World Journal of Nuclear Science and Technology, 2016, 6, 1-14
Published Online January 2016 in SciRes. http://www.scirp.org/journal/wjnst
http://dx.doi.org/10.4236/wjnst.2016.61001

A New ALS Based PMS Design and Its Evaluations

Zhi Xu[1,2*], Daoqing Jiang[3]

[1]Suzhou Nuclear Power Research Institute, Suzhou, China
[2]China Nuclear Power Engineering Co., Ltd., Shanghai, China
[3]Shanghai Keyuan Engineering Technology Co., Ltd., Shanghai, China
Email: *xuzhi@cgnpc.com.cn

Received 26 November 2015; accepted 2 January 2016; published 5 January 2016

Abstract

Westinghouse company (WEC) had developed a Nuclear Regulatory Commission (NRC) approved advanced logic system (ALS) platform based on field programmable gate array (FPGA) technology as the next generation 1E class platform for protection and monitoring system (PMS) development for nuclear power plants. In compliance with the requirements of typical PMS functions, a new ALS based PMS is designed by overcoming the restrictions of communication modules etc. The consistency with data communication independence and isolation, deterministic, diversity requirements etc. is analyzed. The evaluations indicate the design meets the requirements and can be applied for coming projects.

Keywords

ALS, FPGA, PMS, Independence, Isolation, Deterministic, Diversity

1. Introduction

The rapid development of digital computer technology and the widely deployment in nuclear power plant results in the problem of the high complexity of instrument control system (I&C), which is being paid more and more attentions. The software common mode failure (CCF) in nuclear power plant digital control system cannot be eliminated completely with the current technology, therefore, in the development of PMS, the usage of the specific methods to deal with the problem, such as diversity design and/or diversity actuation system, is a common practice. However these methods increase the design, development and licensing difficulties and costs [1].

In 2004, CS Innovations Company (CSI) developed an FPGA technology based system and replaced part of

*Corresponding author.

How to cite this paper: Xu, Z. and Jiang, D.Q. (2016) A New ALS Based PMS Design and Its Evaluations. *World Journal of Nuclear Science and Technology*, **6**, 1-14. http://dx.doi.org/10.4236/wjnst.2016.61001

the obsolete protection system in Wolf Creek nuclear power plant. Based on the successful practice, CIS introduced the ALS to industry as a safety system development platform. It is a "hard" logic based universal platform, which has the characteristics of high reliability and integrity. Main control functions do not rely on the microprocessor or software, but the simple FPGA based hardware architecture [2]. After the acquisition of CSI, WEC continued carrying out a lot of licensing jobs and finally the final safety report was issued by NRC in September 2013. NRC approved that the platform can be used as a solution to solve the problem of diversity and defense in depth for digital safety system, which can be customized for safety system replacement or new safety system development [3].

To satisfy the typical PMS functional requirements, a new PMS based on ALS platform, by overcoming the restrictions of communication modules etc. with minimum development cost, is designed. Based on the requirements in the Nureg-0800, the consistency with the rules and guidelines for the PMS in terms of data communication independence and isolation, deterministic, diversity requirements is studied.

2. ALS Platform

The poor reliability and aging of main steam and feed-water control system in Wolf Creek nuclear power plant resulted in the decision of replacing part of safety related I&C system in 2003. With the supports from Wolf Creek nuclear power plant, CSI developed a new system based on FPGA technology, named ALS platform. And the approval by NRC proved it a successful replacement of safety system in part. On the basis of successful engineering project, CSI introduces ALS platform as a next generation of general safety level platform, claiming the outstanding capability of obsolete safety system partial replacement and the new safety system development for nuclear power plants through customization.

Normally the 19-inch chassis based ALS platform consists of one or more ALS chassis and peripheral components. Each chassis accommodates up to 10 boards. Through the expansion bus, the platform can expend up to 6 chassis, 60 boards in total [3] for a specific application. The slowest system frame is 10 ms [2] in a maximum configuration. The peripheral equipment includes cabinets, power supplies, control panels, assembly panels, and the maintenance station called ALS service unit (ASU). The core ALS platform chassis of the typical architecture is shown in **Figure 1** [4].

The ALS platform consists of core logic board ALS-102, input board ALS-302, ALS-311, ALS-321, output board ALS-402, ALS-421 and communication board ALS-601. Application-specific logic circuit runs in the ALS-102 board, controlling the operation of the system, such as sending instructions to input boards to obtain

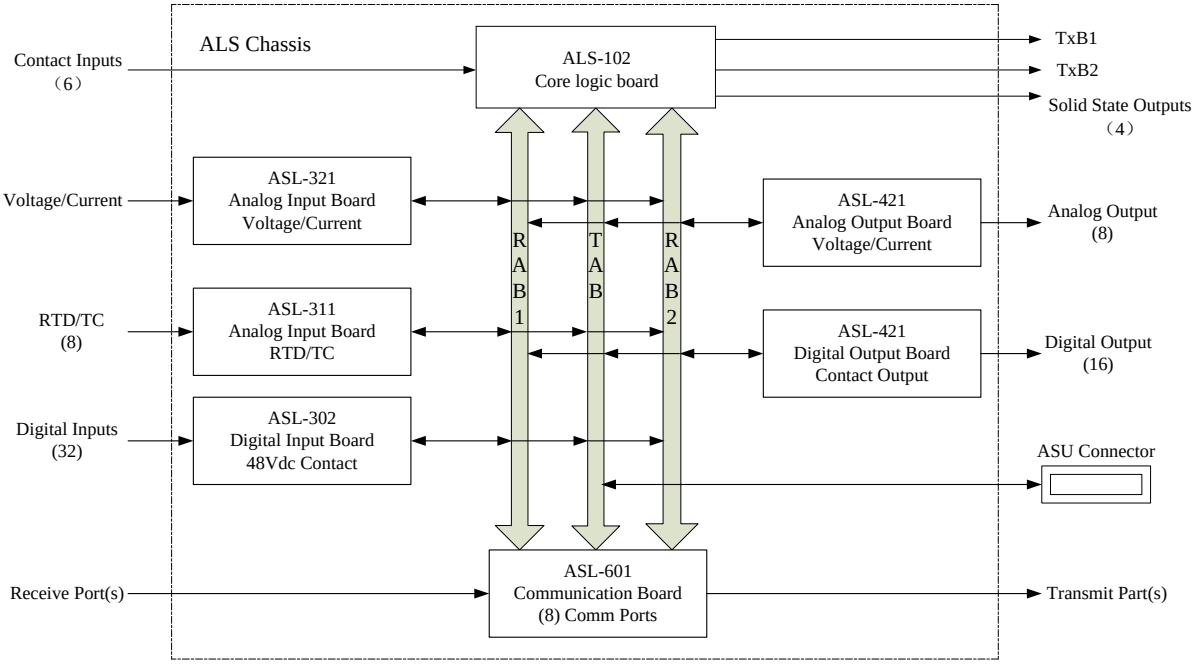

Figure 1. ALS chassis architecture block diagram.

field signals, and sending actuation commands to output boards after calculations. In addition, an ALS-102 board can communicate with external chassis through ALS-601. The board is also equipped with 6 relay contact inputs and 4 solid state relay outputs, which can be used to reset the system alarm and alarm indication.

Input boards are responsible for field signal sampling, signal conditioning, filtering and A/D conversion. Output boards are used to control breakers, relays and other actuated devices. Each channel of input and output boards is isolated and contains powerful self-diagnostics functions. Redundant configuration and other deployed specific test functions ensure that the channels run properly. Each input channel contains surge suppression circuit and filter while each output channel has surge, short circuit and over-voltage protection. All boards have LED panel, which indicates the state of each board. An ALS chassis might be installed multiple input and output boards as application-specific configuration.

An ALS-601 board contains 8 configurable, independent and isolated serial communication channels. The board supports point-to-point differential signaling and communication, providing communications with other external chassis reliably.

NRC evaluates data communication independence and isolation, deterministic, diversity requirements in perspective of ALS platform itself [3]. However it also points out that all these features of the safety system developed with ALS platform, as a whole, must be evaluated in accordance with the requirements in Nureg-0800. Based on the typical functional requirements of PMS and the features of ALS platform, an ALS platform based PMS is designed with a benchmark of AP1000 I&C solution. The design's consistence with standard review plan (SRP) requirements on communication independence and isolation, response time, deterministic and self-diagnosis, test and calibration, and diversity is studied.

3. Typical Function Requirements for PMS

The five principle safety functions for nuclear power plants are reactivity control, residual heat removal, retaining radioactive material and fission product releases control and important state monitoring [5]. Regardless 2nd generation or 3rd PWR plant, protection of the fuel cladding, keeping integrity of the RCS pressure boundary and the containment, are the three key nuclear safety barriers. When these barriers' integrity are threated, emergent shutdown of the reactor, actuation of ESF when necessary, and providing all the necessary information to operators for post accidents, are compulsory functions for PMS [6].

Normally PMS is developed with analog technology, digital technology or hybrid technology [7]. Whatever technology is used, a PMS shall satisfy these requirements in **Table 1**.

4. ALS Based PMS

I&C of nuclear power plants shall ensure the safe, reliable and economical operations of nuclear power plants, under all normal and abnormal emergency and accident conditions, by providing all kinds of control means, protection and monitoring information. The use of distributed control system and advanced control room is widely deployed in nuclear industry [8]. The unified DCS based I&C system for the nuclear island and conventional island control, provides a consistent and effective interface to operators. The whole plant equipment status monitoring and most controls are driven by non-safety DCS in main control room (MCR), meanwhile the display and control of safety class equipment are operated through the safety flat panel display (SD), if both failed, through the dedicated 1E system actuation switches in MCR which are hardwired connected to the lowest level of PMS, the plant can be shutdown and the required ESFs are driven in time. In the event of evacuation of MCR, the shutdown of the reactor and the driven of selected ESFs can be operated by hardwired control switches in remote workstation, to ensure reactor trip (RT) and keep the plant in safety conditions [9]. To improve the availability, maintainability and operability, and the use of suppliers as less as possible and proven advanced digital technology, reduces the variety and quantity of spare parts and the potential interface troubles. Based on functions of the ALS platform and engineering practices in the partial safety system replacement in Wolf Creek, Diablo Canyon [10] [11], taking the PMS design in [5] [9] as an benchmark, a new ALS based PMS is designed. For simplicity, this paper does not consider the non-safety DCS changes, instead focuses on alternations of Common Q, which serves as the safety system platform. However, there is of significant difference between Common Q and ALS in terms of module level communication functions. **Table 2** compares the communication capabilities between the two platforms [12].

Table 1. Key requirements for PMS.

PMS Requirements	Key Details
Redundancy	Segmented, multiple redundant protection groups, sufficient redundancy for connections between redundant divisions in all working conditions.
Independence	Independence for multiple channels inside the system, between 1E system and N1E system, other 1E system with physical separation, electric and communication isolations.
Diversity	To resist CCF.
Simplification	Less equipment, types, interactions, simple software languages.
Failure Safe	Failure will not prevent the safety actions or degrade system to unacceptable level.
Single Failure Criteria	Capability to perform safety functions concurrent with single failure.
Testability	Testability under conditions of power operation and shutdown. No lifting or jumpers required.
Self-Diagnostics	Self-Diagnostics, communication check, data integrity validation and calibration for analog input channels.
Operability	Checking the operational availability and assuring operational availability
Communication	Reliability of communications shall not lower than other parts.

Table 2. Inter rack communication capabilities of Common Q vs. ALS platform.

Common Q Communication Capability		ALS Communication Capability		
2HSLR + 1HSLT	CI631	2TXBs	1TAB	ALS-601
Deterministic, High Performance	High Deterministic, High Performance Bus	Deterministic, High Performance	High Deterministic, High Performance Bus	Deterministic, High Performance
EIA422, up to 3.1 Mb/s	Bus Speed Better than 1.5 Mb/s	EIA-422	EIA-485	up to 921.6 Kb/s
Periodic Point to Point	Periodic Broadcasting	Periodic Point to Point	Periodic	Periodic Point to Point
Unidirectional	Bidirectional	Unidirectional	Bidirectional	Configurable Unidirectional

Normally there are data exchanges among PMS racks. A typical communication within division is shown in **Figure 2** [12].

Due to the restriction of the none of bi-directional bused based communication module for data exchanges among racks, the configurable ALS-601 is deliberately designed in replacement of the CI631 module in Common Q solution.

In this design, each ALS rack configures at least one ALS-601 card. ALS-601 one-way port is configured either sending or receiving to replace HSLT and HSLR in common Q platform. The communication via CI-631, is deployed with a port of the sending configuration plus fan out and receiving port configuration in the corresponding ALS-601. To simplify the racks in the RT and ESF actuation path, only one port is configured as receiving with connection to the ALS-601 sending port in MCR located SD. All other non-critical signals go through SD as required. All the racks are connected to ASU, which is online only upon requirements for maintenance and testing communication via TAB bus. Sequence of events (SOE) signals is sent out to non 1E platform via TXB1 of ALS-102. Meanwhile the TXB2 port in ALS-102 dispatches data to unidirectional gateways, which bridges to non 1E DCS.

SDs are designed with validated and approved software based PC node box and touch LCD display as used in Common Q platform, which minimizes the new module design workload. Moreover neither are in the trip and ESF actuation path and have less importance to critical function, which is an engineering practice [5] [9]. The ASUs are developed with the similar technology.

There is no signal priority selection module in the certified ALS platform. So the CIM and SRNC and RNC are used as AP1000 solution does. The important device feedback signals are transmitted via CIM, SRNC, ALS-601 and RAB. The FPGA based CIM and SRNC modules were developed by CSI and deployed in AP1000, which eliminates requirement for new modules.

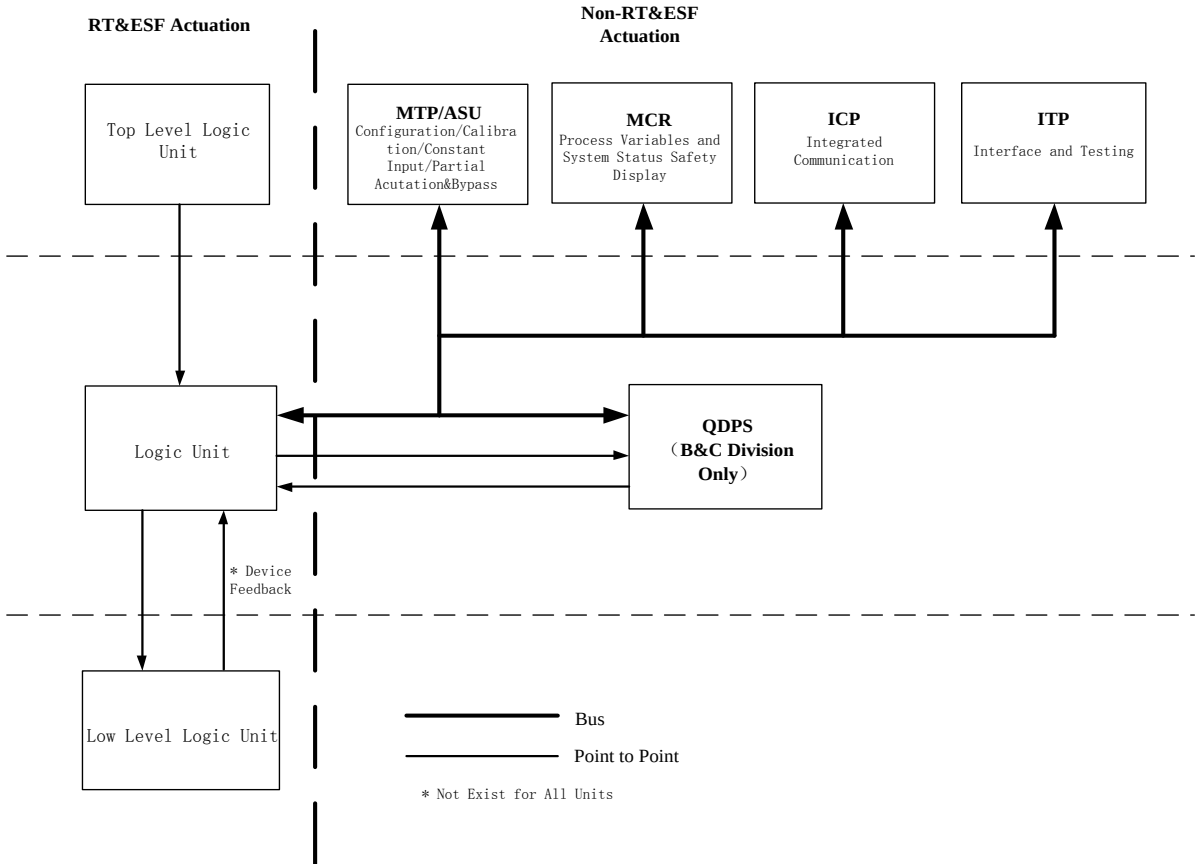

Figure 2. Typical communication among PMS divisional racks.

Thanks to the inherent diversity of ALS platform, all the FPGA based racks, the mentioned software based stations excluded, are of core diversity in favor of diversity. Moreover, to achieve higher diversity feature, additional embedded design diversity are adopted for the critical racks in the direct path of RT and ESF actuation.

To meet the requirements of **Table 1** with lowest cost, the new designed PMS is based on 4 divisions of independence, isolation and redundancy, which is same as NRC approved architecture in AP1000. Refer to **Figure 3** for the overall architecture of a PMS division. **Figure 4** indicates the redundancy of a PMS division.

Where the NIS and BPL are used to collect signals from the field sensors and perform protection function calculations. LCL is used to vote the partial RT and ESF signals from BPL to get functions of trips and actuations and process the hardwired system level actuation switches signals. ILP is used to fan out the system-level ESF actuation commands via the ALS-601, and the safety component-level manual control commands from the SD (for components with onerous consequences only) are distributed down to ILP via ALS-601 as well. The ILPs in each division communicate to the CIM via SRNC. The safety component-level manual control from PLS for components with non-onerous consequences drives CIM with sufficient isolations. ICP transmits data to the other three divisions, and receives data from the other three divisions, and also provides the isolated signals to non-safety system. MTP/ASU provides man-machine interface to the safety system and is used for maintenance and test functions. Manually controlled safety system equipment with onerous consequences is achieved by SD, while manual control of safety system equipment without onerous consequences is carried out via non-safety system normally. The commands from safety system and non-safety system are arbitrated by CIM, which is equipped with local manual control switches. QDPS is mainly used for processing the class 1Evariables required in RG1.97.

The designed architecture in **Figure 3** includes all the functions and interfaces in [5] [9]. In theory, it is an applicable solution. But as a new designed PMS, it is a must to evaluate the system according to the relevant regulations, guidelines, standards. In this paper, according to the requirements in [3] [13], for the designed PMS with ALS platform, the assessment on data communication independence and isolation, deterministic, diversity requirements is carried out.

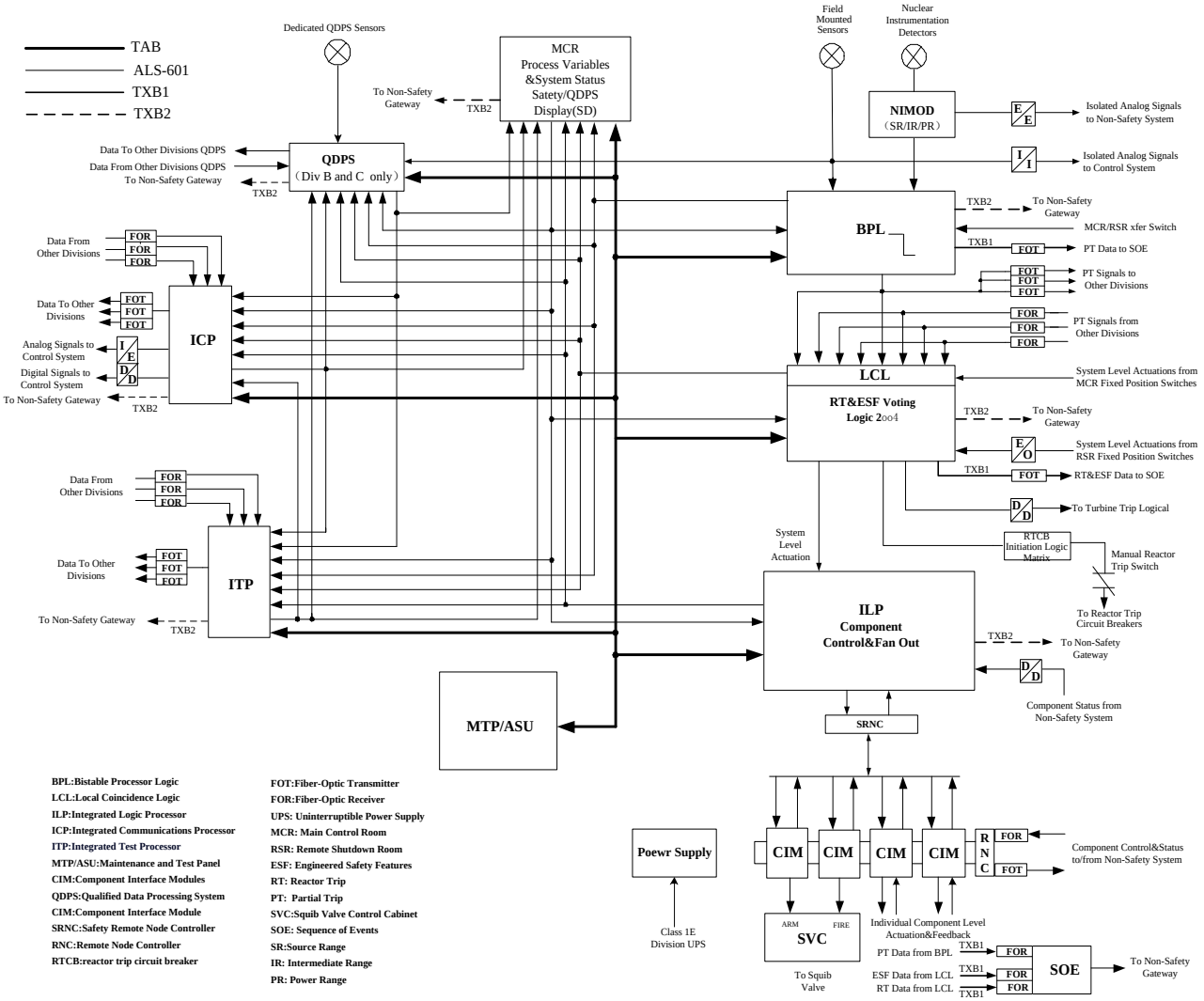

Figure 3. PMS one-division detail based on ALS platform.

5. SRP Requirements Analysis

Although NRC had reviewed the AL platform, it pointed out clearly that the real solution needs to be reviewed as a whole to ensure the relative requirements satisfied with the boards themselves excluded. Most of the current guidelines, standards do not cover the FPGA technologies, however NRC recommend parts of them can be used to assess non-microprocessor system, if applicable. The follows evaluates response time characteristics, deterministic behavior and self-diagnosis, testing and calibration capability etc., based on the existing guidelines and standards, in part and applicable.

5.1. Interdivisional Communication Analysis

Third part of DI&C-ISG-04 [10] directs the evaluation for the software based safety system in interdivisional communication, priority, display station. NRC requires evaluation with applicable criteria for real FPGA based solution at system level.

As shown in **Figure 3**, the design does not use shared maintenance station for multi-divisions. Divisional communication is unidirectional via isolated fiber. The data/signal exchange to non 1E DCS are via isolated unidirectional transmitting, e.g., gateways, and hardwired out, e.g. TXBs. And the flexible and reliable communication boards of ALS via TXB and TAB are evaluated by NRC. Please refer to [11] for more details.

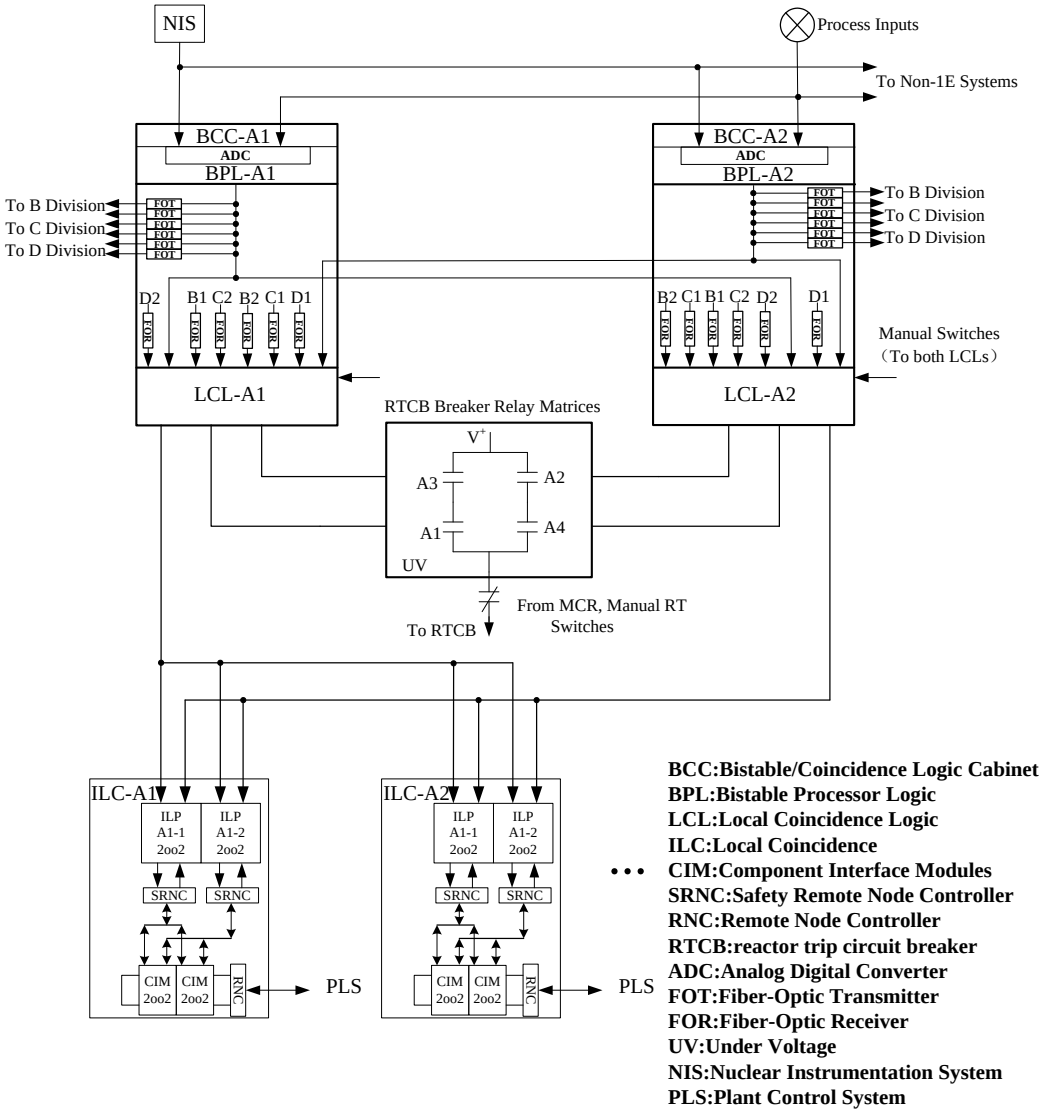

Figure 4. ALS platform based PMS division redundancy diagram.

The design does not have shared control stations and display stations for multiple divisions. The only shared control is the hardwired system level switches, whose outputs are isolated among divisions. Therefore the design meets the requirement in [13]. **Figure 5** indicates the typical cross divisional data flow for the most complex communication channels between division B and division C, which covers more than other communication channels [12].

5.2. System Response Time Analysis [14]

GDC20, 21, 23, 25 in 10CFR50 address the functionality, reliability, testability, failure mode and the ability to cope with reactivity control faults which need prompt response from protection system. To meet the those requirements, BTP7-21 gives real-time assessment guidelines, namely, time segments are allocated to each part of the PMS to ensure the overall response of the whole system meets overall time requirements.

Due to the usage of RAB bus for the critical data exchange between input/output boards and core logic board ALS-102 in ALS platform, the nature of the ALS platform is a “decentralized, centralized and decentralized” system. The operation of chassis has the similar mode as common Q, which is widely used in nuclear industry. Although the ALS-102 core logic operates in parallel, the communication via RAB bus to obtain input signals and

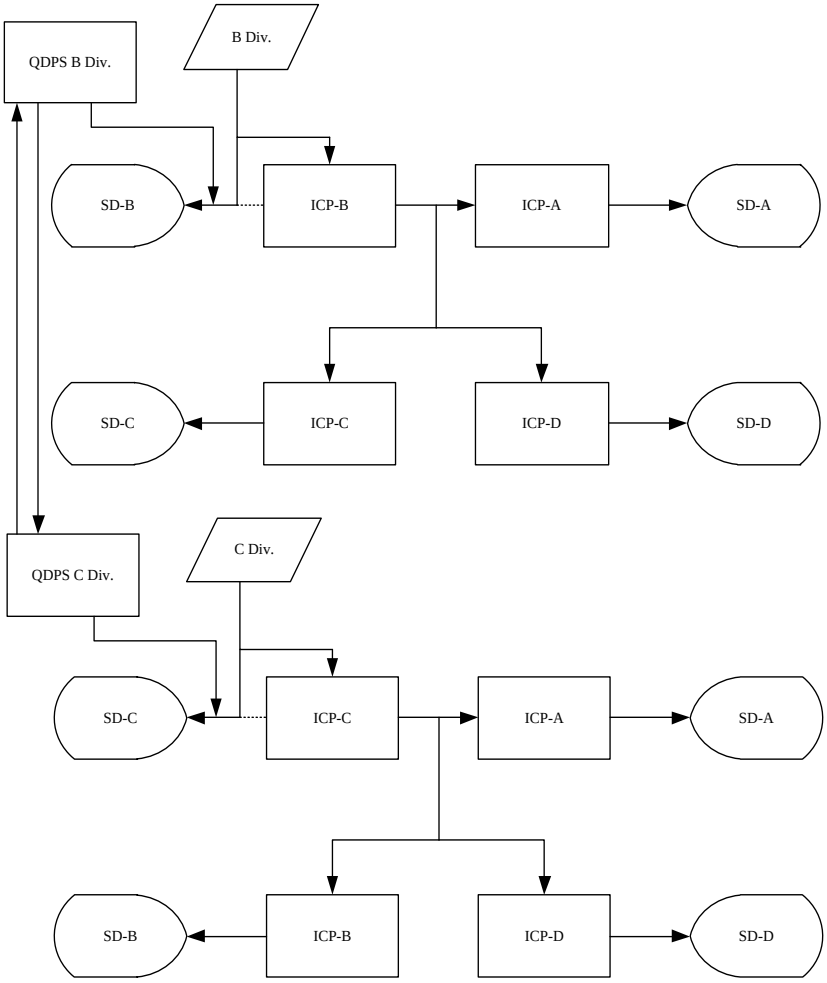

Figure 5. Cross divisional data flow between B&C division.

drive output signals, determines the similarities with other software based system in term of control and operation of I/O boards. According to product specifications, the typical scan cycle for ALS-321 is 95 ± 5 HZ, response time is 90 ms and the stable time is 400 ms. Because ALS-321 board uses a high precision 24 bit A/D converter sigma-delta, the response time for this board is not in the leading position, in comparing with that in [14]. Reference [3] points out that excluding the filtering time for the standard input and output ALS boards can be application-specific configured that might result in additional delays, the actual response time of the boards is fixed in an application.

For all boards in ALS chassis, including the ALS-601 and ALS-102, critical data exchange is conducted via RAB bus. The RAB bus in ALS platform is of redundancy, bi-direction. There is only one ALS-102 working as the “master” station to control all RAB communications in an ALS chassis. RAB uses a universal asynchronous receiver and transmitter (UART) EIA-485 protocol to send and receive data periodically in a fixed format. “Slave” boards respond immediately upon the data requirements from the “master” station and do not respond to broadcasting information. The “master” will retry the request once again if the first request is not responded in time. If the second request fails again, then the “slave” board will be tagged “failure”. Each “slave” board has a communication “watchdog” to monitor the communication with “master” boards. When detecting out the time duration to the latest successful request exceeds a predetermined value, it will automatically stop communication and set itself to “suspend” state until the fault is removed. Base on the proposal in [3], the predetermined value for this design is 2.5 times the frame time. Each transaction is initiated by ALS-102 and terminated by “slave” board. Therefore the communication is essentially a one-way, collision free data transmission. Redundant RAB provides additional error checking function.

The designed communications between the chassis, including cross divisions, shut down and actuation signals are distributed through the ALS-601 board. The port configured as “receive” collects the data from outside of chassis using the UART EIA-422 protocol data, distributes them to the specific data buffer, validates the integrity and then makes them available to be accessed by RAB. Similarly the “transmit” port gets data via the RAB and converts it to be suitable for transmitting with UART EIA-422 protocol. The UART in this design is configured with the medium rate of 460,800 bit/s, 8 bit, 1 odd parity bit, 1 end bit protocol. In case of data transmission error, this design does not support the retransmission, instead responds according to the specific function of signals, for instance, “trip” is generated for the shutdown signal and the default state is set for the ESF signal, meanwhile, activates alarms via TXB2 for operators’ attentions and proper actions. The processing time of ALS-601 board is fixed same as other I/O boards.

Because the logic of ALS platform is fixed when configuration development is completed, the real time delay is determined by the logic itself and the crystal oscillator frequency. Each board inside of an ALS platform, including ALS-102, has a single crystal oscillator only. There is only one ALS-102 working as “master” controller in a chassis, hence the RAB bus control protocol can bound the crystal oscillator drift in other boards. Due to the fact of the crystal oscillator drift is a slow process, this design does not use additional circuit to make real-time monitoring of crystal oscillator drift for ALS-102 for simplicity. Instead the provisions of the proper cycle of surveillance test of time response of PMS are conducted according to the technical specifications.

Similarly the response time delay elements for RT includes the follows: the maximum as-built and as-configured delay time for signal processing in the input board, the maximum time between consecutive accesses to the input board, maximum RAB read data transaction delay, the maximum #1 ALS-102 board as-built and as-configured processing logic delay, the maximum #1 ALS-601 board access cycle delay, RAB transaction delay, the maximum #1ALS-601 as-built and as-configured processing logic delay, the maximum time until the data transmission by #1ALS-601 contains the interested data, the maximum data transmission duration, maximum #2 ALS-601 as-built and as-configured processing delay, the maximum#2 ALS-601 access cycle delay, RAB receives the maximum processing delay, the maximum#2 ALS-102 board as-built and as-configured processing logic delay, maximum output boards access cycle delay, maximum RAB transmission delay, maximum output boards output delay. **Figure 6** shows typical shutdown signal paths.

The response time delay elements for ESF consists of the follows: the maximum as-built and as-configured delay time for signal processing in the input board, the maximum time between consecutive accesses to the input board, maximum RAB read data transaction delay, the maximum #1 ALS-102 board as-built and as-configured processing logic delay, the maximum #1 ALS-601 board access cycle delay, RAB transaction delay, the maximum #1ALS-601 as-built and as-configured processing logic delay, the maximum time until the data transmission by #1ALS-601 contains the interested data, the maximum data transmission duration, maximum #2 ALS-601 as-built and as-configured processing delay, the maximum#2 ALS-601 access cycle delay, RAB receives the maximum processing delay, the maximum#2 ALS-102 board as-built and as-configured processing logic delay, the maximum #3 ALS-601 board access cycle delay, RAB transaction delay, the maximum #3 ALS-601 as-built and as-configured processing logic delay, the maximum time until the data transmission by #3 ALS-601 contains the interested data, the maximum data transmission duration, maximum #4 ALS-601 as-built and as-configured processing delay, the maximum#4 ALS-601 access cycle delay, RAB receives the maximum processing delay, the maximum#3 ALS-102 board as-built and as-configured processing logic delay, maximum output boards access cycle delay, maximum RAB transmission delay, maximum output boards output delay, SNRC and CIM processing delay time. Although the data flow on the CIM is bidirectional, it is not through a communication link, instead of using a simplified digital signal. NRC has evaluated the CIM [15]. Although the specific communication delay time of each board is not available so far, the similar architecture with benchmarked design and the parallel operations of core logic against the serial operations of microprocessors, infers that the time delay could be less than that for the benchmark solution. When making response time analysis, the conservative consider of “just missed a scan cycle” for I/O boards and “just missed a system frame” is required as in [16], however the reservation of load time, which is a must for software based solution to ensure the proper operations of CPU in case of peaking load, is not needed in this design. Because the operation of the FPGA logic processing and microprocessor based solution is significantly different, the time allocation for each part of the PMS is likely to be different from that in [16]. As one of the most important means for design commitments and verifications, real time response measurements should be conducted according to the method in [17], where the test parameter settings for protection functions with multiple variables involved, as well as the appropriate treatment of dynamic compensations for response time measurement, are addressed.

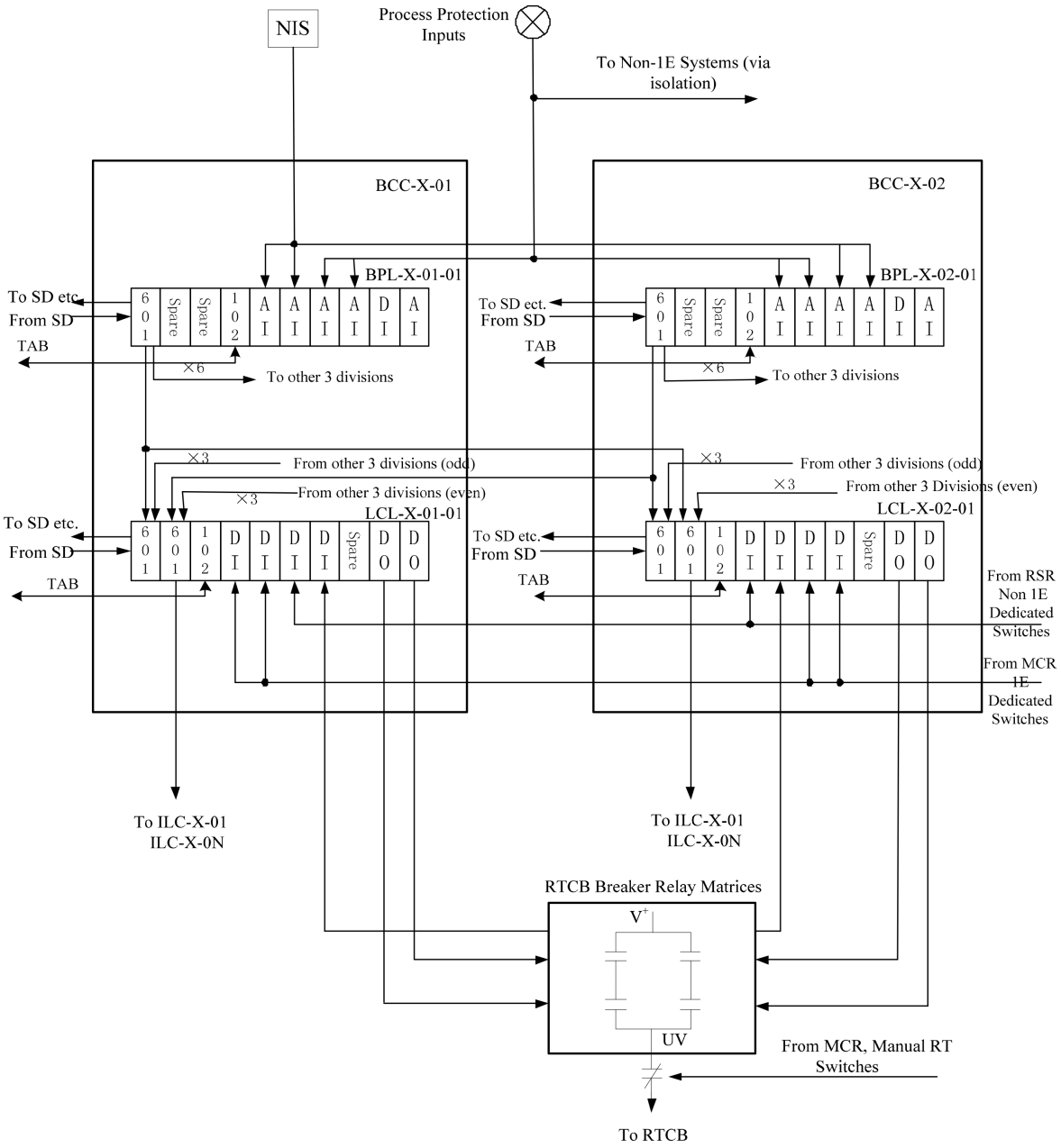

Figure 6. Reactor trip path and ESF logic path.

TXB and TAB are not in safety critical signal flow, hence these buses do not interfere with time response of safety functions. **Figure 6** and **Figure 7** show the design of the typical ESF signal paths. Please refer to [14] for details.

5.3. Deterministic Analysis [14]

Good practices for PMS design with digital microprocessor based computer are addressed in BTP7-21. EPRI TR-107330 describes the deterministic and known features for PMS. Namely, the PMS must be able to complete the tasks required within a predefined fixed time interval. Although these guides are intended for software based system, it does not fully apply to this design because the safety functions do not reply on the software, in placing with FPGA logic, its specifications and guidances on continuous and essentially non-interruptible operating cycles are still valuable for reference.

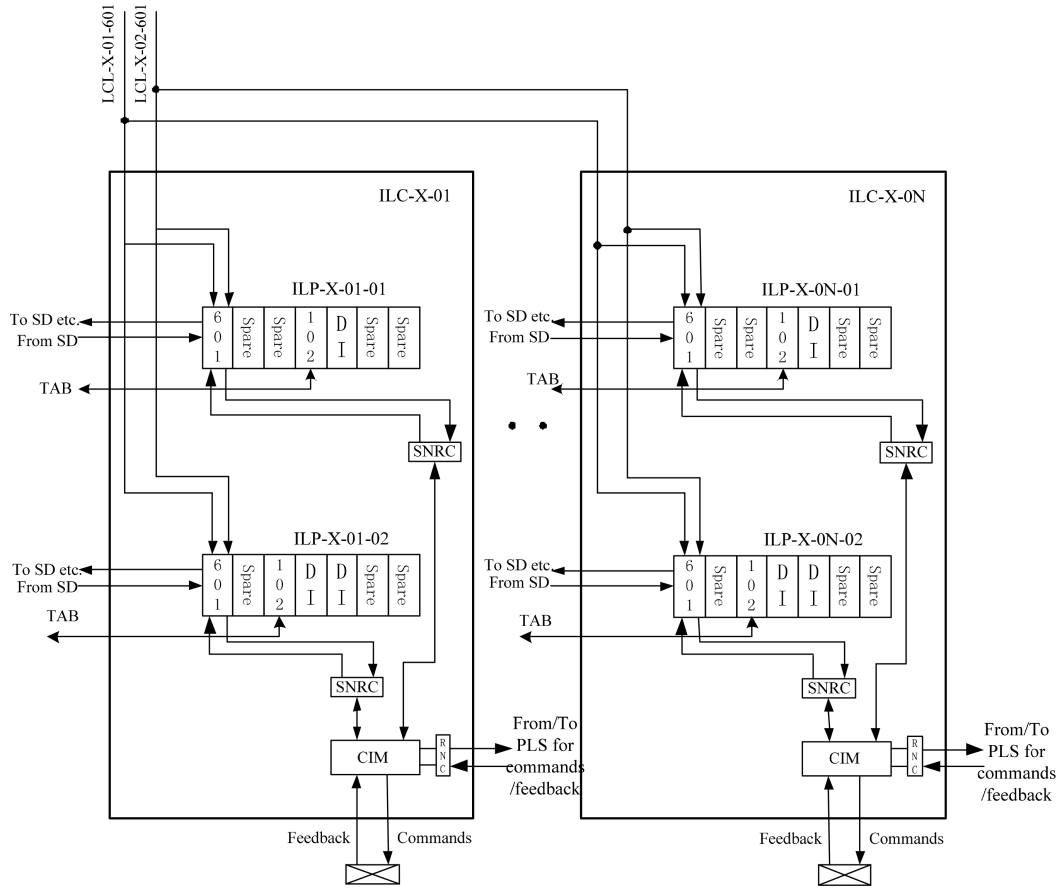

Figure 7. ESF actuation path.

ALS-102 reads data from all input boards and outputs to all output boards once in every system frame interval. Frame period is established and fixed when the development is completed. And the ALS-102 logic and safety signal flow are fixed accordingly. Hence in whatever conditions, all the data acquisitions, calculations and outputs are carried out in fixed intervals. If there are any failures in the signal flow path or missions failed to be completed within the required time intervals, the alarms will be sent to a SD through the ALS-601, meanwhile they are sent to the DDS via TXB2 to notify operators for necessary corrective actions.

The deterministic safety communication is determined by the RAB, ALS-601 and etc. Refer to [11] for details.

Excluding the PC Node Box and the MTP/ASU which are certified microprocessor based computer system, the remaining system is developed with ALS platform. All the safety-level automatic controls, are driven by FPGA based ALS platform. The ALS platform uses combinatorial logic and finite state machine (FSM) to realize the every automatic protection function. The predictable deterministic characteristics of FSM, such as, dedicated resources, only known states supported, only a single new state in each cycle, corresponding to a given state input and one and only one associated transition to the next state, are the valuable and desirable features for PMS. The periodic signal sampling, processing, output and fixed logic processing sequences regardless the contents of data and transmission are designed. This non-event driven mode, in addition to a “master-slave” structure of the RAB bus, fixed system frame, no operating system, no software for control, non-interruption, non-multi-tasking or dynamic task scheduling free and the fixed “point to point” communications between the chassis make the deterministic behavior of the PMS credible.

5.4. Self-Diagnostics, Test and Calibration Capabilities Analysis [14]

GDC 21 of 10CFR50 and10CFR60.36requires the continuous online self-diagnosis of PMS and periodically test

capabilities to validate the system's capability and ensure the possible degradation will not prevent PMS from performing the required protection functions. IEEE603 and EPRI TR-0107330 state the specific corresponding standards and guidances.

The self-diagnostic feature of the ALS platform enables the transmitting of alarm information to the SD through the ALS-601, meanwhile the alarms are sent to the DDS through TXB2 port for operators' corrective responses. Independent logic circuits carry out all board level self-diagnosis in ALS platform and do not affect the logic for safety functions. FPGA's parallel computing features ensures the self-diagnosis does not significantly increase the complexity of the system, which satisfies the requirements in BTP7-17. The self-diagnostic features of PMS monitor and diagnose most of the equipment and circuits, leading to the simplification of the periodic test and operation loads.

The built-in dual core diversity in all ALS boards and the specified embedded diversity for safety actuation ensure the valuable diversity to the PMS. To reduce nuisance failure reports resulting from the temporary external environmental conditions, such as extreme EMI transient, board level non-passing self-test results need to persist before a failure is declared and transmitted. The persistence time is configured 2.5 times the frame time and during this period the logic holds the most recent data before this transient. If the MTP/ASU is connected with the division at this period, the abnormal information is sent to ASU for debug via TAB. All these board level special self-diagnosis, testing capabilities, coupled with the similar architecture in [5] [9], furnish the PMS with super self-diagnosis, test capacity than competitors.

The 4 redundant divisions design ensures when a single division is in the test/maintenance and the other is bypassed, the system still satisfies the single failure criterion. The 8 signal redundancy LCL inputs ensure that the system does not degrade the 2004 logic when a single BPL signal fails or is in test.

ITPs receive all the redundant input signals from different sensors and make continuously compare among divisions. If the deviations among these divisional exceed a predefined vale, then an alarm indicating the failure of sensors, cables or input boards etc. will be generated. All input values, quantity, intra-division and inter-division signal comparison results are available on the SD. On-demand connected ASU can also provide more information.

SRNC and CIM have continuous self-diagnostic functions which ensure the reliable communication between ILPs and field equipment [15].

Manually periodic testing of the design, consisting of a series of overlapping tests, is conducted under the control of administrative management to verify the operability of PMS actuation and to detect hardware faults. The testing bypass must be configured through the ASU, ensuring that the test does not significantly degrade safety functions. Test signals are injected into the safety path and the consequences are monitored downstream in the safety path. The test signals are processed by the PMS hardware and logic just as the normal signals they are replacing. Test signals are injected and monitored at appropriate points along the safety path to ensure that sequential tests properly overlapped. This design does not allow setting two or more channels bypassed.

By substituting known values of the process parameter at the sensor input and verifying that the measured values are within tolerance, the sensor calibration is accomplished. Due to the extensive testing capabilities of ALS platform, lifting of leads or installation of jumpers is not required to perform manual functional or surveillance testing.

The ILP to CIM test should not be performed simultaneously in two redundant ILPs to avoid unintended actuations. The 2002 logic in CIM guarantees that the test does not actuate devices unintentionally. But in order to reduce the probability of non-intended actuation, testing time should be as short as possible, or switch the CIMs to local control mode in time.

Critical component-level commands are actuated manually from SD, which are distributed to the corresponding chassis through the ALS-601. And component feedback status is passed upstream to SD through ILP and the ALS-601.

Considering the requirement of connecting the ASU to system with sufficient frequency defined in technical specifications, the nuclear power signal calibration for gain adjustment and compensation coefficient adjustment is carried out through the ASU rather than from SD.

5.5. Diversity and Defense in Depth Analysis

Defense in depth analysis is compulsory for modern nuclear power plants [18]. Taking AP1000 I&C system as a

benchmark, as **Figure 3** indicates, this design replaces the Common Q with the interfaces and peripheral unchanged. Hence the first echelon, normally non 1E DCS, is excluded in this design. Though the design implies the non-safety DCS is Ovation system based, it can be switched over to others with minus changes. The similarity of the hierarchy and functions with AP1000 makes the evaluations more convenient and light.

The advanced core diversity and embedded diversity features of the platform [4] are deployed in the design which benefits the system a lot. In comparing with Common Q, these additional diversities are of more immunity to CCF. To achieve better diversity, the manufacture of the FPGA modules is required to use different version tools, by different management team, different design team, different development and validation team. And the functional diversities are deployed to maximum as practical. For instance, the overpower delta T is a back up of power arrange high flux rate protection. Moreover the signal diversity is deployed to maximum as practical as possible. For instance, the water level sensor of core make up tank, the pressure sensor of pressurizer, low voltage sensor of batteries and manual switches are of different type to actuate the automatic depression system. With the standard tool and parameters in NUREG/CR-7007 [19], the quantitative diversity of this design could be 0.972, without the widely used diversity actuation system (DAS) in a very conservative calculation [20].

6. Conclusions

Taking the 3rd generation of passive safety nuclear power plant as a benchmark, a new PMS overall structure based on ALS platform is designed. Because the qualified ALS platform does not include any bus based communication boards for communication between chassis, specific design of using point-to-point based ALS-601 communication board, is developed for the inter-divisional and intra-divisional communications. And the design's consistency with SRP, in the perspective of data communication independence and isolation, deterministic, diversity requirements, is studied. The research indicates that the design satisfies the relevant requirements.

Due to no engineering practice of PMS based on ALS platform in the world so far, this new designed solution can be a good reference for the coming engineering projects though there are maybe some refinements and further evaluations required.

References

[1] Xu, Z., Lei, Q. and Chen, D.L. (2014) Diversity Quantitative Analysis on CIM and DAS. *Process Automation Instrumentation*, **35**, 73-76.

[2] Qin, Y.Q., Cao, X.M. and Zhu, M.Y. (2013) Application of FPGA Based Advanced Logic System in Nuclear Power Plant Instrument and Control. *Association for Science and Technology Forum*, **9**, 40-41.

[3] NRC (2013) Nuclear Regulatory Commission Safety Evaluation for Topical Report 6002-00301. Advanced Logic System Topical Report, NRC, Rock Ville.

[4] Warren, O.G. (2013) Advanced Logic System Topical Report-Nuclear Safety Related. CSI, Cranberry Township.

[5] Lin, C.G. and Yu, Z.S. (2008) Passive Safety Advanced Pressurized Water Reactor Technology. Atomic Energy Press, Beijing, 26-29.

[6] Guangdong Nuclear Power Plant Training Center (2007) 900MW PWR Nuclear Power Plant Systems and Equipment. Version 2, Atomic Energy Press, Beijing, 254-317.

[7] Kharchenko, V., Siora, O. and Sklyar, V. (2011) Multi-Version FPGA-Based Nuclear Power Plant I&C Systems: Evolution of Safety Ensuring, Nuclear Power-Control. Reliability and Human Factors, InTech, 27-48.

[8] Zheng, W.Z. (2012) Application of DCS for Protection System in Nuclear Power Plant. *Nuclear Electronics & Detection Technology*, **32**, 438-452.

[9] Sun, H.H., Cheng, P.D., Miu, H.X., *et al.* (2010) Third Generation Nuclear Power Technology AP1000. China Electric Power Press, Beijing, 322-412.

[10] NRC (2009) Highly-Integrated Control Rooms-Communications Issues (HICRc) Interim Staff Guidance. NRC, Washington DC.

[11] Xu, Z. and Lei, Q. (2015) Data Communication Analysis on the Design of PMS Based on the ALS Platform. *Automation & Instrumentation*, **30**, 9-26.

[12] Xu, Z. and Lei, Q. (2015) Data Communication Design of PMS Based on the Advanced Safety Platform. *Nuclear Electronics & Detection Technology*, **35**, 462-467.

[13] NRC (2007) NUREG-0800 Standard Review Plan. NRC, Washington DC.

[14] Xu, Z. and Lei, Q. (2015) System Integrity Analysis on the PMS Designed with the ALS. *Journal of Nuclear Engi-*

neering Technology, **5**, 1-12.

[15] NRC (2011) Final Safety Evaluation Report Related to Certification of the AP1000 Standard Plant Design. NRC, Washington DC.

[16] Wang, J.N., Zhou, A.P., Xi, Y.X., *et al*. (2012) Analysis and Test of Respond Time of Nuclear Power Plant Digital Control System to Reactor Trip. *Nuclear Power Engineering*, **33**, 5-10.

[17] Xu, Z. and Bao, Q. (2015) Analysis on the Response Time Testing of OPΔT/OTΔT Protection. *Nuclear Science and Techniques*, **38**, 040606-1-040606-7.

[18] NRC (1994) NUREG/CR-6303 Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems.

[19] NRC (2009) NUREG/CR-7007 Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems.

[20] Xu, Z. (2016) The Diversity and Defense-in-Depth Analysis of the Design of PMS Based on the ALS Platform. *Process Automation Instrumentation*, **37**, 22-29.