CNIC-00597
TSHUNE-0037

中国核科技报告

CHINA NUCLEAR SCIENCE & TECHNOLOGY REPORT

核电厂安全参数显示系统的设计特点

DESIGN CHARACTERISTICS OF SAFETY PARAMETER DISPLAY SYSTEM FOR NUCLEAR POWER PLANTS

原子能出版社

中国核情报中心
China Nuclear Information Centre

张源芳：清华大学核能技术设计研究院副研究员，1961年毕业于清华大学工程物理系核物理电子学专业，1964年该专业研究生毕业。

Zha Yuanfang: Associate professor of the Institute of Nuclear Energy Technology, Tsinghua University. Graduated from the Department of Engineering Physics of Tsinghua University in 1961, majoring in nuclear physical electronics and graduated from the same speciality as a postgraduate in 1964.

CNIC-00597
TSHUNE-0037

核电厂安全参数显示系统的设计特点

张源芳
（清华大学核能技术设计研究院，北京）

摘　要

介绍了清华大学开发的核电厂安全参数显示系统的设计特点，其中包括了系统功能上的新特点：(1)分层显示结构；(2)显示格式设计中的人因技术；(3)核电厂安全状态的自动诊断；(4)安全参数显示系统使用范围的扩展；(5)灵活的硬件结构。同时还介绍了新的设计方法：(1)完全采用国际设计标准；(2)严格选择安全参数；(3)在多任务操作系统下开发软件；(4)使用核电厂模拟器作为验证工具。

DESIGN CHARACTERISTICS OF SAFETY PARAMETER DISPLAY SYSTEM FOR NUCLEAR POWER PLANTS

Zhang Yuanfang
(INSTITUTE OF NUCLEAR ENERGY TECHNOLOGY,
TSINGHUA UNIVERSITY, BEIJING)

ABSTRACT

The designing features of safety parameter display system (SPDS) developed by Tsinghua University is introduced. Some new features have been added into the system functions and they are: (1) hierarchical display structure; (2) human factor in the display format design; (3) automatic diagnosis of safety status of nuclear power plant; (4) extension of SPDS use scope; (5) flexible hardware structure. The new approaches in the design are: (1) adopting the international design standards; (2) selecting safety parameters strictly; (3) developing software under multitask operating system; (4) using a nuclear power plant simulator to verify the SPDS design.

Safety parameter display system (stimulation) of the nuclear power plant has been completed after three-year development and passed the verification and validation organized by The National Nuclear Safety Commission of China in this year. Comparing the SPDS developed by our project team with the similar kind of safety instrumentation systems developed by other institutes of our country and the SPDS issued by other countries, this SPDS has some new ideas and characteristics in the system function and design method.

1 COMPLETE ADOPTING INTERNATIONAL DESIGN STANDARDS

In order to let our designed system to achieve the advanced world level and to carry on the technical exchange with other countries or the related international organizations, the general international design standards must be adopted. When we designed this SPDS, we collected and adopted all international standards about the SPDS issued by International Electrotechnical Commission (In fact, these standards have been or will be adopted equivalently as the national standards of China). Among them there are two main standards.

(1) IEC 960: Function Design Criteria for a Safety Parameter Display System for Nuclear Power Stations, which was issued by IEC in 1988. This standard was worked out based on the experience summary of the SPDS development of each country within recent 10 years. It includes the detailed requirements about the general performance, function design criteria, display format, data validation, operability requirement and function testing of the SPDS.

(2) IEC 880: Software for Computers in the Safety System of Nuclear Power Stations, which was issued by IEC in 1986. This standard completely stipulates the design principle, progamming method and testing criterion used to design a software for computers in the safety system of nuclear power plants.

Based on the complete analysis of these standards, all clauses of these standards are adopted strictly, except that the system avilability requirement is relaxed limitedly because of the nature of this simulation system. Our experience proves again that this step is the basic guarantee for our designed system to achieve the advanced world level.

2 STRICT SELECTION OF SAFETY PARAMETERS

The SPDS should be designed to bring together a minimum set of the plant safety parameters which can aid the operators to analyze and diagnose the plant abnormality and assists the operators to select the most effective corrective actions. The number of the safety parameters can not be too less that they are not enough to reflect exactly the overall safety status of the nuclear power plant and the number can not be too much that it might follow the same disastrous road of the old instrument panel. Therefore, it is a main technical key in the SPDS design to select carefully each safety parameter.

(1) Selecting safety parameters starting from the point of safety analysis of the nuclear power plant. In order to guarantee safe operation of the nuclear power plant and avoid radioactivity leaking out from the reactor system, the general safety function can be divided into six critical safety functions. It includes reactivity control, reactor core cooling, core heat removal, pressure boundary integrity, containment and coolant inventory. Several parameters should be selected to indicate the safety function integrity degree for each critical safety function. According to the importance and reliability of each parameter to reflect the general safety of whole plant or a certain critical safety function, 8 parameters showing the general safety of whole plant, 45 parameters indicating integrity degree of six critical safety functions and 64 auxiliary parameters determining further the accident cause are selected finally.

(2) Verifying the accuracy of the safety parameter selection starting from the point of using the emergency procedure of the nuclear power plant. The emergency operating procedure is a criterion followed by operators to deal with all significant accidents of the nuclear power plant. The parameters in the procedure used by operators to judge accident occurrance and its nature and to make decision to take corrective actions should be consistent and identical with the safety parameters selected in the SPDS. Therefore, the main parameters in the emergency procedure can be used to prove the reasonableness and accuracy of the safety parameter selection. End Path Procedure and Function Restoration Procedure created by Westinghouse Corporation are analyzed. It is proved that the safety parameter set selected through safety analysis is consistent with the main parameter set used in the emergency procedure and satisfies the need of emergency procedure use.

3 EXPLICITLY ADOPTING HIERARCHICAL DISPLAY STRUCTURE

According to the requirement of information concentration and simple display format, it is obvious that too many parameters can not be displayed in a picture. In fact, the amount of the parameters related with plant safety is quite big. It is not possible definitely to fully present the overall safety status of whole plant with a picture. In order to solve this contradiction, a hierarchical display structure is adopted. In the past, a two level display structure is used in some SPDS, but its context and complication is not very definite and clear.

Principle of hierarchical display: All safety parameters are divided into several display levels according to their importance related to the plant safety and their usage purposes; also the parameters in same level are divided into several pictures according to their inherent relations for the plant safety.

Division of display level: In our system, all pictures are divided into three levels: (1) the first level is to reflect the general safety of whole plant, amount to three pictures; (2) the second level is to reflect the integrity degree of each critical safety function, amount to six pictures; (3) the third level is to reflect the operating status of the main plant systems, amount to ten pictures.

The main picture of the first level is an ordinary display. The second level is automatic display which can be changed automatically guided by the diagnosis result of the plant accident. All pictures including the third level can be manually selected by operator at any time.

Due to the clear definition of levels and perfect picture control method, this hierarchical display structure not only solves the contradiction that each picture must be as simple as possible but the safety context concerned by the SPDS should be as deep and broad as possible, but also can assess any plant safety parameter with a minimum of operation actions.

4 APPLICATION OF HUMAN FACTOR IN THE DISPLAY FORMAT DESIGN

The design of display format should accord with the demands of human factor so that the SPDS can be accepted easily by the operators and the largest amount of

information can be obtained quickly and correctly from it. During the design of this system, the following factors are considered:

(1) Whole screen is divided into three fixed areas (title area, graph display area and man-machine interface area) and two windows (astronomical time window and a small size of the general safety octagon window). According to the regular for people to search information, the most important parameters are placed successively in the middle, top and left side of a picture.

(2) The graph that can be dynamically changed is adopted as far as possible to reflect the change of the safety parameters, such as the change of a bar length used to show the change of a parameter value, the change of an octagon pattern used to show the change of the general safety status, because the graph information and its dynamical change has the largest possibility to attract operator's attention.

(3) CRT technology, such as various color and color changing, twinkle and sound is adopted fully so that the graph pattern is clear and its change can be easily distinguished.

(4) A convenient man-machine interactive system is provided with combination of the keyboard function and menu prompt so that any pictures of the three levels can be assessed simply and easily.

5 AUTOMATIC DIAGNOSIS OF THE SAFETY STATUS AND DIAGNOSIS DIVERSIFICATION

According to the design standard of the SPDS, it is required to provide only safety parameters exactly as they are, not the automatic diagnosis of the plant safety status. In order to let the SPDS to play more important role, in our system an automatic diagnosis function is added and this diagnosis criterion is diversified.

(1) Critical safety function diagnosis. This is a diagnosis directed against the safety function of the nuclear power plant. The critical safety status tree suggested firstly by Westinghouse Owner Group is adopted to diagnose the integrity degree of the critical safety function. Diagnosis results of each function are divided into four grades: emergency, serious deviation, abnormal and normal condition, which is presented with a red, orange, yellow and green indicator separately.

(2) Design basis accident diagnosis. This is a diagnosis directed against accident symptom. Eight parameters which are related directly to the design basis acci-

dent and which values are changed sensitively following accident development are selected. An octagon consists of this eight parameters and its eight-diagonal lines are taken as eight parameter coordinate axes. When the plant is in a safe condition, the octagon consisted by eight selected parameters is a regular octagon. If any design basis accident occurs, the octagon will be distorted into an irregular octagon due to deviation of any parameter from the normal range.

The diagnoses oriented to the critical safety function and oriented to the design basis accident are started from two different points of view but they are complement each other. Diagnosis diversification and their cross check each other is very useful to guarantee reliability and accuracy of diagnosis result.

6 EXTENSION OF USE SCOPE OF THE SPDS

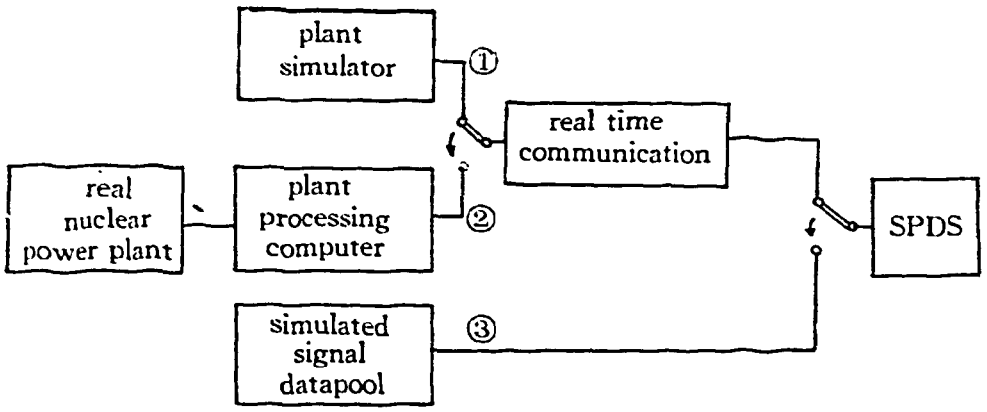
In general, the SPDS is used mainly to monitor the safety status of the nuclear power plant after reactor trip, because there is no problem of the plant safety function monitoring in the normal operation condition. According to our analysis, the basic method and pattern adopted in safety monitoring can be completely extended to monitor main operating parameters in the normal condition.

(1) The display and diagnosis is divided into two groups. One is for the safety parameter monitor under the plant emergency condition, another is for the normal parameter deviation monitor under the plant normal condition. According to our analysis, the safety parameters monitored under the plant emergency condition are basically consistent with the main parameters monitored underthe normal condition, only a few parameters are different. In the first display level where the number of display parameters is limited strictly, the optimum parameters of two monitors should be selected more carefully according to their particular requirements.

(2) The similar automatic diagnosis method is applied to monitor the deviation of the normal operating parameters in order to detect the abnormal phenomena which are caused by improper operator actions, operation degradation and early development of accident. Of course, the judgement criteria, parameters and setpoints selected for two monitors are different. The changing point from the normal parameter deviation monitor to the safety parameter monitor is the activation of the reactor trip or safety injection. When the monitor is changed, the judgement criterion, as well as its parameters, setpoints and parameter scales in display is changed synchronously.

7 FLEXIBLE HARDWARE STRUCTURE FOR MULTIPURPOSE USE

In order to meet the both requirements of adding a SPDS simulation system in the simulator of Beijing Nuclear Power Plant SimulationTraining Center and producing the project evaluation of a SPDS used in the real nuclear power plant, also considering the actual situation that a SPDS is not required to be a qualified safety system or necessary to meet the single-failure criterion, so the following hardware construction is adopted: (1) a high qualified minicomputer as the main body of the SPDS, (2) using a communication system to connect the SPDS with its monitored object, such as the plant system itself or the plant simulator, to obtain the safety parameters. This hardware system can meet the following applications:



(1) Using a real time data communication system to link with a plant simulator to obtain the required safety parameters from the datapool of the simulator computer, this structure can be used as a simulation system of the SPDS in a PWR simulator.

(2) Using a real time data communication system to link witha plant processing computer of a real nuclear power plant to obtain the required safety parameters from the database of this computer, this structure can be used as a real SPDS in an actual nuclear power plant.

This structure is very useful in the special situation that the plant has been put

to operation but the SPDS was not installed originally. It is very difficult to add a set of the sensors for the SPDS, but, in general, the plant processing computer might have those safety parameters required by the SPDS.

(3) Connecting with simulated signal datapool, this structure can be used to demonstrate the plant operation nature and SPDS function in off-line mode, unconnecting the plant simulator or the plant processing computer.

8 DEVELOPMENT OF SOFTWARE UNDER MULTITASK O-OPERATING SYSTEM OS/2

OS/2 is a multitask operating system used in the minicomputer PS/2 issued by IBM corporation of America in recent year. It has a more powerful system function than that of the single task operating system DOS.

Multitask: OS/2 operating system provides multitask dispatch (control), communication and protection function which can guarantee the reliable and simultaneous operation of multitask. According to function definition, the whole software of the SPDS is divided into five tasks such us communication, display, diagnosis, emergency procedure guide and print, in the meantime, the program in a task can be also divided into several modules according to their nature and character. Besides, several common data areas, such as dynamic operating data, historic recording data, diagnosis result data, are created for multitask shared data to carry on interactive data communication of all tasks. Therefore, whole SPDS consists of a hierarchical structure software in the building block way and a full modularization is achieved in code development. It lays a fundation to increase the efficiency of software design, to decrease the error rate of code development and to realize the extension of software structure.

Real time: All functions of the SPDS should respond the change of plant status on time. Its responsive speed should catch up with the fierce transient of the nuclear power plant. The modules related to the real time response are transmission of safety data to the common data area in the communication task, judgement of the plant status in the diagnosis task, data renewal of the dynamic parameters and man-machine interactive response in the display task. OS/2 operating system provides a powerful real time service, interrupt service and priority dispatch so that the SPDS can meet the perfect real time requirement. At present, renewal interval of

the dynamic data is 4 s and the mean time of a display changing is 5 s.

9 OVERALL EVALUATION OF THE SPDS USING A SIMULATOR AS TEST TOOL

The SPDS is a new conceptual safety system of the nuclear power plant. It is necessary to carry on a strict project verification and effect validation. In the past time there was not a full scale simulator so that the V&V is conducted only with a simple test method under the laboratory condition or with a long term examinution in the real nuclear power plant. Obviously, the effect of these test methods might not be very good. After the middle of the 1980s, all of advanced countries recommend the simulator as a test tool to conduct an overall evaluation of the SPDS, esp, to test the design functions of the SPDS with the plant accident manoeuvres on the simulator. The following tests have been completed and their related conclusions are drawn:

(1) Testing of system functions

The accuracy of the safety parameter selection: The tests show that each selected safety parameter is necessary and adequate to reflect a certain kind of the plant safety function or the accident which may occur in a real nuclear power plant.

The correctness of the diagnosis function: The tests show that two dignosis criteria can judge correctly the critical safety functions and the basis design accidents separately and a cross check of their diagnosis results is useful to guarantee the diagnosis reliability.

(2) Testing of system use effect

In the simulated control room, the use effect with and without this SPDS is verified and compared. The tests show that this SPDS is very useful in assisting operators to earily find the symptom of accidents, to judge the accident nature, to select a related emergency procedure and to implement a corrective action quickly and correctly under anomalous conditions.

(3) Testing of system use efficiency

The use efficiency of the SPDS is related closely to the system integrity and man-machine interactive system performance. The tests show that the display format is consistent with the principle of human factor and this system may be accepted and understood easily by operators. The tests also show that the man-machine

interactive system is convenient and reliable to respond any operator commands to control this SPDS.

ACKNOWLEDGMENT

Give thanks to The National Nuclear Safety Commission of China and International Atomic Energy Agency for their great support to this research project.

核电厂安全参数显示系统的设计特点
原子能出版社出版
（北京 2108 信箱）
中国核情报中心排版
北京市海淀区三环快速印刷厂印刷
☆
开本 787×1092 1/16 · 印张 1 · 字数 15 千字
1992 年 2 月北京第一版 · 1992 年 2 月北京第一次印刷
ISBN 7-5022-0621-3
TL · 365

CHINA NUCLEAR SCIENCE & TECHNOLOGY REPORT

ISBN 7-5022-0621-3
TL • 365

P.O.Box 2103
Beijing, China

China Nuclear Information Centre