 doi:10.20944/preprints202208.0254.v1

Article

Dynamic Reliability Analysis of Level Control System of Steam Generator based on BDMP

Tian-Mi Zhou [1,*], Di-Liang Li [1], Feng Qin [1], Lin-Lu Xia [2], Xi-Yu Chen [2] and Shi-Liang Zhou [2,3,*]

[1] Research Institute of Nuclear Power Operation, Wuhan, 430223, China
[2] North China Electric Power University, Beijing, 102206, China
[3] Beijing Key Laboratory of Passive Nuclear Safety Technology, Beijing, 102206, China
*Corresponding author: zhoutm@cnnp.com.cn (T.-M. Zhou); zhoushiliang@ncepu.edu.cn(S.-L. Zhou)

Abstract: Steam Generator Level Control System (SGLCS) is one of the key instrumentations and control subsystems to ensure the safe operation of nuclear power plants. It is highly recommended to perform reliability analysis for SGLCS for making better maintenance strategy. SGLCS is a digital control system with complex redundant configuration and failure\self-diagnosis\repair action, traditional fault tree is not applicable due to its static property, Markov model is not a good choice too because of heavy burden of creating state transition graph for even medium-size system. Boolean Logic Driven Markov Process (BDMP) can describe complex failure-repair state transition via 'trigger link' and three kinds of leaf nodes, as well as keep compact and easy-read struct like fault tree. So BDMP is adopted to analysis reliability of SGLCS. Graphical BDMP modeling environment KB3 and Monte Carlo simulator YAMS is used for BDMP modeling and quantitative analysis respectively, and unavailability of SGLCS is obtained. The contribution of three parts of SGLCS to the unavailability of the system is also evaluated, and it is found that the water supply flow control part contributes the most to the failure of SGLCS.

Keywords: steam generator water level control system; dynamic reliability; Boolean Logic Driven Markov Process; unavailability

1. Introduction

Digital Instrumentation and Control Systems (DICS) are used widely in nuclear power plants (NPP), and reliability of DICS has a significant impact on NPP safety [1]. Steam Generator (SG) is a key equipment of NPP. Keeping water level in reasonable range is necessary to ensure the safe operation of reactor and turbine. Therefore, SGLCS reliability directly affects the safe operation of NPP [2]. It is very difficult if not impossible to describe SGLCS using fault tree, because SGLCS is with many redundancies and repairs.

BDMP is a powerful dynamic reliability modeling formalism which enables the analyst to combine concepts inherited from fault trees and Markov models in a new way. BDMP is not only nearly as simple to use as fault-trees, but also can model systems in which there are strong dependencies between components [3]. BDMP have been widely used in the reliability analysis of various systems in power plants [4], power grids [5] and utilized dynamic security modeling [6].

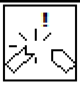
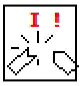
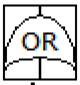
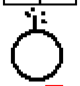
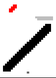
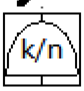
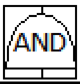
2. Presentation of the BDMP Formalism

The BDMP model is mainly composed of top events, bottom events (leaves), logic gates, trigger links and logic links. The elements of the BDMP model are shown in Table 1. An example of the BDMP model is shown in Fig.1. According to the basic concept of fault tree, the top node (UE_1) in the BDMP model is root node, while the bottom nodes (F_1, F_2, I_1, SF_1) are leaf nodes (leaves). In the BDMP model, the trigger link is from the trigger node to the triggered node. Value, relevant pattern and required pattern are the three most important attributes of each node in the BDMP model, which together

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 August 2022 doi:10.20944/preprints202208.0254.v1

determine the dynamic behavior of the BDMP model. The failure mechanism of each leaf node in the BDMP model is different. Leaf nodes of type f_leaf (F_1, F_2) can fail only when they are in both relevant pattern and required pattern. Leaf nodes of type i_leaf, (I_1) can fail only when the required pattern changes. When leaf nodes of sf_leaf type (SF_1) are in relevant pattern, their required pattern and non-required pattern correspond to two different failure rates [8, 9].

Table 1. Leaves and links in BDMP model.

type	symbols	features
f_leaf		A base event that describes the operation failure of a device. The time of failure is exponentially distributed, and the time of repair is also exponentially distributed
i_leaf		A base event that describes the required failure of a device, which can occur when the operating mode of a device changes (active or standby). This kind of fault can be repaired, and the repair time is distributed exponentially
sf_leaf		A base event that describes the failure of standby equipment. This leaf node has two different failure rates, namely, operation failure rate and standby failure rate. This kind of fault can be repaired, and the repair time is distributed exponentially
or_gate		OR logic gates, execution logic and algorithms
undes_event		Top events of the BDMP model
trigger_link		Trigger link, a logical link with trigger function
logic_link		Logic link, a logical link between different events
k_out_of_n_gate		Voting logic gates (e.g. 3 choose 2,4 choose 1, etc.), execute logic and algorithms
and_gate		AND logic gates, execution logic and algorithms

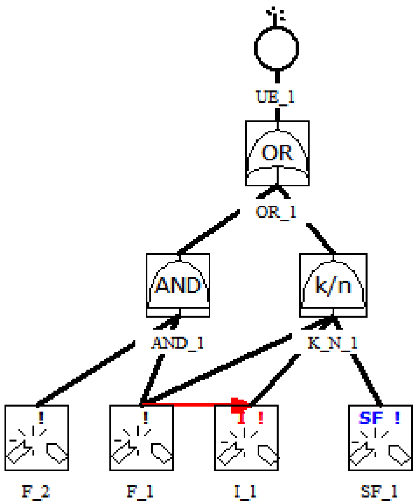


Figure 1. Example of BDMP model diagram.

3. Steam Generator Level Control System

SGLCS is composed of feedwater control system and main feed water pump speed regulation system. The function of the steam generator water level control system are as follows:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 August 2022 doi:10.20944/preprints202208.0254.v1

1. Control feedwater flow to maintain programmed water levels of steam generators, and

2. Control the main feed pump speed to maintain programmed differential pressure of main feed water regulating valve.

3.1. Feedwater control system

The feedwater control system (FWCS) for one SG is shown in Figure 2. Each SG has an identical system. The FWCS uses the following inputs to control the position of main feed water regulating valve:

1) One of two pressure-compensated steam flow channels (selectable),

2) One of two feedwater flow channels (selectable),

3) One of three steam generator water level channel (selectable),

4) A programmed reference water level generated by one of first-stage pressure channels of turbine.

Steam flow signal and feedwater flow signal are compared to produce a flow error signal, which is combined with the level error signal as the input to the feed water regulating valve controller. The flow signals are also compared to provide steam flow/feed flow mismatch alarms.

The water level error signal is equal to deviation between the actual level signal with the reference level. The reference level is generated by turbine first-stage (impulse) pressure. Since impulse pressure is proportional to turbine load, the steam generator reference levels are depend on turbine load.

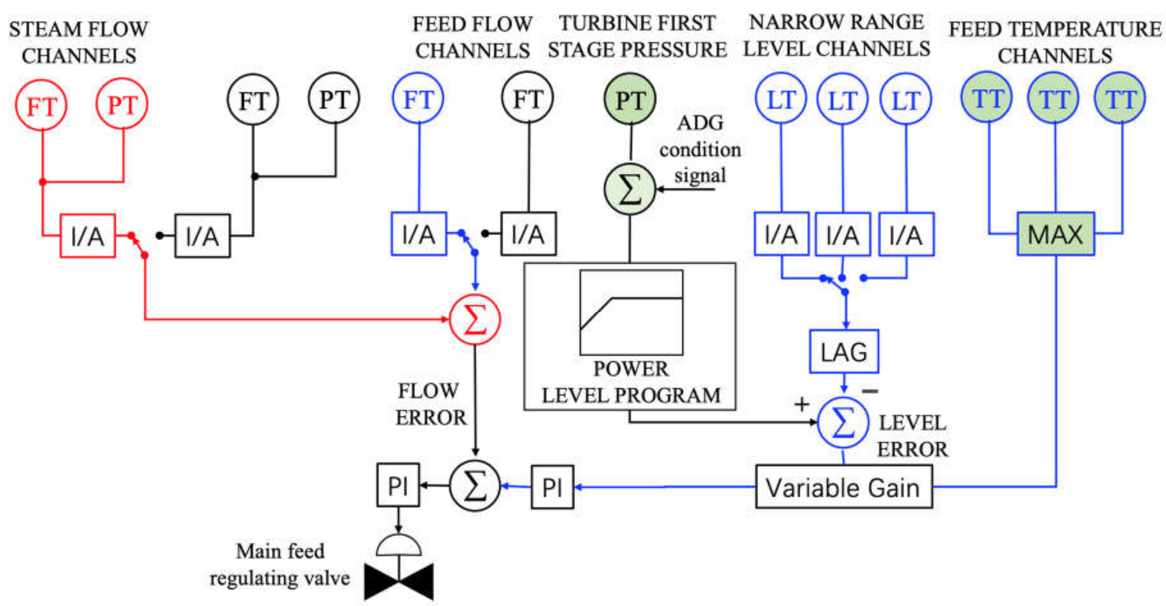


Figure 2. Feedwater control system.

Feedwater control system (FWCS) are consisting by three independent parts and a shared part. Each of three SGs has its own independent part, while three SGs use the same shared part. Independent part control feed water flow by changing position of main feed water regulating valve to regulate water level. The main function of the shared partis is to set water level control gain according to load signal of turbine and maximal value among three main feed water temperatures.

The system structure diagram of shared part and independent part is shown in Fig.4 and Fig.5, respectively.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 August 2022 doi:10.20944/preprints202208.0254.v1

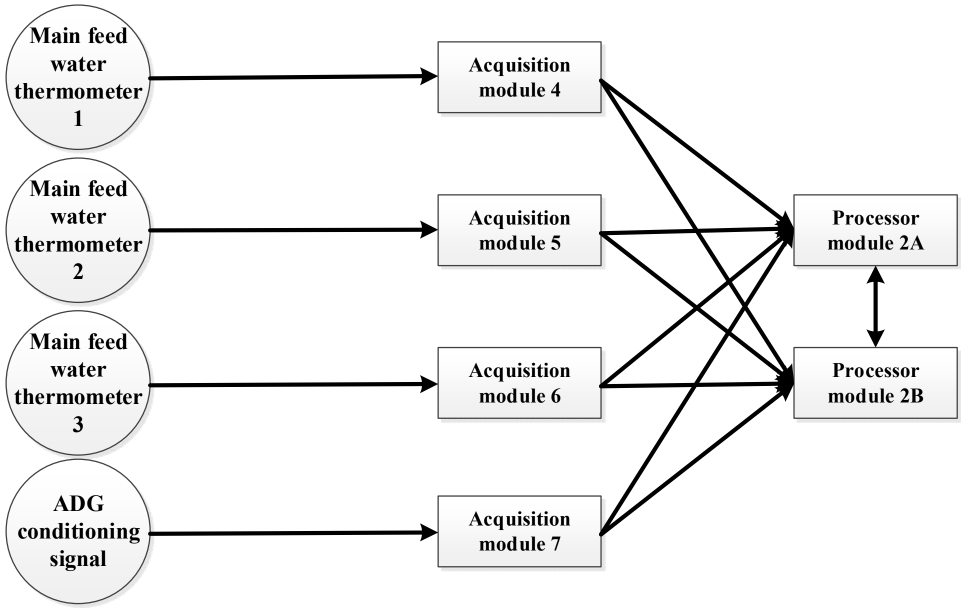


Figure 4. The shared part of feedwater control system.

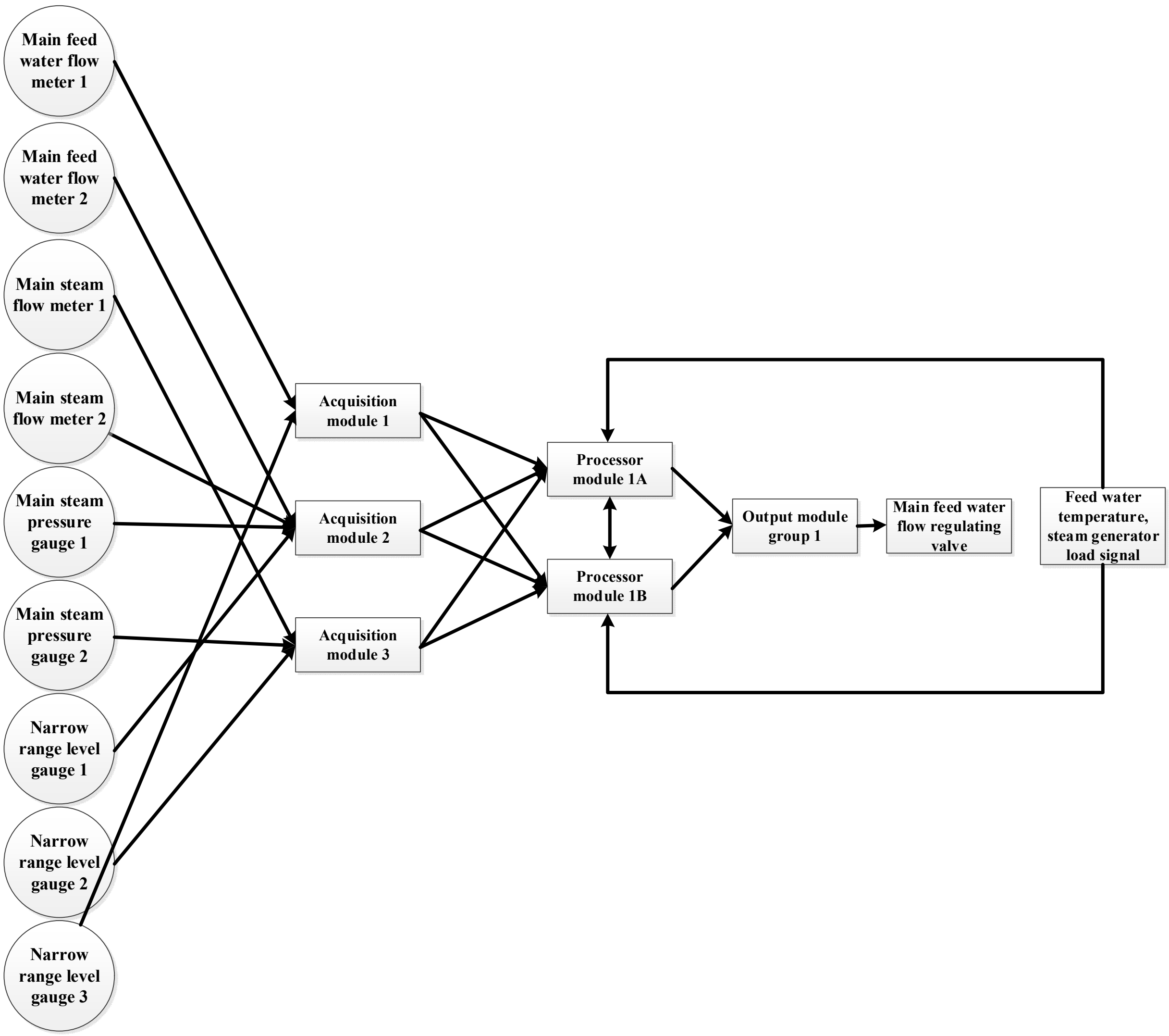
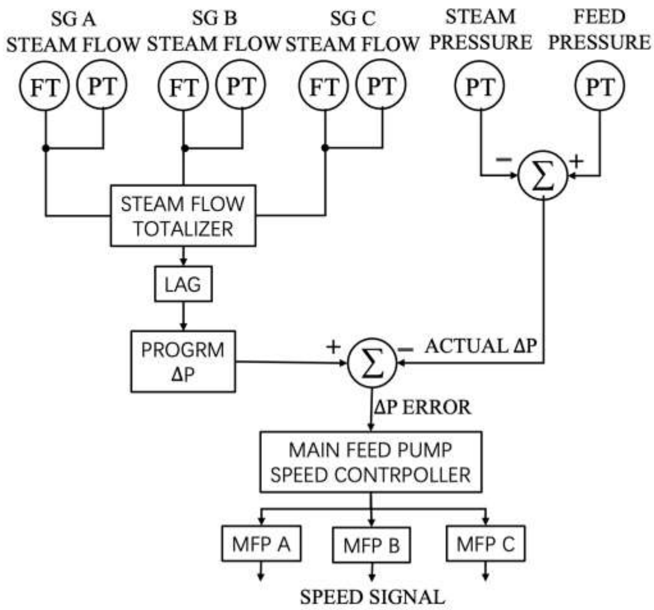


Figure 5. The independent part of feedwater control system.

3.2. Main feed water pump speed regulation system

The main function of main feed water pump speed regulation system is to maintain differential pressure ΔP between main steam pipe and main feed water pipe at a preset value ΔP_{ref}, while ΔP_{ref} increases with the increase in turbine load. The system input is main steam flow signal and mismatch of ΔP and ΔP_{ref}, and the output is the pump speed setting value. Feed water system of a NPP unit is equipped with 3 electric water feed pumps [10], and differential pressure ΔP is measured by three differential pressure gauges.



The system structure diagram of main feed water pump speed regulation system is shown in Fig.6.

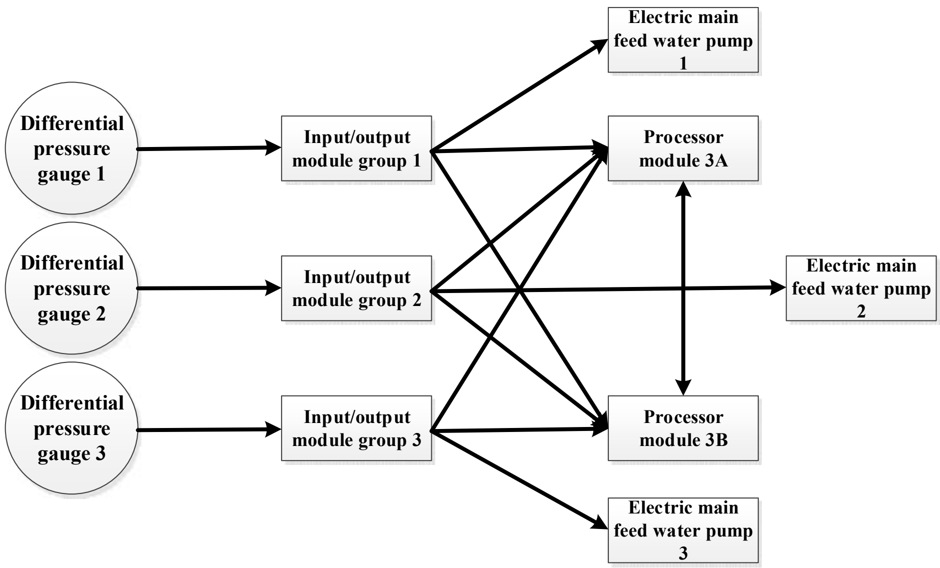


Figure 6. Main feed water pump speed regulation system.

4. BDMP modeling and quantitative analysis

4.1. Modeling assumptions

Ignore system failures due to human error, such as failures caused by operator's mistake.

1) Component failures caused by hardware malfunction or software exception are not treated explicit.
2) Assuming that the power plant is operating under conditions greater than 20% FP, the bypass control valve is fully opened at this time. Ignore the failure of the bypass control valve.

4.2. BDMP model

The BDMP model of independent part, the BDMP model of shared partis and the BDMP model of main feed water pump speed regulation system is shown in Fig.7, Fig.8 and Fig.9 respectively.

Thanks to the BDMP formalism, it is easy to model dynamic features and interactions between components, such as failure-repair, master-standby switchover is formalized; Different type of failures, such as standby failure, required failure and operation failure are indicated by suitable kind of leaf.

Switchover of master and standby CPU, AO modules, AI modules and power modules are modeled by corresponding trigger links (red dashed lines). Standby failures of CPU, AO modules, AI modules and power modules are also described via sf_leaf. Required failure of standby pump is expressed using i_leaf. All faults are repairable, and the repair time is distributed exponentially.

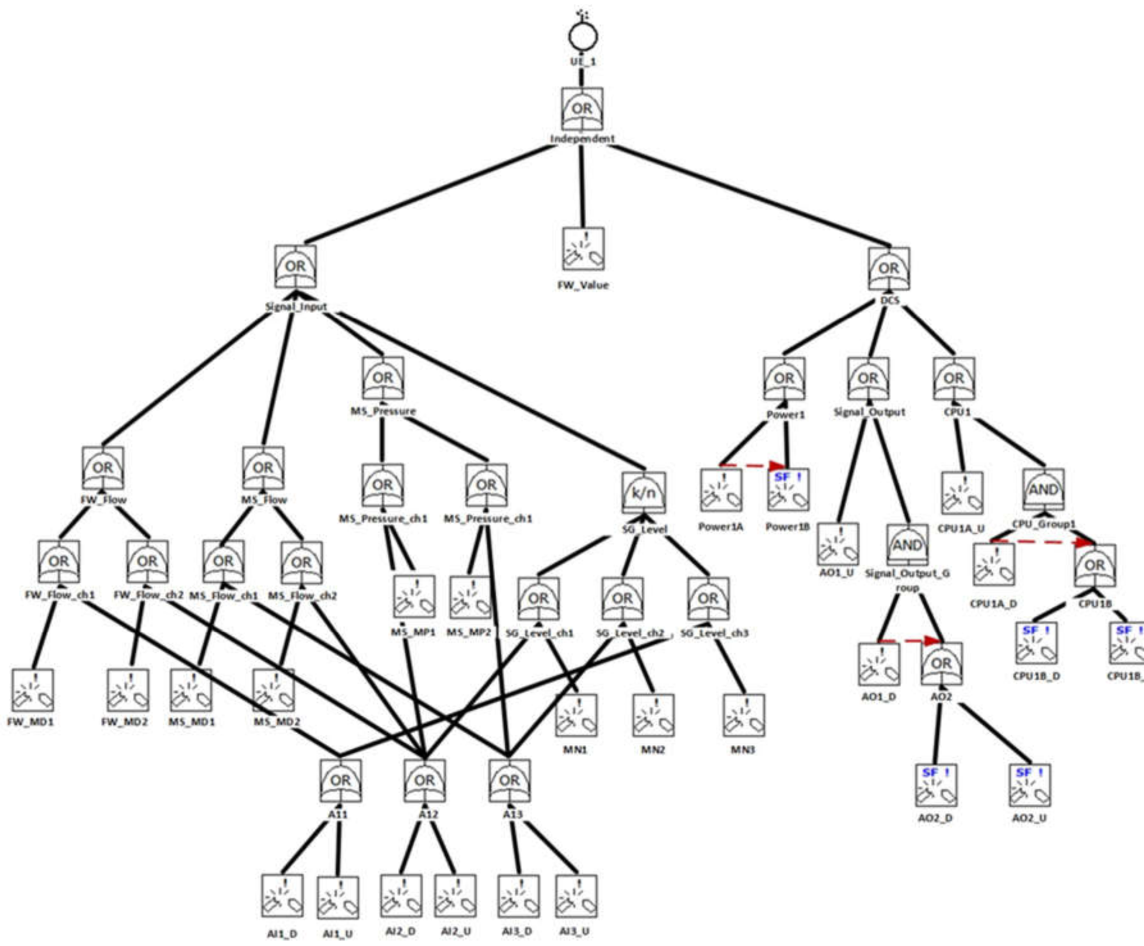


Figure 7. BDMP model of feedwater control system (independent part).

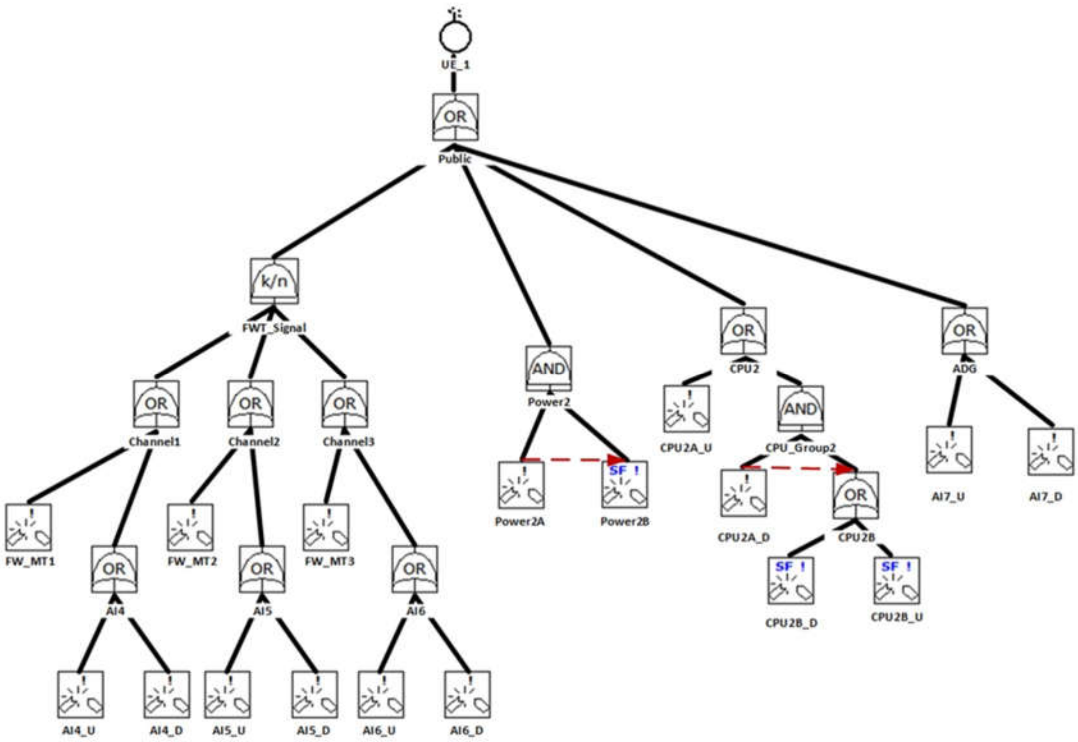


Figure 8. BDMP model of feedwater control system (shared part).

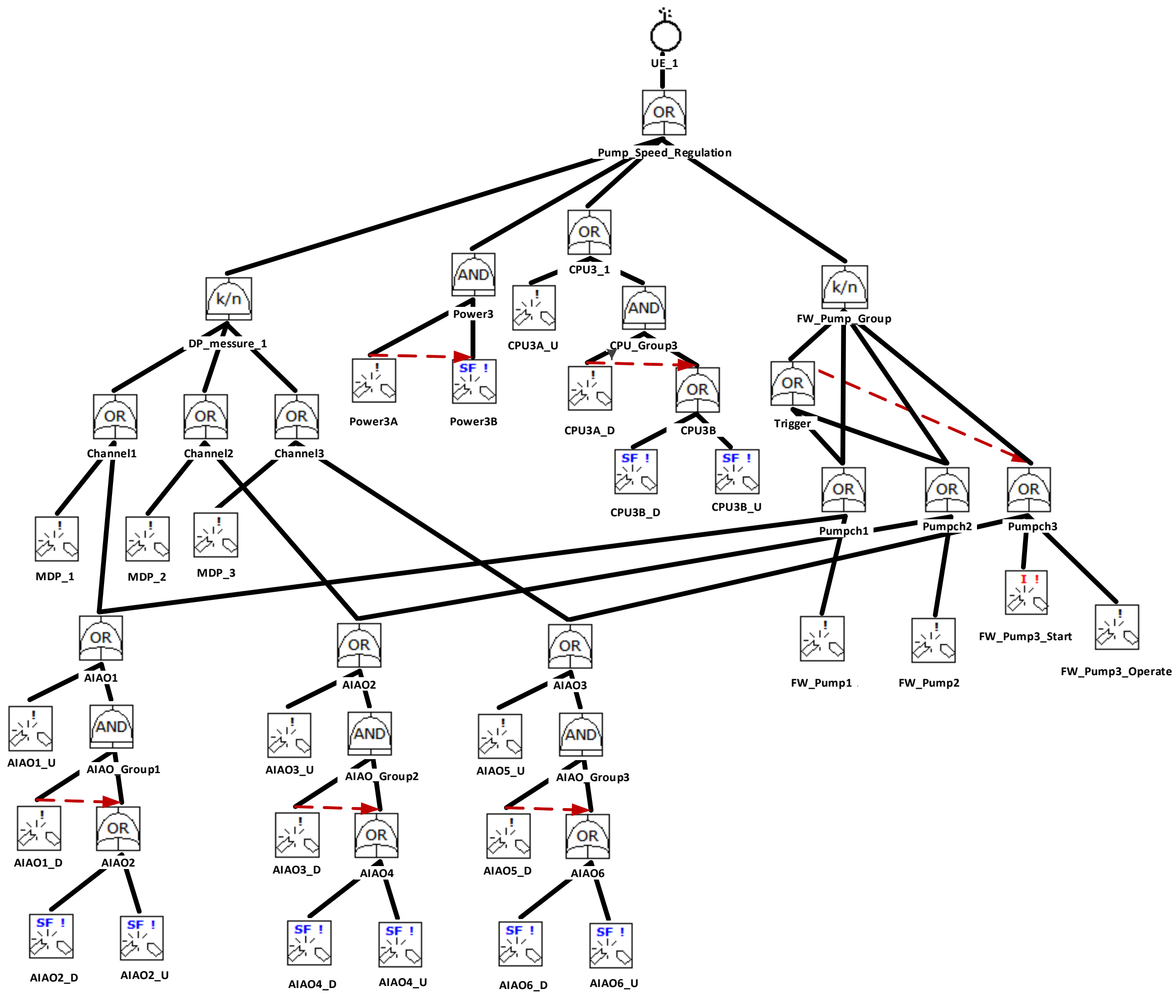


Figure 9. BDMP model of main feed pump speed regulation system.

4.3. Reliability data

The parameters of each leaf node in the BDMP model [11-15] are shown in Table 2

Table 2. Reliability data sheet.

Name	Meaning	Failure Rate λ(1/hour)	Repair rate μ (1/hour)
FW_MD1,FW_MD2	Main feed water flowmeter failure	1.4×10^{-6}	0.5
MS_MD1,MS_MD2	The main steam flowmeter failure	1.4×10^{-6}	0.5
MS_MP1,MS_MP2	Main steam pressure gauge failure	1.4×10^{-6}	0.5
MN1,MN2,MN3	Level gauge failure	1.4×10^{-6}	0.33
FW_MT1,FW_MT2,FW_MT3	Main feed water thermometer failure	1.4×10^{-6}	0.33
MDP_1,MDP_2,MDP_3	Differential pressure gauge failure	1.4×10^{-6}	0.33
AI1_D,AI2_D,AI3_D,AI4_D, AI5_D,AI6_D,AI7_D	Detectable failure of analog input module	3.564×10^{-6}	0.25
AI1_U,AI2_U,AI3_U,AI4_U, AI5_U,AI6_U,AI7_U	Undetectable failure of analog input module	3.6×10^{-8}	1.14×10^{-4}
Power1A,Power2A,Power3A	The A power supply of the redundant power supply group failure	6.5×10^{-7}	0.5
Power1B,Power2B,Power3B	The B power supply of the redundant power supply group failure	Operating failure rate and standby failure rate are both 6.5×10^{-7}	0.5
CPU1A_D,CPU2A_D,CPU3A_D	Detectable failure of the redundant processor module group A	2.772×10^{-7}	0.25
CPU1A_U,CPU2A_U,CPU3A_U	Undetectable failure of the redundant processor module group A	2.8×10^{-9}	1.14×10^{-4}
CPU1B_D,CPU2B_D,CPU3B_D	Detectable failure of the redundant processor module group B	Operating failure rate and standby failure rate are both 2.772×10^{-7}	0.25
CPU1B_U,CPU2B_U,CPU3B_U	Undetectable failure of the redundant processor module group B	Operating failure rate and standby failure rate are both 2.8×10^{-9}	1.14×10^{-4}
AO1_D,AO2_D	Detectable failure of analog output module	6.0489×10^{-7}	0.25
AO1_U,AO2_U	Undetectable failure of analog output module	6.11×10^{-9}	1.14×10^{-4}
AIAO1_D,AIAO2_D,AIAO3_D, AIAO4_D,AIAO5_D,AIAO6_D	Detectable failure of analog input/output module	3.564×10^{-6}	0.25
AIAO1_U,AIAO2_U,AIAO3_U, AIAO4_U,AIAO5_U,AIAO6_U	Undetectable failure of analog input/output module	3.6×10^{-8}	1.14×10^{-4}
FW_Valve	The main feed water flow control valve failure	1.69×10^{-7}	0.083
FW_Pump1,FW_Pump2, FW_Pump3_Operate	Operation failure of the main feed pump	3.48×10^{-6}	0.035
FW_Pump3_Start	Boot failure of the main feed water pump	2.02×10^{-4}	0.035

6. Quantitative analysis and results

Figaro 0 script for BDMP of SGLCS is generated via KB3 [16], and it used as input file of a Monte Carlo simulation tool called YAMS [17] for quantitative analysis. As shown in Fig.10, the YAMS analysis result is 1.45176E-3.

It can be seen from Fig.11 that unavailability of feedwater control system (independent part) accounts for about 73.8% of the unavailability of the entire SGLCS, and the unavailability of feedwater control system (common part) accounts for about 24.4%, and the main feed water speed regulation system is less than 2.0%. The results show that the failure of the feedwater control system is the main cause of the failure of SGLCS in NPPs.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 August 2022 doi:10.20944/preprints202208.0254.v1

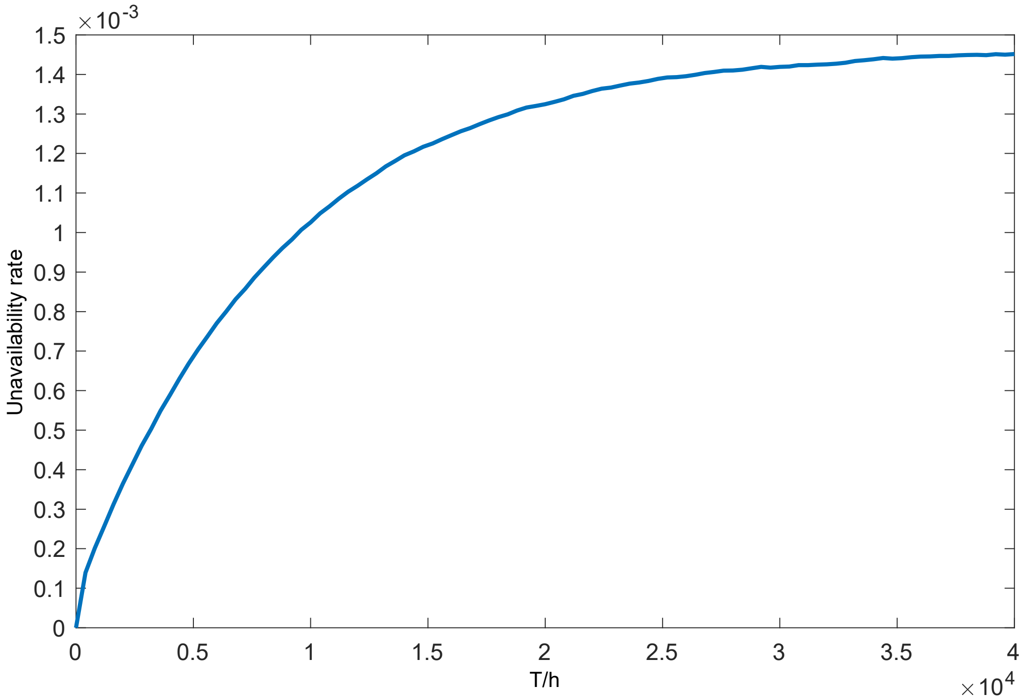


Figure 10. Comparison diagram of unavailable rate of SGLCS.

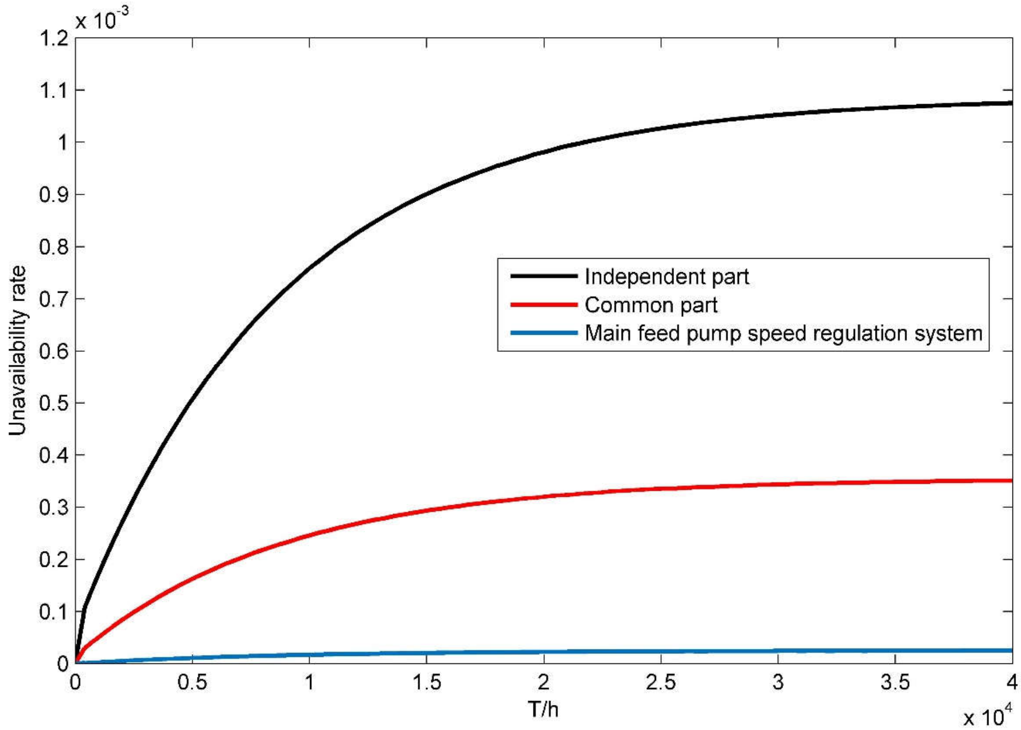


Figure 11. Three-part unavailability diagram of SGLCS.

6. Conclusions

SGLCS is one of large sub-system in digital I&C system of NPP, including more than 35 components, and some components have several failure modes. It's challenge to perform dynamic reliability analysis for SGLCS via traditional dynamic reliability formalization method, such as Markov chain or Petri net. BDMP allows the definition of complex dynamic models while remaining nearly as readable and easy to build, so BDMP is adopted for SGLCS dynamic reliability analysis, It may the first application of BDMP on large digital control system.

BDMP model for SGLCS is built, and unavailability is obtained via YAMS. The failure of feed water flow regulation sub-system (independent part) contributes the most to the unavailability of SGLCS. Operation and maintenance strategies could be refined to improve the reliability of SGLCS.

Acknowledgments: This work was supported by Scientific Research Program for Young Talents of China National Nuclear Corporation (NO.RINPO A180705). The work is also co-funded by Equipment pre-research Key Laboratory Fund project (6142A07200311).

Conflicts of Interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] WANG Hao, YU Jiawei, ZHOU Shiliang, et al. Reliability Assessment for Steam Generator Water Level Control System in NPP Based on BDMP[J]. Atomic Energy Science and Technology, 2017, 51(12): 2330-2337.

[2] Xiang Hongyi, Feng Xiaoxia, Liu Jianguang, Liu Daoguang, Yu Hang, et al. Model Predictive Control for Nuclear Steam Generator Water Level[J]. Science and Technology Innovation Herald, 2017,(14):167-170.

[3] Marc Bouissou, Jean-Louis Bon. A new formalism that combines advantages of fault-trees and Markov models: Boolean logic driven Markov processes. Reliability Engineering & System Safety, 2003, 82(2): 149-163

[4] Bouissou, Marc. "A benchmark on reliability of complex discrete systems: emergency power supply of a nuclear power plant." arXiv preprint arXiv:1703.06575 (2017).

[5] A. I. Sarwat, A. Domijan, M. H. Amini, A. Damnjanovic and A. Moghadasi, Smart Grid reliability assessment utilizing Boolean Driven Markov Process and variable weather conditions. 2015 North American Power Symposium (NAPS), 2015, pp. 1-6.

[6] Piètre-Cambacédès, Ludovic, and Marc Bouissou. "Beyond attack trees: dynamic security modeling with Boolean logic Driven Markov Processes (BDMP)." 2010 European Dependable Computing Conference. IEEE, 2010.

[7] Piètre-Cambacédès L, Bouissou M. Beyond Attack Trees: Dynamic Security Modeling with Boolean Logic Driven Markov Processes (BDMP)[C]// Dependable Computing Conference. IEEE, 2010:199-208.

[8] Kriaa S, Bouissou M, Pietre-Cambacedes L. Modeling the Stuxnet attack with BDMP: Towards more formal risk assessments[C]// International Conference on Risk and Security of Internet and Systems. IEEE, 2012:1-8.

[10] Chen Xiyu. A quantitative analysis method of DCS dynamic reliability based on BDMP [D].Beijing: North China Electric Power University, 2019..

[11] International Atomic Energy Agency. Component Reliability Data for Use in Probabilistic Safety Assessment[M]. Vienna: IAEA, 1988.

[12] Chinese Nuclear Power Plant Equipment Reliability Data Report [R]. Beijing: National Nuclear Safety Administration, 2015.

[13] SINTEF R D. Reliability Data for Safety Instrumented Systems–PDS Data Handbook[J]. Edition, SINTEF A, 2010, 13502.

[14] Qian Hong, Gu Yaqi, Liu Xinjie. Reliability of Digital Pressure Control Device of Nuclear Pressurizer Based on Dynamic Fault Tree[J]. Nuclear Power Engineering, 2019, 40(3): 103.

[15] Mortazavi S M, Mohamadi M, Jouzdani J. MTBF evaluation for 2-out-of-3 redundant repairable systems with common cause and cascade failures considering fuzzy rates for failures and repair: a case study of a centrifugal water pumping system[J]. Journal of Industrial Engineering International, 2018, 14(2): 281-291.

[16] Bouissou, Marc. "Automated dependability analysis of complex systems with the KB3 workbench: the experience of EDF R&D." Proceedings of the international conference on energy and environment. 2005.

[17] Bouissou, Marc. "A simple yet efficient acceleration technique for Monte Carlo simulation." Proceedings of the 22nd European Safety and Reliability Conference (ESREL'13). 2013.