Software Configuration Management Plan for Anti-lock braking system in Automobiles

Engineering Safety Critical Systems

ISO-26262 (Fitash-ul-Haq, Mohammad Abbas, Ahsan Shabbir, Ali Raza)

Table of Contents

(This page is left blank intentionally)

Software Configuration Management Plan for Anti-lock braking system in Automobiles

1. Overview

1.1 Scope

The following plan complies with the instruction set provided in ISO-26262 standard. It is part of a series of four plans our team documented to make the system design more flexible and understandable with each plan satisfying a specific requirement. This document is the software configuration management plan for ABS system in cars. The SCMP handles any change being made during and after development of ABS systems whilst any change shall pass through all other plans. Other plans are also attached along.

2. References

This standard shall be used in conjunction with the following publications:

IEEE Std 1042-1987 (Reaff 1993), IEEE Guide to Software Configuration Management.

ISO 26262: https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-1:v1:en

3. Definitions and acronyms

3.1 Definitions

The definitions below describe specific terms as used within the context of this standard.

3.1.1 Control point (project control point): A project agreed on point in time or times when specified agreements or controls are applied to the software configuration items being developed, e.g., an approved baseline or release of a specified document/code.

3.1.2 Release: The formal notification and distribution of an approved version.

3.2 Acronyms

The following acronyms appear within the text of this standard:

CCB configuration control board
CI configuration item
SCM software configuration management
ABS Anti-lock Braking System
FTA Fault Tree Analysis
PHA Preliminary Hazard Analysis
PHL Preliminary Hazard List
SSAP System Safety Assessment Planning
SHA System Hazard Analysis
ECU Electronic Control Unit
CAN Controlled Area Network
SSHA Subsystem Safety Hazard Analysis

4. The Software Configuration Management Plan

The classes that will be covered in this plan are stated in Table 1.

Table 1—SCM classes of information

Class of information	Description	IEEE Std 828-1998 reference
Introduction	Describes the Plan's purpose, scope of application, key terms, and references	4.1
SCM management	(Who?) Identifies the responsibilities and authorities for accomplishing the planned activities	4.2
SCM activities	(What?) Identifies all activities to be performed in applying to the project	4.3
SCM schedules	(When?) Identifies the required coordination of SCM activities with the other activities in the project	4.4
SCM resources	(How?) Identifies tools and physical and human resources required for execution of the Plan	4.5
SCM plan maintenance	Identifies how the Plan will be kept current while in effect	4.6

4.1 Introduction

Software configuration management plan determines the changes that can be made during and after development of a system. It keeps track of changes and deals with what and how of evolution. The objectives of our project are stated in Table 1. Any requirement change that isn't related to these requirements will be called out of scope and will be excluded from project.

Table 1 Requirements

System should run diagnostic test for ABS failure on ignition
System should notify driver and display signal light for ABS failure
System should prevent from sudden wheel lock on applying breaks
System should shift to normal breaks if ABS fails
System should reduce acceleration gradually upon applying breaks
System should disable ABS if speed is below 20 km/h and vice versa

4.1.1 Work breakdown

Our project is broken down into a number of phases stated in table 2.

Table 2 work breakdown

Planning
Requirement Engineering
Designing
Development
Analyzing static code
Testing

Where our planning phase have been divided into three categories including Functional Safety assessment plan, Safety plan and Verification and Validation Plan (V&V). See documents attached with same names. The milestones to be achieved are also shown in Table 3 below.

Table 3 Milestones

Milestones	**Estimated Completion Timeframe**
Analyzing COT for ABS-system	3 days
Project Planning	1 Week
Requirement Engineering	5 days

Milestones	Estimated Completion Timeframe
Designing	4 days
Analyzing	2 weeks
Testing	4 weeks
Deployment	6 weeks

4.2 SCM management

The software configuration management consists of following sections.

4.2.1 Organization

The organization deals with safety assessment of Anti-lock braking systems for automotive systems. All the actors along with their responsibilities have been stated in section 4.2.2.

4.2.2 SCM responsibilities

Role	Description
Project Sponsor	Provides executive team approval and sponsorship for the project. Has budget ownership for the project and is the major stakeholder and recipient for the project deliverables.
Project Director	Provides overall management to the project. Accountable for establishing a Project Charter, developing and managing the work plan, securing appropriate resources and delegating the work and insuring successful completion of the project. All project team members report to the project manager. Handles all project administrative duties, interfaces to project sponsors and owners and has overall accountability for the project.
Steering Committee	Provide assistance in resolving issues that arise beyond the project manager's jurisdiction. Monitor project progress and provide necessary tools and support when milestones are in jeopardy.
Stakeholder	Key provider of requirements and recipient of project deliverable and associated benefits. Deliverable will directly enhance the stakeholders' business processes and environment. Majority of stakeholders for this project will be agency leads, CIO's, and project management representatives.
Team Member	Working project team member, who analyzes, designs, develops, tests and improve the project.

OEM	The OEM is responsible for providing systems that's under test. This is beyond the scope of our class project but it is included in stakeholders.

4.2.3 Applicable policies, directives, and procedures

The policies, directives and procedures for the SCM plan are according to ISO 26262. All the constraints that are applied are taken from the standard as well.

4.3 SCM activities

4.3.1 Configuration identification

The Anti-lock braking system consists of following software modules

- ECU
- Translator from electric pulses to digital signals
- Ignition timing
- Staged injection
- Speed limit analyzer
- Brake-fuel analyzer
- Safety check
- Pulse rate of paddle's pressure checker

The safety assessment of above modules have been discussed in Verification and Validation plan.

4.3.1.1 Identifying configuration items

The CI's that are to be delivered have been stated in the section above. The baseline that is considered while development are schedule, cost and scope baselines. These baseline are affected by each change in software after deployment and while development of the system too. Any development of change is system is managed under ISO 26262 to keep the system under scope and base line maintained. These baseline documents along with system have to be approved by Validation and Verification plan (see attached documents).

4.3.1.2 Naming configuration items

This modules specifies how versioning of system is controlled. We have allocated all of the CI's in DOORS. DOORS is a requirement management tool that keeps track of all versions and requirements. It makes traceability possible for complex systems.

4.3.1.3 Acquiring configuration items

All the CI's are distributed among different computers to protect data against any disaster and to share it with other stakeholders. While requirements can be handled, protected and acquired through DOORS. DOORS database enables shared user administration that allows sharing of data among stakeholders too.

4.3.2 Configuration control

The configuration control have following phases,

- Identification and documentation of the need for a change
- Analysis and evaluation of a change request
- Approval or disapproval of a request
- Verification, implementation, and release of a change

All of these phases are approved by Functional Safety Assessment plan and Validation and Verification plan and then are developed by the development team.

4.3.2.1 Requesting changes

The change is requested through a template consisting of following elements

- Name of the component being changed
- Date of request
- Presumed impact of change
- Need for change
- Urgency for change

The request is also documented in DOORS.

4.3.2.2 Evaluating changes

The request for change forwarded to Validation and Verification plan and is analyzed to see what impact it has on system.

4.3.2.3 Approving or disapproving changes

If the change is approved, it is added to the DOORS, from where it awaits for the development phase. It is rejected if vice versa.

4.3.3 Configuration audits and reviews

See Validation and Verification plan for audits and reviews.

4.3.4 Subcontractor/vendor control

Anti-lock braking systems isn't manufactured by a single vendor, it consists of COTs. These COTs are verified by Validation and Verification plan and are then proceeded to next iteration. The COTs are carefully examined because they can cause problems while integrating to system.

4.4 SCM schedules

The prime purpose of this plan is to regulate configuration management. Any milestone to be achieved should be tagged with deadline and all the dependencies shall be noted down in DOORs.

4.5 SCM resources

Any Configuration to be made shall be made acquaintance with specific tools and techniques viable for the solution. Our used tools are show in Table 4.

Table 4 Tools

• MATLAB/Simulink • DOORS

4.6 SCM plan maintenance

It consists of how's and what's. Appropriate actors are assigned to cater the change. Validation and Verification plan can be consulted to see what is the change and how can it be catered.

5. Tailoring of the plan

Our Software Configuration Management plan follows ISO 26262 for automotive systems. Our goal was to do Software configuration management of Anti-lock braking system. We divided it into sections (explained above) that provides flexible management of any change that occurs during or after production. We have explained how, what, when and where of SCM in ABS. Roles have been assigned appropriate responsibilities and process is simplified by following a structure that ensures everything is according to what was expected.

5.1 Downward tailoring

We have to omit some sections intentionally that were related to deployment. As our scope is limited yet, we can't state those sections. However designing is complete, we can add rest of the sections as well.

6. Conformance to the standard

Our Software Configuration management plan follows ISO-26262 to conform that our work product is legal and applicable on specific automotive systems.