

RSA-MIL-STD-79

REQUIREMENTS FOR DEVELOPMENT AND MAINTENANCE OF SAFETY RELATED SOFTWARE IN DEFENCE EQUIPMENT AND SYSTEMS

SCOPE

1. Purpose

The purpose of this document is to specify the requirements for the development and maintenance of all safety related software in defence equipment and systems in South Africa. It will also ensure that the software performs its intended function with a level of confidence in safety that complies with the technical integrity required of such a system.

Technical integrity levels of a system needs to be determined from:

1. Flight Safety requirements
2. Vulnerability requirements
3. Availability requirements
4. Mission Criticality requirements

On a system level, the criticality level required of the software then needs to be determined from these parameters (see note 6). This standard assumes that the system level criticality has already been determined and does not address the issue of determining the level of the software.

2. Applicability

This standard refers to a number of procedures, techniques, practices and tools which when followed or used correctly will reduce but not necessarily eliminate the probability that the software will contain errors. This standard refers only to technical suitability and in no way absolves either the designer, the producer, the supplier or the user from statutory and all other legal obligations relating to health and safety at any stage.

This document describes the requirements for the procedures and technical practices for the development of safety related software in defence equipment and systems by referring to all the guidelines for the software life cycle process objectives and outputs as described in RTCA/DO-178B. It furthermore also refers to specific clauses from Def Stan 00-55.

3. Introduction

This standard specifies the requirements for all safety related software in defence equipment and systems: It relates only to software and does not deal with safety of the whole system. Evidence of the safety principles applied during the development of safety related software in defence equipment/systems contributes to the overall system safety case.

This document specifies the following for the development and in-service use of safety related software in defence equipment/systems:

1. Safety management
2. Roles and responsibilities
3. Failure condition and software level
4. Software planning process
5. Software development process
6. The verification processes
7. Testing of outputs of integration
8. Verification of verification process results
9. Software configuration management process
10. Software quality assurance process
11. Certification liaison process
12. Certification and in-service use
13. Software of differing safety integrity levels