Considerations on Fail Safe Design for Design Basis Accident (DBA) vs. Design Extension Condition (DEC): Lesson Learnt from the Fukushima Accident

Jun Su Ha [a*] and Sung-yeop Kim [b]
[a]*Nuclear Eng. Dept., Khalifa Univ. of Science, Technology and Research, PO Box 127788, Abu Dhabi, UAE*
[b]*Dept. of Nuclear and Quantum Eng., KAIST, Guseong-dong, Yuseong-gu, Daejeon, 305-701, Republic of Korea*
[*]*Corresponding author: junsu.ha@kustar.ac.ae*

1. Introduction

On March 11, 2011, an extremely severe nuclear accident was triggered by the great earthquake followed by the devastating tsunami at the Fukushima Daiichi Nuclear Power Plant (NPP). When the earthquake occurred, Unit 1 of the Fukushima Daiichi plant was in normal operation at the rated electricity output; Units 2 and 3 were in operation within the rated heat parameters of their specifications; and Units 4 to 6 were undergoing periodical inspections [1]. In short, Units 1, 2 and 4 lost all power; Unit 3 lost all AC power, and later lost DC before dawn of March 13, 2012. Unit 5 lost all AC power. After the water retreated, debris from the flooding was scattered all over the plant site.

Many of reports on lessons learnt from the Fukushima accident have been published and lots of relevant issues have been discussed worldwide to improve and eventually ensure the nuclear safety. One of the issues is concerning the fail safety design which has been thought of as an ensuring feature for the nuclear safety. The fail safety design is referred to as an inherently safe design concept where the failure of an SSC (System, Structure or Component) leads directly to a safe condition [2]. Usually the fail safe design has been devised based on the design basis accident (DBAs), because the nuclear safety has been assured by securing the capability to safely cope with DBAs. Currently regards have been paid to the DEC (Design Extension Condition) as an extended design consideration [3]. Hence additional attention should be paid to the concept of the fail safe design in order to consider the DEC, accordingly.

In this study, a case chosen from the Fukushima accident is studied to discuss the issue associated with the fail safe design in terms of DBA and DEC standpoints. For the fail safe design to be based both on the DBA and the DEC, a Mode Changeable Fail Safe Design (MCFSD) is proposed in this study. Additional discussions on what is needed for the MCFSD to be applied in the nuclear safety are addressed as well.

2. A Case Study: Fukushima Unit #1

In this section a fail safety design adopted in Fukushima unit #1 is described, reviewed and then finally discussed in terms of DBA and DEC standpoints.

2.1 Brief Description on the System

The Fukushima NPP unit #1 is equipped with Mark-1 containment which consists of the Primary Containment Vessel (PCV) and the Reactor Building (RB) enclosing the PCV as shown in Fig. 1.

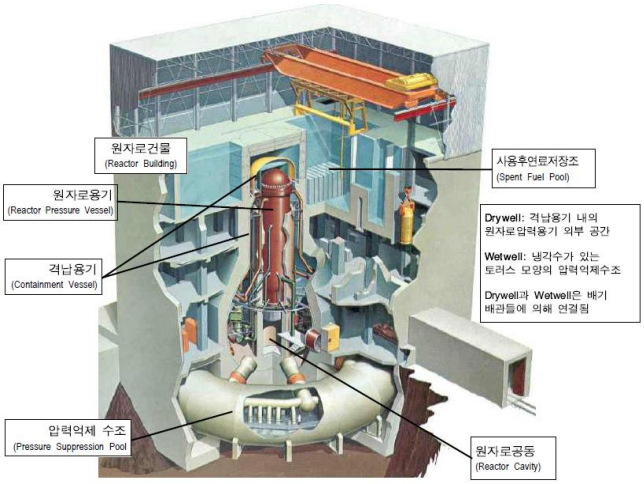

Fig. 1. Structure of Mark-I Containment and Reactor Building in Fukushima NPP unit #1 [4].

The safety systems of Fukushima unit #1 are summarized in Table I. The SLC provides the boric acid to the reactor core on failure or insufficiency of the reactor shutdown by the control rods. The HPCI is required to cool down the reactor core in LOCA (Loss Of Coolant Accident). Two-train IC system is a passive system which has capability of core cooling by natural convection. The CS installed inside the reactor core provides cooling capacities during LOCAs. The ADS is automatically activated when the pressure in reactor core should be reduced.

Table I: Safety systems in Fukushima NPP unit #1 [4]

Safety Function	Safety System
Containment	● Mark-I type
Reactor Shutdown	● Control Rod ● Standby Liquid Control (SLC)
High Pressure Safety Injection	● High Pressure Coolant Injection (HPCI) ● Isolation Condenser (IC)
Low Pressure Safety Injection	● Core Spray (CS)
Reactor Depressurization	● Automatic Depressurization (ADS)

2.2 A Fail Safe Design Considered

In this study, the fail-safe design of two motor-operated valves of MO-3A and 3B installed in the IC system is reviewed and examined as shown in Fig. 2. The fail safe design is NCFC (Normal Close Fail Close). The valves are closed during normal operation and opened in accidental situations automatically or manually. However if they fail, they are closed to prevent steam from damaging the IC pipes, which lead to direct release of contaminated steam to environment [4].

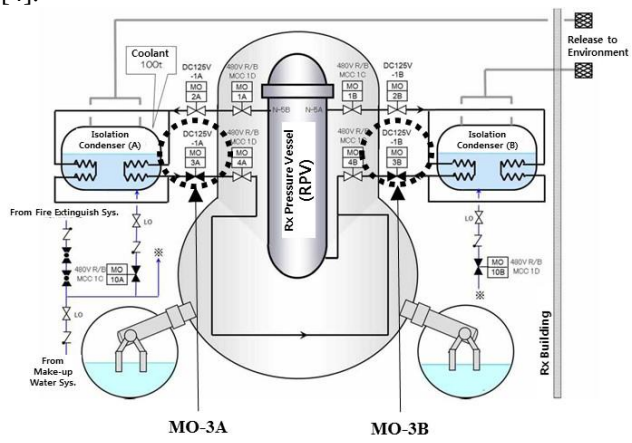

Fig. 2. Two motor-operated valves of MO-3A and 3B with NCFC (Normal Close Fail Close) fail safe design [4].

2.3 The Accident Sequence Analysis

The accident sequence in Fukushima unit #1 is analyzed here in terms of before and after the tsunami, because unit #1 was operated safely as designed before the tsunami as follows:

- **Before the Tsunami**

1. (T+0h00m) Earth quake: 3.11, 14:46
2. Automatic reactor trip (shutdown)
3. No off-site power (due to earth quake)
4. No power supply to RPS (Reactor Protection System)
5. Containment Isolation and no feedwater
6. Main Steam Isolation (MSI)
7. EDG (Emergency Diesel Generator) OK!!!
8. Power supply to safety systems
9. Rx power & water level reduced
10. **Safely controlled**!!!
11. (T+0h06m) RPV (Rx Pressure Vessel) pressure increased (due to MSI)
12. 2 Div. (A&B) IC start cooling down
13. Operators aware of rapid decrease in the pressure
14. Operators stop both ICs, because cool-down speed exceeds 55˚ C/hr (Tech. Spec.)
15. To control RPV pressure, operators continue opening and closing MO-3A (from relevant Emergency Operating Procedure (EOP))

- **After the Tsunami**

16. (T+0h41m) Tsunami: 3.11, 15:27
17. (T+0h51m) Flooding in Turbine Building Basement (Unit #1)
18. Loss of EDG & AC/DC Power source
19. (T+0h56m~1h09m) Loss of MCR lighting and I&C
20. Not applicable of EOP and accident management guidelines
21. Operators not aware of the situation (also the final state of MO-3A)
22. Operators not knowing the fail-safe design of MO-3A & 3B (NCFC)
23. (T+03h32m) DC power partially restored and (T+03h39m) operators closed MO-3A after observing no vapor from IC tanks
24. (T+6h33m) Temporary power restored in MCR and (T+6h44m) operators opened MO-3A after observing vapor from IC tanks
25. MO-3A failed due to loss of I&C power and closed (NCFC: Normal Close Fail Close)
26. Loss of residual heat removal through IC
27. Struggling to provide water into the reactor core (ex. through fire protection system)
28. Failure due to the high pressure
29. **Continuous core damage**
30. Struggling continuously to cool down the reactor with waters from fire engines and seawaters afterwards

In step 23, operators closed MO-3A to prevent steam from damaging the IC pipes, which might lead to direct release of contaminated steam to environment, because operators thought no waters in the IC tanks, which was reported later. However, 65% and 85% of water left in the IC tanks, respectively, which was reported later, as well [4]. They inferred no waters in in the IC tanks from their observation of no vapor in the IC tank. Later they were correctly aware of the situation and opened MO-3A. However it was closed eventually because of the fail safe design of NCFC (Normal Close Fail Close) as shown in step 25.

2.4 Considerations on the Fail Safe Design

The fail safe design of NCFC of MO-3A and 3B was devised based on the DBA to prevent steam from damaging the IC pipes, which might lead to direct release of contaminated steam to environment during DBAs. However in the Fukushima accident, it is thought that MO-3A and 3B should have remained open after the failure considering that they had been continuously struggling to cool down the reactors with waters provided from fire engines and seawaters afterwards, as shown in step 30.

From the viewpoint of DBAs, the fail safety design of NCFC is appropriate because the reactor was designed and proved to safely cope with DBAs. The safety can be secured by the NCFC design to prevent over-heated and over-pressurized steam from damaging the IC pipes because the reactor must be designed to have no core damage during DBAs. The only risk of radioactive release to environment is attributed to interfaces between the reactor coolant system and the IC system.

Currently the design extension condition (DEC) including severe accidents should be considered during designing and licensing NPPs according to IAEA Safety Standards Series No. SSR-2/1 (2012) [3]. Hence concepts on the fail safe design need to be changed to be based on not only the DBA but also the DEC. If a same configuration of fail-safe design (e.g., NCFC) is applicable to both the DBA and the DEC conditions, it is most favorable. However if it is not applicable to both conditions such as MO-3A and 3B fail-safe design, a new concept for the fail-safe design should be devised.

2.5 Mode Changeable Fail Safe Design (MCFSD)

For the fail safe design to be based both on the DBA and the DEC, a Mode Changeable Fail Safe Design (MCFSD) is proposed in this study. If an accidental situation of interest is a DBA condition, a DBA mode fail safe design is applied. However the situation is DEC condition, a DEC mode fail safe design should be applied. As an example for a safety-grade valve, several design options might be possible as shown in Table II. As mentioned in the previous section, the same configuration to both the DBA and DEC conditions is most favorable. However the configuration should be different upon the modes. The MCFSD might be a promising option for a future fail-safe design. It should be based on rigorous and clear analysis results on safety how to configure the MCFSD for the DBA and DEC modes.

Table II: Example of the mode changeable fail safe design for a safety grade valve

Mode (DBA-DEC)	Mode Changeable Fail Safe Design
NCFC-NCFC (Same Configuration)	● DBA mode : Normal Close Fail Close ● DEC mode : Normal Close Fail Close
NCFO-NCFO (Same Configuration)	● DBA mode : Normal Close Fail Open ● DEC mode : Normal Close Fail Open
NCFC-NCFO (Different Configuration)	● DBA mode : Normal Close Fail Close ● DEC mode : Normal Close Fail Open
NCFO-NCFC (Different Configuration)	● DBA mode : Normal Close Fail Open ● DEC mode : Normal Close Fail Close

2.6 What Is Needed for MCFSD

For the MCFSD to be applied in the nuclear safety, firstly well-developed and verified analysis tools (e.g., computer codes) for severe accidents are required, because the fail-safe design in the DEC mode should be verified and validated with appropriate and precise analysis results. Secondly, there should be clear criteria for discrimination of the DBA and the DEC modes for the MCFSD to be changed according to the modes (or conditions). In the plant protection system (PPS), several important process parameters are used for the safety function of automatic shutdown. Similar to this safety function method with the PPS, a set of important parameters and setpoint values in each parameter might be used as criteria for determining the DBA and the DEC modes. Thirdly, it should be checked out whether the MCFSD of interest is mechanically and/or physically achievable or not. In some cases, a MCFSD of a component might be applicable only in conceptual level and not be manufactured physically (or mechanically). In other cases, passive system might not be applicable only active system applicable in actual design. Hence a kind of trade-off might be considered in devising actual applications of the MCFSD.

3. Conclusions

One of the lessons learnt from the Fukushima accident should include considerations on the fail-safe design in a changing regulatory framework. Currently the design extension condition (DEC) including severe accidents should be considered during designing and licensing NPPs. Hence concepts on the fail safe design need to be changed to be based on not only the DBA but also the DEC. In this study, a case on a fail-safe design chosen from the Fukushima accident is studied to discuss the issue associated with the fail safe design in terms of DBA and DEC conditions. For the fail safe design to be based both on the DBA and the DEC, a Mode Changeable Fail Safe Design (MCFSD) is proposed in this study. Additional discussions on what is needed for the MCFSD to be applied in the nuclear safety are addressed as well.

REFERENCES

[1] The Fukushima Nuclear Accident Independent Investigation Commission, "The Official Report of the Fukushima Nuclear Accident Independent Investigation Commission", The National Diet of Japan, 2012.
[2] G. Petrangeli, Nuclear Safety, Elsevier BH, 2006.
[3] IAEA, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1, Vienna, 2012.
[4] KNS Committee on the Fukushima Accident, Fukushima Nuclear Power Plant Accident Analysis Report, Korean Nuclear Society, 2013.