Reliability Engineering and System Safety 135 (2015) 81–91

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Three suggestions on the definition of terms for the safety and reliability analysis of digital systems

Man Cheol Kim [a], Carol S. Smidts [b,*]

[a] School of Energy System Engineering, Chung-Ang University, 84 Heukseok-ro, Dongjak-gu, Seoul, Republic of Korea
[b] Nuclear Engineering Program, Department of Mechanical and Aerospace Engineering, The Ohio State University E418 Scott Laboratory, 201W, 19th Ave, Columbus, OH 43210, USA.

ARTICLE INFO

Article history:
Received 28 June 2013
Received in revised form
16 October 2014
Accepted 18 October 2014
Available online 6 November 2014

Keywords:
Digital system
Instrumentation and control
Safety system
Probabilistic safety assessment
Probabilistic risk assessment

ABSTRACT

As digital instrumentation and control systems are being progressively introduced into nuclear power plants, a growing number of related technical issues are coming to light needing to be resolved. As a result, an understanding of relevant terms and basic concepts becomes increasingly important. Under the framework of the OECD/NEA WGRISK DIGREL Task Group, the authors were involved in reviewing definitions of terms forming the supporting vocabulary for addressing issues related to the safety and reliability analysis of digital instrumentation and control (SRA of DI&C). These definitions were extracted from various standards regulating the disciplines that form the technical and scientific basis of SRA DI&C. The authors discovered that different definitions are provided by different standards within a common discipline and used differently across various disciplines. This paper raises the concern that a common understanding of terms and basic concepts has not yet been established to address the very specific technical issues facing SRA DI&C. Based on the lessons learned from the review of the definitions of interest and the analysis of dependency relationships existing between these definitions, this paper establishes a set of recommendations for the development of a consistent terminology for SRA DI&C.

1. Introduction

As digital instrumentation and control (DI&C) systems are increasingly introduced into nuclear power plants (NPPs), growing attention has been given to safety concerns associated with these systems. In [1], the National Research Council raised key issues associated with the use of DI&C systems in NPPs. In [2], Yoshikawa describes the history of DI&C systems introduction into NPPs since the fully digitalized main control room of Kashiwazaki–Kariwa Unit 6 in 1996. In [3], Kang and Sung identify important factors affecting the probabilistic safety assessment (PSA) of DI&C systems. Li and Jiang [4] provide an overview of the applications of PSA to DI&C systems. Several authors such as Smidts and Li [5] and Park and Jang [6] have also conducted research to develop the methods for assessing the reliability of safety-critical software in DI&C systems. Quantitative safety and reliability analysis of digital systems in other applications can also be found in related literature such as Dugan et al. [7] and Yau et al. [8].

As a result of this increased interest, engineers and researchers have become familiar with DI&C systems and their related terminology. However, concerns exist regarding whether these terms are being correctly understood and if they are being consistently used among various individuals, between different countries, and across a variety of disciplines. Even though authors such as Christensen et al. [9] and Aven [10] have discussed the concept of risk and associated terminology, few studies broach the terminology specifically used to discuss the safety and reliability analysis of digital systems.

A *digital system* is a system that uses discrete (discontinuous) values to represent information. This is in contrast to the continuous values used in an analog system. The term “digital system” incorporates a wide variety of systems regardless of their complexity; for example, simple digital circuits that consist only of logic gates at one end, and, supercomputers at the other end of the spectrum can both be considered digital systems. In nuclear power plants, digital systems with various levels of complexity are used, but these systems comprise only a small portion of the total number of digital systems found in industry.

The need for this paper stems from the lack of clear definitions for terms used in the safety and reliability analysis of digital instrumentation and control (SRA DI&C) systems. As a result of this deficiency, dissimilar terms are used interchangeably or similar

[*] Corresponding author.
E-mail addresses: charleskim@cau.ac.kr (M.C. Kim), smidts.1@osu.edu (C.S. Smidts).

http://dx.doi.org/10.1016/j.ress.2014.10.022
0951-8320/© 2014 Elsevier Ltd. All rights reserved.

Table 1
Various terms for digital systems generating safety-related plant protective signals.

Term	Source	Reference
Programmable electronic system	IEC 61508	[12]
Computer-based safety systems	IEEE Std 603-1998	[13]
Digital computer-based systems	IEEE Std 7-4.3.2-2003	[14]
(Digital) computer-based I&C systems	Branch technical position HICB-14	[15]
Digital computers in safety systems	Regulatory guide 1.152	[16]
Electric equipment important to safety	Regulatory guide 1.89	[17]
Computer systems in nuclear reactor protection systems	NUREG/CR-6101	[18]
Software-based safety systems	Liwang	[19]
Programmable system	Pavey et al.	[20]
Programmable digital safety I&C system	Authen et al.	[21]
Digital I&C systems for safety system	JNES	[22]

Table 2
The definition of “fault” from different standards.

Standard	Definition
IEC 61508 [12]	Abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function.
IEC 62340 [23] IEC 61513 [24]	Defect in a hardware, software or system component.
IEEE Std 7-4.3.2-2003 [14]	(1) A defect in a hardware device or component; for example, a short circuit or broken wire. (2) An incorrect step, process, or data definition in a computer program.
IEEE Std 610.12-1990 [25]	(Note) This definition is used primarily by the fault tolerance discipline. In common usage, the terms “error” and “bug” are used to express this meaning.

terms interpreted differently by researchers and engineers across countries and disciplines. Without a common definition of terms, resulting miscommunication can hinder the resolution of important technical issues such as those related to the modeling of DI&C systems in probabilistic risk assessment (PRA), and the resulting inability to characterize the impact on risk of the introduction of such technology. The need for and importance of international consensus on terms is a necessity when the use of DI&C is in the context of systems with the potential for disasters of significant proportion which can cross national boundaries such as nuclear, chemical, etc, as well as in technological areas where various countries combine their efforts to complete the building or the installation of an outfit such as a nuclear power plant.

Under the framework of the OECD/NEA WGRISK (Work Group on Risk) DIGREL (Digital Reliability) Task Group [11], experts from thirteen different countries,[1] twenty different institutes,[2] and with various backgrounds[3] are discussing the development of a taxonomy of DI&C failure modes for PRA and therefore the problem of a common DI&C terminology has come at the forefront since it is a necessary condition to the establishment of a taxonomy. In this paper, we provide (1) the lessons learned from our review of the definition of terms in existing standards within the umbrella of our contributions to the task group modified and revised through the many valuable inputs of our colleagues on the task group and (2) guidelines for the use of SRA DI&C in future standards or for the revision of the current related standards.

2. Current status of terminology

Our review focused on terms used to describe and analyze safety and reliability problems associated to a sub-group of digital systems, i.e. those that generate safety-related plant protective signals. These digital systems include the engineered safety features actuation system (ESFAS) and the reactor trip system (RTS) (sometimes called a “reactor protection system”). Alternative terms in standards and publications used to describe this sub-group of digital systems are provided in Table 1.

As can be seen in Table 1, many terms are used to refer to this particular sub-group of DI&C systems. A one-to-many relationship exists between the sub-group of “DI&C systems that generate safety-related plant protective signals” and its “*forms*” in the literature. Our review indicates that this is a common occurrence —“many” terms are oftentimes used to denote a “single” *concept* (*many-to-one*) or that “one” term can be used to signify “two or more” concepts (*one-to-many*). In Section 2.1, we provide an analysis of the “forms” in the standards of the three most fundamental concepts in safety and reliability analysis: fault, error, and failure. These three concepts are fundamental since they help us understand the process of generation of a failure. In Section 2.2, we provide an analysis of the safety classification of a system, which is important because it specifies the depth and the rigor of the analysis the system should be subjected to.

2.1. Fault, error, and failure

Fault, *error*, and *failure* are fundamental terms used to analyze a system's reliability. Our review discovered that these terms are defined differently in several international standards.

[1] Canada, Czech Republic, Finland, France, Germany, Hungary, Italy, Japan, the Netherlands, Slovakia, South Korea, Sweden, and the United States.

[2] AREVA; Brookhaven National Laboratory (BNL); Canadian Nuclear Safety Commission (CNSC); Électricité de France (EDF); Enel Ingegneria e Innovazione; Gesellschaft für Anlagen- und Reaktorsicherheit (GRS); Institut de radioprotection et de sûreté nucléaire (IRSN); Institut für Sicherheitstechnologie (ISTec); Japan Nuclear Energy Safety Organization (JNES); Korea Atomic Energy Research Institute (KAERI); Nuclear Energy Agency (NEA); Nuclear Research and Consultancy Group (NRG); Nuclear Research Institute (NRI) Rez plc; Organization for Economic Co-operation and Development (OECD); RELKO; Risk Pilot; Systems and Control Laboratory, Computer and Automation Research Institute, Hungarian Academy of Sciences (MTA SZTAKI); The Ohio State University (OSU); U.S. Nuclear Regulatory Commission (NRC); and VTT Technical Research Center of Finland.

[3] Nuclear I&C, software engineering, and PRA, among others.