Hindawi
Science and Technology of Nuclear Installations
Volume 2021, Article ID 5529570, 10 pages
https://doi.org/10.1155/2021/5529570

Research Article

The Implementation of Diverse Actuation System in ACPR1000 Nuclear Power Plants

Zhen-Ying Wang, Zhi-Yun Liu, Ting-Wei Ma, Chen Sun, Liu Liu, Yu Huang, and Gang-Miao Guo

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, Shenzhen 518100, China

Correspondence should be addressed to Zhen-Ying Wang; wangzhenying@cgnpc.com.cn

Received 25 January 2021; Revised 26 May 2021; Accepted 24 August 2021; Published 6 September 2021

Academic Editor: Massimo Zucchetti

In order to improve the capability of dealing with software common cause failure (CCF) of digital reactor protection and monitoring system (RPMS), the diverse actuation system (DAS) is introduced for ACPR1000 nuclear power plants. From economic and feasibility point of view, the solution of DAS sharing with RPMS sensors and actuators is suggested; after capturing the function requirement of DAS, the automatic functions and manual functions assigned to it are determined based on transient analysis of design basic accidents concurrent with software CCF of RPMS. The independent verification proves that the reactor can be fallen back to and maintained at safety shutdown state, thanks to these DAS functions. Insight into probabilistic safety assessment proves significant reductions of risks are contributed. The critical technical issues while implementing DAS, such as measures to ensure its diversity from RPMS, precautions for preventing from its spurious actuation, isolation and independency from RPMS, and its testability and maintainability, are deliberately settled to improve its engineering reliability and alleviate the impact on RPMS as far as possible. Field programmable gate array technology that is diversified from RPMS is chosen to build DAS of ACPR1000 nuclear power plant, and the commissioning test verifies that it is capable of performing its designed functions. At last, a set of DAS-specific, paper-based, and event-oriented emergency operating procedure is developed, verified, and validated. Until now, the DAS system has always been successfully operating in all ACPR1000 nuclear power plants for several years.

1. Background

Anticipated transient without scram (ATWS) is one of the accidents that must be considered in design of nuclear power plants. From the causes point of view, there are two types of ATWS: (1) ATWS caused by mechanical block of control rods, which is generally mitigated by emergency boration function; (2) reactor trip breakers fail to open due to failure of reactor protection and monitoring system (RPMS) or failure of reactor trip breakers themselves; generally a diverse actuation system (DAS) is necessary to alleviate the consequences of this kind of ATWS. At present, nearly all newly built nuclear power plants adopt digital control system (DCS), because of its function-centralization, software-sharing, and widespread use of communication technology, digital RPMS is vulnerable to software common cause failure (CCF), and countermeasures have to be taken while implementing DCS. DAS is considered as one of the most effective methods to deal with such failure.

As for mitigation of ATWS, nuclear regulations worldwide have been putting more emphasis on diversity and defense in depth of instrumentation and control systems in nuclear power plants (EuR organization [1], NRC [2], and IAEA [3]). The United States of America Federal Regulations 10CFR50 [4] clearly requires that "each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS. This equipment must be designed to

perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system." Nuclear industry has been also making great efforts to the issue. Preckshot [5] and Thomas et al. [6] suggested some strategies and methods for performing diversity and defense in depth of instrumentation and control system. IAEA [7] identified and discussed common criteria for the design of DAS at nuclear power plants. Xiao et al. [8] illustrated the design principle and design flow of DAS. Zhan et al. [9] suggested a method to determine protection functions and parameter signals of DAS. Tian et al. [10] analyzed the acceptance criteria for DAS protection signals. As for implementation of DAS, He and Guo [11] proposed a miniaturization method to optimize the scale of DAS. Wang and Sun [12] identified the critical technical issues while implementing DAS. Yan et al. [13] suggested an overall verification method for DAS thanks to simulation technology. Probabilistic risk assessment (PRA) is also introduced into DAS design. Torok [14] investigated benefits and risks associated with DAS thanks to probabilistic analysis. Zhan and Zhang [15] discussed the PRA application in DAS design.

After the Fukushima nuclear accident, it is realized that for nuclear power plants, the beyond-design-basis accidents (BDBA) are also possible to happen and even their probabilities are extremely low (Miller et al. [16] and NNSA [17]). This prompts the exploration of some new concepts such as accident tolerant fuels and also urges that a series of measures aiming to improve the ability to mitigate BDBAs have been taken for CPR1000 nuclear power plants; that is, the improved ACPR1000 nuclear power plant has come into being. Compared with the limited several special ATWS scenarios taken into account for CPR1000 nuclear power plants (EDF [18] and Zhang et al. [19]), the ATWS scenarios for ACPR1000 nuclear power plant tend to comprehensively cover the scenarios that all design-basis accidents (DBA) concurrent with failure of reactor trip (RT) as long as it may trigger RT or actuate engineered safety features (ESF). This paper gives an overview of the work related to DAS of ACPR1000 nuclear power plant; the scale of DAS is determined after capturing its functional requirements; the detailed design, the implementation, and procedure development on it are discussed. For ACPR1000 nuclear power plant, DAS provides comprehensive and diversified protection for RPMS; it is of great significance to reduce the risk induced by software CCF of RPMS and enhance the safety level.

2. Function Requirement of DAS

ACPR1000, as an improved generation II nuclear power plant derived from CPR1000 nuclear power plant, the implementation of DAS for it needs to be considered from the aspects of economy and feasibility. For ACPR1000, if DAS is set up in pursuit of absolute independency from RPMS just like that of AP1000 nuclear power plants (Westinghouse [20, 21]), it is obviously unrealistic as a large number of DAS-specific instruments and actuators, such as circuit breakers and valves, have to be properly equipped with. Considering that DAS aims to deal with software CCF of digital RPMS and the CCF will not lead to unavailability of RPMS existing instruments and actuators if special precautions are reasonably taken, it is principally acceptable for DAS to share these instruments and actuators with RPMS (Zhou et al. [22]). Therefore, ACPR1000 DAS is authorized to focus on dealing with software CCF of digital RPMS and is exempted from failure of RPMS instruments and process equipment; then, any addition of instruments and process equipment dedicated to DAS is avoided, which minimizes the impact on relative process systems at the same time.

As for digital RPMS, special measures have to be taken to ensure that probability of software CCF is extremely low (IEC [23]); functional diversity and equipment diversity are adopted to lower the probability to as low as an order of 10^{-3} per reactor year. DAS, as the backup of RPMS, scale should be as small as reasonable; that is, the functions assigned to it should be as reduced as reasonable; its architecture and external interfaces should be as simplified as reasonable also. As a DBA concurrent with software CCF of RPMS is taken as a BDBA, the systems and equipment involved in mitigating the consequence of it need not meet the single-failure criterion (IEEE [24]), which means that the redundancy of them is avoided; therefore, for the purpose of minimizing DAS scale, the automatic functions and manual functions assigned to it should actuate only one train of the process systems and equipment, which are necessary to mitigate the consequences of ATWS; however, if transient analysis proves that both two trains of the process system and equipment are necessary to meet acceptance criteria of accident analysis, then DAS should be assigned to actuate both the train A and train B process systems and equipment.

The following aspects are concerned to minimize the interactions with RPMS:

(1) To ensure the independency of RPMS, sufficient physical and electrical isolation are carried out between DAS and RPMS

(2) As spurious actuation of DAS may disturb operation of process systems, which may eventually result in actuation of RPMS, effective measures are taken to reduce the possibility of spurious actuation of DAS

(3) In case of a DBA, if RPMS has actuated correctly, measures are taken to ensure that DAS will not actuate repeatedly

In terms of human-machine interface (HMI), the function and scale of auxiliary control panel (ACP) is not changed after DAS is implemented; original manual controls and display signals on ACP are not changed either, because any change of ACP, as the only safety-classified HMI in ACPR1000 nuclear power plant, may implicate conclusions promised in safety analysis report (Sun and Jiang [25]).

3. Dimension of DAS

3.1. Deterministic Method for DAS Functions. For ACPR1000 nuclear power plant, dimension of DAS is technically based on the results of transient analysis of ATWS, as suggested in

[1], the scope of transient analysis covers each Category II, III, and IV operating conditions listed in safety analysis report as long as it may trigger RT or actuate ESF; software CCF of RPMS is considered as a cumulative failure under these operating conditions. Full power operation is assumed as the initial condition as it represents the most possible operation condition during the whole lifespan of nuclear power plant. From the point of view of limiting DAS scale, analysis method of best estimation is chosen and realistic assumptions and calculation modes are adopted, conservative assumptions and calculation models while performing DBA safety demonstration are abandoned, because it may underestimate the ability of process systems (especially nonclassified systems) responding to initial events, and then some useful recovery strategies may be ignored.

In the event of a DBA concurrent with software CCF of RPMS, thanks to automatic and manual functions assigned to DAS, the reactor should be brought to and maintained at safety shutdown state (Zhao et al. [26]); that is, (1) the core maintains at subcritical state; (2) residual heat of the core can be continuously removed; and (3) radioactive release into the environment is within the limit. For ACPR1000 nuclear power plant, acceptance criteria of ATWS long-term accident analysis to safety shutdown state can be decoupled as follows:

(1) For small break loss-of-coolant accidents (LOCA) and non-LOCA accidents, connection of residual heat removal system (RHRS) can guarantee long-term cooling of reactor; then it can be considered as reaching to safety shutdown state

(2) For medium- or large-break LOCA, it is necessary to verify that operation of low-pressure safety injection system and containment spray system can effectively remove decay heat in a long time

The grace period of operator's intervention is determined to be 20 minutes (Liu et al. [27]); that is, when a DBA concurrent with software CCF of RPMS occurs, if the interval from giving a clear accident indication in main control room to starting the required mitigation action is within 20 minutes, then the mitigation action should be actuated automatically; otherwise, it is assigned to be actuated manually by operator. For ACPR1000 nuclear power plant, critical safety functions assigned to DAS and their actuation types are shown in Table 1. The automatic protection logics and related set points are determined based on ATWS transient analysis at the same time, in order to prevent DAS from actuating RT and ESF before RPMS actuation when there is no software CCF existing in RPMS, as shown in Table 2, set points initialized in DAS are slightly higher or lower than those in RPMS so as to delay the automatic actuation of DAS, the time of delay ensures that DAS automatic action will not be triggered or will be automatically locked before actuation if RPMS works normally, locking signals directly come from feedback signals of relevant actuators, which are not affected by software CCF of RPMS.

Considering that software CCF of RPMS will also lead to failure of the nonprotection functions localized on safety-classified DCS platform, such as flow rate control of auxiliary feedwater, regulating control of air dumping valves, etc., these functions are also necessary for the reactor to be fallen back to and to be maintained at safety shutdown state after the accidents, hence are assigned to DAS also.

As for alarm signals representing occurrences of the accidents, as well as indications of physical parameters monitoring reactor state and critical safety functions, they are necessary for post-accident diagnosis and orientation and thus are deployed on DAS, such as the radioactive alarm signals of steam generators and the indication of subcooling margin of coolant at core outlet, etc. (Wang et al. [28] and He et al. [29]). Considering that calculation process of reactor pressure vessel water level (RPVL) measurement based on differential pressure between the upper and lower extremities of the vessel is very complicated (He et al. [30]), RPVL measurement is not assigned to DAS to cut cost and limit its scale, monitoring of post-accident core cooling state on DAS is then depending on subcooling margin and temperature at core outlet (Wang et al. [31]), which has certain influence on development of accident mitigation strategy on DAS.

3.2. Independent Verification of DAS Functions. Independent verification, aiming to verify that the reactor can be brought to and maintained at safety shutdown state thanks to DAS functions after DBAs concurrent with software CCF of RPMS, is performed by individuals not involved in DAS design. The typical transients, including loss of offsite power, feedwater line break, steam line break (SLB), steam generator tube rupture, and LOCA, are analyzed using CATHARE code. As an example, Table 3 shows the sequence of SLB concurrent with RPMS failure, after DAS automatic actions have made the reactor achieve a controlled state, the operator begins to manually cool and depressure primary system in a controlled way, as shown in Figure 1, the reactor is smoothly fallen back to conditions of RHRS connected (primary pressure below 3.2 MPa and temperature at core outlet below 180°C) and reaches safety shutdown state eventually.

3.3. Insight into PRA. PRA is used to demonstrate and evaluate merits of DAS functions quantitatively. The core damage frequency (CDF) and large release frequency (LRF) without and with DAS functions are compared, as shown in Table 4, relatively significant reductions of CDF and LRF are earned with DAS functions, as these functions diversify reactor protection functions such as RT and ESF actuation; hence, the reliability of protection functions and capability of response to the accidents is improved considerably.

4. Detailed Design of DAS

4.1. Diversity Design. In order to prevent it from being affected by software CCF of RPMS, diversity between DAS and RPMS from sensor inputs (excluding sensors) to final outputs (excluding actuators) is comprehensively concerned, including the following:

Table 1: Critical safety functions and actuation types on DAS.

Critical safety functions	System functions	Trains	Actuation type (A: auto, M: manual)
Criticality control	RT and turbine trip	—	A/M
Primary water inventory and core cooling	Safety injection	A	A/M
	Reactor coolant pumps trip	A/B	A
Heat sink	Auxiliary feedwater control	A/B	A/M
	Main steam line isolation	A	A/M
	Main feedwater isolation	A	A/M
	Air dumping valves control	A	M
Primary integrity	Pressurizer safety valve control	A	M
Containment integrity	Containment isolation	A	M
	Containment spray	A	M

Table 2: Automatic actions and set points on DAS.

DAS automatic actions	Actuation signals	Set points	
		DAS	RPMS
RT/turbine trip	Pressurizer pressure high	16.90 MPa	16.55 MPa
	Pressurizer pressure low3	12.7 MPa	13.10 MPa
	Any loop low flow rate	82% nominal flow	88.8% nominal flow
	Steam generator low-low water level	0% narrow range	15% narrow range
	Power range high neutron flux	118% full power	109% full power
	Safety injection	—	—
Safety injection	Low low pressurizer pressure	11.50 MPa	11.83 MPa
Main feedwater isolation	Any steam generator high water level	90% narrow range	75% narrow range
	Safety injection	—	—
Main steam line isolation	Low steam line pressure concurrent with high steam line flow	2.90 MPa, 120% nominal flow	3.45 MPa, 120% nominal flow
Motor auxiliary feedwater pumps startup	Any steam generator low-low water level concurrent with low feedwater flow	0% narrow range, 6% nominal flow	15% narrow range, 6% nominal flow
	Safety injection	—	—
Turbine auxiliary feedwater pumps startup	Any steam generator low-low water level concurrent with feedwater flow low	0% narrow range, 6% nominal flow	15% narrow range, 6% nominal flow

Table 3: Sequence of SLB concurrent with RPMS failure.

Events	Time, s
Steam line break	0
Main steam line isolation	3
RT due to power range high neutron flux	7.9
Safety injection due to low low pressurizer pressure	21.1
Main feedwater isolation	36.1
Auxiliary feedwater pumps startup	146.4
Operator intervention:	
Isolate ruptured steam generator	
Control level of intact steam generators	1208.0
Switch over high pressure safety injection into charging	
Cooling with 28°C/h	1654.2
Depressure by normal spray	8401.7
Reach conditions of RHRS connected	17820.9

(1) Sensor signals shared by DAS and RPMS are distributed to DAS before being inputted into RPMS; conventional analog circuits are adopted for these distribution modules

(2) DAS is constructed with equipment and platform diversified from RPMS

(3) Different from RT of RPMS by opening the reactor trip breakers, the RT signal emitted by DAS is sent to the power cabinets of rod control and position monitoring system, and RT is realized by directly cutting off the power supply of control rod drive mechanism

4.2. Prevention of Spurious Actuation. To avoid spurious actuation caused by any credible single failure, the following measures are taken in DAS design:

(1) "Energizing-actuation" design to prevent spurious actuation caused by power loss or component failure

(2) Redundant input channels which distributed from protection groups are equipped to participate in voting logic, so that single-channel failure or channel bypass will not lead to spurious automatic actuation

(3) Redundant subsystems are configured in the automatic action voting logic to reduce the probability of spurious actuation

(4) The default values, which are alternative values to participate in voting logic after detecting signal failure, are determined based on the principle of "failure nonactuation" and are reasonably embedded in engineering configuration to considerably avoid the risk of spurious actuation (Wang et al. [32])

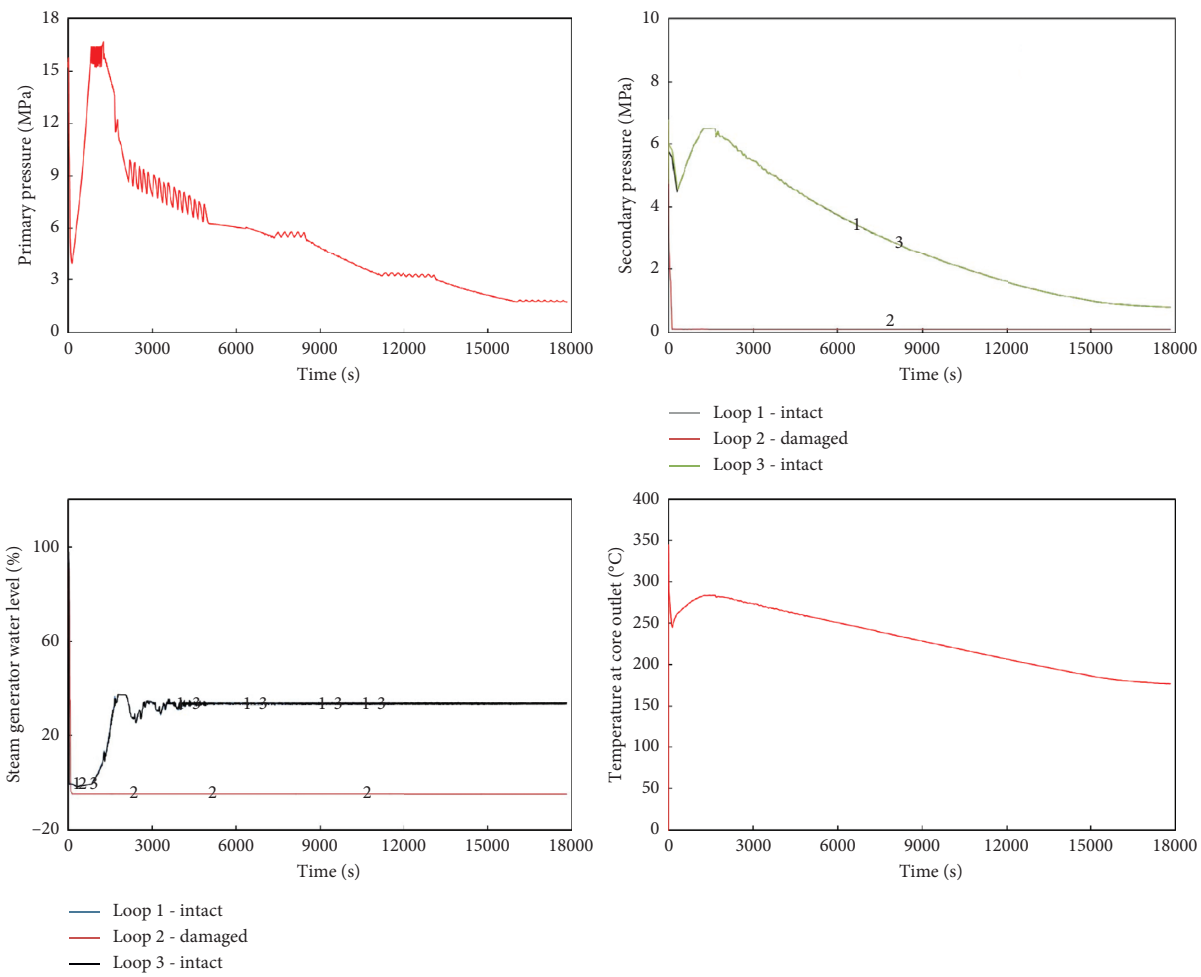


Figure 1: Trends of critical parameters after SLB concurrent with RPMS failure.

Table 4: Insight of PRA.

		Without DAS functions	With DAS functions	Decrease %
CDF	Internal events	$3.05E-06$	$2.81E-06$	7.9
	Internal fire	$3.01E-06$	$2.74E-06$	9.0
	Hazards	$2.72E-08$	$2.57E-08$	5.5
LRF	Internal events	$4.87E-07$	$4.27E-07$	12.3
	Internal fire	$2.07E-07$	$1.89E-07$	8.7
	Hazards	$4.19E-09$	$3.96E-09$	5.5

(5) All manual operations on DAS are in the manner of "Operation + Release" to minimize the probability of triggering manual action by mistake

(6) To avoid spurious actuation caused by fire in main control room, all manual and automatic operations on DAS are blocked after transferring over to remote shutdown station

(7) DAS as a whole meets the seismic Class I requirements, which means it can withstand the safety shutdown earthquake

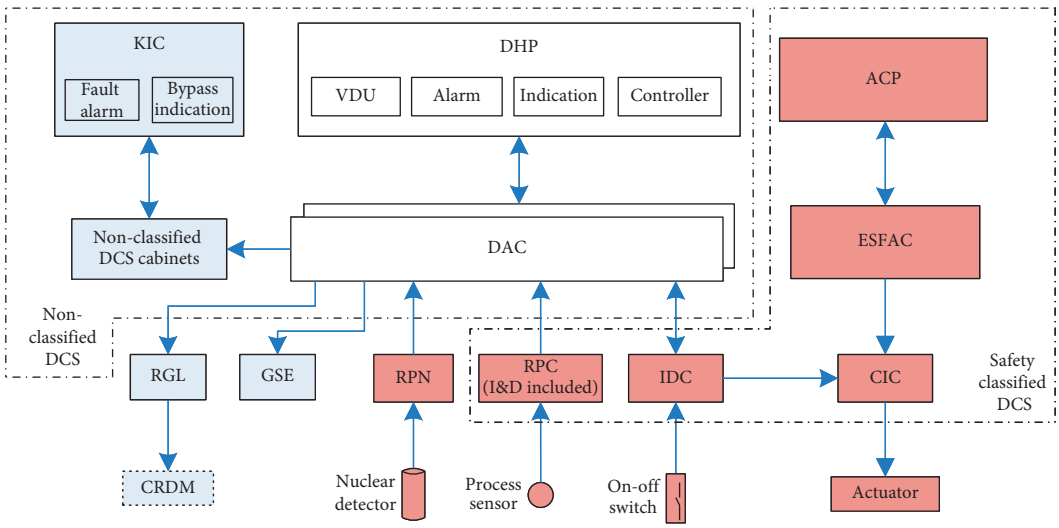
4.3. Isolation and Independency. DAS has to be physically and electrically isolated from RPMS, the following measures are taken:

(1) DAS cabinets and RPMS cabinets are arranged in different rooms, which belong to different fire zones

(2) Sensor signals shared by DAS and RPMS are isolated. The isolation modules (relays, optic couplers, etc.) are planted in RPC and IDC cabinets which belong to safety-classified DCS, as shown in Figure 2

(3) Actuation signals emitted by DAS are sent to component interface cabinets of RPMS, where priorities of command signals are managed by simple, fully verified, solid-state circuit and are exempted from software CCF of RPMS (Shi et al. [33])

(4) Two independent uninterruptible power supplies different from those of RPMS are equipped for DAS,



ACP: Auxiliary Control Panel
CIC: Component Interface Cabinet
CRDM: Control Rods Drive Mechanism
DAC: Diverse Actuation Cabinet
DHP: Diverse HMI Panel
ESFAC: Engineered Safety Feature Actuation Cabinet
GSE: Turbine Control System
IDC: Isolation and Distribution Cabinet
I&D: Isolation and Distribution
KIC: Computerized HMI
RGL: Rod Control and Position Monitoring System
RPC: Reactor Protection Cabinet
RPN: Nuclear instrument System
VDU: Visible Display Unit

Figure 2: DAS interface.

and ventilation of DAS cabinet rooms is independent of that of RPMS cabinet rooms

4.4. Testability and Maintainability. The operation status monitoring of DAS itself is integrated in nonclassified DCS, and the status can be continually displayed on KIC, as shown in Figure 2. Meanwhile, DAS automatic action logic has redundant subsystems and the "2 out of 2" logic can prevent DAS spurious actuation while singly testing one subsystem. The bypass switch can bypass the fault input channel individually to ensure that DAS functions normally during maintenance.

5. Implementation of DAS

5.1. DAS Architecture. As shown in Figure 3, DAS is architecturally divided into two levels: field control level (Level 1) and human-machine interface level (Level 2). Level 1 is composed of field control stations (FCS), which perform the functions of signal processing such as acquisition and calculation. Level 2 is composed of DHP and server cabinet, which performs information management and human-machine interaction function.

5.2. Field Control Level. Applying field programmable gate array (FPGA) technology to instrument and control system of nuclear power plant has been becoming one of the hot research topics in recent years, many institutions and organizations have been actively exploring and studying in this topic (IEC [34], Bobrek et al. [35], J. Naser [36], Bobrek et al. [37], Chen et al. [38], Xiao et al. [39], and Wei et al. [40]). Considering that FPGA technology has been successfully practiced in quite a number of nuclear power plants around the world (Westinghouse [41], Liu et al. [42], and Ma et al. [43]), it is decided that DAS of ACPR1000 nuclear power plant is built based on FPGA technology. The Level 1 design keeps to traditional distributed control concept and aims to achieve high integration and simplification as far as reasonable. By performing function analysis and allocation, primary functions and secondary functions are allocated to different FPGA cards, thus reducing the coupling degree of each processing unit. A single FCS can support as much as 400 input variables to participate in protection and monitoring. FCS includes automatic logic cabinets and manual logic cabinets, both of which are possessed of functional redundancy configuration. Two automatic logic cabinets collect sensor signals conditioned and distributed by RPMS and generate automatic RT signal and ESF actuation signals after thresholds comparison and voting logic; "2 out of 2" logic is carried out to actuate RT and drive ESF. Two manual logic cabinets are functioning to realize equipment-level manual control logic and alarm management, manual control of regulating valves, as well as periodic test interface with other systems.

5.3. Human-Machine Interface Level. The server in Level 2, which is nonredundant, performs information management, logging and archiving, as well as calculation functions. LDU is used for server normal maintenance, periodic test, and operating status display. Analog hardware and digital

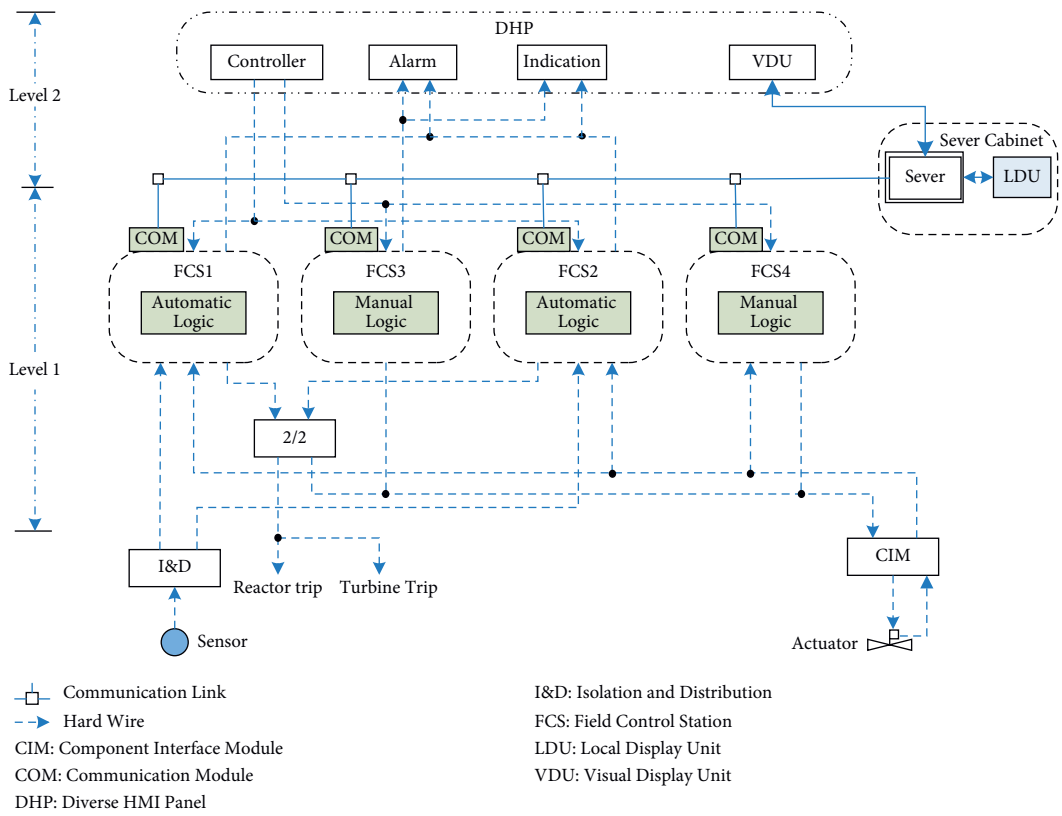


Figure 3: DAS architecture and composition.

interface are ergonomically arranged on DHP, analog hardware includes hand controllers necessary for operators to perform manual operations, digital interface is an operator work station with VDU, which provides system flowcharts and monitoring display, as well as control of equipment of process systems.

5.4. Verification and Validation. Verification and validation of DAS equipment is performed during factory test and commissioning test. Factory test includes unit testing, integration testing, and system testing, which are carried out progressively. Unit testing focuses on individual unit such as input and output channel etc., integration testing addresses functions assigned on DAS such as automatic RT, ESF, etc., while system testing aims to verify the overall response capability of DAS such as response time, fault monitoring, etc.

Commissioning test aims to verify the capability of DAS performing its designed functions under designed conditions, that is, to validate the design requirement by comparing the conformity between test results and test criteria deduced from the designed function. Commissioning test is carried out from simple to complex and from the local to the whole, after finishing DAC cabinet function test and DHP function test, the automatic and manual logic test is carried out, and finally the combined logic test and system performance test are performed. By this, all the functions of DAS, including safety functions and operating functions, are thoroughly verified.

6. Procedure Development on DAS

Emergency operating procedure (EOP) is used to guide operators to control and fall back reactor to safety shutdown state after accidents (Mišák [44]). As DHP only supports a limited number of functions, and considering that some nonclassified functions can still be controlled on KIC when DAS is activated, these nonclassified functions are beneficial to control reactor state after accidents to some extent (e.g., normal spray on KIC can be used to depressure primary coolant system effectively); they are thus reasonably considered while developing EOP on DAS.

Different from the state-oriented EOP for KIC and ACP, a set of DAS-specific, simplified, paper-based, and event-oriented EOP is developed. After DAS is activated, RPMS fault alarm (KDS400KA/AA) will appear both on KIC and on DHP at the same time, following guidance of alarm sheet, the operation team will confirm RPMS failure and then initiate initial orientation to direct to appropriate accident mitigation strategy, thanks to which the reactor is fallen back to and maintained at safety shutdown state. During this period, safety state of the reactor is kept under constant surveillance by safety technical engineer, which constructs the defense in depth of emergency operating on DAS, as shown in Figure 4. After software CCF of RPMS has been repaired, the emergency organization will decide whether to exit DAS emergency operation after estimating the reactor state thoroughly. The set of EOP has been verified and

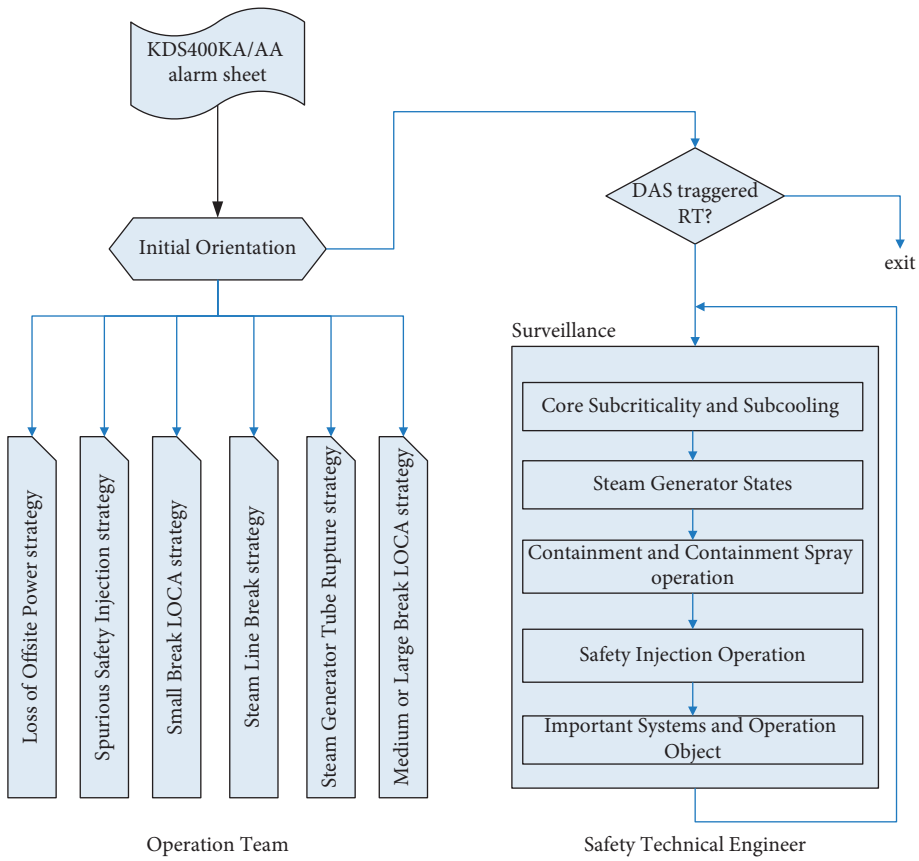


Figure 4: Emergency operating strategies on DAS.

validated on full-scope simulator of ACPR1000 nuclear power plant.

7. Conclusion

Implementation of DAS can specifically mitigate the consequences of DBA concurrent with software CCF of digital RPMS, for commercial mature nuclear power plants, a balance between cost and benefit has to be sought while implementing DAS. As for ACPR1000 nuclear power plant, the solution that DAS sharing instruments and actuators with RPMS can reduce the impact on existing process systems as reasonable as possible and achieve the purpose of coping with software CCF of RPMS effectively with as low cost as possible.

We hope that the reactor can be fallen back to and maintained at safety shutdown state thanks to DAS in case of DBA concurrent with software CCF of RPMS. In order to limit the scale of DAS, DAS should, unless necessary, only actuate one train of the process systems and equipment necessary to mitigate the consequences of ATWS as far as possible. According to a grace period of 20 minutes for operator intervention, the automatic protection functions including their set points and manual functions to be assigned to DAS are discriminated based on transient analysis of ATWS; the other functions to be assigned to DAS to meet the goal of accident mitigation are also screened out, the independent verification performed by individuals not involved in DCS design proves that the reactor can be fallen back to and maintained at safety shutdown state thanks to these DAS functions; what is more, PRA demonstrates significant reductions of risks are contributed. While designing and implementing DAS, special precautions are taken to ensure its diversity, to prevent its spurious actuation, to realize its isolation and independency from RPMS, and to support its testability and maintainability. FPGA-based technology that is diversified from RPMS is chosen to build DAS of ACPR1000 nuclear power plant, which involves the specific implementation of field control level and human-machine interface level. Finally, a set of paper-based and event-oriented EOP dedicated to DAS is developed. At present, the DAS has always been successfully operating in all ACPR1000 nuclear power plants for several years; it also provides a technical reference for DAS design of the generation III nuclear power plant HPR1000.

Abbreviations

ACP: Auxiliary control panel
ATWS: Anticipated transient without scram
CCF: Common cause failure
DAS: Diverse actuation system
DBA: Design-basis accident
DCS: Digital control system
DHP: Diverse human-machine interface panel
EOP: Emergency operating procedure

ESF: Engineered safety feature
FCS: Field control station
FPGA: Field programmable gate array
HMI: Human-machine interface
KIC: Computerized HMI
LOCA: Loss-of-coolant accident
RPMS: Reactor protection and monitoring system
RPVL: Reactor pressure vessel water level
RT: Reactor trip
VDU: Visual display unit.

Data Availability

The data used in this paper are part of the plant operation data, which are proprietary and cannot be disclosed.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

References

[1] EuR Organization, "European utility requirements for LWR nuclear power plants rev. D," *Chapter 10—Instrumentation & Control and Human-machine Interface—Section 5.3.1.5 Prevention of Common-Cause Failures*, Vol. 2, EuR Organization, Lyon, France, 2012.

[2] NRC, *Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems (BTP7-19)*, NRC, Washington, DC, USA, 2012.

[3] IAEA, *Design of Instrumentation and Control Systems for Nuclear Power Plants (SSG-39)*, IAEA, Vienna, Austria, 2016.

[4] NRC, *10 CFR 50.62 Requirements for Reduction of Risk from Anticipated Transients Without Scream (ATWS) Events for Light-water Cooled Nuclear Power Plant*, NRC, Washington, DC, USA, 2015.

[5] G. G. Preckshot, *Method for Performing Diversity and Defense-In-Depth Analyses of Reactor Protection Systems (NUREG/CR-6303)*, NRC, Washington, DC, USA, 1994.

[6] W. R. Thomas, B. Randy, and C. M. Sacit, *Diversity Strategies for Nuclear Power Plant Instrumentation and Control System (NUREG/CR-7007)*, ORNL, Oak Ridge, TN, USA, 2010.

[7] IAEA, *Criteria for Diverse Actuation Systems for Nuclear Power Plants (TECDOC-1848)*, IAEA, Vienna, Austria, 2018.

[8] P. Xiao, H. C. Liu, and J. X. Zhou, "Design of diverse actuation system in nuclear power plant," *Nuclear Power Engineering*, vol. 35, no. 2, pp. 90–93, 2014.

[9] W. H. Zhan, B. B. Zhang, and Z. Xu, "Determination of protection function and parameter signal of diverse actuation system," *Atomic Energy Science and Technology*, vol. 50, no. 9, pp. 1647–1652, 2016.

[10] H. W. Tian, Z. H. Guang, and P. Xiao, "Analysis and confirming of acceptance criteria in diverse actuation system signals design for nuclear power plants," *Nuclear Power Engineering*, vol. 38, no. S2, pp. 146–148, 2017.

[11] X. M. He and W. Guo, "Research on the miniaturization of diversity actuation system in nuclear power plant," *Process Automation Instrumentation*, vol. 38, no. 7, pp. 38–45, 2017.

[12] Z. Y. Wang and G. Sun, "Analysis research on the critical technical issues in implementation of DAS," *Process Automation Instrumentation*, vol. 38, no. 3, pp. 9–12, 2017.

[13] M. Yan, W. G. Gu, and S. C. Li, "Research of nuclear power plant diverse actuation system overall verification method," *Nuclear Electronics & Detection Technology*, vol. 35, no. 3, pp. 248–252, 2015.

[14] R. Torok, *Benefits and Risks Associated with Expanding Automated Diverse Actuation System Functions*, EPRI, Palo Alto, CA, USA, 2008.

[15] W. H. Zhan and B. B. Zhang, "PSA application in the diverse actuation system design," in *Proceedings of the 2017 25th International Conference on Nuclear Engineering (ICONE 25)*, Shanghai, China, July 2017.

[16] C. Miller, A. Cubbage, and D. Dorman, *Recommendations for Enhancing Reactor Safety in the 21st Century*, NRC, Washington, DC, USA, 2011.

[17] NNSA, *General Technical Requirement for Improving Action after the Fukushima Nuclear Accident*, NNSA, Beijing, China, 2012.

[18] EDF, *Framatome, Design and Construction Rules for System Design of 900 MWe PWR Nuclear Power Plants*, EDF, Paris, France, 1995.

[19] Y. B. Zhang, B. Zhang, and W. J. Huang, "Analysis of diversity and independence for ATWT mitigation system in nuclear power plant," *Nuclear Power Engineering*, vol. 35, no. 2, pp. 77–79, 2014.

[20] Westinghouse, *AP1000 Diverse Actuation System Planning and Functional Design Summary Technical Report (WCAP-17184-NP, Rev. 0)*, Westinghouse, Pittsburgh, PA, USA, 2009.

[21] Westinghouse, *AP1000 Instrumentation and Control Defense-In-Depth and Diversity Report (WCAP-15775, Rev. 4)*, Westinghouse, Pittsburgh, PA, USA, 2010.

[22] W. H. Zhou, H. Jiang, and H. Q. Peng, "Discussion on instrumentation & control design features of DAS in PWR," *Atomic Energy Science and Technology*, vol. 48, no. 11, pp. 930–934, 2014.

[23] IEC, *Software for Computers Important to Safety for Nuclear Power Plants-Part 2: Software Aspects of Defense against Common Cause Failures, Use of Software Tools and of Pre-developed Software (IEC Std 60880-2-2000)*, IEC, Geneva, Switzerland, 2000.

[24] IEEE, *IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (IEEE Std 379-2014)*, IEEE, New York, NY, USA, 2014.

[25] Y. B. Sun and X. H. Jiang, "Layout design of advanced control room of pressurized water reactor NPP," *Nuclear Power Engineering*, vol. 29, no. 3, pp. 73–77, 2008.

[26] H. Zhao, C. Li, and S. B. You, "Design characteristics of ACPR1000 technical scheme of Unit 5&6 of Yangjiang NPP," *Nuclear Science & Engineering*, vol. 40, no. 3, pp. 431–436, 2020.

[27] C. W. Liu, X. H. Zhang, and W. Chen, "Research and design of non-intervention time after accident for HPR1000 reactor," *Nuclear Power Engineering*, vol. 40, no. S1, pp. 50–54, 2019.

[28] Z. Y. Wang, C. Sun, and B. Wu, "Estimation of measurement uncertainties for subcooling margin of coolant at core outlet in CPR1000 NPPs," *Nuclear Power Engineering*, vol. 36, no. 2, pp. 24–27, 2015.

[29] Z. X. He, B. Li, and J. Wu, "Design of inadequate core cooling monitoring system in Qinshan Phase II Extension Project," *Nuclear Power Engineering*, vol. 29, no. 1, pp. 5–9, 2008.

[30] Z. X. He, J. H. Yu, and X. F. Li, "Design of cooling monitoring system based on SOP," *Nuclear Power Engineering*, vol. 33, no. 5, pp. 107–110, 2012.

[31] Z. Y. Wang, R. S. Li, and K. B. Sun, "Dimension of the forced vessel water level based on subcooling margin of core outlet

coolant in CPR1000 nuclear power plants," *Energy Procedia*, vol. 127, pp. 103–109, 2017.

[32] Z. Y. Wang, H. L. Li, and W. B. Zheng, "Analysis research on the fallback values of digital instrument and control system in NPP," *Process Automation Instrumentation*, vol. 32, no. 5, pp. 24–27, 2011.

[33] G. L. Shi, B. Zhang, and W. Y. Yang, "Priority management system scheme design for ACPR1000 reactor protection system based on FirmSys," *Nuclear Power Engineering*, vol. 40, no. 2, pp. 85–89, 2019.

[34] IEC, *Nuclear Power Plants—Instrumentation and Control Important to Safety-Development of HDL—Programmed Integrated Circuits for Systems Performing Category a Functions (IEC Std 62566—2012)*, IEC, Geneva, Switzerland, 2012.

[35] M. Bobrek, D. Bouldin, and D. E. Holcomb, *Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems (NUREG/CR-7006)*, NRC, Washington, DC, USA, 2010.

[36] J. Naser, *Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems (TR-1019181)*, EPRI, Palo Alto, CA, USA, 2009.

[37] M. Bobrek, D. Bouldin, and D. Holcomb, *Survey Of Field Programmable Gate Array Design Guides And Experience Relevant To Nuclear Power Plant Applications*, ORNL, Oak Ridge, TN, USA, 2007.

[38] Y. J. Chen, C. L. Zhang, and M. Qi, "Research on the application of FPGA in diversity system of nuclear power plants," *Process Automation Instrumentation*, vol. 35, no. 2, pp. 46–59, 2014.

[39] P. Xiao, J. X. Zhou, and H. C. Liu, "Application of defense-in-depth and diversity strategy in safety DCS research and development," *Journal of Shanghai Jiao Tong University*, vol. 52, no. s1, pp. 14–19, 2018.

[40] R. C. Wei, F. H. Sun, and X. X. Shui, "Reliability improvement of instrument and control systems in nuclear power plant with triple module redundancy technology," *Journal of Shanghai Jiao Tong University*, vol. 52, no. s1, pp. 166–170, 2018.

[41] Westinghouse, *AP1000 Design Control Document Rev. 19—Volume 5 Chapter 7—Instrumentation and Controls—Section 7.7.1.10 Diverse Actuation System*, Westinghouse, Pittsburgh, PA, USA, 2011.

[42] B. Liu, M. X. Liu, and J. Ding, "Study on diversity of priority actuate control system for nuclear power plants," *Journal of Shanghai Jiao Tong University*, vol. 52, no. s1, pp. 107–112, 2018.

[43] X. Y. Ma, X. J. Huang, and D. Wang, "Design and verification on nuclear safety class digital instrument control system based on FPGA," *Nuclear Power Engineering*, vol. 42, no. 2, pp. 115–120, 2021.

[44] J. Mišák, *Development and Review of Plant Specific Emergency Operating Procedures*, IAEA, Vienna, Austria, 2006.