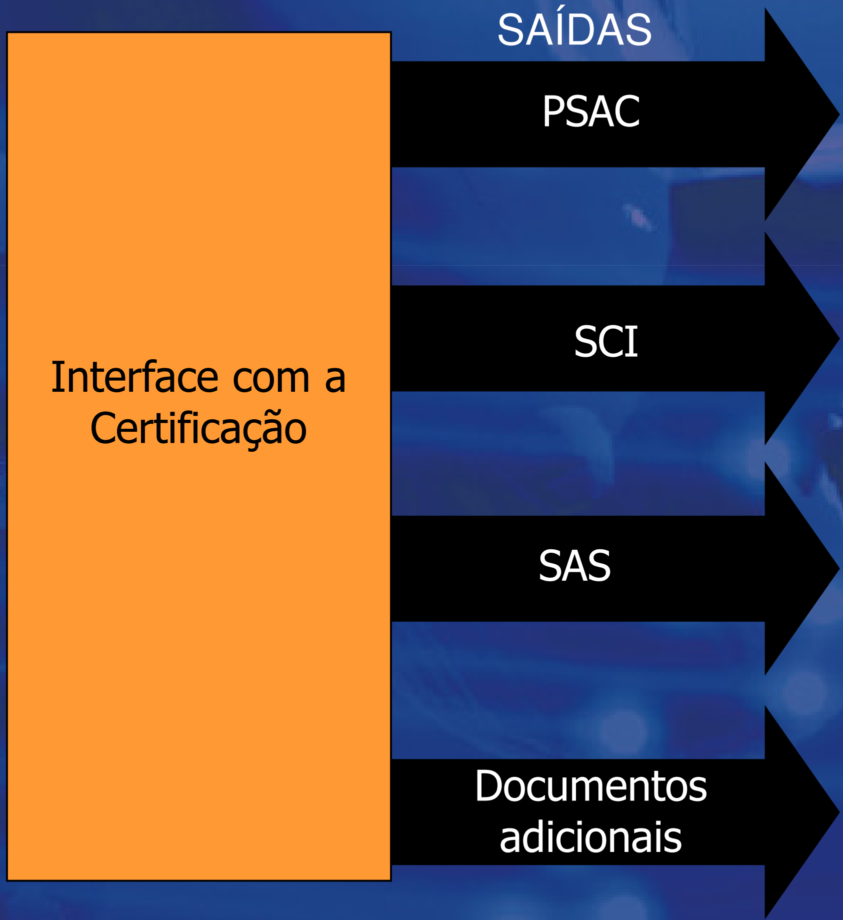
Interface com a Autoridade

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

Planejamento	Requisitos	Verificação
	Projeto	Controle de Configuração
	Codificação	Garantia da Qualidade
	Integração	Interface com Autoridade

Interface com a Autoridade

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica



- Documentação mínima submetida à autoridade de certificação
  - PSAC: Plan for Software Aspects of Certification
  - SCI: Software Configuration Index
  - SAS: Software Accomplishment Summary

Interface com a Autoridade

DCA-BR
Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

- **Tabela A-10**

(Processo de interface com a Autoridade)

	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Communication and understanding between the applicant and the certification authority is established.	9.0	○	○	○	○	Plan for Software Aspects of Certification	11.1	①	①	①	①
2	The means of compliance is proposed and agreement with the Plan for Software Aspects of Certification is obtained.	9.1	○	○	○	○	Plan for Software Aspects of Certification	11.1	①	①	①	①
3	Compliance substantiation is provided.	9.2	○	○	○	○	Software Accomplishment Summary	11.20	①	①	①	①
							Software Configuration Index	11.16	①	①	①	①

LEGEND:

●	The objective should be satisfied with independence.
○	The objective should be satisfied.
Blank	Satisfaction of objective is at applicant's discretion.
①	Data satisfies the objectives of Control Category 1 (CC1).
②	Data satisfies the objectives of Control Category 2 (CC2).

Conclusão

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

Planejamento	Requisitos	Verificação
	Projeto	Controle de Configuração
	Codificação	Garantia da Qualidade
	Integração	Interface com Autoridade


Objetivo:
Apresentar uma
Visão geral da RTCA DO-178B

Referências

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

- RTCA DO-178B: "Software Considerations in Airborne Systems and Equipment Certification"
- Livro: Avionics Certification: A complete guide to DO-178 (software) and DO-254 (hardware)
- STANAG 4671: Standardization Agreement – Subject: Unmanned Aerial Vehicles Systems Airworthiness Requirements (USAR)
- SAE ARP 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

Obrigada!

“Certamente, o futuro
está na navegação aérea
e o desafio do presente é
trabalhar para o futuro.”
Victor Hugo, 1869