Chapter 11
Requirements to Products and Processes for Software of Safety Important NPP I&C Systems

Vladimir Sklyar
National Aerospace University KhAI, Ukraine

Andriy Volkoviy
Mellanox Technologies Ltd., Kyiv R&D Center, Ukraine

Oleksandr Gordieiev
Banking University, Ukraine

Vyacheslav Duzhyi
National Aerospace University KhAI, Ukraine

ABSTRACT

Features of software as a component of instrumentation and control (I&C) systems are analyzed. Attention is paid to the importance of functions performed by software and hazards of such software. Requirements for characteristics of software as a component of I&C systems are analyzed. Different regulatory documents are considered in order to disclose common approaches to the use of dedicated software and off-the-shelf software components. Classification of software, as well as classification of requirements, is described. Criteria of selection and structuring of requirements, as well as criteria for software verification, are defined. As long as the characteristics of software components directly depend on the quality of the processes of software development and verification, requirements for software life cycle processes are considered.

DOI: 10.4018/978-1-6684-3702-5.ch011

INTRODUCTION

Regardless of the purpose and application area any modern digital systems has software as integral part of the system. Instrumentation and control systems are not exceptions and may include software in many various forms: firmware and embedded software (written for particular hardware and usually executed without an operating system), system software (e.g. operating systems and platforms), middleware and device drivers, application software (typically written to be run under operating systems and usually interact with users), configuration for FPGA devices, etc. Software of different forms and types has specific properties. Moreover functions that are performed by software impose constraints on both software as a product and software lifecycle as a processes. For example, use of operating systems and application software has a very limited scope in safety important systems.

In the context of safety important I&C systems, increase in portion of software-produced or software-supported functions requires more attention to software. In this chapter software (SW) for nuclear power plant's (NPP) instrumentation and control (I&C) systems is concerned. That means that references to specific regulations for nuclear power engineering are given, particular terminology and classifications are used.

BACKGROUND

The increase of the number of nuclear power plant I&C software executed functions causes an increase of the "weight" of software device defects and its possible sources of failures. Based on different estimates such defects cause up to 70% of the failures of computer systems of critical application complexes, of the total number of those attributed to nuclear power plant I&C systems (Everett, 1998) (Lyu, 1996). Given this, the present trend is having an increasing dynamic role over time.

In the 1960s software defects caused up to 15% of the failures, and in the 1970s it was 15-30%, and by the year 2000 they were the cause of up to 70% of computer system failures. This trend shows up even more in space rocket technology (Aizenberg, 2002). Analysis of the cause of accidents and catastrophes of space rocket systems, where on board and ground computer systems have already been in use for several decades, allows one to determine that in the past 40 years each fifth accident is related to failure of a digital control system. Six of seven failures of these systems were caused by the occurrence of software defects. One such defect of computer software of the Ariane-5 navigational system in 1997 led to an accident which cost nearly one half billion dollars (Adziev, 1998). In nuclear power generation programmable I&C systems have had a shorter history, however, here also there have been accidents due to software defects.

The reliability of software, as for the I&C system as a whole, depends on the design quality at stages that directly precede development of the software:

- Development of requirements for I&C system.
- Mathematical modeling.
- Software implemented functioning algorithms.

Errors committed at these stages become sources of complex defects in software. In this sense, software, on the one hand, accumulates the deficiencies of the preceding stages, and on the other hand, is