engineering proceedings

MDPI

Proceeding Paper

Analysis of the Fallback Values of Digital Control Systems in Nuclear Power Plants †

Zhenying Wang *, Liu Liu *, Zhiyun Liu, Yu Huang, Mingxin Hu and Tingwei Ma

China Nuclear Power Engineering Company, Ltd., Shenzhen 518000, China
* Correspondence: wangzhenying@cgnpc.com.cn (Z.W.); louisegesgranges@icloud.com (L.L.)
† Presented at the 8th International Symposium on Sensor Science—China, Nanjing, China, 29–31 March 2023.

Abstract: A digital control system (DCS), based on the Mitsubishi MELTAC + HOLLIAS platform, has been developed in ACPR1000 nuclear power plants. To fully utilize the superiority of digitalized technology, an analysis of fallback value setting in a DCS was conducted. Fallback values, as the substitution of invalid signals when they are detected in a DCS, are in a uniquely dominant position to determine the system behavior and consequences of a nuclear power plant's operation, as they participate in the control logic in place of invalid signals. After briefly introducing both the architecture of the ACPR1000 DCS and the invalidity management mechanism of signals, the failure mode of signals from sensors to DCS cabinets, the analysis range for fallback values, analysis principles a nd method, the implementation of modes for various signals, and engineering applications are summarized in this paper. This study is significant for enhancing the reliability of the instrument and control system itself and guaranteeing the safety level of nuclear power plants.

Keywords: nuclear power plant; digital control system; fallback value; reliability; safety

1. Background

A digital control system (DCS), as a mature control technology, has been widely used in nuclear power plants. Compared with the control logic built on operational amplifiers and relays, a DCS significantly increases the robustness of instrumentation and control (I&C) engineering and, hence, enhances the economy of nuclear power plants [1,2]. A DCS generally adopts fieldbus technology, and signals are transmitted through networks with a virtual ring structure, which has high communication reliability [3–5]. In order to meet the requirements of single-failure criteria [6], internal signal processing and logic voting in a DCS are redundant, and the power supplies of a DCS are diversified. In a DCS, all the data are sent to a bus network (fieldbus, control bus, system bus, etc.); depending on the transmission process, the sampling interval of data acquisition is between 50 ms and 200 ms (the delay of data delivering or data acquisition is between 50 ms and 200 ms).

Generally, the signals of field sensors and feedback signals of field actuators are standardized; all these signals are acquired by input modules and are sent to central processing units (CPUs) of a DCS. The fault-monitoring mechanism integrated in the DCS itself can detect the validity of signals hierarchically [7]. An analysis of the system response to signal failure has become a meaningful task in the design process of DCSs. In a DCS, it is easy to realize substitute values for failure signals, that is, fallback value setting. Fallback values are various, and they can be a low-range value, high-range value, set value, and last valid value, etc., with each value corresponding to a different and even contrary system response. To determine a fallback value, it is necessary to comprehensively consider various factors and fully weigh its influence on nuclear safety, the protection and maintenance of equipment, and the availability of the plant, etc. [8,9].

Some pilot studies related to fallback value setting have been carried out, such as the fast nuclear island maintenance strategy by setting fallback values [10], the fault diagnosis

Citation: Wang, Z.; Liu, L.; Liu, Z.; Huang, Y.; Hu, M.; Ma, T. Analysis of the Fallback Values of Digital Control Systems in Nuclear Power Plants. *Eng. Proc.* **2023**, *49*, 2. https://doi.org/10.3390/engproc2023049002

Academic Editor: Huangxian Ju

Published: 14 March 2024

and fallback value setting of analog input signals [11], implementation modes of fallback values [12], validation methods for fallback values [13], etc., although, nowadays, signal fault detection for nuclear power plants using machine learning has become a hot research topic [14,15]; these studies have generally suggested an expert system independent of the DCS. As for fallback value setting, it is of great significance, as it is directly related to the robustness of the DCS, the safety of plant operation, and equipment protection. This study discusses the work surrounding the fallback value setting of a DCS in ACPR1000 nuclear power plants, which is based on the Mitsubishi MELTAC + HOLLIAS platform. The invalidity management mechanism, failure modes of signals, analysis range for fallback values, analysis method, the implementation of modes, and engineering application are summarized.

2. DCS Description

2.1. Structure

An ACPR1000 DCS (supplied by Mitsubishi Electric Corporation (Tokyo, Japan) and China Techenergy Co., Ltd. Consortium (Beijing, China)) has been developed based on the Mitsubishi MELTAC + HOLLIAS platform. The HOLLIAS platform is dedicated to realizing normal control and adjustment as well as the monitoring of plant operation and mostly involves non-classified (NC) functions; this platform is also widely used in conventional power plants; the MELTAC platform is dedicated to safety classified (1E) functions, which include a reactor protection system (RPS) [16], a core cooling and monitoring system (CCMS) [17], as well as safety-related (SR) functions.

As shown in Figure 1, the ACPR1000 DCS consists of three levels: (1) Level 0, the process system interface layer, is mainly composed of sensors, breakers, actuators, and other field devices, and it performs the function of monitoring the operating parameters of process systems, as well as provides a low-voltage power supply for process equipment such as actuators; (2) Level 1, the automatic control and protection layer, mainly includes a plant standard automation system (PSAS), which consists of a great many field control stations (FCSs), RPS, and special I&C subsystems, such as a turbine and generator control subsystem (TGCS), and it performs functions of signal acquisition, logic processing, automatic control, and signal communications; (3) Level 2, the operation and information management layer, is the digital human–machine interface, which is composed of a process information and control system (PICS) and a safety information and control system (SICS), providing digital control means for the plant [18].

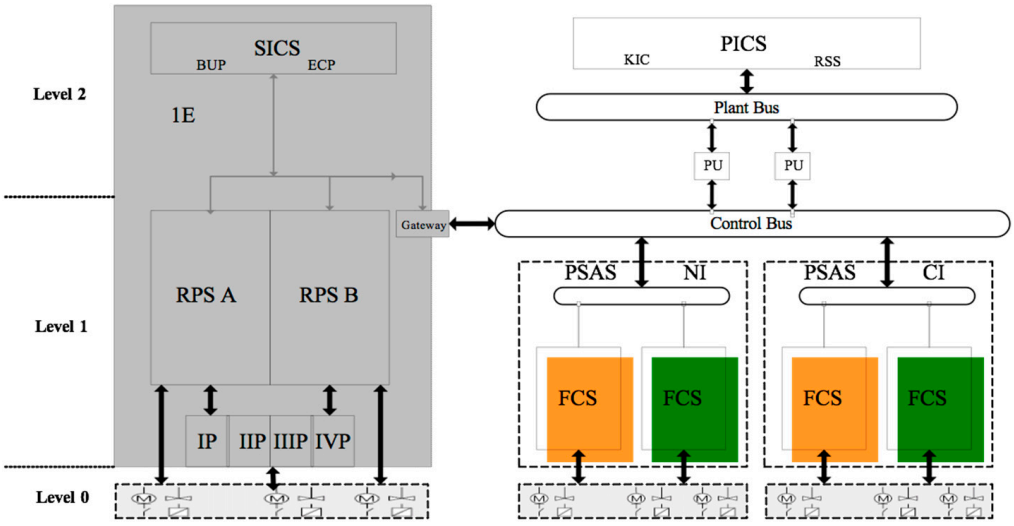

Figure 1. DCS architecture.

2.2. Invalidity Management

The concept of signal invalidity management is introduced into the DCS. Signals transmitted and managed in the DCS are generally accompanied by a "quality state" indicating whether the signal is valid or not. As an attribute of the signal besides its physical value, the quality state is generated and transmitted along with the signal. As long as the invalidity of a signal is detected, the quality state of the signal is changed to mark its invalidity. For invalid signals, the quality state not only can be configured to participate in the function logic related to the signals but can also trigger I&C alarms on the PICS, indicating the invalid state of the signal so as to guide operators to analyze and discover the cause of the fault. More importantly, the invalid state can also activate the corresponding fallback value that has been set in advance. Taking the MELTAC platform as an example, the quality state consists of 8 bits in 1 byte, in which signal quality state information, such as card error, over-range, etc., is included; the specific meaning of each bit is shown in Figure 2.

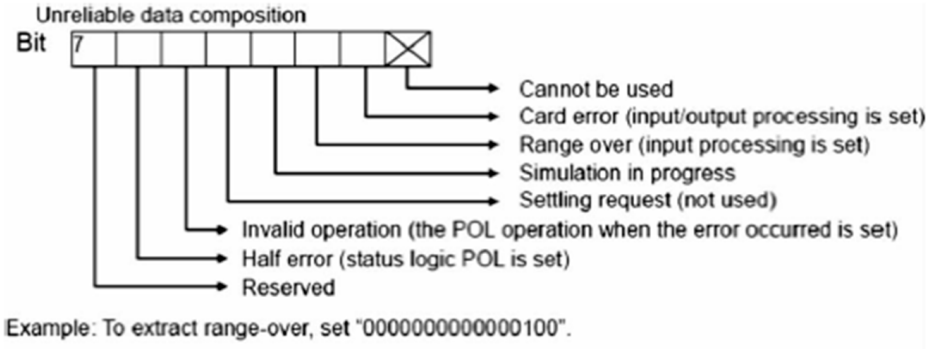

Figure 2. Quality state.

As for signals transmitted through hardwires, only the physical values of the signals are transmitted and thereby do not involve the issue of invalidity management.

2.3. Failure Mode of Signals

As fallback values are anticipated to be activated after detecting signal failure, it is beneficial to analyze and to identify failure modes of various signals. As for the ACPR1000 DCS, the failure modes of signals are generally divided into the following categories:

(1) Failure in level 0, which includes sensor failure, disconnection, signal shaking, etc.; this kind of failure is detected by input modules. After a failure, the corresponding input module detects an abnormal change in input electrical signals and then informs CPUs to set the quality state of the signal as "invalid".

(2) Failure in the level 1 component, which includes failure of input modules, power loss in the level 1 component, and so on. A CPU periodically monitors the working state of the level 1 component; after detecting a failure, the CPU sets the corresponding signal quality state as "invalid", and the physical value of the signal in the CPU is not refreshed any more. Typical functions of a level 1 failure diagnosis include an input and output (IO) module watchdog timer diagnosis, IO module and CPU communication failure mode diagnosis, etc.

(3) Communication failure within the level 1 cabinet, which includes network failure, gateway failure, etc. After a communication failure, the receiving cabinet detects the signal transmission failure and sets the network signal quality state as "invalid", and the physical value of the signal is not refreshed any more.

3. Analysis of Fallback Values

3.1. Scope

Looking into the architecture of the ACPR1000 DCS, signals between level 0 and level 1, signals between level 1 and level 1, and signals between level 1 and level 2 are analyzed, as shown in Figure 3. Signals from level 0 to level 1 include the signals from conventional instruments to FCSs and the signals from protection channel instruments (which include four protection channels, I P, II P, III P, and IV P, as shown in Figure 1). The signals acquired by the reactor protection cabinet (RPC) and sent to an FCS after isolation and distribution (as shown in A in Figure 3) need to be analyzed, as they participate in the normal control and regulation of a plant's operation.

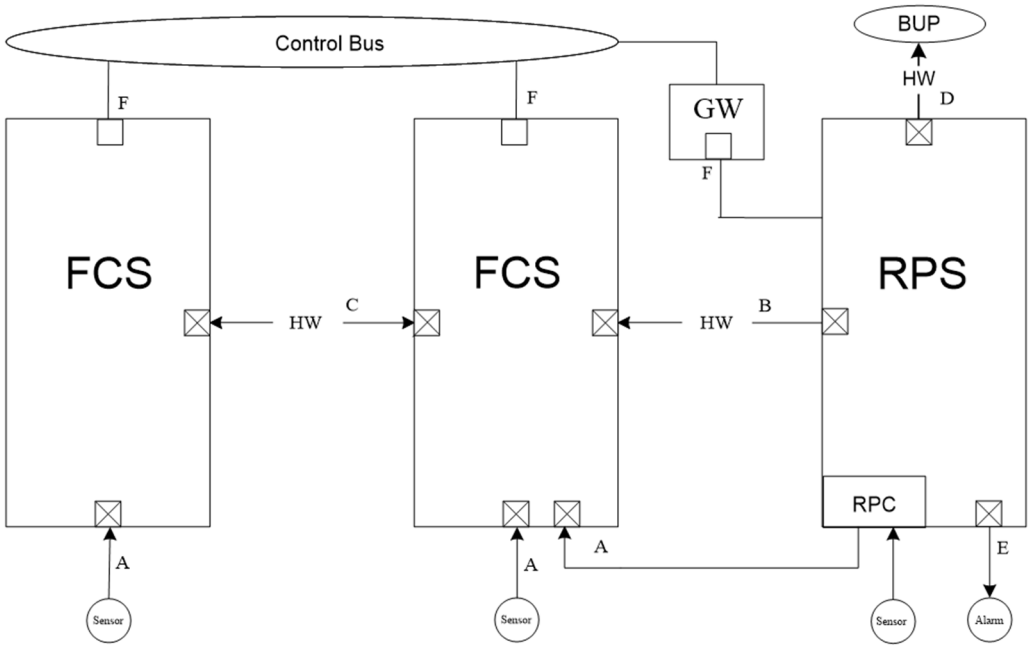

Figure 3. DCS fallback value sketch map.

Signals within the level 1 cabinet mainly consider signals between different classified levels as well as signals between different trains, including the hard-wired signals between two platforms. The hard-wired signals from 1E DCS to NC DCS are control signals with a higher requirement of response time; the fallback values of these kinds of signals are set both in the sending end and the receiving end, with the former aiming to detect possible internal failure in 1E DCS and the later aiming to detect possible failure of hard-wire disconnection (as shown in B in Figure 3). Hard-wired signals between train A and train B mainly refer to the signals between FCSs of different trains and signals between FCSs within the same train (as shown in C in Figure 3). Hard-wired signals from level 1 to level 2 mainly refer to signals that are sent to the SICS (as shown in D in Figure 3).

As for some special systems, such as the neutron flux measurement system and plant radiation monitoring system, their functions are integrated into third-party cabinets, and consequences of sensor failure have been considered in system design; therefore, it is generally unnecessary to analyze fallback value settings of such systems. However, there are some special signals from level 1 to level 0, such as signals to trigger a local high neutron flux sound alarm and the field indicator light needing to be analyzed; the fallback values of these kinds of signals can be set in the DCS as required to determine whether to trigger alarms and indicator lights or not when they are invalid (as shown in E in Figure 3).

For network signals between two platforms and between different FCSs, the quality state of the signal is transmitted through the network, and the receiving end can detect transmission failure; the fallback values of such signals are generally set at the receiving end and gateways (as shown in F in Figure 3).

3.2. Analysis Method for Fallback Values

It can be predicted that the behavior of process systems and the consequences of signal failure on the plant depend on the fallback value of the signal to some extent. The different fallback values chosen correspond to different responses; in some cases, they may have the opposite influence on the safety and economy of the plant. The principle of determining a fallback value is that it must not damage the nuclear safety of the plant, while taking into account the economy of the plant.

When determining a fallback value, experience feedback from the plant's operation and maintenance are gathered and analyzed; various factors relative to the issue are comprehensively considered to determine an optimal value.

The following factors are mainly considered in the process of determining fallback values:

(1) The monitoring of signal failure, whether the failure can be monitored by operators in the main control room, and how difficult it is;
(2) The consequence of signal failure, the influence on process systems and plant operation, if it will lead to automatic actions, and what the behavior of the systems involved is;
(3) The functional redundancy of the signal; if there is any substitution of functions relative to the signal;
(4) The safe position of the actuators, which mainly considers whether the fallback value setting is consistent with the safe position of the actuators, as long as the actuators are involved in the control logic the signal participates in.

Finally, based on the results of the analysis above, the fallback value of the signal is determined after weighing the safety, availability, equipment, and personnel protection of the plant.

3.3. Implementation of Fallback Values

Considering the internal fault monitoring mechanism of the MALTEC platform, the fallback values can be set thanks to the analog signal state-monitoring function block (AUE) and the on-off signal state-monitoring function block (DUE). Combined with some simple logic function blocks, fallback values are implemented during DCS configuration.

The implementation modes of fallback values in the MELTAC platform are shown in Figure 4. After a signal failure is monitored, the output value of the AUE or DUE is set to "1" to indicate the invalidity of the signal. For Figure 4A, a fallback value of "1" is realized for an on–off signal. For Figure 4B, a chosen value is assigned to function block SET, which will be activated when AUE is "1". As for the implementation of the last valid values for analog signals, in order to avoid "spurious" last valid values in processing because of the asynchrony between the processing period of the CPU and that of the IO modules, over-speed judgment is introduced into signal diagnosis. When an analog signal fails, the physical value of the signal of the previous acquisition cycle and latter acquisition cycle will sharply change. By introducing a 20% over-speed judgment module, the last valid value will be memorized in time when the signal value changes more than 20% in the previous two cycles, as shown in Figure 4C.

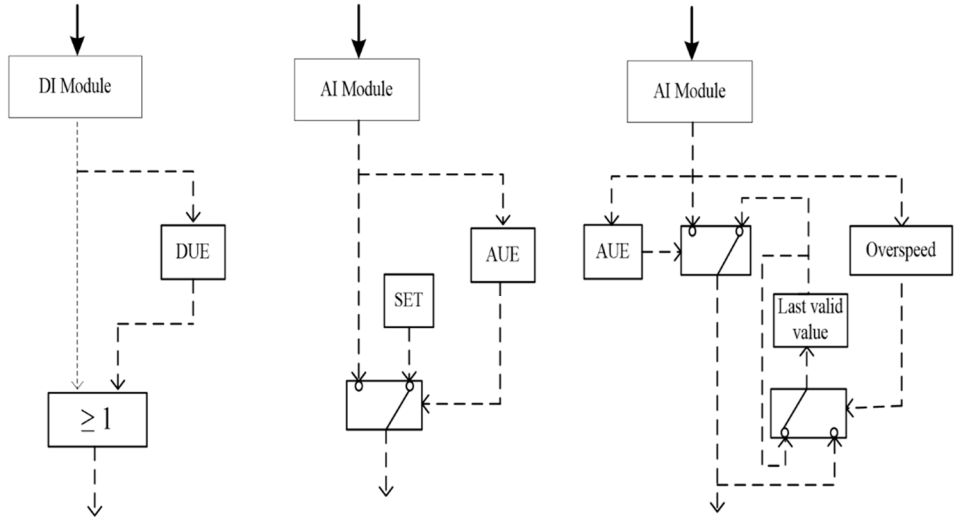

Figure 4. Implementation of fallback values in the MELTAC platform.

3.4. Engineering Application

As responses under accident conditions have been considered while determining fallback values for these signals, emergency operating procedures (EOPs) are optimized according to fallback value analysis results; for example, considering spurious display and alarm due to signal failure, redundant and substitute instrument information is introduced into EOPs, thus improving the robustness of an emergency operation. Meanwhile, DCS power loss analysis and fire risk analysis are carried out, referring to fallback value analysis, as DCS power loss or a fire in nuclear island may lead to a massive failure of sensors; the overall impact of DCS power loss or fire on a plant's operation depends on the corresponding fallback values to a certain extent [19,20].

3.5. Verification and Validation

First of all, by checking the outputs after simulating an invalid input signal of the DCS cabinet, a verification of fallback values is carried out during a factory test. Secondly, a verification of fallback values is carried out on a design verification platform, which integrates the function logic of process systems; after inserting a failure signal and replacing the signal with its fallback value, the behavior of process systems and the involvement of the plant's state are observed on the design verification platform, and the bias from the anticipated consequence is identified and analyzed. What is more, the results of DCS power loss are validated during plant commissioning, and this also naturally validates some fallback values related to DCS power loss. Verification and validation results show that the fallback values can achieve expected consequences in cases of supposed signal failure, and the impact on the load of CPUs is almost negligible.

4. Conclusions

How to make full use of the advantages brought about by digital technology is a challenge that must be faced in DCS design. In this paper, the principles, analysis method, implementation, and verification and validation of fallback values for the ACPR1000 DCSd, which have been applied into several ACPR1000 nuclear power plants, were discussed. Setting fallback values optimizes system function, avoids unnecessary spurious actuation and mis-actuation of the plant's control system, and improves the safety level and economy of the plant. In this paper, fallback values based on the MELTAC + HOLLIAS platforms were analyzed, lbut for other nuclear power plants adopting different DCS technologies, the failure mode, invalidity management mechanism, scope of fallback values, and im-

plementation modes should be considered when carrying out fallback value analysis by considering the characteristics of a DCS platform.

Author Contributions: Conceptualization, Z.W. and L.L.; methodology, Z.W.; validation, Z.L.; formal analysis, Z.W.; investigation, Z.W. and L.L.; resources, Z.W.; data curation, Y.H.; writing—original draft preparation, Z.W.; writing—review and editing, L.L. and Z.L.; supervision, M.H.; project administration, T.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: All authors are employed by China Nuclear Power Engineering Company, LTD. And we declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Yang, Q. Application status and development trend of digital I&C system in nuclear power plant. *Nucl. Power Eng.* **1998**, *19*, 124–129.
2. Liu, W.R. The developing status of the instrument and control systems in nuclear power stations. *Process Autom. Instrum.* **1997**, *18*, 1–5.
3. Zhou, H.X. Data communication of TXP/TXS system in Tianwan nuclear power plant. *Nucl. Power Eng.* **2006**, *27*, 67–70.
4. Zhang, Y.; Han, B. Research on application of fieldbus in power plant unit control. *Process Autom. Instrum.* **2008**, *29*, 18–21.
5. Meng, L. Application of fieldbus technology in power plant. *Process Autom. Instrum.* **2005**, *26*, 33–35.
6. *IAEA Safety Standards SSG-39*; Design of Instrumentation and Control Systems for Nuclear Power Plants. IAEA: Vienna, Austria, 2016.
7. Zhou, H.X. Failure mode and effect analysis for digital reactor protection system in Tianwan nuclear power plant. *At. Energy Sci. Technol.* **2007**, *41*, 702–706.
8. Wang, Z.Y.; Li, H.L.; Zheng, W.B. Analysis research on the fallback values of digital instrument and control system in NPP. *Process Autom. Instrum.* **2011**, *32*, 24–27.
9. Liu, Z.Y.; Wang, Z.Y.; Zhang, X.C.; Li, M. Analysis research of fallback value related to RPC loss of power in NPPs. *Nucl. Electron. Detect. Technol.* **2012**, *32*, 416–420.
10. Zhao, H.B.; Gong, A.C.; Wang, Z.G. Based on DCS system failure analysis of the nuclear island fast maintenance strategy. *Instrumentation* **2015**, *22*, 84–87.
11. Zhao, Y.F.; Zhou, L. Fault diagnosis and management of analog input signal for the safety class DCS in nuclear power plant. *Instrumentation* **2020**, *21*, 70–73.
12. Wang, S.W.; Li, G.J.; Sun, W.; Tian, Y. Default value realization research of CPR1000 safety classified DCS platform. *J. Mech. Electr. Eng.* **2017**, *34*, 100–104.
13. Su, Z.K.; Zhao, H.B.; Zhang, H.X. Study on the setting and validation methods for CPR1000 DCS default value. *Chin. J. Nucl. Sci. Eng.* **2010**, *30*, 9–13.
14. Choi, J.H.; Lee, S.J. Consistency index-based sensor fault detection system for nuclear power plant emergency situations using an LSTM network. *Sensors* **2020**, *20*, 1651. [CrossRef] [PubMed]
15. Choi, J.H.; Lee, S.J. A sensor fault-tolerant accident diagnosis system. *Sensors* **2020**, *20*, 5839. [CrossRef] [PubMed]
16. Liu, H.C.; Wang, T.T.; Wang, H.J.; Zhou, J.X.; Liu, G.M.; Xu, D.F. Design of digital reactor protection system of Ling'ao phase II NPP. *Nucl. Power Eng.* **2008**, *29*, 1–4.
17. He, Z.X.; Yu, J.H.; Li, X.F. Design of cooling monitoring system based on SOP. *Nucl. Power Eng.* **2012**, *33*, 107–110.
18. Sun, Y.B.; Jiang, X.H. Layout design of advanced control room of pressurized water reactor NPP. *Nucl. Power Eng.* **2008**, *29*, 73–77.
19. Wang, Z.Y.; Zheng, W.B.; Li, H.L.; Li, S.; Li, M. Review on loss of power supply incident analysis for Ling'ao phase II NPP. *Npp. Nucl. Power Eng.* **2011**, *32*, 51–57.
20. Wang, Z.Y.; Shi, Y.M.; Liu, L. Fire safety design of CPR1000 nuclear power plants. In Proceedings of the IEEE 2nd International Conference on Power, Electronics and Computer Applications, Shenyang, China, 21–23 January 2022.