Understanding the Software Configuration Management Plan (SCMP) in DO-178C

1. Introduction

In the realm of airborne systems, software reliability and safety are paramount. The **DO-178C** standard provides guidelines to ensure that software developed for airborne systems meets stringent safety and reliability requirements. A critical component of this standard is the **Software Configuration Management Plan (SCMP)**, which outlines the processes and procedures for managing software configurations throughout the development lifecycle.

The SCMP ensures that all software artifacts are systematically controlled, changes are tracked, and the integrity of the software is maintained. This article provides an in-depth exploration of the SCMP, its significance in the DO-178C framework, and best practices for its implementation.

2. The Role of Configuration Management in DO-178C

Configuration Management (CM) is an integral process in DO-178C, ensuring that software products are consistently defined and maintained throughout their lifecycle. The SCMP serves as the blueprint for implementing CM activities, detailing how software items are identified, controlled, and audited.

Key objectives of CM in DO-178C include:

- **Configuration Identification**: Defining and labeling software items to be controlled.
- **Change Control**: Managing changes to software items in a controlled manner.
- **Configuration Status Accounting**: Recording and reporting the status of software items.
- **Configuration Audits**: Verifying that software items conform to their requirements and are correctly documented.

By adhering to these objectives, the SCMP ensures that software changes are systematically managed, reducing the risk of errors and enhancing traceability.

3. Structure of the SCMP

A well-structured SCMP typically includes the following sections:

3.1. Introduction

- **Purpose**: Outlines the objectives of the SCMP.
- **Scope**: Defines the boundaries of the configuration management activities.
- **References**: Lists related documents and standards.

3.2. Configuration Management Organization

- **Roles and Responsibilities**: Details the personnel involved in CM activities and their responsibilities.
- **Organizational Structure**: Describes the hierarchy and reporting relationships.

3.3. Configuration Identification

- **Configuration Items (CIs)**: Identifies the software items to be controlled.
- **Naming Conventions**: Specifies the naming standards for CIs.
- **Versioning**: Details the version control mechanisms.

3.4. Change Control

- **Change Request Process**: Describes how changes are proposed, evaluated, and approved.
- **Impact Analysis**: Outlines the process for assessing the effects of proposed changes.
- **Change Implementation**: Details how approved changes are implemented and documented.

3.5. Configuration Status Accounting

- **Status Reporting**: Specifies how the status of CIs is tracked and reported.
- **Metrics**: Defines the metrics used to assess CM activities.

3.6. Configuration Audits

- **Audit Types**: Describes the types of audits (e.g., functional, physical) conducted.
- **Audit Procedures**: Details the steps involved in conducting audits.
- **Audit Reporting**: Specifies how audit findings are documented and addressed.

3.7. Tools and Resources

- **CM Tools**: Lists the tools used for configuration management activities.
- **Training**: Outlines the training requirements for personnel involved in CM.

4. Configuration Management Processes

4.1. Configuration Identification

This process involves identifying and defining all software items that need to be controlled. It includes:

- Assigning unique identifiers to each CI.
- Establishing baselines for different stages of development.
- Documenting the relationships between CIs.

4.2. Change Control

Change control ensures that all changes to CIs are systematically managed. The process includes:

- Submitting change requests with detailed descriptions.
- Evaluating the impact of proposed changes.
- Approving or rejecting changes based on evaluations.
- Implementing approved changes and updating documentation.

4.3. Configuration Status Accounting

This process involves tracking the status of CIs throughout the development lifecycle. It includes:

- Maintaining records of the current status of each CI.
- Generating reports on the status and history of CIs.
- Providing stakeholders with up-to-date information on CM activities.

4.4. Configuration Audits

Configuration audits verify that CIs conform to their requirements and are correctly documented. The process includes:

- Planning and scheduling audits.
- Conducting audits to assess compliance.
- Documenting audit findings and corrective actions.

5. Integration with Other DO-178C Plans

The SCMP is closely linked with other DO-178C plans, including:

- **Software Development Plan (SDP)**: Outlines the overall software development process.
- **Software Verification Plan (SVP)**: Details the verification activities to ensure software correctness.
- **Software Quality Assurance Plan (SQAP)**: Describes the quality assurance activities to ensure compliance with standards.

Integration ensures consistency across all aspects of software development and facilitates effective communication among teams.

6. Best Practices for Implementing the SCMP

Implementing an effective SCMP involves adhering to best practices, such as:

- **Early Planning**: Develop the SCMP early in the project to guide CM activities from the outset.

- **Stakeholder Involvement**: Engage all relevant stakeholders in the development and review of the SCMP.
- **Tool Selection**: Choose appropriate CM tools that support the project's needs and integrate with other systems.
- **Training**: Provide comprehensive training to personnel involved in CM activities.
- **Continuous Improvement**: Regularly review and update the SCMP to incorporate lessons learned and process improvements.

7. Challenges and Solutions

Implementing the SCMP can present challenges, including:

- **Complexity of Managing Multiple CIs**: Utilize automated tools to manage and track CIs efficiently.
- **Resistance to Change**: Foster a culture that values CM and emphasizes its importance to project success.
- **Ensuring Compliance**: Conduct regular audits and reviews to ensure adherence to the SCMP.

By proactively addressing these challenges, organizations can enhance the effectiveness of their CM processes.

8. Conclusion

The Software Configuration Management Plan (SCMP) is a vital component of the DO-178C standard, ensuring that software configurations are systematically managed throughout the development lifecycle. By defining clear processes for configuration identification, change control, status accounting, and audits, the SCMP helps maintain software integrity, facilitates traceability, and supports compliance with certification requirements.

Implementing an effective SCMP requires careful planning, stakeholder engagement, appropriate tool selection, and a commitment to continuous improvement. By adhering to best practices and proactively addressing challenges, organizations can enhance the quality and reliability of their airborne software systems.

DO-178C Software Configuration Management Plan (SCMP) Checklist

1. General Information

- SCMP title, document ID, version number, and date
- Project/system name and software context
- Applicable Design Assurance Level (DAL)

- Scope and objectives of configuration management clearly defined
- References to DO-178C and related plans (SDP, SVP, SQAP)

2. Configuration Management Organization

- Configuration management roles and responsibilities identified
- Reporting structure and CM authority defined
- Interfaces with development, verification, and QA teams described

3. Configuration Identification

- List of Configuration Items (CIs), including:
    - Requirements documents
    - Design and architecture artifacts
    - Source code files
    - Test cases and procedures
    - Executables and binaries
- Unique identifiers or naming conventions defined
- Versioning strategy specified
- Baseline definitions (development, integration, release) provided

4. Change Control

- Change Request (CR) process described
- Change proposal submission, review, and approval steps outlined
- Change impact analysis procedure defined
- Change implementation and verification steps included
- Links to regression testing and verification updates provided

5. Configuration Status Accounting

- Method for tracking status of each CI throughout its lifecycle
- Records of change history, versions, and approval dates maintained
- Reporting procedures and status report frequency specified

- Metrics defined (e.g., number of change requests open/closed)

6. Configuration Audits

- Functional Configuration Audit (FCA) process defined
- Physical Configuration Audit (PCA) process defined
- Audit scheduling and frequency outlined
- Criteria for audit success/failure and corrective actions described
- Audit report creation and approval procedures included

7. Tools and Resources

- List of configuration management tools (e.g., Git, SVN, PTC, ClearCase)
- Description of how each tool supports CM tasks
- Access control and user permission strategy defined
- Tool configuration and backup procedures documented

8. Access Control and Security

- Procedures for granting, modifying, and revoking access to CIs
- Role-based permissions described (e.g., read, write, approve)
- Security controls for protecting configuration repositories included

9. Integration with Other Plans

- Interfaces with:
    - Software Development Plan (SDP)
    - Software Verification Plan (SVP)
    - Software Quality Assurance Plan (SQAP)
- Roles shared or divided among teams clarified

10. Milestones and Reviews

- CM milestones defined (e.g., initial baseline, code freeze, release)
- CM review and approval gates documented
- Criteria for baseline release and CI acceptance specified

11. Training and Personnel Qualifications

- Required skills and knowledge for CM team members identified
- CM training program described
- Tool usage training and documentation provided

12. Maintenance and Updates to the SCMP

- SCMP document version control in place
- Procedures for periodic review and updates defined
- Authority for modifying the SCMP identified

13. Certification Readiness

- SCMP aligns with DO-178C objectives (primarily Table A-8)
- SCMP content consistent with PSAC and other plans
- Configuration records and audit trails are available for DER/FAA/EASA review
- Traceability maintained between configuration changes and impacted lifecycle data