Evaluation of Reliability for Fail-Safe Valve in SMR from a PSA Perspective

Kibeom Son[a], Sung-Min Shin[a], Jin Hee Park[a]*

[a]Korea Atomic Energy Research Institute, 111, Daedeok-daero, Yuseong-gu, Daejeon-si, 34057, Korea
*Corresponding author: jhpark6@kaeri.re.kr

***Keywords :** fail-safe valve, SMR, system reliability

1. Introduction

In nuclear power plants, especially in passive safety systems of Small Modular Reactors (SMRs), many valves adopt fail-safe principles to ensure the plant transitions to a safe state upon power loss [1]. However, this design can lead to spurious operations, causing unplanned shutdowns, transients, and economic costs.

Modern designs illustrate trade-offs: NuScale's Emergency Core Cooling System (ECCS) employs two serially connected normally closed trip valves for each Reactor Vent Valve (RVV) and Reactor Recirculation Valve (RRV), reducing spurious actuation risk by requiring both to open. In addition, Containment Isolation Valves (CIVs) can isolate containment even if only one of the two valves closes [2]. In all cases, design must balance between two risks—demand failure to actuate and spurious operation—by prioritizing which to minimize.

This paper conducts a reliability evaluation to determine the optimal trade-off design between demand failure and spurious operation in representative SMR systems composed with fail-safe valves. Additionally, the idea of equipping a valve with heterogeneous support systems is included to reduce the frequency of spurious operation [3].

2. Methods and Results

2.1 Reliability Optimization Factor of Fail-Safe Valve

A passive safety system is designed to mitigate accidents using natural forces, such as gravity, rather than external power. These systems are categorized according to the need for actuation signals, external energy, mechanical movement, or fluid transport. A core concept is the fail-safe principle, in which valves maintain their normal open or closed position when external power and control signals are available, but shift to a safe state when these are lost. In accidents, valves transition to mitigate the event, while in normal operation they hold their position to avoid spurious operation.

To achieve both functions, reliability-optimized configurations must be developed, considering factors such as the number, type, and configuration of valves, as well as energy sources.

Table I: List of System Reliability Optimization Factors

Optimization Factor	Description
Failure Modes	Classified into spurious operation during normal operation and demand failure during accident conditions
Success Criteria	Number of trains and components required to meet the system success criteria
Component Types	Detailed failure modes vary depending on the type of component
Number of Trains and Components	The number of trains and components constituting a system affects the success criteria
Component Configuration	Components may be arranged in series or parallel
Type of Power Supply System	Failure rates differ depending on the type of external energy source applied to valves
Support System Train Arrangement	Arrangement of external power supply and control signal systems connected to components
Dependency Model	Common-cause failures are dominant factors in determining system reliability
Others	Ex: Presence of special-purpose devices such as Inadvertent Actuation Blocks (IABs)

Table 1 presents a list of optimization factors that determine the reliability of fail-safe systems from a PSA perspective. Here, the support system refers to the external power sources and control signal systems used to maintain the valve in its intended position.

2.2 Description of Fail-Safe System

Representative reference systems composed of fail-safe valves include the CIV and the ECCS of NuScale. Among them, the ECCS consists of the RVVs and the RRVs, and the RRV incorporates a component called the IAB to prevent spurious operation.

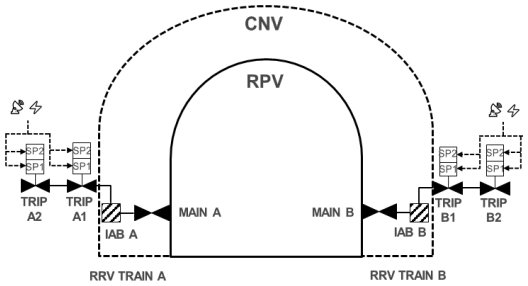


Figure 2: Schematic of the RRV in ECCS.

Figure 1 provides a simplified representation of the ECCS RRV, which is divided into trains A and B. Each train consists of a main valve, an IAB, two trip valves, and a dedicated support system for each trip valve. In this study, we considered a design concept in which heterogeneous support systems are provided for a single valve as an idea to prevent spurious operation [3].

Table 2: Detailed Failure Modes of RRV

Failure Mode / Component	Normal Operation	Accident Mitigation
Failure Mode	Spurious operation	Demand failure
Main Valve Body (Mechanical Failure)	Failure to maintain closed position	Failure to open
Trip Valve Body (Mechanical Failure)	Failure to maintain closed position	Failure to open
Trip Valve Support System (Power Supply)	Failure to maintain power supply	Failure to cut off power
Trip Valve Support System (Control)	Spurious actuation signal generation	Failure to generate actuation signal
IAB (Mechanical Failure)	Failure to maintain open position	Failure to close

Table 2 summarizes the failure modes of each component of the RRV. During normal operation, the main valve and trip valve bodies must remain in the closed position, and the trip valve power system must continuously supply electricity to maintain the closed position of the trip valve body. In addition, the control system must not generate spurious signals; if such a signal occurs, the trip valve body will open.

In accident conditions, the main valve and trip valve bodies must open, and the control system must successfully generate the actuation signal. Due to the fail-safe characteristics, the power supply to the trip valve is interrupted during an accident, which causes the trip valve body to open. However, if the power is not successfully cut off, the trip valve body may fail to open.

The IAB, which is included only in the RRV, prevents the main valve from opening in case of an spurious actuation signal during normal operation. Under accident conditions, the main valve opens when the pressure difference between the RPV and the CNV reaches the setpoint.

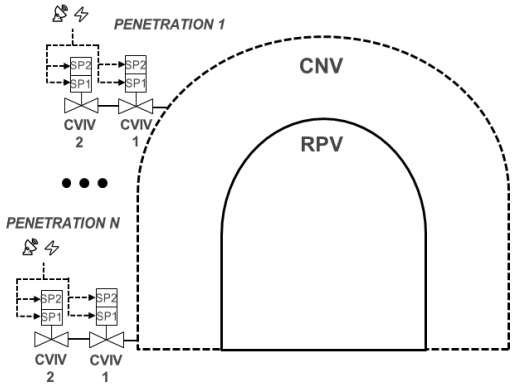


Figure 2: Schematic of the CIV

Figure 2 provides a simplified representation of the arrangement of the CIVs, in which numerous containment penetrations are each connected to their respective systems. For isolation valves that are initially open, the success criterion under accident conditions is that all penetrations are successfully closed, while under normal operation the success criterion is that all penetrations remain open. The CVIV can be regarded as having the trip valve of the RRV serve as the main valve. In this study, a total of 50 penetrations was assumed for the quantification.

Table 3: Detailed Failure Modes of CIV

Failure Mode / Component	Normal Operation	Accident Mitigation
Failure Mode	Spurious operation	Demand failure
CIV Body (Mechanical Failure)	Failure to maintain opened position	Failure to close
CIV Support System (Power Supply)	Failure to maintain power supply	Failure to cut off power
CIV Support System (Control)	Spurious actuation signal generation	Failure to generate actuation signal

Table 3 summarizes the failure modes of each component of the CIV. Compared with the RRV, differences exist in the presence of the IAB, the number of trains, and the initial valve position.

2.3 Quantification of Fail-Safe System

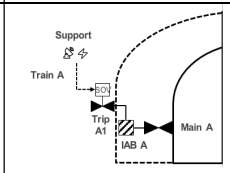
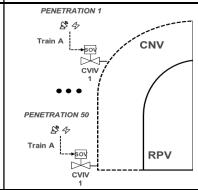
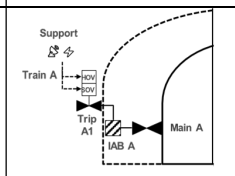
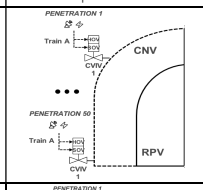
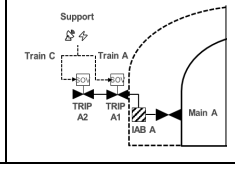
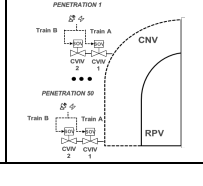
For the quantification of fail-safe systems, eight representative configurations were selected, and their schematic representation based on the ECCS is shown in Table 4. The cases can be summarized as follows

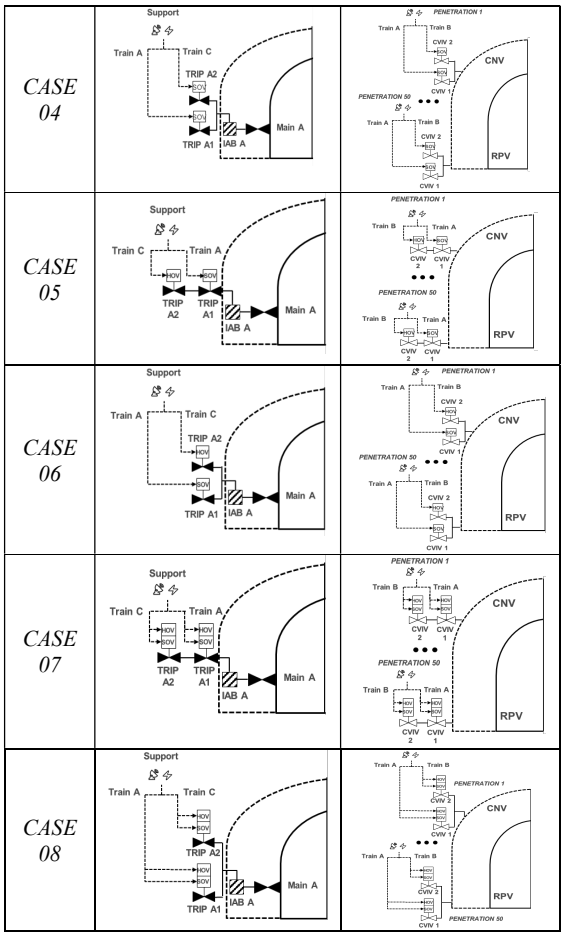
- *CASE01*: Base case with one trip valve and one support system
- *CASE02*: Base case with redundancy applied to the power source
- *CASE03*: Increased trip valve redundancy compared to the base case, arranged in series
- *CASE04*: Increased trip valve redundancy compared to the base case, arranged in parallel
- *CASE05*: Increased diversity of power supplies compared to *CASE03*
- *CASE06*: Increased diversity of power supplies compared to *CASE04*
- *CASE07*: Power source redundancy added to *CASE03*
- *CASE08*: Power source redundancy added to *CASE06*

The assumptions for performing the quantification are as follows:

- Information on ECCS and RRV valve assemblies: NuScale [2]
- System fault-tree modeling: AIMS PSA code
- Component failure rate data: NUREG-CR/6928 [4]
- Common-cause failure data: NUREG-CR/5497 [5]
- Failure rates of power and control systems: from existing commercial NPP PSA model
- Mission time for running failure: 8,760 hours
- Support systems considered: Solenoid-Operated Valve (SOV) or Hydraulic-Operated Valve (HOV)
- Failure rate of the hydraulic system: assumed to be twice that of the power system

Table 4: Schematic of Representative Cases

CASE	Schematic of normal operation	
	RRV	CIV
CASE 01 (BASE CASE)		
CASE 02		
CASE 03		



Figures 3 and 4 present graphs comparing the system reliability of the RRV and CIV, as well as the relative difference with respect to the base case, under accident conditions and normal operation, respectively.

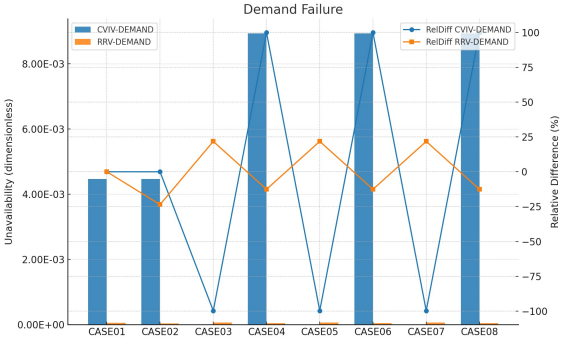


Figure 3: Quantification results of demand failure for the RRV and CIV by case

When comparing the demand failure of the CIV across different cases, it is observed that the serial arrangement of CIVs is more favorable for accident mitigation, while redundancy of the support systems has little effect. For the RRV, the most significant factor in

a positive direction is not the number of trip valves, but rather the presence of redundancy.

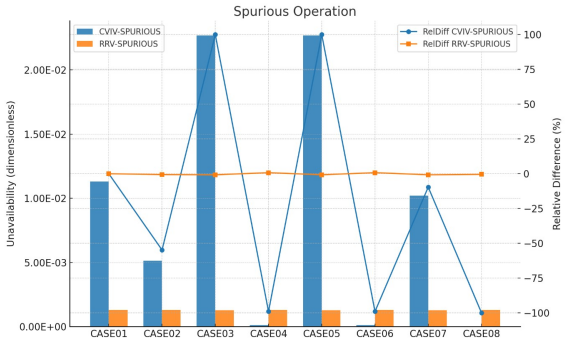


Figure 4: Quantification results of spurious operation for the RRV and CIV by case

When comparing the spurious operation of the CIV across different cases, it is observed that a serial arrangement of CIVs is more favorable for accident mitigation, and redundancy of the support systems alone can reduce the unavailability to about half of that in the base case. For the RRV, however, there is little difference in unavailability among the cases because the IAB functions to prevent spurious operation.

Based on the optimization factor, the lessons learned from the interpretation of the quantification results can be summarized as follows.

- For systems with more than two valves, the combination of configuration (series/parallel) and initial position (closed/opened) leads to different favorable failure modes
- Specifically, valves that are initially open are more advantageous in preventing demand failure when arranged in series, while valves that are initially closed are more advantageous in preventing spurious operation when arranged in series
- For both systems, diversifying external power sources to minimize the impact of common-cause failures does not contribute significantly to reliability improvement
- In the case of the RRV, the influence of the main valve dominates all failure modes due to the valve's actuation mechanism and the component failure data
- The IAB, consistent with its design purpose, is advantageous in preventing the spurious operation failure mode, resulting in similar reliability across all configurations. However, it has a relatively minor negative effect on demand failure

In conclusion, based on the assumptions regarding the current systems, failure modes, and data, the optimal trade-off case between failure modes is identified as *CASE02* or *CASE07* for the CIV, while *CASE02* is found to be the optimal design for the RRV. These results suggest that applying the concept of power source redundancy to systems composed of fail-safe valves is a valid approach.

3. Conclusions

In this study, a reliability assessment was conducted to identify the optimal trade-off point between demand failure and spurious operation in representative SMR systems composed of fail-safe valves. A distinctive feature of the analysis was the application of power source redundancy as a sensitivity analysis case to prevent spurious operation. The quantification results indicate that the redundancy concept is effective in reducing the unavailability of both failure modes; however, such conclusions may vary depending on the modeling conditions.

ACKNOWLEDGMENTS

This work was supported by an Innovative Small Modular Reactor Development Agency grant funded by the Korean Government (MSIT) (No. RS-2023-00258118).

REFERENCES

[1] International Atomic Energy Agency, IAEA Safety Culture in Nuclear Installations: Guidance for Use in the Enhancement of Safety Culture, IAEA-TECDOC-1624, Vienna, 2009.
[2] NuScale Power, LLC, NuScale Standard Plant Design Certification Application, US460 Design Certification (DCA), Washington, D.C., 2023
[3] Korea Atomic Energy Research Institute, Fail-safe valve device and reactor equipment including the same, Korean Patent Application No. 10-2024-0115072, 2024.
[4] Idaho National Laboratory, Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants: 2020 Update, INL/EXT-21-65055, Idaho Falls, ID, 2021.
[5] Idaho National Laboratory, CCF Parameter Estimations 2020 (Revision 1), INL/EXT-21-62940 Rev.1, Idaho Falls, ID, 2021.