A review on the research status of reliability analysis of the digital instrument and control system in NPPs

Q Z Liang¹, Y Guo¹ and C H Peng¹,*
¹ Department of Engineering and Applied Physical, University of Science and Technology of China, No.96, JinZhai Rd, Hefei, Anhui, China

*Corresponding Author:pengch@ustc.edu.cn

Abstract. The widely use of digital instrument and control (I&C) systems in nuclear power plants (NPPs) and their important role in plant safety put forward the requirement for developing reliability modeling for digital systems with the capacity to be integrated into the existing probabilistic safety analysis (PSA) framework. However, challenges arise in the reliability analysis which mainly come from the modeling of complex interactions among the system hardware, software, controlled process physics, and operator. Generally, these factors are analyzed separately since at present there isn’t universal methods for modeling them in a uniform framework. In this paper, the research status of reliability modeling methodologies, software reliability assessment methods and human reliability analysis for digital instrument and control systems in NPPs were introduced. The survey results show that ET/FT is still the mainstream method in reliability studies of digital systems in NPPs, and DFM is a dynamic method with great potential. At present, there is no generally accepted software reliability analysis method. The researches about human errors under digital environment and the theoretical basis of corresponding human reliability analysis method is being developed.

1. Introduction
In nuclear power plants (NPPs), instrument and control (I&C) systems are used to realize functions such as monitoring, control and protection. The performance level of I&C systems has a significant impact on the safe, reliable and economical operation of the plant.

With the rapid development of computer technology, I&C systems in NPPs are gradually transformed from analog systems to digital instrument and control systems (DI&CS) [1]. Westinghouse has replaced the original analog protection system with Eagle21 on nine units of five PWR plants, including Sequoyah [2]. Surry-1 and -2 815MW PWR NPPs have started to be renovated with Ovation and Advant digital platform systems from Westinghouse. Three PWR plants, PALO verde-1, -2 and -3, were digitally upgraded in 2003 with Advant platform systems [3]. Since 1984, France has installed 20 sets of digital protection system SIPN in 1300M PWR plants and the accumulated operation experience has exceeded 100 reactor years. The use of SIPN was good, and on this basis, the second-generation SIPN system (SIPN-2) was developed from the late 1980s, which was planned to be installed in the newly built N4 series NPPs [4]. In the early 1980s, Canada began to partially apply digital technology in CANDU600 reactor protection systems, and the fully digital protection systems developed on this basis were used in Darlington pant. In Japan, Hitachi's fully digital protection system was applied to Kashiwazakikariwa 6 and 7 advanced boiling water reactors
in 1996 and 1997[5]. Other nuclear power countries such as Germany and Russia are also making great efforts to develop and apply digital instrumentation systems in NPPs.

In China, digital technologies were beginning to be use in NPPs since Tianwan nuclear power plant introduced TXP & TXS system (AREVA/SIEMENS) in 1996. Subsequently, CPR1000 series nuclear power projects, including Lingao Phase-II (same I&C systems as Tianwan plant), Hongyanhe plant (Mitsubishi MELTAC platform used for safe-related systems and HOLLiAS platform used for non-classified systems), Ningde, Yangjiang and other plants, all adopt DI&CS. At the same time, some NPPs in China have completed digital upgrading of their analog instrument systems, such as the digitalization of the KIT/KPS system for units 1 and 2 of Daya Bay nuclear power plant, and the upgrading of the analog reactor protection system (RPS) to digital system in Qinshan Phase-I. In addition, DI&CS are also used in some experimental reactors, for example, CEFR-25 and HTGR 10 [6].

The widespread use of DI&CS is the inevitable trend of nuclear power development. Since control and protection functions of DI&CS play a crucial role in NPPs safety, failure of the systems would lead to safety actions such as reactor shutdown and turbine trip. In serious cases, it may lead to core damage, release of radioactive materials to the environment, and even seriously endanger the public safety. NRC (Nuclear Regulatory Commission) reviewed statistical dates from 1994 to 1999 in LER (Licensor Event Report) database, with the results showing that 8% of the incidents are associated with the digital systems failure and the effect of 9% of the trip events is caused directly by the digital systems failure. In the published literature of Bickel J.H., a statistical study on a total of 1.27 million hours of operation data of the protection system of digitized reactors in the first generation of seven NPPs in the United States shows that there were 141 incidents affecting the safe operation of the plant [7]. The research results of KAERI (Korea Atomic Energy Research Institute) indicate that the probability of core damage result from the failure of safe-related DI&CS is between 6% and 10%. According to incomplete statistics, from 2000 to 2005 71 unplanned trips took place in the five domestic NPPs in service, among which 26 were caused by I&C systems.

It is necessary to develop reliability modeling for DI&CS with the capacity to be integrated into the existing probabilistic safety analysis (PSA) framework. Whereas, special dynamic characteristics associated with DI&C systems bring about challenges in the reliability analysis for the systems. Because of the dynamic interactions, some factors need to be considered, such as sequence of component failure [8], timing of failure [9,10], exact value of process variable at the time of failure [11,12], failure propagation between hardware and software, software reliability [52-53,58], and human error events [65]. Currently, there are not appropriate methods with the capacity modeling the interactions among controlled process-hardware-software-human in a unified framework. Generally, they were assessed individually with different methods. The research status of current reliability modeling methodologies, quantitative software reliability methods and human reliability analysis for DI&CS in NPPs are introduce in follow sections.

2. Current reliability modeling methodologies for DI&CS
Since 1990s, NRC has conducted a series of research programs related to DI&CS in NPPs and is the most in-depth institution within this field. Sponsored by NRC, some research institutions, such as Brookhaven National Laboratory, University of Virginia and the Ohio State University, successively developed reliability assessment methodologies for DI&CS and has issued a series of documents, including NUREG/CR-6901 [13], -6942 [9], -6985 [10] about the development of dynamic methods and -6962 [14] and -6997 [8] studying the feasibility and applicability of traditional methods.

In addition, Committee on the Safety of Nuclear Installations (CSNI), KAERI, Nordic nuclear safety research (NKS) and VTT technical Research Center of Finland have also performed researches on reliability assessment methods for DI&CS in NPPs and gain some achievement. In China, the research field started late and static analysis method is still the mainstream, and complete reliability evaluation framework hasn’t been established.
2.1. Research on traditional reliability modeling methodologies
In NUREG/CR-6962 and 6997, two traditional methods, that is, ET/FT (Event Tree/Fault Tree) and Markov model, were applied in reliability modeling of the benchmark system (i.e., a digital feedwater control system (DFWCS) in a pressurized water reactor) to identify the capacities and limitations of the traditional methods for reliability modeling of DI&CS.

ET/FT is the method used in the current NPP PSA framework and has been applied in some reliability assessment researches of DI&CS. J.H. Bickel applied ET/FT in risk evaluation for the first-generation digital reactor protection system in U.S. NPPs [7]. P.V. Varde et al used ET/FT to estimate failure probability of the protection system of APR1400 [15], and H.G. Kang et al adopted ET/FT to assess the unavailability of the digital engineered feature actuation system of a South Korea NPP [16] respectively. S. J. Lee et al established a PSA model by ET/FT, which can capture the fault-tolerant characteristics of the digital system in NPPs [17]. H.X. Zhou et al used ET/FT analyze the reliability of digital protection system of Tianwan NPP [18]. S.L. Zhou et al. adopted ET/FT to evaluate the probability of partial and total loss of automatic and manual regulation functions of digital nuclear power control system [19].

Strictly speaking, Markov is not a traditional method, because it can capture some of the dynamic characteristics of digital systems, such as repair, the sequence of component failures [8,20]. However, in NUREG-6997, it was considered as a traditional method since it wasn’t used to model dynamic interactions between DI&CS and controlled process (defined as Type I interactions in NUREG/CR-6901). There are some studies about Markov model applied to DI&CS in NPPs. Y. C. Huang et al adopted Markov to analyze reliability of typical functional safety digital control system of nuclear island [20]. Z. Qing et al used Markov to established reliability model of the safety-relate 2-out-of-4 digital control system in NPPs [21], and L. Y. Wu et al perform reliability assessment of typical three-channel of the system by Markov [22], respectively.

The limitation of the traditional method that without the capability to model Type I interactions is the main obstacle for the application of the methods in reliability modeling for DI&CS, especially for control system in which the Top Event may be dependent on the sequence of component failure, timing of failure, and the value of the controlled process variables when component fails. The major deficiency of ET/FT is that the method can’t model time- and sequence- dependent behaviors of digital systems [23] and handle multi-state failure [24]. Nevertheless, according to the findings of NUREG/CR-6997, ET/FT is applicable for reliability modeling of safety-related protection systems. For the protection system, once the system is actuated, feedback from the NPP will not affect the system startup, that is, the Type I interaction does not exist or is very weak. The report also pointed out that for the protection system using dynamic method may not get better results but will increase the difficulty and workload of the assessment. Markov model can capture some dynamic characteristics of digital systems such as the sequence of component failure but is easily suffered by the explosion problem of state space [25], which makes it difficult to apply the method to an actual system. Generally, DI&CS in NPPs is complex and the number of components is large such result in an exponential increase of the Markov model, which may lead to infeasibility of model construction and solution.

2.2. Research on traditional reliability modeling methodologies
NUREG/CR-6901 defined a method that explicitly model Type I dynamic interactions of DI&CS as dynamic method and summarized current dynamic reliability modeling methodologies for DI&CS and the methods mainly include three main categories:
1) Continue time methods
   • CET (Continue Event Tree)
   • CCCMT (Continue Cell-to-cell Mapping Technique)
2) discrete-time methods:
   • DYLAM (Dynamic Logical Methodology)
   • DETAM (Dynamic Event Tree Analysis Method)
• DDET (Dynamic Discrete Event Tree)
• ADS (Accident Dynamic Simulator)
• ISA (Integrated Safety Assessment)
• MCDET (Monte Carlo Dynamic Event Tree)
• Markov/CCMT (Markov/Cell-to-cell Mapping technique)

3) methods with graphical interfaces:
• DFM (Dynamic Flowgraph methodology)
• Petri nets
• DFT (Dynamic Fault-trees)
• ESD (Event-sequence Diagram)
• GO-FLOW

The report developed the desirable characteristics for the methodologies and evaluated them against these characteristics, with result indicates that none satisfies all requirements and DFM is the top one that provides most advantages, followed by Markov/CCMT. Furthermore, NUREG/CR-6942 and -6985 had demonstrated the feasibility and applicability of these two methods, and NEA/CSNI/R (2009) [26] and NKS -230 [27] also recommend the methods as candidate methods for reliability modeling of DI&CS.

2.2.1. Research on reliability analysis of DI&CS based on DFM. The DFM is a directed graph model in which failure of system component and corresponding dynamic interactions associated with DI&CS are represented by graphic element. Basic elements used to construct a DFM model and an example are shown in Figure 1.

Process variable nodes are used to represent physical and software variables, which are connected by causality edges representing cause-and-effect relationship among the variable nodes. Component failure states, changes of physic process operation modes, and software switching actions are modeled by condition nodes that are connected by condition edges condition edges indicating actual discrete behavior of the system. Transfer box and transition box represent the relationships among process variable nodes and the latter contains time element.

Analyses of a DFM model mainly include deductive and inductive analysis. The deductive analysis is performed by backtracking the time steps defined by the analyst and the causality of the DFM model, resulting in timed prime implicants (TPIs) for a Top Even predefined. A TPI is the minimum combination of variable state at specified time that result in Top Event. Inductive analysis is performed by following the causality of the model step by step in time and to gain the result for given initial condition.

DFM has been successfully applied in some studies on reliability assessments of digital systems in nuclear industries. NUREG/CR 6465 applied DFM in safety analysis for the control software in an advanced reactor and developed the support tool [28]. T. Aldemir et al used DFM to conduct reliability analysis for the DFWCS [10,11]. P. McNelles et al used DFM for optimization design for a post-accident monitoring system in Westinghouse AP1000 NPP [29]. I. Karanta et al adopted DFM to conduct reliability research for the digital feedwater control system of Olkiluoto units 1 and 2 [30]. By DFM, G. Apostolakis et al verified the design of a software system for controlling boron-containing water injection into the reactor's main feed water system [31]. X.M. Guo used DFM in reliability analysis for a digital dual microprocessor control system architecture in NPP [32], and S.L. Zhou et al used DFM to evaluate the reliability of the digital automatic power control system in an NPP [33].

DFM is a dynamic method with great potential. However, the method has some defects, mainly including the rough partitioning of the system state space that may lead to modeling inaccuracy and usual large time step defined for computational feasibility [9,32]. The coarse portioning of the system state may result in not accurate model construction. Large analysis time step may lead to not sufficient result. Additionally, integrating the result of a DFM model into the current PSA framework is a challenge for the widespread use of the method in NPP PSA [9].
2.2.2. Research on reliability analysis of DI&CS based on Markov/CCMT. The Markov/CCMT (Markov/Cell-to-cell Mapping technique) describes system behaviors by discrete time and discrete system state space consisting of system configurations (component state combinations) and process variable state. The transitions between the configurations are modeled by Markov. The process variables state space is partitioned into cells (example see Figure 2) with predefined Top Events. The CCMT is used to model the transitions between cells and Markov model is used to represent the transitions between system configurations. The probability of Top Event is derived by combining the probabilities of the above two transitions.

The applications of Markov/CCMT in reliability assessments for digital systems are few, and most of the research is about the feasibility and solution of the model. T. Aldemir et al performed the feasibility analyses of the application of Markov/CCMT to reliability assessment of digital systems in NPP [10,11]. J. Yang et al proposed a backtracking algorithm to improve the computational efficiency of Markov/CCMT deductive analysis [34]. Based on a digital dual microprocessor control system architecture, X.M. Guo explored the applicability of Markov/CCMT [32].

The practical application of the methodology suffers weakness from computation aspect, including computer storage requirements and computation times [9,35]. The sensitivity analysis of time discretization and state space discretization was performed in the reliability analysis of a simple level control system with result indicating that a refined enough partitioning of state space and a cautious choice of time step are necessary for accurate model construction; however, a refined partitioning may cause prohibitive computer storage requirements and a small time step may lead to long computation times [35].

3. Development of software reliability analysis methods

Software reliability assessment is an important research direction in digital industry. Since 1960s, hundreds of software reliability modeling methods have been developed but none is universal. Especially, there isn’t methods suitable for software reliability modeling of DI&CS in NPPs. In addition, for safety-related protection system in NPPs, the probability of software failure under the demand state obtains more attentions in PSA and the required probability associated with such system in license process generally is extremely low. A software reliability assessment method applicable to DI&CS in NPPs should be a method with capacities for estimation of software failure probability on demand with a very low value.

One of the most widely used methods is software reliability growth model (SRGM). A SRGM uses test data to establish the empirical formula of the expected number of failures as a function of time [36,37]. There have been developed a large number of SRGMs, such as S-shaped model [38], inflection S-shaped model [39], and discrete time SRGMs [40]. However, none is generally superior to the others. Even though some studies show that the optimal SRGM can be determined for specified
application, such as [41,42], the method may not be the best choice for software reliability modeling for safety-related digital systems in NPPs, because it needs an extremely long time for software reliability growing to a very high level associated with such systems.

Testa-based method is also one of commonly used software reliability assessment methods. The method quantifies software reliability through applying standard statistical methods to analyze software test data. Test cases are generated from the software’s operational profile and usually different form each other. Test-based methods include black-box test and white-box test [43]; the former regards software as an entirety and the latter considers software's interior structure. May et al. described white box test as a partition-based method which partitions software into several subsets and perform testing for each subset [44]. The black-test method concerns and the functionality of software and different approaches, such as frequentist and Bayesian [45], can be used to derive upper confidence bound for failure probability at any confidence level. NUREG/CR-7044 [46] recommend test-base method as one candidate method for software reliability assessment and NUREG/CR-7234 [47] subsequently developed a test-based method to evaluate the probability of failure on demand of digital protection systems in NPPs.

Unlike the purely data-driven methods described above, Bayesian Belief Network (BBN) method explicitly models causal factors. BBN uses a probabilistic graphical model which consists of random variables containing information about software and directed acyclic graphs that determine conditional independencies among random variables [48,49]. BBN methods provide the ability to integrate diverse information about software such as empirical data and expert judgments for assessing quality of software development lifecycle activities and to model parameter uncertainties. There have been some applications of BBN to software reliability assessment non-nuclear industry and obtained satisfactory results [50,51]. Some researches sponsored by NRC, such as NUREG CR-7044 and -7233 [52], made attempts to apply BBN methods to DI&CS in NPPs and illustrated the feasibility of the method. The research results indicate that challenges of application of BNN may come from extensive modeling efforts, availability of documentations of software development life cycle activities, and verifiability of the accuracy of expert judgments used to quantify the quality of the activities.

In addition to the above three categories, there are some other software reliability quantification methods. Neufelder proposed methods to evaluate software’s failure rate and the methods were implemented in a software tool named Frestimate [53]. NUREG/CR-0019 [54] developed metrics methods which estimate software failure rate and probability by correlating software engineering metrics and software reliability. NUREG/CR-6848 [55] and -7042 [56] conducted preliminary and large-scale validation of the method. Rule/standard based methods estimate software reliability based on the standard (such as IEC 61508) for safety-related systems which designates the target failure probability for failure on demand and the target failure rates for different safety integrity levels [57]. But the estimate is cursory and uncertainty should be considered.

4. Research on human reliability analysis under digital environment

Digital human-machine interfaces change the environment in MCR and bring about new impacts on operator behavior. A study by NRC indicated that digital human-machine interfaces can enhance operator performance, reduce workload, and are well accepted. Entrusted by NRC, Brookhaven National Laboratory conducted a research about computer-based systems and found evidence of two kinds of negative effects [58]. Lee et al researched on human error under digital MCR and shown that six types of errors arise [59].

Most of the current human reliability analysis (HRA) methods were developed prior to the introduction of digital human-machine interfaces in MCR, so the new impacts on the operator's performance cannot be properly considered. Julius et al point out issues and insights associated with the application of current HRA techniques to digital systems and indicated that no existing HRA method can adequately addresses digital environment [60]. E.M. Hicking et al. studied the feasibility and applicability of three commonly used HRA methods, namely THERP, ASEP and SPAR-H, to the digital MCR [61]. The study shows that, in most cases, these methods provide an overly optimistic
assessments of human error probability (HEP) compared to empirical data. The result means that the assumption that improved performance reduces HEP is invalid.

The introduction of digital human-machine interfaces has put forward new requirements for HRA methods, and it is necessary to update the existing HRA methods or develop new HRA framework. X.F. Tian et al pointed out that it is necessary to study the performance feature of the operator under digital environment and to develop new performance shaping factors [62]. I. Jang et al. indicated that digital MCR applies software-based control and analysis for software control mission is need to determine operator errors that may occur [63]. The research of Liinasuo et al shown that the commonly separation of operator actions into diagnosis and execution isn’t appropriate for description of operator’s behavior under digital environment [64].

R.L. Boring et al. [65] pointed out the requirements of HRA method for digital MCR : (1) systematically review the operational experience of human error events related to digital human-machine interfaces recorded by the non-nuclear industry with rich digital human-machine interfaces experience; (2) identify specific human error events in the operation of the control room of nuclear power plant using digital HISs; (3) it is necessary to establish the unique PSFs of digital human-machine interfaces and the empirical basis of quantification; (4) verify and study the influence of digital human-machine interfaces on operator performance by using the research simulator; (5) develop guidelines to include and quantify these human errors in HRA and PRA.

5. Discussions and Conclusions

As digital instrument and control systems are widely used in NPPs. The development of methodologies for reliability modeling of digital systems obtains significant attention. However, so far most of technical communities don’t reach a consensus on the method for that. This paper provided an introduction for the research status of development of reliability modeling methodologies, software reliability analysis and human reliability analysis for digital instrument and control systems in NPPs.

Traditional methods, such as ET/FT and Markov model, have limitations in reliability modeling for DI&CS. Nevertheless, the review result shows that ET/FT is still the mainstream method in the reliability analysis of DI&CS in NPPs since the method is mature in theory, easy to use, and compatible with the current PSA framework of NPPs. Especially, the method is commonly used in reliability modeling of protection systems in NPPs for that its feasible and applicable for the modeling of protection system have been demonstrated. DFM is a dynamic method with great potential. Its feasibility and applicability have been verified in many researches, but there are still some limitations, including the partition of process variable states and the time steps of deductive analysis, which need to be coordinated between model accuracy, model construction difficulty and calculation feasibility. In addition, the integration of the method results with the current PSA framework of NPPs is also a problem.

Hundreds of software reliability modeling methods have been developed and mainly are categorized as: 1) software reliability growth model, 2) Testa-based method, 3) Bayesian belief net model, and 4) other methods. BBN model and test-based method are approaches with great potential for evaluation of the probability of software failure of DI&CS in NPPs. Furthermore, the combining BBN and test-based method can benefit from the advantages of the two approaches, that is, BBN is used to obtain a prior distribution of software reliability parameters and test is performed to obtain the data needed for Bayesian update.

DI&CS provide digital man-machine interface in MCR such change the work environment for the operator. Digital environment may provide potential of improvement of operator performance. At the same time, impacts of MCR environment on operator behavior change. Since current HRA methods were almost proposed before the appearance of digital MCR, it is necessary to update the existing HRA methods or develop a new HRA framework. The requirements for new HRA method are in research and so far, there is not an appropriate approach for human reliability assessment under digital environment.
Acknowledgment
This work is financially supported by Science and Technology on Reactor System Design Technology Laboratory of Nuclear Power Institute of China.

References
[1] NUREG/CR-6888 Emerging Technologies in Instrumentation and Controls: An Update [R]. U.S. Nuclear Regulatory Commission, 2006
[2] W.R. Liu. The Developing Status of the Instrument and Control Systems in Nuclear Power Stations [J]. Process Automation Instrumentation, 1997. 18(9):1-5
[3] J. Shi, M.Y. Jiang, et al. Current Status for Upgrades of Key Technology of Digitized Instrument and Control System in Nuclear Power Plant [J]. Nuclear Power Engineering, 2004, 23(2):29-32
[4] Q. Yang. Application Status and Development Trend of Digital I&C System in Nuclear Power Plant [J]. Nuclear Power Engineering, 1998, 19(2):124-128
[5] X.L. Xu, R.J. Guo. Digital instrument control system and its application in nuclear power plants [J]. High Technology Letter, 1997(1):59-62
[6] Q. Ma, Q. Luo, et al. Research on Domestic and International Research Reactor Control System [J]. INSTRUMENTATION, 2019,26(3):40-43
[7] Bickel J.H., Risk implications of digital reactor protection system operating experience [J]. Reliability Engineering and Systems Safety, 2008, 93(1): 107-124
[8] NUREG/CR-6997 Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods [R]. U.S. Nuclear Regulatory Commission, 2009.
[9] NUREG/CR-6942 Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments [R]. U.S. Nuclear Regulatory Commission, 2007.
[10] NUREG/CR-6985 A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems [R]. U.S. Nuclear Regulatory Commission, 2009.
[11] Aldemir, T., 1989. Quantifying setpoint drift effects in the failure analysis of process control systems [J]. Reliability Engineering and System Safety 24, 33–50.
[12] Hassan, M., Aldemir, T. A data base oriented dynamic methodology for the failure analysis of closed loop control systems in process plants. Reliability Engineering and System Safety 1990, 27, 275–322.
[13] NUREG/CR-6901 Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments [R]. U.S. Nuclear Regulatory Commission, 2006.
[14] NUREG/CR-6962 Traditional Probabilistic Risk Assessment Methods for Digital Systems [R]. U.S. Nuclear Regulatory Commission, 2008.
[15] KAERI/TR-2467 Reliability Study: Digital Engineered Safety Feature Actuation System of Korea Standard Nuclear Power Plant [R]. Korea Atomic Energy Research Institute, 2003
[16] H.G. Kang, and S.C. Jang. A Quantitative Study on Risk Issues in Safety Feature Control System Design in Digitalized Nuclear Power Plant [J]. Nuclear Science and Technology, 2008, 45:8, 850-858
[17] S.J. Lee, W. Jung, J.E. Yang. PSA model with consideration of the effect of fault-tolerant techniques in digital I&C systems [J]. Annals of Nuclear Energy, 2016
[18] H.X. Zhou, W.G. Wang. Reliability Analysis of Digital Reactor Protection System of Tianwan Nuclear Power Plant [J]. Nuclear Electronics and Detection Technology, 2009, 29(6): 1272-1276
[19] S.L. Zhou, Y.Y Liu, W. Du. Fault Tree Based Reliability Analysis for Digital Reactor Power Control System of Nuclear Power Plant [J]. Nuclear Science and Engineering, 2013, 33(4): 419-427
[20] Y.C. Huang. One Reliability Assessment Methodology of Functional Safety digital Control System for Nuclear Power Plant Based on Markov Modeling [D]. Shanghai Jiao Tong University, 2015

[21] Q. Zhang, Q. Ma, B. Xu, Y, Peng. Safety Level of Nuclear Power Plant DCS Based on Markov Functional Safety Analysis [J]. INSTRUMENTATION, 2016, 23: 76-81

[22] L.Y. Wu, Q. Ma, B. Xu, Q, Zhang. Study on Availability of Nuclear Power Security DCS Based on Markov [J]. INSTRUMENTATION, 2017, 24: 61-65

[23] Walker M., Yiannis, Papadopoulos, Qualitative temporal analysis: Towards a full implementation of the Fault Tree Handbook [J]. Control Engineering Practice, 2009, 17: 1115–1125.

[24] M.O. Locks, Synthesis of fault trees: an example of non-coherence. IEEE Transactions on Reliability, 1979, 28: 12–15.

[25] Y.D. Shu, J.S. Zhao, A simplified Markov-based approach for safety integrity level verification [J]. Journal of Loss Prevention in the Process Industries, 2014, 29: 262-266.

[26] NEA/CSNI/R (2009)18 Recommendations on Assessing Digital System Reliability in Probabilistic Risk Assessments of Nuclear Power Plants [R]. Nuclear Energy Agency/Committee on the Safety of Nuclear Installations, 2009.

[27] NKS-230 Guidelines for reliability analysis of digital systems in PSA context [R]. VTT Technical Research Center of Finland, 2010

[28] NUREG/CR-6465 Development of Tools for safety Analysis of Control Software in Advanced Reactors [R]. U.S. Nuclear Regulatory Commission, 1996.

[29] P. McNelles, L.X. Lu, M.A. Jaoude, Dynamic Flowgraph Methodology Assessment of an FPGA-Based Postaccident Monitoring System for Westinghouse AP1000 Nuclear Power Plants [J]. Journal of Nuclear Engineering and Radiation Science, 2015

[30] I. Karanta, M. Maskunitty, Reliability of digital control systems in nuclear power plants — Modelling the feedwater system [R]. VTT Technical Research Centre of Finland, 2009

[31] C.J. Garrett, S.B. Guarro, G.E. Apostolakis, The Dynamic Flowgraph Methodology for Assessing the Dependability of Embedded Software Systems [J]. IEEE Transactions on Systems, Man. and Cybernetics, 1995(25)5:824-840

[32] X.M. Guo. Research on Reliability Analysis Methods of Digital I&C System for Nuclear Power Plant [D]. Tsinghua University, 2011

[33] S.L. Zhou, H. Wang, C. Tian. Dynamic Flowgraph Methodology Used in Reliability Analysis of Digital Instrumentation and Control System in NPP [J]. Nuclear Science and Engineering, 2018, 38: 88-97

[34] J. Yang, Z.B. Wen, Y. Ming, Bidirectional implementation of Markov/CCMT for dynamic reliability analysis with application to digital I&C systems [J]. Reliability Engineering and System Safety, 2019 (185):278–290

[35] T. Aldemir, Computer-aided Markov fault modeling of process control systems [J]. IEEE Transactions on Reliability, 1987, 36: 133–144.

[36] IEEE Std 1633TM-2016 IEEE Recommended Practice on Software Reliability [S], Institute of Electrical and Electronics Engineers, 2016

[37] M.R. Lyu, Editor-in-Chief. Handbook of Software Reliability Engineering [M]. McGraw-Hill, 1996.

[38] S. Yamada, M. Ohba, S. Osaki. S-Shaped Reliability Growth Modeling for Software Error Detection [J]. IEEE Transactions on Reliability, 1983; 32(5): 475- 484.

[39] M. Ohba, M. Kajiyama. Inflection S-Shaped Software Reliability Growth Model [C]. IPS Japan, Proceedings WGSE Meeting, 1983; 28: 144-162.

[40] S. Yamada, S. Osaki. Discrete Software Reliability Growth Models [J]. Applied Stochastic Models and Data Analysis, 1985; 1(1): 65-77.

[41] C. Stringfellow, A. Andrews, An Empirical Method for Selecting Software Reliability Growth Models [J]. Empirical Software Engineering, 2002, pp. 319 – 343
[42] H.S. Son, H.G. Kang, S.C. Chang. Procedure for Application of Software Reliability Growth Models to NPP PSA [J]. Nuclear Engineering and Technology, 2009, 41(8): 1065-107
[43] R.S. Pressman, Software Engineering, A Practitioner’s Approach [R]. McGraw-Hill Higher Education, 2001.
[44] J. May, G. Hughes, A.D. Lunn, Reliability Estimation from Appropriate Testing of Plant Protection Software [J]. Software Engineering Journal, 1995.
[45] P. Haapanen, J. Korhonen, U. Pulkkinen, Licensing Process for Safety-Critical Software-Based Systems [R]. Radiation and Nuclear Safety Authority (STUK), Finland, 2000.
[46] NUREG/CR-7044 Development of Quantitative Software Reliability Models for Digital Protection Systems of Nuclear Power Plants [R]. U.S. Nuclear Regulatory Commission, 2013
[47] NUREG/CR-7234 Development of A Statistical Testing Approach for Quantifying Safety-Related Digital System on Demand Failure Probability [R]. U.S. Nuclear Regulatory Commission, 2017
[48] B. Littlewood, J. L. Verall, A Bayesian reliability growth model for computer software [J]. Applied Statistics, 1973, 22(3): 332–346
[49] B. Littlewood, D. Wright. The use of Multilegged Arguments to increase Confidence in Safety Claims for Software based Systems: A Study based on a BBN Analysis of an Idealized Example [J]. IEEE Transactions on Software Engineering, 2007, 33(5)
[50] B.A. Gran, Assessment of Programmable Systems Using Bayesian Belief Nets [J]. Safety Science, 2002, 40, pp. 797-812
[51] A. Helminen, Case Study on Bayesian Reliability Estimation of Software Design of Motor Protection Relay [J]. SAFECOMP, 2007, pp. 384-396
[52] NUREG/CR-7233 Developing a Bayesian Belief Network Model for Quantifying the Probability of Software Failure of a Protection System [R]. U.S. Nuclear Regulatory Commission, 2018
[53] A.M. Neufelder, How to Predict Software Defect Density during Proposal Phase [C]. Proceedings of the IEEE 2000 National Aerospace and Electronics Conference, 2000
[54] NUREG/CR-0019 Software Engineering Measures for Predicting Software Reliability in Safety Critical Digital Systems [R]. U.S. Nuclear Regulatory Commission, 2000
[55] NUREG/CR-6848 Preliminary Validation of a Methodology for Assessing Software Quality [R]. U.S. Nuclear Regulatory Commission, 2004
[56] NUREG/CR-7042 A Large-Scale Validation of a Methodology for Assessing Software Reliability [R]. U.S. Nuclear Regulatory Commission, 2011
[57] IEC 61508 Function Safety of Electrical/Electronic/Programmable Safety-Related Systems [S]. International Electrotechnical Commission, 2005
[58] NUREG/CR-6690 The Effects of Interface Management Tasks on Crew Performance and Safety in Complex, Computer-Based Systems: Overview and Main Findings [R]. U.S. Nuclear Regulatory Commission, 2002
[59] S.J. Lee, J. Kim, S.C. Jang, Human Error Mode Identification for NPP Main Control Room Operations Using Soft Controls [J]. Nuclear Science and Technology, 2011(48):6:902-910
[60] J.A. Julius, P. Moieni, J. Grobbelaar et al. Next Generation Human Reliability Analysis – Addressing Future Needs Today for Digital Control Systems [C]. PSAM12, Probabilistic Safety Assessment and Management Conference, 2014, Hawaii, USA.
[61] E.M. Hicking, J.E. Bowie, Applicability of human reliability assessment methods to human-computer interfaces [J]. Cognition, Technology & Work, 2013(15):19-27
[62] T.X. Feng, J.X. Wei, L.J. Gong, Research on HRA methods and application for digital human-system interfaces design [C]. PSAM12, Probabilistic Safety Assessment and Management Conference, 2014, Hawaii, USA.
[63] I. Jang, A.R. Kim, W. Jung, P.H. et al. A Framework of Human Reliability Analysis Method Considering Soft Control in Digital Main Control Rooms [C]. 16th International Conference
on Human-Computer Interaction, 2014, Heraklion, Greece

[64] M. Liinasuo, M. Porthin. Updating Human Reliability Analysis - insights from Human Factors oriented control room validation [R]. VTT Technical Research Center of Finland, 2015

[65] R.L. Boring, Human Reliability Analysis for Digital Human-Machine Interfaces: A Wish List for Future Research [C]. PSAM12, Probabilistic Safety Assessment and Management Conference, 2014, Hawaii, USA