An integrated platform for dynamic reliability analysis in Living PSA context

Jun Yang[1)], Wanqing Chen[2)], Chenyu Jiang[3)], Ming Yang[4)]

1) School of Electric Power Engineering, South China University of Technology, 381 Wushan Road, Guangzhou, 510641, China (youngjun51@hotmail.com)
2) China Ship Development and Design Center, 268 Zhangzhidong Road, Wuhan, 430064, China (569108969@qq.com)
3) School of Electric Power Engineering, South China University of Technology, 381 Wushan Road, Guangzhou, 510641, China (jcy14788@outlook.com)
4) College of Physics and Optoelectronic Engineering, Shenzhen University, 3688 Nanhai Road, Shenzhen, 518061, China (mingyang@szu.edu.cn)

***Abstract*—In this paper, we present an integration platform for dynamic reliability and probabilistic risk analysis. The platform consists of four key components: i) simulation-based fault injection analytics providing a new paradigm for determination of probabilistic mapping scheme based on the execution traces of the system dynamic characteristics; ii) a matrix-based infrastructure which supports unsupervised learning on Markov/CCMT modeling and updating; iii) an enhanced hybrid compute engine implementing for dynamic reliability analysis with additional consideration of the interactions among systems and phased mission problems; iv) a success-oriented safety monitor facilitating system configuration management and online risk monitoring. The integrated dynamic reliability, risk and safety management platform is developed in JAVA and MATLAB/Simulink environment. Finally, risk-informed decision support is envisioned with the Living PSA integration and platform optimization.**

***Keywords*—dynamic reliability analysis; phased-mission problem; Living PSA; Markov/CCMT; GO-FLOW**

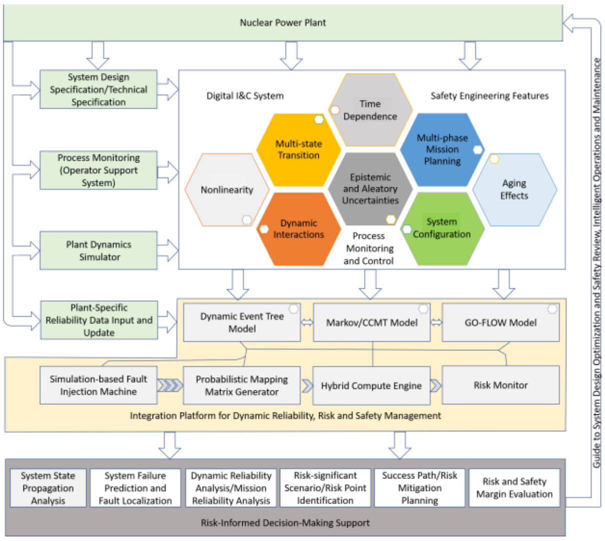
I. INTRODUCTION

Today, digital transformation becomes a hot topic covering for almost every field of industrial applications, even for the safety critical industries such as energy systems, aerospace and petrochemical engineering, etc.[1]. While the widespread implementation of digital nuclear applications is just starting out due to the conservative safety and security considerations as well as higher safety standards and rigorous safety review process in nuclear industry[2]. The primary reason nuclear power plants refrain from the digitalizing process is the not completely clear behavioral mechanisms involved in embedded system[3]. It is because the Instrumentation and Control (I&C) systems involving with human interactions work as the neural center of nuclear power plants. Any latent ambiguity and uncertainty must be avoided or removed to an extreme in digital system design and review phase. Another major issue for the delay of digital implementation of I&C systems in nuclear power plants is that the evaluation process is rather complicated due to the features of dynamic interactions, time-dependent problems, loop structures, linear and non-linear aspects as well as uncertainty issues, etc[4]. The credibility of analysis methods and analysis results is not quite enough for reflecting the real-world complex interactive process of digital I&C systems. Consensus on comprehensive analytical methods and tools used for dynamic reliability modeling and analysis of digital systems in Probabilistic Safety Assessment (PSA) context is still lacking[5].

The reliability and risk evaluation of digital systems in nuclear power plants can be traced back to the early 2000s[6]. During the year 2005-2009, Nuclear Regulatory Commission (NRC) conducted a pilot study on the reliability and safety analysis of nuclear digital I&C systems. Thereafter, a series of intensive review and comparative analysis reports[6][7] are conducted and pointed out that the traditional methods are no longer applicable to the dynamic reliability and risk analysis digital control systems due to their complicated dynamic characteristics. The single dynamic method is also commonly limited to a particular problem solving and is difficult to achieve a global solution towards all issues involved in the complex dynamic process control and safety operation. It is therefore research trend is also suggested to focus on the advanced integration techniques for comprehensive safety analysis of digital control systems. The existing mainstream dynamic reliability and risk methods include dynamic fault tree/event tree, Dynamic Flowgraph Methodology (DFM), Markov/Cell-to-Cell-Mapping Technique (Markov/CCMT), Monte Carlo simulation method, Bayesian network, Petri nets, and GO-FLOW methodology, etc[8]. Among them, DFM method and Markov/CCMT method are deemed as the two most promising dynamic methods appropriate for reliability and risk analysis of digital I&C systems[7]. The two approaches of DFM and Markov/CCMT for reliability analysis of digital I&C systems in nuclear power plants are later on in detail compared and discussed with case studies contributing to the regulatory side[9]. An algorithm for deductive implementation of Markov/CCMT is also proposed by the authors for risk-significant system scenario identification[10] and software fault localization[11]. The backtracking algorithm is further applied to the aerospace and automotive domains for identification of risk-significant scenarios to system failure[12]. The algorithm is efficient for one-directional backtracking search analysis, but it could quickly result in numerical catastrophe when handling the calculation of a large-scale matrix of system probabilistic mapping scheme. Meanwhile, how to determine the probabilistic mapping scheme is a task emphasis and difficulty in the implementation of Markov/CCMT analysis, especially for complex nonlinear system. There is also lack of an integration platform to facilitate Markov/CCMT modeling and analysis of dynamic systems. Therefore, an integrated platform augmented with a hybrid compute engine is developed based on Discrete-time Dynamic Event Tree (DDET), Markov/CCMT and GO-FLOW methodology in this study for dynamic reliability, risk and safety management in PSA context. The integrated tool supports for fault injection testing, automatic modeling and learning update, dynamic mission reliability analysis, and risk-based safety management.

The rest of the paper is organized as follows. Section II introduces the overall framework of the integrated dynamic reliability, risk and safety management platform. A simulation-based fault injection machine and a probabilistic mapping matrix generator are discussed in Section III and IV, respectively. The hybrid compute engine aiming for dynamic reliability and risk analysis is developed in Section V. An enhanced safety monitor is envisioned based on our previous work of risk monitor in Section VI. The conclusions are given in Section VII.

II. Framework of an Integrated Platform for Dynamic Reliability, Risk and Safety Management



Nuclear Power Plant
System Design Specification/Technical Specification
Process Monitoring (Operator Support System)
Plant Dynamics Simulator
Plant-Specific Reliability Data Input and Update
Digital I&C System
Safety Engineering Features
Time Dependence
Multi-state Transition
Multi-phase Mission Planning
Nonlinearity
Epistemic and Aleatory Uncertainties
Aging Effects
Dynamic Interactions
Process Monitoring and Control
System Configuration
Dynamic Event Tree Model
Markov/CCMT Model
GO-FLOW Model
Simulation-based Fault Injection Machine
Probabilistic Mapping Matrix Generator
Hybrid Compute Engine
Risk Monitor
Integration Platform for Dynamic Reliability, Risk and Safety Management
System State Propagation Analysis
System Failure Prediction and Fault Localization
Dynamic Reliability Analysis/Mission Reliability Analysis
Risk-significant Scenario/Risk Point Identification
Success Path/Risk Mitigation Planning
Risk and Safety Margin Evaluation
Risk-Informed Decision-Making Support
Guide to System Design Optimization and Safety Review, Intelligent Operations and Maintenance

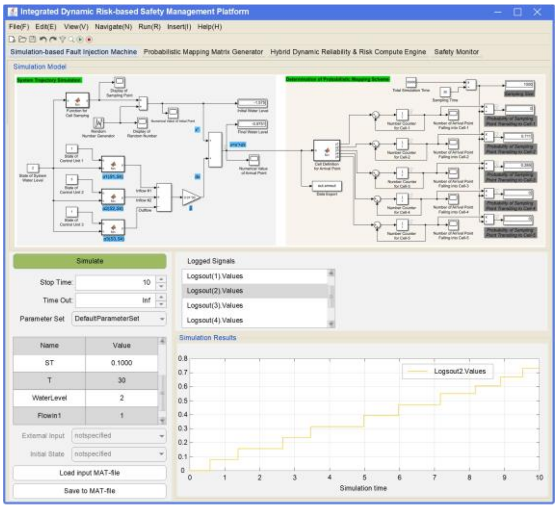
Fig. 1 Framework of the integrated platform for dynamic reliability, risk and safety management

The framework of dynamic reliability, risk and safety management platform is shown in Fig.1. The framework is tailored for comprehensive accident causation and safety management by integrating the extended dynamic PSA with risk assessment of digital I&C systems. The complex features of digital I&C systems involved in the process monitoring and control such as nonlinearity, multi-state transition, dynamic interactions, time dependence, epistemic aleatory uncertainties, multi-phase mission planning, system configuration changes and aging effects etc. are difficult to be described and characterized by one single method and model. It is therefore an integration approach that combines the discrete-time dynamic event tree model (DDET)[13], Markov/CCMT model[14], and GO-FLOW model[15] is developed within the platform for facilitating simulation-based fault injection testing, automatic modeling and unsupervised learning to probabilistic mapping matrix scheme of process interactions involved with digital I&C systems as well as for providing a powerful hybrid compute engine in support of Living PSA applications and risk monitor in nuclear power plants. The aforementioned plant behavioral characteristics can be elaborated from either system design specification/technical specification, process monitoring facilitated by operator support system in main control room, or plant dynamics simulator, or combinations of the above. The overall PSA models are organized in separate divisions, where each focuses on different aspects of risk assessment. The DDET model is applied to accident sequence precursor analysis, where the headers representing system function failure can be further explicitly modeled by Markov/CCMT or GO-FLOW method. To be more specific, the dynamic process interaction involved with failure of digital I&C systems are modeled by Markov/CCMT. The various analytical applications including dynamic process reliability analysis, system state propagation analysis, system failure prediction and fault localization, risk-significant scenario/risk point identification, etc. of digital I&C systems can be done with Markov/CCMT model. The multi-phase mission of safety engineering features with frequent system configuration changes and aging effects in accident mitigation can be taken into account in GO-FLOW models. In addition, success path or risk mitigation planning can be carried out based on the identification of minimum path set in time series by GO-FLOW method. The safety margins obtained for risk investigations in an integrated solution are used as essential inputs to support risk-informed decision-making process for guiding system design optimization and safety review, intelligent operation and maintenance activities. The key components of platform for dynamic reliability, risk and safety management include 1) simulation-based fault injection machine; 2) probabilistic mapping matrix generator; 3) hybrid compute engine; 4) living PSA and risk monitor, which will be discussed in the following Sections.

III. Simulation-based Fault Injeciton Machine

On one hand, the fault injection machine is tailored for exploring the operation and failure mechanisms of digital I&C systems, of which the complex nonlinear and uncertain system dynamic behaviors are usually difficult to capture by analytical methods. On the other hand, the problem of obtaining exact integration equations for representation of non-linear aspects of system dynamics can also be effectively addressed by the simulation-based fault injection testing with Monte Carlo sampling and path tracing. The model-implemented fault injection can be integrated into the simulation of digital I&C systems in either MATLAB/Simulink or LabVIEW modeling and simulation environment. The simulation-based fault injection machine developed in MATLAB/Simulink environment is shown in Fig. 2.

In order to obtain the probabilistic mapping scheme for Markov/CCMT analysis in an efficient way, an equal-weight quadrature scheme is proposed as an alternative solution to continuous integration within the framework of simulation-based fault injection. It has been validated by our previous studies[11] the simulation-based testing results approximated by equal-weight quadrature scheme are getting closer to the exact analytical solution when enough more trials are performed. For modeling stochastic behaviors in simulation digital I&C systems, the continuous process variables are discretized and abstracted as cell points randomly distributed in the system state space under given component configurations. The mathematical functions and operation of complex process control systems can be estimated and mimicked through random sampling and statistical modeling. These cell points will be sampled with a random selection from the input probability distribution for the whole system state space and simulated for trajectory generation so as to uncover the phenomenon tied to system dynamics. The automatic generation and update of probabilistic mapping scheme is readily to implement with the Monte Carlo simulation-based fault injection machine.


Integrated Dynamic Risk-based Safety Management Platform
File(F) Edit(E) View(V) Navigate(N) Run(R) Insert(I) Help(H)
Simulation-based Fault Injection Machine
Probabilistic Mapping Matrix Generator
Hybrid Dynamic Reliability & Risk Compute Engine
Safety Monitor
Simulation Model
System Trajectory Simulation
Determination of Probabilistic Mapping Scheme
Simulate
Logged Signals
Simulation Results
Logsout2.Values
Simulation time
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
1
2
3
4
5
6
7
8
9
10
Load input MAT-file
Save to MAT-file

Stop Time: 10

Time Out: Inf

Parameter Set: DefaultParameterSet

Name	Value
ST	0.1000
T	30
WaterLevel	2
Flowin1	1

External Input: notspecified

Initial State: notspecified

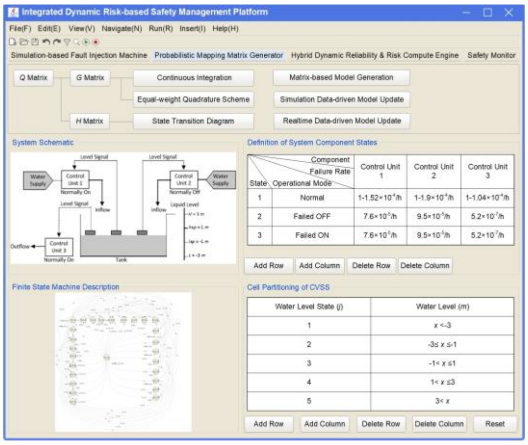
Logsout(1).Values
Logsout(2).Values
Logsout(3).Values
Logsout(4).Values

Fig. 2 Simulation-based fault injection machine

IV. PROBABILISTIC MAPPING MATRIX GENEAROR

Based on the Monte Carlo simulation process for system dynamic trajectories tracing, the conditional probability mapping relations of system state transitions can be obtained from the statistical tests. A probabilistic mapping scheme generator implemented with a matrix-based infrastructure is further developed to facilitate the process for automatic modeling and update of Markov/CCMT model. The probabilities of system state transitions are mapped and coded into matrices so as to improve the search efficiency among system state space.

As shown in Fig. 3, the Markov/CCMT model of system dynamic interactions under epistemic and aleatory uncertainties (Q matrix) is consisted of two coupling parts: Markov chain of state transitions among physical components (H matrix) and CCMT model representation of system dynamic behaviors under given physical component configurations (G matrix). The H matrix of Markov transition probability mapping relations can be determined from state transition diagram, which is usually elicited from Failure Modes and Effects Analysis (FMEA) and Finite State Machine (FSM) description. The G matrix of cell-to-cell transition probability mapping relations can be generated by continuous integration on the exact mathematical models or estimated by the simulation-based equal-weight quadrature scheme described above in the case of that the exact integral equations are difficult to obtain for complex non-linear process control systems. Meanwhile, the probabilistic mapping matrix generator supports both simulation data-driven model update and real-time data-driven model update in accordance with the different sources of input data.


Integrated Dynamic Risk-based Safety Management Platform
File(F) Edit(E) View(V) Navigate(N) Run(R) Insert(I) Help(H)
Simulation-based Fault Injection Machine
Probabilistic Mapping Matrix Generator
Hybrid Dynamic Reliability & Risk Compute Engine
Safety Monitor
Q Matrix
G Matrix
H Matrix
Continuous Integration
Equal-weight Quadrature Scheme
State Transition Diagram
Matrix-based Model Generation
Simulation Data-driven Model Update
Realtime Data-driven Model Update
System Schematic
Water Supply
Control Unit 1
Control Unit 2
Control Unit 3
Level Signal
Inflow
Outflow
Tank
Finite State Machine Description
Add Row
Add Column
Delete Row
Delete Column
Reset

Definition of System Component States

State	Operational Mode	Control Unit 1	Control Unit 2	Control Unit 3
1	Normal	1-1.52×10^{-4}/h	1-1.9×10^{-4}/h	1-1.04×10^{-4}/h
2	Failed OFF	7.6×10^{-5}/h	9.5×10^{-5}/h	5.2×10^{-7}/h
3	Failed ON	7.6×10^{-5}/h	9.5×10^{-5}/h	5.2×10^{-7}/h

Cell Partitioning of CVSS

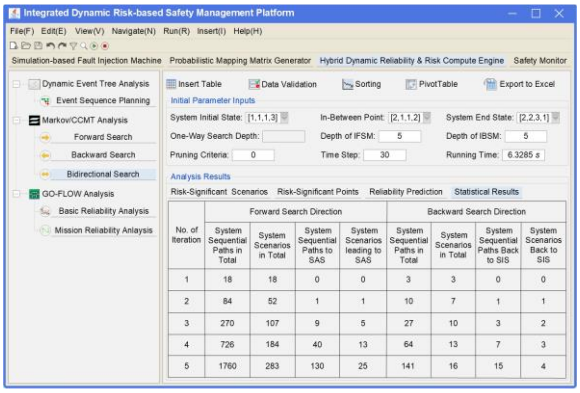
Water Level State (j)	Water Level (m)
1	x <-3
2	-3≤ x ≤-1
3	-1< x ≤1
4	1< x ≤3
5	3< x

Fig. 3 Probabilistic mapping matrix generator

The functional segmentation of matrix generator, system schematic view, finite state machine description, definition of system physical component states, and cell partitioning of Continuous Variable State Space (CVSS) endowed in the visual display design of probabilistic mapping matrix generator can effectively assist analyst in Markov/CCMT modeling and validation.

V. HYBRID DYNAMIC RELIABLITY COMPUTE ENGINE

In this Section, a hybrid dynamic reliability and risk compute engine based on the integration of DDET, Markov/CCMT and GO-FLOW method is presented for comprehensive risk and safety assessment of the whole safety barriers of failure prevention, process monitoring, abnormality control, accident mitigation, and emergency response management. Fig. 4 shows the user interface for hybrid compute engine.


Integrated Dynamic Risk-based Safety Management Platform
File(F) Edit(E) View(V) Navigate(N) Run(R) Insert(I) Help(H)
Simulation-based Fault Injection Machine
Probabilistic Mapping Matrix Generator
Hybrid Dynamic Reliability & Risk Compute Engine
Safety Monitor
Dynamic Event Tree Analysis
Event Sequence Planning
Markov/CCMT Analysis
Forward Search
Backward Search
Bidirectional Search
GO-FLOW Analysis
Basic Reliability Analysis
Mission Reliability Anlaysis
Insert Table
Data Validation
Sorting
PivotTable
Export to Excel
Risk-Significant Scenarios
Risk-Significant Points
Reliability Prediction
Statistical Results

Initial Parameter Inputs

System Initial State: [1,1,1,3] In-Between Point: [2,1,1,2] System End State: [2,2,3,1]

One-Way Search Depth: Depth of IFSM: 5 Depth of IBSM: 5

Pruning Criteria: 0 Time Step: 30 Running Time: 6.3285 s

Analysis Results

No. of Iteration	Forward Search Direction				Backward Search Direction			
	System Sequential Paths in Total	System Scenarios in Total	System Sequential Paths to SAS	System Scenarios leading to SAS	System Sequential Paths in Total	System Scenarios in Total	System Sequential Paths Back to SIS	System Scenarios Back to SIS
1	18	18	0	0	3	3	0	0
2	84	52	1	1	10	7	1	1
3	270	107	9	5	27	10	3	2
4	726	184	40	13	64	13	7	3
5	1760	283	130	25	141	16	15	4

Fig. 4 Hybrid compute engine

As shown in Fig. 4, The hybrid compute engine combines a dynamic event planning algorithm, a multiway Markov/CCMT search algorithm and an optimized GO-FLOW algorithm, which aims at expanding solutions to dynamic reliability and probabilistic risk assessment problems. The DDET planning algorithm is mainly concerned with the evolution of event scenario in PSA context. The versatile Markov/CCMT search algorithm is capable of multi-direction search analysis such as forward search, backtracking and bidirectional implementation with analytic applications covering dynamic reliability quantification, risk significant scenario identification, fault localization and system state propagation analysis, etc. The optimized GO-FLOW algorithm implemented with flexible computation (cut-off criterion) on time-dependent mission reliability of safety engineering systems is able to provide better support for Living PSA and risk monitor applications in nuclear power plants.

VI. Safety monitor

An enhanced safety monitor is envisioned based on our previous work[16] in risk monitor using the optimized GO-FLOW method, which is shown in Fig. 5.

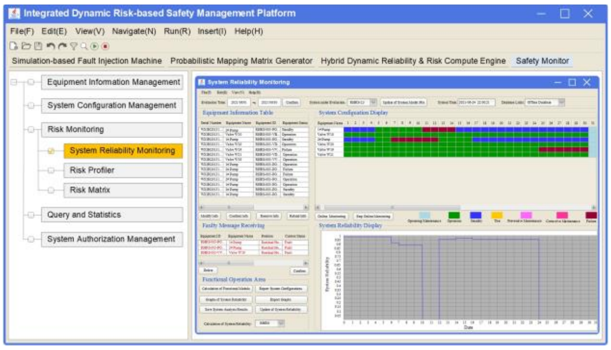

Integrated Dynamic Risk-based Safety Management Platform
File(F) Edit(E) View(V) Navigate(N) Run(R) Insert(I) Help(H)
Simulation-based Fault Injection Machine
Probabilistic Mapping Matrix Generator
Hybrid Dynamic Reliability & Risk Compute Engine
Safety Monitor
Equipment Information Management
System Configuration Management
Risk Monitoring
System Reliability Monitoring
Risk Profiler
Risk Matrix
Query and Statistics
System Authorization Management
System Reliability Monitoring
Equipment Information Table
System Configuration Display
Faulty Message Receiving
System Reliability Display
Functional Operation Area
System Reliability
Date

Fig. 5 Safety monitor

The infrastructure of our previous risk monitor includes basic functional modules for equipment information management, system configuration management, risk monitoring, query and statistics, system authorization management. In the newly integrated safety monitor, some new features such as human-centered operation feasibility analysis as well as operation supervision and audit are also incorporated into the risk-informed operation and maintenance framework to build a more powerful tool. The impacts of failure of digital I&C systems on plant risk and safety are also being considered to extend the scope of existing PSA for providing better decision-making support.

VII. Conclusions

In this paper, an integrated platform for dynamic reliability, risk and safety management of nuclear power plants is presented. The systematic risk analysis process including system dynamics modeling and simulation, dynamic reliability and risk assessment, risk management is implemented based on the integration of DDET, Markov/CCMT and GO-FLOW method within the integrated platform. The integration platform boosting with these kernel algorithms can be effectively extended in high-performance applications towards dynamic risk control and safety management in nuclear power plants.

Acknowledgement

This work was supported by the Guangdong Basic and Applied Basic Research Foundation under No. 2019B1515120060 and No. 2019A1515111124.

References

[1] P. C. Verhoef, T. Broekhuizen, Y. Bart, et al., Digital transformation: a multidisciplinary reflection and research agenda, *Journal of Business Research*, vol. 122, pp.889-901, 2021.

[2] S. A. Arndt, Regulatory oversight of nuclear power plant digital technology use. Nuclear News, February 2015.

[3] M. D. Muhlheim, W. P. Poore, A. M. Nack, et al., Developing a technical basis for embedded digital devices and emerging technologies, NUREG/CR-7273, 2021.

[4] IAEA, Design of instrumentation and control systems for nuclear power plants, Specific Safety Guide, No. SSG-39, 2016.

[5] S. Authen, K. Bjorkman, J. E. Holmberg, et al., Guidelines for reliability analysis of digital systems in PSA context-Phase 1 status report. NKS-230, 2010.

[6] T. Aldemir, D. W. Miller, M. P. Stovsky, et al., Current state of reliability modeling methodologies for digital systems and their acceptance criteria for nuclear power assessments. NUREG/CR-6901, 2006.

[7] T. Aldemir, M. P. Stovsky, J. Kirschenbaum, et al., Dynamic reliability modeling of digital instrumentation and control systems for nuclear reactor probabilistic risk assessments. NUREG/CR-6942, 2007.

[8] E. Zio, Reliability engineering: old problems and new challenges. *Reliability Engineering and System Safety*, vol. 94, pp.125-141, 2009.

[9] T. Aldemir, S. Guarro, D. Mandelli, et al., Probabilistic risk assessment modeling of digital instrumentation and control systems using two dynamic methodologies. *Reliability Engineering and System Safety*, vol. 95, pp.1011-1039, 2010.

[10] J. Yang, T. Aldemir, An algorithm for the computationally efficient deductive implementation of the Markov/Cell-to-Cell-Mapping technique for risk significant scenario identification. *Reliability Engineering and System Safety*, vol. 145, pp. 1-8, 2016.

[11] J. Yang, T. Aldemir, C. Smidts, A deductive method for diagnostic analysis of digital instrumentation and control systems. *IEEE Transactions on Reliability*, vol. 67(4), pp.1442-1458, 2018.

[12] M. Hejase, A. Kurt, U. Ozguner, et al., Identification of risk significant automotive scenarios under hardware failures. Proceedings of the 2nd International Workshop on Safe Control of Autonomous Vehicles (SCAV 2018), Porto, Portugal, April 2018.

[13] A. Alfonsi, C. Rabiti, D. Mandelli, et al., Dynamic event tree analysis through RAVEN. Proceedings of ANS PSA 2013 International Topical Meeting on Probabilistic Safety Assessment and Analysis, Columbia, SC. September 22-26, 2013.

[14] T. Aldemir, Computer-assisted Markov failure modeling of process control systems. *IEEE Transactions on Reliability*, vol. 36, pp. 133-44, 1987.

[15] T. Matsuoka, M. Kobayashi, GO-FLOW: a new reliability analysis methodology. *Nuclear Science and Technology*, vol. 98(1), pp. 64-78, 1988.

[16] J. Yang, M. Yang, H. Yoshikawa, et al., Development of a risk monitoring system for nuclear power plants based on GO-FLOW methodology. *Nuclear Engineering and Design*. vol. 278, pp. 255–267, 2014.