

Definition and Verification of Critical Safety Functions in Software

Howard D. Kuettner, Jr., Philip R. Owen; APT Research, Inc.; Huntsville, Alabama

Keywords: system safety, software safety, software testing, software analysis

Abstract

Since 1994, APT Research, Inc. has applied a 15-step process to software safety. This paper describes the process and focuses on steps 10 through 14, where the critical safety functions are defined and verified. The authors explain the importance of identifying safety critical software functions and requirements and describe a method to positively impact the developer's test program and remove the need for independent software safety testing. Tailoring the software system safety effort focuses resources in the areas of greatest return, providing for a true, value-added software system safety effort.

Introduction

Software safety brings the different engineering disciplines together to focus on how software affects the safety of the system. Software may directly control mechanical, electrical, explosives, electromagnetic, laser and other obviously hazardous functions. Man-machine interfaces, that are software controlled, need clear, accurate, and timely data to facilitate safe decisions. Software system safety typically requires knowledge from a diversity of engineering disciplines. Systems engineering provides the overview necessary to integrate and understand how the software impacts the system performance. Software engineering provides the expertise necessary to understand how the software must perform to support the system requirements. Software engineers also understand that the software development policies, procedures, and their implementation influence the overall software quality.

APT's 15-step Process

Software system safety is a new and evolving discipline. Various organizations are continuously updating, simplifying and improving their processes. The APT 15-step process implements software safety concepts as outlined in MIL-STD-882 (ref. 1) and STANAG 4404 (ref. 2).

Table 1 depicts the 15 steps and provides the description, purpose, program phase, and responsible organization for each step. The program phases shown in column four are the standard set defined in MIL-STD-498 (ref. 3). The responsible organizations in column five presume a management organization that is typical of a defense development program: separate organizational elements are associated with systems engineering, software engineering, safety engineering, and an active Safety Working Group (SWG).

Figure 1 illustrates, in a typical timeline, the integration of the 15-step process into an overall development program. The time phasing of the 15 steps in relation to program milestones and the system safety analysis process is shown.

The scope of this paper is limited, and not all steps included in the 15-step process are described in detail. It is important to note that Software Configuration Management (SCM) is not addressed as an independent step in this process, but is an integral part of the 15-step process. The steps that tailor the safety effort, define the tests for critical functions, plan for verification and validation (V&V) testing, perform/monitor V&V testing, and review test results are described in detail in the following pages. Definitions of terms used in this paper are in the Appendix.



***Thank you for your
interest in our papers!***

*For the rest of the paper, please email
knewton@apt-research.com*