Design of Defence in Depth for I&C System in Pressurized Water Reactor Nuclear Power Plant

Tao Fu(✉), Gong-Jie Li, and Li-Ming Zhang

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, China
futao@cgnpc.com.cn

Abstract. The design of Instrumentation and Control (I&C) system in nuclear power plan needs to consider the problems of Common Cause Failure (CCF) and independence of itself in addition to meeting the overall Defence in Depth (DiD) target of the plant and ensuring the correct and reliable implementation of monitoring, control and protection functions under various operation conditions. The requirements of International Atomic Energy Agency (IAEA) are summarized in this paper. A design scheme of DiD for I&C system of Nuclear Power Plant (NPP) is introduced. in this paper. The compliance of DiD design for I&C system with the requirements of IAEA is analyzed. The analysis concludes that the I&C design scheme basically meets the requirements of IAEA. At the same time, the improvement of diversity should be further studied. The study of this paper provides valuable reference for the continuous improvement of the design of I&C systems in NPP.

Keywords: DiD · Independence · Diversity

1 Introduction

DiD is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. If one level of protection or barrier were to fail, the subsequent level or barrier would be available. The independent effectiveness of the different levels of defence is a necessary element of DiD.

After Fukushima nuclear accident, the design concept of DiD of new NPP has been further developed. Higher targets are put forward for the DiD levels and the independence between DiD levels. The development of this design concept is introduced in IAEA Safety Standards Series No. SSR-2/1 [1], Safety of NPP: Design. The concepts of Design Extension Condition (DEC) and practical elimination are introduced for the first time. The purpose of the fourth level of DiD is adjusted from "address severe accidents in which the design basis may be exceeded and to ensure that radioactive releases are kept as low as practicable" to "mitigate the consequences of accidents that result from failure

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2021
Y. Xu et al. (Eds.): SICPNPP 2020, LNEE 779, pp. 164–176, 2021.
https://doi.org/10.1007/978-981-16-3456-7_18

of the third level of DiD". Furthermore, the independence requirement between each level of DiD is emphasized.
For the I& C system of NPP, it is necessary to provide monitoring and control means for the process systems which are included in all levels of DiD. On the other hand, the I&C system itself should also meet the design requirements of DiD to ensure that the failure of one level of defence is compensated for by the following one. This paper summarizes the design requirements of DiD of I&C system in IAEA and introduces a design scheme of DiD for I&C system of NPP.

2 Requirements of IAEA

2.1 Requirements of IAEA SSR2/1

IAEA SSR2/1 defines design requirements for the structures, systems and components of a NPP, as well as for procedures and organizational processes important to safety which are required to be satisfied for safe operation and for preventing accidents which could jeopardize safety, or for mitigating the consequences of such accidents, were they to occur.

The Levels of DiD
IAEA SSR2/1 defines five levels of defence:

- The first level of defence can prevent deviations from normal operation and the failure of items important to safety. This level of defence requires that the plant be soundly and conservatively sited, designed, constructed, maintained and operated in accordance with quality management and appropriate and proven engineering practices. In order to satisfy these targets, careful attention is paid to the selection of materials and appropriate design codes, and to the quality control of the manufacture of items and construction of the plant, as well as to its commissioning. Design options that reduce the possibility of internal hazards contribute to the prevention of accidents at this level of defence.
- The the second level of defence can detect and control deviations from normal operational conditions to prevent anticipated operational occurrences (AOOs) from escalating to accident states at the plant. Despite the care taken to prevent postulated initiating events (PIEs), the (PIEs) are likely to occur over the operating lifetime of a NPP. The second level of defence requires the provision of specific systems and features in the design, the confirmation of their effectiveness by safety analysis, and the establishment of operating procedures to prevent such initiating events, or otherwise to mitigate their consequences, and to return the plant to a safe condition.
- For the third level of defence, it is assumed that, although very unlikely, the escalation of certain AOOs or PIEs might not be controlled at a preceding level and that an accident could develop. Such accidents are postulated to occur in the design of the plant which requires that inherent and/or engineered safety features, safety systems and procedures can prevent damage to the reactor core or prevent radioactive releases which require off-site protective actions and return the plant to a safe condition.

– The fourth level of defence can minimize the consequences of accidents which result from failure of the third level of DiD. This is achieved by preventing the progression of such accidents and minimizing the consequences of a severe accident. The safety target in the case of a severe accident is that only protective actions that are limited in terms of lengths of areas and time of application would be necessary and that off-site contamination would be avoided or mitigated. Accident sequences which would lead to an early radioactive release or a large radioactive release are required to be practically eliminated.
– The fifth and final level of defence can minimize the radiological consequences of radioactive releases which could possiblely result from accidents. This requires the provision of adequately equipped emergency response facilities and emergency procedures and emergency plans for on-site and off-site emergency response.

Application of DiD
The DiD design shall be incorporated in the design of a NPP. The levels of DiD shall be independent as far as is practicable.

The design shall ensure that an escalation to accident conditions for all failures or deviations from normal operation which are likely to occur over the operating lifetime of the NPP can be prevented by the first, or at most the second, level of defence.
The levels of DiD shall be independent as far as practicable to avoid the failure of one level influencing other levels. In particular, safety systems shall as far as is practicable be independent of safety features for DECs (especially features for mitigating the consequences of accidents involving the melting of fuel).

2.2 Requirements of IAEA TECDOC 1791 [2]

IAEA TECDOC 1791 provides insights and approaches in support of the practical application of the new crucial requirements described in IAEA SSR2/1.

DiD Strategy
IAEA TECDOC 1791 describes two different approaches of DiD (see Table 1).

– Approach 1, i.e. the association of DECs without core melt to level 3, has the advantage that each level has clear targets regarding the progression of the accident and the protection of the barriers, i.e. level 3 to prevent damage to the reactor core and level 4 to mitigate severe accidents for preventing off site contamination.
– Approach 2, i.e. the grouping of DECs without core melt and with core melt in level 4, facilitates however the differentiation between the set of rules for design and safety assessment to be applied for DECs from those for DBA.

The formulation of the Approach 1 is used in the IAEA TECDOC 1791.

Table 1. Levels of DiD For the design of new NPP.

Level of defence Approach 1	Target	Essential design means	Essential operational means	Level of defence Approach 2
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction of normal operation systems, including monitoring and control systems	Operational rules and normal operating procedures	Level 1
Level 2	Control of abnormal operation and detection of failures	Limitation and protection systems and other surveillance features	Abnormal operating procedures/emergency operating procedures	Level 2
Level 3a	Control of design basis accidents	Engineered safety features (safety systems)	Emergency operating procedures	Level 3
Level 3b	Control of DECs to prevent core melt	Safety features for DECs without core melt	Emergency operating procedures	Level 4 a
Level 4	Control of DECs to minimize the consequences of severe accidents	Safety features for DECs with core melt. Technical Support Centre	Complementary emergency operating procedures/ severe accident management guidelines	Level 4b
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	On-site and off-site emergency response facilities	On-site and off-site emergency plans	Level 5

Design for Effective Independence of Levels of DiD

Safety features which are designed to minimize the consequences of core melt accidents need to be independent from features which are designed to mitigate DBAs.

Level 3 needs to be independent from levels 1 and 2 as far as reasonably practicable. The ability of the safety systems to execute their function would not be jeopardized by

a postulated single initiating event, or by failures of systems which are designed for normal operation and AOOs in order to avoid challenging excessively levels 3b or 4. This includes also shared support systems between these levels.
Safety features for DEC which are designed to backup SSCs performing safety functions, need to be independent from SSCs postulated to fail in the accident sequence.
The safety features performed in level 3b are used to control multiple failures affecting a safety system.
Systems which are designed to control AOOs would be independent from systems for normal operation as far as reasonably practicable. Generally, AOOs are controlled by non-safety systems and ultimately by the reactor trip system. A postulated single initiating event or single equipment failure of systems designed for normal operation would not jeopardize the ability of the reactor trip system to execute its functions. The diverse safety features implemented in level 3b (e.g. with Diverse Actuation System (DAS) I&C system) are used to control multiple failures resulting in the total loss of the reactor trip system. Limitations systems (level 2) usually share components with the control systems. A full independence of these systems might lead to excessive complexity which is not justified by the benefits to safety.

Independence of Levels of DiD in Relation to I&C Systems
I&C systems have a relevant role for executing safety functions in all levels of DiD. The correspondence between the level of DiD and the different functions together with some recommendations to enhance independence of different levels are summarized below:

- Level 1. To this level belong the functions necessary to operate the plant during normal operation modes and to maintain the main plant parameters within the specified range.
- Level 2. To this level belong the functions to prevent AOOs from escalating into accident conditions. This level also includes the reactor trip function and the limitation functions which are designed to control AOOs without activating the reactor trip as much as possible.
- Limitations system (level 2) need to be separated from the operational I&C (level 1) to the extent feasible. Separation may not be performed where it would lead to increase significantly the number of data transfer between these two I&C systems (e.g. between I&C limitations and controls where the controlled equipment is the same).
- Level 3. To this level belong the functions which are designed to automatically control design basis accidents (DBAs) without exceeding acceptance criteria and the functions which are designed to bring and to maintain the reactor in safe shutdown state following a DBA.
- Initiation of reactor trips and safety systems need to be processed in a separated and independent I&C system from the I&C systems which are used for operational states and the I&C systems which are used for level 3b. It is necessary to ensure that failures of systems classified in a lower safety class will not prevent the Reactor Protection System (RPS) from executing its functions. Back up functions which are used to prevent that combinations of PIEs with CCFs in the I&C systems escalate to a core melt accident belong to level 3b.

– Level 4. I&C systems dedicated to the mitigation and monitoring of a core melt accident need to be separated and independent from any other I&C systems. This requires the independence of their respective power sources.

In existing designs, some I&C functions may be executed by a single I&C system in order to reduce the volume of data to communications and exchange within I&C systems. That may be the case for some limitation and control functions, or with the RPS which often performs both the reactor trips and the actuation of the safety systems. In that case the physical separation is not required but the functions need to be decoupled.

Independence is intended to prevent the propagation of failures from system to system or between redundant channels and is achieved by implementing communication independence, functional independence and avoiding interconnections in I&C systems. The data transfer needs to be secured and the shared signals decoupled (e.g. Data transfer between the redundant channels of the RPS are necessary for the voting logic) if independence is not implemented. Physical separation is intended to prevent CCFs due to internal hazards.

Considerations About Sensors

The efficacy of all four levels depends upon sensor response but this does not imply that all sensors must be diverse or independent. Nevertheless the independence between systems assigned to different levels of DiD, and between redundant trains of a safety system, must not be jeopardized by the sensors (e.g. redundant trains within a safety system must not share instrumentation).

The following considerations apply:

– Diversity and independence between the DAS and the RPS must not be impaired by sensors to the extent possible.
– Monitoring the key parameters for the management of DBAs and DECs without significant fuel degradation would also be possible using sensors different from those used to initiate the operation of the safety systems and DEC safety features respectively. Sensors which are used for the protection and for the monitoring would not fail because of a common cause to the extent possible.
– Monitoring the key parameters for the management of core melt accidents need to be to the extent possible executed by dedicated sensors, and in particular it need not be dependent on the power source which is used for DBA management. Sharing sensors with other DiD levels may be acceptable provided the sensors are qualified for the environmental conditions prevailing in case of a severe accident and an adequate number of redundant sensors are performed with effective independence and separation. In this case the shared sensors need to provide input to different I&C systems only through appropriate devices. The DAS needs to be separated, independent and diverse from the RPS.
– Sharing sensors between levels 1, 2 and 3a may be acceptable provided an adequate number of redundant sensors are implemented with effective independence and separation. In this case the shared sensors need to provide input to different I&C systems only through appropriate isolation and buffering devices.

– It is a good practice to rely on different physical parameters to minimize the consequences of failure of sensors due to common causes for the monitoring of plant parameters or for the automatic actuation of safety systems in accident conditions.

2.3 Requirements of IAEA SSG-39 [3]

IAEA SSG-39 provides recommendations about the design of I&C systems to satisfy the requirements described in IAEA SSR2/1. IAEA SSG-39 provides guidance about the overall I&C architecture and about the I&C systems important to safety in NPP for meeting the safety argets of the plant.

Design Basis for I&C Systems
The functions which are allocated to the I&C systems include those functions which provide control and information capabilities relevant to operation of the plant in the various modes of operational states and in accident conditions. The targets of these functions, corresponding to the concept of DiD, are to:

– Prevent deviations from normal operation;
– Detect failures and control abnormal operations;
– Control accidents which are within the plant design basis;
– Mitigate consequences in DECs;
– Minimize the radiological consequences of accidents.

DiD within the overall I&C architecture is achieved by means of independent lines of defence, so that the following line of defence can compensate for the failure of one line of defence.

The overall I&C architecture should neither compromise the independence of the different levels of the DiD applied at the plant., nor the independence of safety system divisions

2.4 Summary

There is not a unanimous understanding about the association of all the levels of DiD with the plant states established in SSR-2/1. The point of discrepancy is the association of DECs without core melt to one of the levels of DiD established in SSR-2/1. Some Member States associate them to the level 4 and others associate them to the level 3.

The requirements of DiD in IAEA are as follows:

– Initiation of reactor trips and safety systems need to be processed in a independent and separated I&C system from the I&C systems which are used for normal operation and the I&C systems which are used for level 3b.
– I&C systems which are dedicated to the monitoring and mitigation of a core melt accident need to be independent and separated from any other I&C systems. This requires the independence of their respective power sources.

– A single I&C system may perform some I&C functions. That may be the case for some limitation and control functions, or with the RPS which often processes both the reactor trips and the actuation of the safety systems.
– The DAS needs to be independent, separated and diverse from the RPS.
– Monitoring the key parameters for the management of core melt accidents need to be to the extent possible executed by dedicated sensors.
– Sharing sensors between levels 1, 2 and 3a may be acceptable provided an adequate number of redundant sensors are performed with effective independence and separation.
– It is a good practice to rely on different physical parameters to minimize the consequences of failure of sensors due to common causes for the monitoring of plant parameters in accident conditions or for the automatic actuation of safety systems.

3 Design of DiD for I&C System

3.1 DiD of I&C System

The I&C system implement the following functions:

– Monitor the plant to provide the necessary information, during Operational states and accident conditions.
– Maintain the operating parameters of process systems or equipment within the stipulated limits of the operating states.
– Initiate mitigation functions to ensure the power plant reach safe state and to limit radioactive release to the environment in accident conditions.

New overall I&C architecture shown in Fig. 1 is designed in this paper.

New I&C defence lines within the overall I&C architecture are established to support the plant DiD levels which is in accordance with the approach 1 in IAEA TECDOC 1791. The I&C defence lines are as follows:

– Preventive line of defence. This defence line controls main plant parameters within their expected operating range and prevents potential deviations from normal operation. This defence consists of CLS which performs control and limitation function in normal operation states.
– Main line of defence: This defence line mitigates the consequences of DBAs and brings the plant to the safe state. This defence line consists of RPS which performs reactor trip, engineered safety feature actuation and other post-accident mitigation functions under DBA.
– Diverse defence line: This defence line mitigates the consequences of the DBAs concurrent with the CCF of the main line of defence. The technology implemented by diverse defence line is fundamentally diverse from the technology implemented by main line of defence. This defence line consists of DAS which provides a diverse means of reactor trip and engineered safety feature actuation that is not affected by the postulated CCF

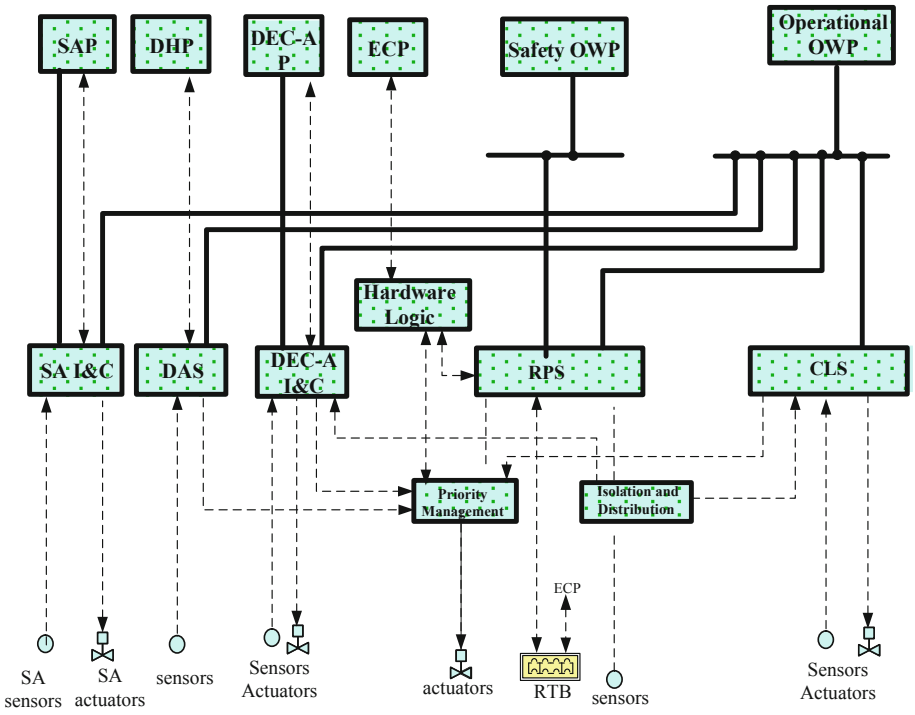

Fig. 1. Overall I&C architecture

– Risk reduction line: This defence line mitigates the consequences of DECs without core melt (failures in mechanical systems); This defence line consists of DEC-A I&C.
– Severe accident defence line: This defence line performs the managing and monitoring functions under severe accident with independent Uninterruptible Power Supply. This defence line consists of SAI&C.

The priority management module, isolation and distribution module adopt the hardware circuit technology to reduce the risk of CCF

The relationship between lines of defence and levels of plant DiD, as well as I&C systems at each defence line is shown in Table 2.

Table 2. Defence lines of I&C corresponding to levels of DiD of the plant

Plant DiD level		I&C lines of defence	System
Prevention of abnormal operation and failures	1	Preventive line	CLS
Control of abnormal operation and detection of failures	2		
Control of DBAs	3a	Main defence line	RPS
Control of DECs to prevent core melt	3b	Diverse defence line	DAS
		Risk reduction defence line	DEC-A I&C
Control of DECs to mitigate the consequences of severe accidents	4	Severe accident defence line	SAI&C

3.2 Compliance Analysis with Requirements of IAEA

The compliance analysis between DiD design and requirements of IAEA is shown in Table 3.

Table 3. Compliance analysis between requirements of IAEA and DiD design

Requirements of IAEA	Compliance analysis	Result
Initiation of reactor trips and safety systems need to be processed in a separated and independent I&C system from the I&C systems used for operational states and the I&C systems used for level 3b	The RPS is independent from the DAS and DEC-A I&C. See subclause 3.3 for details	Satisfied
I&C systems dedicated to the mitigation and monitoring of a core melt accident need to be separated and independent from any other I&C systems. This requires the independence of their respective DC power sources	The SAI&C is independent from other systems. See subclause 3.3 for details	Satisfied
Some I&C functions may be executed by a single I&C system. That may be the case for some control and limitation functions, or with the RPS which often processes both the reactor trips and the actuation of the safety systems	The CLS executes control and limitation function in normal operation states. The RPS executes reactor trip, engineered safety feature actuation and other post-accident mitigation functions under DBA	Satisfied

(*continued*)

Table 3. (*continued*)

Requirements of IAEA	Compliance analysis	Result
The I&C backup system (DAS) needs to be separated, independent and diverse from the RPS	The DAS is separated, independent and diverse from the RPS. See subclause 3.3 and 3.4 for details	Satisfied
Monitoring the key parameters for the management of core melt accidents need to be to the extent possible executed by dedicated sensors	The sensors used for management of core melt accidents are dedicated and employed by the SAI&C	Satisfied
Sharing sensors between levels 1, 2 and 3a may be acceptable provided an adequate number of redundant sensors are implemented with effective separation and independence	The RPS and CLS share some common sensors. These signals are collected by the RPS and transfered to the CLS by the isolation device which is classified as part of the RPS	Satisfied
For the automatic actuation of safety systems or for the monitoring of plant parameters in accident conditions, it is a good practice to rely on different physical parameters to reduce the consequences of failure of sensors due to common causes	The reactor trip function in the RPS can be initiated by at least two functional diverse parameters	Satisfied

3.3 Independence Analysis

Independence Between the Main Defence Line and Preventive Line
The RPS is separated from the CLS by appropriate distances or physical barriers in accordance with IEC 60709 [4].

For the signal exchange between the RPS and the CLS, the electrical isolation and communication isolation in accordance with IEC 60709 is achieved to prevent the failure propagation from the CLS to the RPS. The isolation device is classified as part of the RPS.

Independence Between the Main Defence Line and Diverse Defence Line, Risk Reduction Line
The RPS, DAS and DEC-A I&C are seismically qualified, so the physical barriers or distance between them is not required.

There is no communication between the RPS, DAS and DEC-A I&C. For the hardwired interface between the RPS, DAS and RPS, the electrical isolation in accordance with IEC 60709 is achieved to prevent the failure propagation from the DAS and DEC-A I&C to the RPS. The isolation device is classified as part of the RPS.
The sensors employed by the DAS are different from the sensors employed by the RPS.

Independence Between the Severe Accident Defence Line and Other Defence Lines
The SAI&C is seismically qualified and separated from the non-seismically qualified system by appropriate distances or physical barriers in accordance with IEC 60709.

There is no hardwired interface between the SAI&C and other systems. For communication the between the SAI&C and the CLS, the communication isolation in accordance with IEC 60709 is achieved to prevent the failure propagation from the CLS to the SAI&C.
The sensors and actuators employed by the SAI&C is different from the sensors and actuators employed by other systems.
The power source of the SAI&C is independent from the power source of other systems.

3.4 Diversity Analysis

The diversity principle is applied to the overall design of I&C systems through signal diversity, equipment diversity and function implementation diversity to cope with CCF.

- Signal diversity: a safety action is initiated based upon the value of different plant parameters. The reactor trip function in the RPS can be initiated by at least two functional diverse parameters corresponding to the same DBA in the I&C design;
- Equipment diversity: The RPS and the DAS are implemented by diverse technology. When the RPS (the main defence line) is unavailable due to the CCF, the DAS (the diverse defence line) can perform the required functions.
- Function implementation diversity: In addition to automatic function, manual reactor trip, engineered safety feature actuation function can be realized by ECP. The command from ECP is realized by hardware logic and bypass digital system.

4 Conclusion

The design of DiD for I&C system in this paper meets the requirements of DiD level design, independence and diversity proposed by IAEA. However, optimization can be continued in the following areas:

- The diversity can be improved. The CLS, RPS and DAS all adopt different platforms.
- For the equipment shared by multiple DiD levels, such as priority management module, isolation and distribution module, Attention should be paid to the requirements of the latest international regulations and standards, and the international good experience feedback practice. The mechanism of CCF is studied. The appropriate improvement measures are taken to deal with the CCF.

The design of the I&C system should be consistent with the overall DiD concept of the NPP. However, there are certain characteristics in the I&C system. For example, while emphasizing the independence and diversity of DiD levels, consideration should be taken to avoid excessive complexity of the I&C system. The cost and maintainability of the I&C system should also be considered

References

1. International Atomic Energy Agency, SSR 2/1: Safety of Nuclear Power Plants: Design. IAEA, Vienna (2016)
2. International Atomic Energy Agency, TECDOC 1791: Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants. IAEA, Vienna (2016)
3. International Atomic Energy Agency, SSG-39: Design of Instrumentation and Control Systems for Nuclear Power Plants. IAEA, Vienna (2016)
4. International Electrotechnical Commission, IEC 60709: Nuclear power plants - Instrumentation, control and electrical power systems important to safety – Separation. IEC, Geneva (2018)