Concept of advanced back-up control panel design of digital control room

JIANG Guojin, SUN Yongbin, TAN Ke, ZHANG Liming, SHI Ji, ZHANG Xuegang, HUANG Weijun, MAO Ting, and LIU Yanzi

I&C design department, Department, CNPEC, Shenhua Building.No 7018 Beihuan Road, Shenzhen, 518000, P.R.China (jiangguojin@cnpec.com.cn, sunyongbin@cnpec.com.cn, tanke@cnpec.com.cn, zhangliming@cnpec.com.cn, shiji@cnpec.com.cn, zhangxuegang@cnpec.com.cn, huangweijun@cnpec.com.cn, maoting@cnpec.com.cn, liuyanzi@cnpec.com.cn)

Abstract: Back-up control panel (BCP) of digital main control room (DMCR) is the back-up means for main computerized control means (MCM). This paper focus on technical issues for advanced design of back-up panel (BCP) for CPR1000 using qualified computer-based video display unit to display plant process indication and alarms. Human factors engineering (HFE) issues also have been considered in the BCP design. Then, as the mean to fulfill safety target of nuclear power plant (NPP), an ideal ergonomic design method is exploited for advanced BCP design.

Keyword: back-up control panel; human factor engineering; digital main control room; main computerized control means

1 Introduction

Recently, Digital Control System（DCS）and digital main control room (DMCR) have been widely applied to Generation 2 and Generation 3 nuclear power plants (NPPs) around the world. In order to introduce a workstation-based main control room (MCR) of CPR1000 in China, the authors of this paper assumed that the MCR is comprised of the following operating facilities to support the operating staffs for efficient and safe plant operation：

(i) 4 sets of operator workstations (OWPs).
(ii) A large display panel (LDP) for display of overall plant operational and safety assessment data
(iii) A back-up panel (BCP) which provides controls and information for all class 1E, safety-related components and critical operator action independent of the OWPs.

These operating facilities are designed to meet with an operation philosophy of advance MCR as illustrated Fig.1. As seen from Fig.1, this is composed by three-layer frame of plant information level, system level information and component level information.

The main computerized control means (MCM) for DMCR should be realized by plant information and control system (PICS) with the availability of 99.99%. And therefore, total loss of PICS has to be taken into consideration during the process of DMCR design so that a workstation-based DMCR should provide with the qualified back-up means. The DMCR should contain several functions of hardwired controls, alarms and indicators to maintain the state of nuclear power plant for a short period and then to bring it to a safe shutdown state when the MCM becomes unavailable situation due to a common mode failure.

Therefore besides the MCM, the DMCR should be also fitted with BCP which consists of hardware and software controls as well as monitoring means. The BCP should be designed as a back-up means of the MCM. The BCP should also provide with sufficient control and monitoring means to bring and maintain the plant in a safe state as a backup of MCM, for both in normal conditions and in Design Basis Accidental situations that are probable during a planned or unplanned unavailability of the MCM.

Received date: July 4, 2011
(Revised date: September 30, 2011)

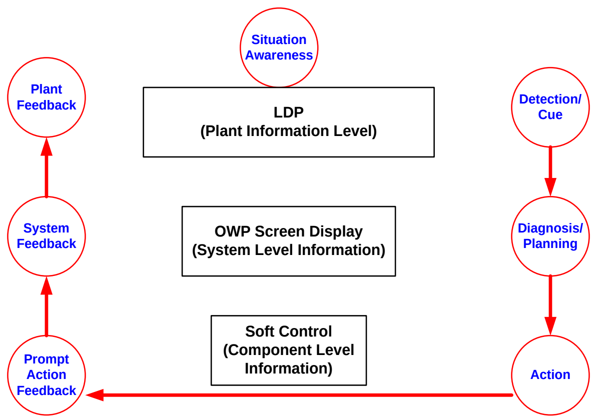

Fig. 1 Operation philosophy on workstation-based MCR.

2 Necessary of advanced BCP

In the both cases of Generation 2 and Generation 3 NPPs, the size of DMCR is fixed due to the limitation of NI structure. In the current design of DMCR, the BCP consists of controls, indicators and alarm tiles of conventional type, which occupy large space in the DMCR. And also, to use conventional devices for the BCP will lead to a falling-off in design flexibility.

To overcome the inherent inflexibility of spatially dedicated Man Machine Interface (MMI) on conventional BCP, the current designing of NPP should consider so that the BCP can adopt with the computer based MMI technologies instead of using conventional type of indicators and alarm tiles. In order to accomplish the advanced BCP design, a large number of spatially dedicated indicators, alarm tiles in a traditional BCP have to be replaced by a few common multi-functions Video Display Unit (VDU). These MMI devices, so called Qualified Display System (QDS), Post Accident Monitoring System (PAMS) and QDS-N (non-safety), consist of a computer-based Flat Panel Display (FPD) device with a touch sensitive screen which can provide with important functions of indication and alarm of plant systems and components.

The approaches and methodologies which are taken in designing for advanced MMI device application can be also applied for the designing of BCP. In the subsequent Chapter 3, major features of the QDS-N are also explained how the QDS-N was designed into the system to better cope with regulatory requirements. The authors of this paper utilized various international standards [1-8] as listed in the references during the course of this presented pilot study.

3 Issues for advanced BCP design

3.1 Design overview of advanced BCP

3.1.1 Configuration of BCP

The overall Configuration for MMI Assignment on BCP is illustrated in Fig. 2. On the proposed design the advanced BCP consists of the six items as described below:

(i) Spatially dedicated control devices for safe shutdown and emergency operation procedure.

(ii) Spatially dedicated indicators to provide backup

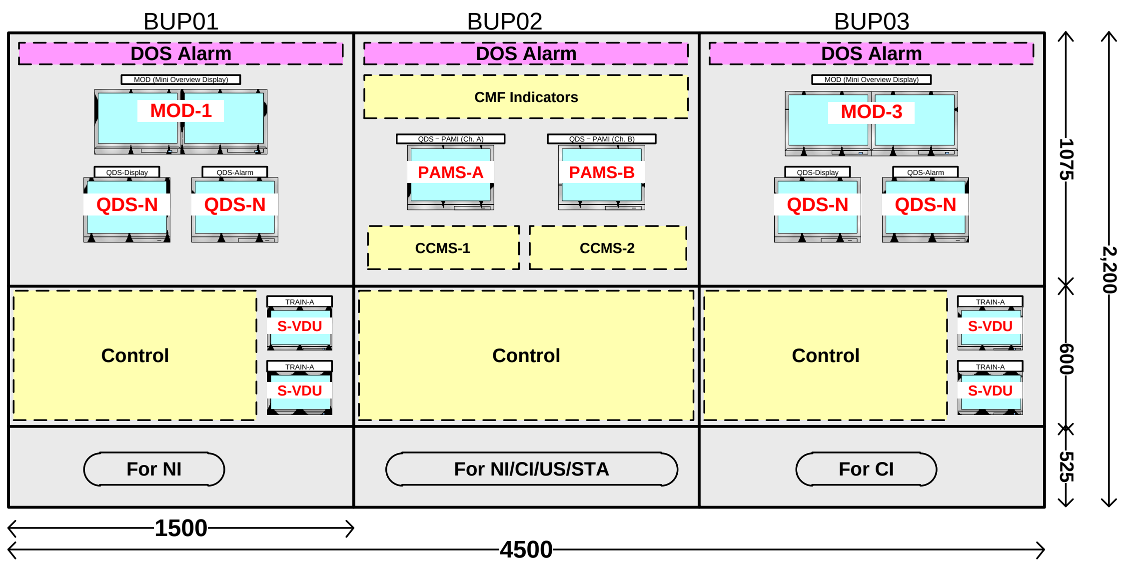

Fig. 2 Overall configuration for MMI assignment.

indication of QDS PAMS FPD. If the design of QDS-PAMS satisfies with the safety design requirements, then these indicators can be deleted. So, these indicators are optional.

(iii) Two sets of QDS-N FPDs for plant key parameters related to plant safety

(iv) Two sets of QDS PAMS for indication for the variables requested in R.G. 1.97 Cat. 1 and some of Cat. 2 variables (one for Train A and the other for Train B).

(v) Three sets (or two sets) of Mini-Overview Display (MOD) for plant overview.

(vi) Spatially dedicated alarm tiles to provide DOS alarms

3.1.2 Functional assignment of BCP

Figure 3 shows overall functional assignment on the BCP to meet with the regulatory requirements and also to achieve the mission of BCP satisfactorily.

3.2 Design of QDS-N

In this subsection, the design features of QDS-N are described one by one in the below.

Allocation - Two sets of the QDS-N FPDs are located on the BCP to allow access to information or selected trends during performing State Oriented Procedure (SOP) or safe shutdown. One set is for the NI operator, while the other one set for the CI operator. Each set of the QDS FPD consists of one display FPD and one alarm FPD. However, an alarm FPD can be switched to a display FPD by the operator's selection.

System Configuration – The QDS-N consists of the following equipment:

(i) Two sets of QDS-N FPDs (18.1 inch x 2 FPDs),

(ii) Redundant QDS-N servers, and

(iii) Redundant QDS-N Network (non-classified class)

Diversity - The QDS-N should satisfy the condition of diversity from PICS OWP, in order to protect against common mode failure of OWP.

Qualification – The QDS-N is qualified seismically and environmentally in order to provide the information, alarms for plant safety and key parameter both during and after the seismic design basis event. The QDS-N and MOD need not be qualified as Safety or Safety-Related software. All software is Non-Classified (NC).

Communication between QDS-N and PICS - The QDS-N servers should include the necessary

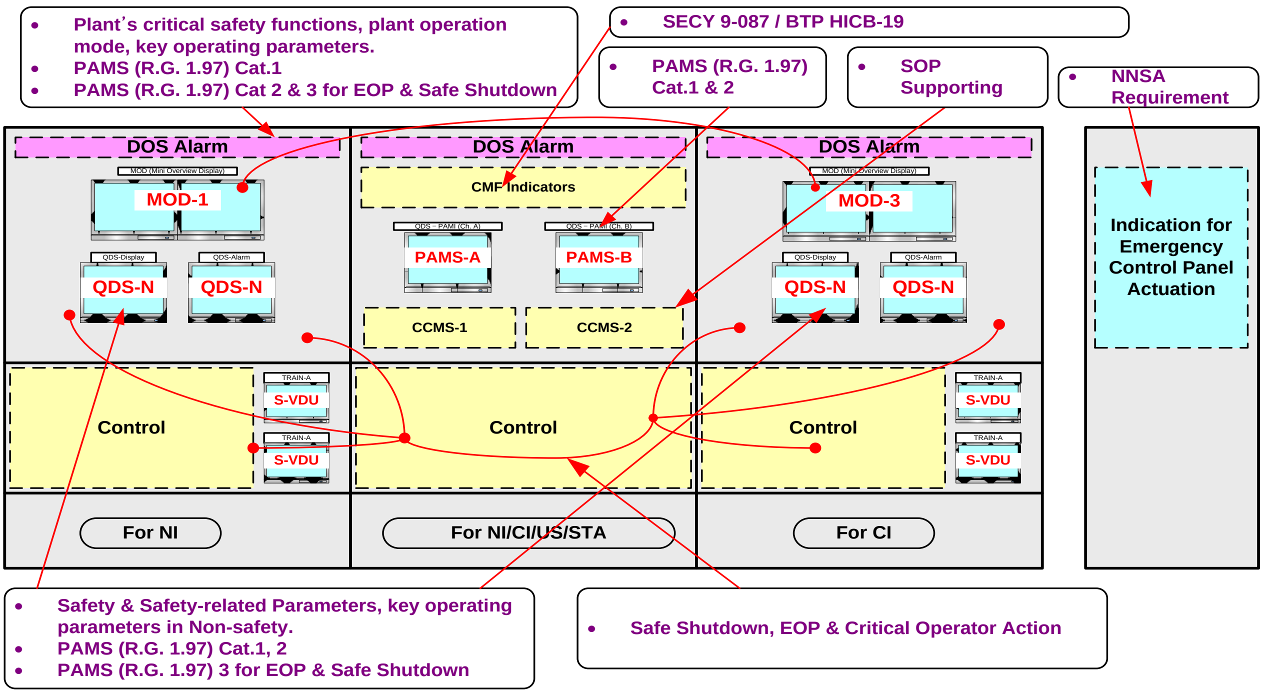

Fig. 3 Overall function assignment on BCP.

communications interface to connect with PSAS from which it can receive process information and alarms processing information.

3.3 QDS-PAMS

Detailed design description for QDS PAMS is provided on 'Requirement for QDS' and 'QDS Concepts and Qualification.

3.4 Mini-overview display (MOD)

In the current designing of MCR, there exists no plant overview display device in the MCR when the MCM is unavailable. It would make the operators some inconvenience and inconsistency to operation circumstance. Therefore, Mini-overview display (MOD) is introduced in QDS-PAMS.

As far as the configuration of MOD is concerned, three sets (or two sets) of MOD are provided on the BCP: one set is for NI operator, one set is for CI operator, and the other set is for US and SA.
Each set of MOD is located above vertical section on the BCP 01, 02 and 03. A MOD consists of two Qualified FPDs of 18.1 inch in size and Qualified processors.

The MOD functions work continuously during the entire period of the system in normal operation except when the MOD equipment is being tested or maintained.

3.5 Backup indication for QDS PAMS

The BCP provides the backup indication for PAMS Cat. 1 variable to comply with the Chinese NNSA apprehension according to the use of computer-based VDU.

Approximately 50 indicators in total are provided for PAMS Cat. 1 variables for Train A and B.
Backup Indication is implemented by spatially dedicated hardwired indicators. These indicators are located below QDS PAMS FPD.

3.6 Optimizing BCP layout base on HFE method

The purpose of BCP layout optimization is to decrease the workload of operators by means of reasonable division of sub function area and adjustment of the location of different sub function area in accordance with logically related operational sequence.

According to the current BCP size, functional distribution of both the hardware and software components and the importance of BCP controls can be analyzed. And then the operation sequence and frequency of BCP equipments can be figured out by means of mathematics method. The result could be reliable due to statistical analysis.

Based on the result, the BCP layout can be optimized by specific arithmetic method to minimize the operators' workload for the operation especially in case of applying accident procedure. Combining the operator's experience and layout requirement of HFE, the optimizing result can be revised and the final layout design can be optimized successfully.

3.7 Functional and task analysis optimization

Based on the functional and task analysis, the control and information used for the operators during the MCM failure mode or all Design Basis Accident (DBA) conditions are determined for the optimization of the BCP. These functions are assigned on the BCP or between BCP and ECP when you limit the controls and information for each specific situation. This would lead to retain only the minimum means to operate the situations to be handled from the BCP.

The control and monitoring on BCP is different from that by PICS, because not all the MCM equipments are supported by BCP. That means the numbers of control and monitoring should be limited for each accident type. For the equipments which do not belong to urgent operation in accident, they can be controlled locally and not needed on BCP. The precondition of this situation is that the operator has enough time to operate in local place. For example, in the reactor condition of completely unloaded mode or accidental mode, operator should operate the valves of Reactor Cavity and Spent Pit Cooling System (PTR). After analyzing this case, the operation time of PTR valves is not so urgent in case of the reactor condition where completely unloaded mode or accidental mode, so the operator could finish the operations locally according to the a certain pre-determined rules. These equipments are not needed to set on BCP.

4 Conclusion

The advanced BCP will achieve the safety target of NPP by applying both conventional and digital monitoring and control means. However, the ergonomics effect of shift team will be increased by introducing the same style MMI is applied to VDU on BCP. This will be the subject of further studies in future.

Nomenclature

ATWS	Anticipated Transients without Scram
BDBA	Beyond Design Base Accident
CMF	Common Mode Failure
CPR1000	Chinese Pressure water Reactor
DCS	Digital Control System
DBA	Design Basis Accident
ECP	Emergency Control Panel
ESFAS	Engineering Safety Feature Actuation System
HEF	Human Factors Engineering
I&C	Instrumentation and Control
MCR	Main Control Room
MMI	Man Machine Interface
NPP	Nuclear Power Plant
OWP	Operator Workstation
PTR	Reactor Cavity and Spent Pit Cooling System
PWR	Pressurized Water Reactor
P-VDU	Recording Visual Display Unit
POP	Plant Overview Panel
RPS	Reactor Protect System
S-VDU	Safety Visual Display Unit
SG	Steam Generator
SOP	State Oriented Procedure

Acknowledgments

I would like to appreciate the design team of Main Control Room system for their kind contributions and their comprehensive study in BCP optimization method for Chinese Pressure water Reactor NPP design.

References

[1] United States Nuclear Regulatory Commission: NUREG-0700 Human-System Interface Design Review Guidelines Revision 2, 2002.

[2] Electrical and Electronics Engineers, Inc.: IEEE 603Standard Criteria for Safety Systems for Nuclear Power Generating Stations, 2009.

[3] Electrical and Electronics Engineers, Inc.: IEEE 7-4.3.2 Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, 2010.

[4] United States Nuclear Regulatory Commission: SECY 93-087 Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs, 1993.

[5] International Electro-technical Commission: IEC 964 Design for Control Rooms of Nuclear Power Plant, 1984.

[6] United States Nuclear Regulatory Commission: R.G. 1.97 Instrumentation for Light-water-cooled NPP to Access Plant and Environs' Conditions During and Following an Accident, 1983.

[7] United States Nuclear Regulatory Commission: NUREG 0737 Clarification of TMI Action Plan Requirements, 1980.

[8] United States Nuclear Regulatory Commission: NUREG 0636 Functional Criteria for ERF, 1980.