Chapter 26
Diversity and Multi-Version Systems

Alexander Siora
Research and Production Corporation Radiy, Ukraine

Vyacheslav Kharchenko
Centre for Safety Infrastructure-Oriented Research and Analysis, Ukraine

Vladimir Sklyar
Research and Production Corporation Radiy, Ukraine

Eugene Brezhnev
Centre for Safety Infrastructure-Oriented Research and Analysis, Ukraine

ABSTRACT

To protect safety-critical systems from common-cause failures that can lead to potentially dangerous outcomes, special methods are applied, including multi-version technologies operating at different levels of diversity. A model representing different diversity types during the development of safety-critical systems is suggested. The model addresses diversity types that are the most expedient in providing required safety. The diversity of complex electronic components (FPGA, etc.), printed circuit boards, manufacturers, specification languages, design, and program languages, etc. are considered. The challenges addressed are related to factors of scale and dependencies among diversity types, since not all combinations of used diversity are feasible. Taking these dependencies into consideration, the model simplifies the choice of diversity options. This chapter presents a cost effective approach to selection of the most diverse NPP Reactor Trip System (RTS) under uncertainty. The selection of a pair of primary and secondary RTS is named a diversity strategy. All possible strategies are evaluated on an ordinal scale with linguistic values provided by experts. These values express the expert's degree of confidence that evaluated variants of secondary RTS are different from primary. All diversity strategies are evaluated on a set of linguistic diversity criteria, which are included into a corresponding diversity attribute. The generic fuzzy diversity score is an aggregation of the linguistic values provided by the experts to obtain a collective assessment of the secondary RTS's similarity (difference) with a primary one. This rational diversity strategy is found during the exploitation stage, taking into consideration the fuzzy diversity score and cost.

DOI: 10.4018/978-1-5225-1933-1.ch026

INTRODUCTION

To guarantee required level of dependability, safety and security of computer-based systems for critical (safety-critical, mission-critical and business-critical) applications a diversity approach is used. This approach implies development, choice and implementation of a few diverse design options of redundant channels for created system. Probability of CCF of safety-critical systems may be essentially decreased due to selection and deployment of different diversity types on the assumption of maximal independence of redundant channels realizing software-hardware versions.

Risk of CCF is the main factor of reducing redundant I&C systems dependability. Diversity and defense-in-depth is the required principle of development for NPP I&C systems important for safety, first of all, reactor trip systems (Jonson, 2010).

Diversity is the general approach used for decreasing CCF risks of I&C systems, because differences in hardware and software components, development and verification technologies, implemented functions, etc. can mitigate the potential for common faults (Jonson, 2010, NUREG/CR-6303, 1994).

One of the key theoretical and practical problems is diversity estimation and optimization of used version redundancy capacity. Diversity related decisions should be made at the first design stages, because ones affect safety and cost of NPP I&C system. There are risks of the inaccurate or untrustworthy assessment of diversity and I&C system safety as a whole.

If diversity indicator is overstated, it causes increasing risks of CCF. If result of assessment is understated, it increases costs unreasonably at the production, implementation and operation stages.

This circumstance calls for that a lot of international and national standards and guides contain the requirements to use diversity in safety-critical systems, first of all, in NPP I&Cs (RTS), aerospace on-board equipment (automatic/robot pilot, flight control systems), railway automatics (signalling and blocking systems), service oriented architecture (SOA)-based web-systems (e-science) etc. (Pullum, 2001; Wood et al., 2009; Gorbenko et al., 2009; Kharchenko et al., 2010; Sommerville, 2011).

BACKGROUND

In a modern world, there are many various regulations, which, in general case, cover the most important areas widely used by the mankind. It is possible to distinguish those related (in some way) to safety important I&C systems, grouped into several sets to cover general issues of critical I&C systems at various lifecycle stages (including their development, operation and maintenance), security, as well as covering various technology-related aspects.

Application of the modern information and electronic technologies and component-based approaches to development in critical areas, on the one hand, improve reliability, availability, maintainability and safety characteristics of digital I&Cs. On the other hand, these technologies cause additional risks or so-called safety deficits. Microprocessor (software)-based systems are typical example in that sense. Advantages of this technology are well-known, however a program realization may increase CCF probability of complex software-based I&Cs. Software faults and design faults as a whole are the most probable reason of CCFs. These faults are replicated in redundant channels and cause a fatal failure of computer-based systems. It allows to conclude that “fault-tolerant” system with identical channels may be “non-tolerant” or “not enough tolerant” to design faults. For example, software design faults caused more than 80% failures of computer-based rocket-space systems, which were fatal in 1990 years