Preliminary Review on the Application of the Single Failure Criterion to Passive Safety Systems

Sera Jeon, Seong-Su Jeon, Youngjae Park*
FNC Tech. Co. Ltd., Floor 32, Heungdeok IT Valley, 13 Heungdeok 1-ro, Giheung-gu, Yongin-si, Gyeonggi-do, 16954, South Korea
**Corresponding author: ypark1227@fnctech.com*

Keywords : single failure criterion, passive safety system, passive containment cooling system

1. Introduction

To ensure the safety of nuclear power plants, the Single Failure Criterion (SFC) has been established as a key principle of safety design. Under the SFC, it is required that system safety functions be preserved even in the event of a single component failure, and this principle has long been recognized as a fundamental basis for the reliability and safety of nuclear facilities. For active components such as pumps and motor-operated valves, which are dependent on external power, control signals, or operator actions, the likelihood of failure is relatively high; therefore, the application of the SFC to these components has been considered an important safety principle.

In recent reactor designs, however, passive safety systems have been introduced to avoid such vulnerabilities by excluding active components. These systems are operated without external power or operator action, relying instead on natural physical phenomena such as gravity, natural circulation, and pressure differentials. Given these structural and functional differences, it is necessary to assess whether the conventional application of the SFC remains appropriate for passive safety systems, or whether alternative interpretations and approaches are warranted.

In this study, the applicability of the SFC to passive safety systems is examined, focusing on the Passive Containment Cooling System (PCCS) of the i-SMR, and the associated analytical considerations are discussed.

2. Definition of Single Failure Criterion (SFC)

The Single Failure Criterion (SFC) is a fundamental concept in the safety design of nuclear power plants, requiring that essential safety functions be maintained even in the event of a single failure. The U.S. Nuclear Regulatory Commission (NRC) defines the SFC in the General Design Criteria (10 CFR 50, Appendix A) as follows: “A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), result in a loss of the capability of the system to perform its safety function. [1]”

This definition implies that a single failure is an event that renders a component incapable of performing its intended safety function, and that multiple failures caused by a single initiating event are regarded as a single failure. However, in considering how to apply the Single Failure Criterion (SFC) to both active and passive components in practical reactor design, reference was made to SECY-77-439 as an interpretive guidance document. In this document, a realistic approach to the application of the SFC is provided, including the following principles [2]:

- The application of the Single Failure Criterion does not require postulating every conceivable failure.
- For example, reactor vessels or certain structural elements are not assumed to fail even when combined with other low-probability events, because the probability of the resulting event scenario is considered sufficiently small.
- In general, when applying the Single Failure Criterion, only those systems or components with a credible likelihood of failure are assumed to fail.

In fluid systems, the application of the Single Failure Criterion can be categorized into active and passive failures, which are defined as follows [2]:

- Active failure: Failure of a component that relies on mechanical movement or external actuation for its operation, or unintended movement that prevents the completion of its safety function. (Examples: Failure of motor-operated or air-operated valves to reach the correct position, spurious valve opening/closing, or pump failure to start/stop on demand.)
- Passive failure: Breach of the fluid pressure boundary or mechanical damage affecting a flow path. (Examples: Leakage from pipes or valves due to failed seals, line blockages, or check valves failing to seat properly.)

3. Approaches for Applying the Single Failure Criterion to Passive Safety Systems

3.1. Review of Active Failures in i-SMR PCCS

To examine the application of the Single Failure Criterion (SFC) to passive safety systems, this study considers the PCCS of the i-SMR as a case and derives practical approaches based on its design features. The PCCS is a passive safety system designed to reduce containment pressure and remove heat under all accident conditions, including severe accidents, without external power or operator action, relying solely on natural circulation. Its main components consist of include Passive Containment Cooling Heat Exchanger (PCCHX) inside the containment, connecting piping, isolation valves, and the external Emergency Cooling Tank (ECT), as illustrated in Fig. 1.

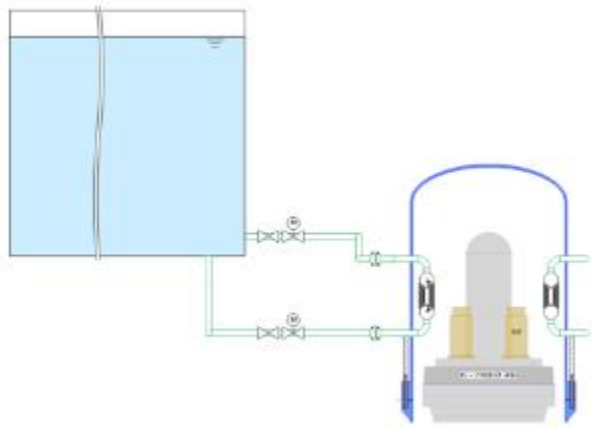

Fig. 1. Schematic diagram of i-SMR PCCS

Among these, the isolation valves are motor-operated valves (MOVs), which could potentially be categorized as active components. A useful reference case in this regard is the Safety Injection System (SIS) of the APR1400. The APR1400 Design Control Document Tier 2 specifies that the discharge isolation valve of the Safety Injection Tank (SIT), which is an MOV, is normally locked open in the control room. This arrangement ensures that even under three potential failure modes—fails closed, fails opened, or fails to open on Safety Injection Actuation Signal—the safety function is not compromised. In accordance with the classification approach for fluid systems presented in SECY-77-439, such a valve can therefore be treated as a passive rather than an active component [2][3].

By the same logic, the isolation valves in the PCCS are MOVs also locked in the open position and, following SECY-77-439, are classified as passive components. Consequently, active failures are excluded from the failure assumptions for the PCCS. This review thus focuses primarily on the potential single failures of passive components, particularly those involving fluid pressure boundary damage and mechanical damage to the fluid flow path.

3.2. Review of Passive Failures in Terms of Fluid Pressure Boundary Damage

3.2.1. PCCS Piping

Classification of the PCCS piping is required because the section between the inlet isolation valve, PCCHX, and the outlet isolation valve penetrates the containment vessel. Since the PCCS piping operates under near-atmospheric pressure and ambient temperature conditions, it is conservatively classified as “medium-energy piping” according to the criteria in Table I [4]. For medium-energy piping, rupture is not postulated, and only leakage is considered [4]. Furthermore, for Class 2, Class 3, and nonsafety-class piping, if the calculated stress under service Level A and B conditions does not exceed 40% of the allowable limit (0.4 Sm), the postulation of leakage cracks may be excluded [5]. Accordingly, for PCCS piping conservatively classified as medium-energy, rupture need not be postulated and leakage postulation may be limited to cases not otherwise screened out by the stress criterion.

Table I: Classification of high-energy piping and medium-energy piping [4]

Piping type	Definition	Remarks
High-energy piping	Operating temperature ≥ 93.3 °C or operating pressure ≥ 1.9 MPa	Rupture/ Leakage considered
Medium-energy piping	Operating temperature ≤ 93.3 °C and operating pressure ≤ 1.9 MPa	Leakage considered

3.2.2. Isolation valves and heat exchangers

The PCCS is classified as an Engineered Safety Feature (ESF), and therefore isolation valves are generally required both inside and outside the containment vessel [6]. However, because the PCCS forms part of the Reactor Coolant Pressure Boundary (RCPB), and rupture or leakage in the containment penetration region is excluded from consideration, the system is operated in a closed-loop configuration in which the system fluid is not directly connected to the containment atmosphere. Owing to this characteristic, a single isolation valve installed outside the containment vessel can be considered sufficient to satisfy the system’s isolation function [6].

Furthermore, even in the event of leakage or damage in the PCCHX, the system design characteristics limit the potential for fluid ingress or flooding into the containment vessel. Accordingly, flooding of the containment building due to PCCHX failure is excluded from the scope of this review.

3.2.3. Safety Evaluation under Valve Leakage Assumptions

Assuming the capacity of ECT is 1,000 m^3 and a valve leakage rate is 1.0 GPM (≈ 5.45 m^3/day),

complete depletion would be expected after about 184 days. During the typical accident mitigation periods of 24 hours and 72 hours, as well as the longer-term perspective of 30 days, the cumulative leaked volumes would be about 5.45 m^3 (0.55%), 16.35 m^3 (1.64%), and 163.5 m^3 (16.3%), respectively. These results indicate that, under reasonable geometric assumptions, leakage at this level would not hinder the PCCS from performing its long-term cooling function.

In addition, the potential leakage of the PCCS isolation valve can be managed within an acceptable range by comprehensively considering design margins, leak detection and prevention systems, and periodic testing. This approach provides a reasonable basis for reconsidering the appropriateness of the conservative assumption that system failure should be immediately postulated.

3.3. Review of Passive Failures in Terms of Mechanical Damage to the Fluid Flow Path

The PCCS is designed with large-diameter piping, by which the likelihood of flow obstruction caused by debris or valve malfunctions is inherently reduced. In addition, the system is designed without orifices, and debris control measures are in place for the ECT to limit potential sources of flow blockage.

Even if partial blockage of the PCCHX tubes were to occur, sufficient heat transfer margin is incorporated in the design to ensure that any reduction in system performance would not impair its safety functions. Furthermore, periodic inspection and testing are conducted to detect potential blockages, and component replacement is feasible when necessary.

Therefore, under the single failure assumption, the risk of a direct loss of PCCS safety functions due to mechanical damage is assessed to be of limited significance, considering the design and operational provisions.

4. Conclusion

This study examined the application of the Single Failure Criterion (SFC) to the Passive Containment Cooling System (PCCS), a key passive safety system in the i-SMR. Unlike conventional active safety systems, the PCCS is designed to perform its safety functions through natural circulation without external power or operator action, under both normal conditions and design basis accident scenarios. Based on the review, it was determined that active failure is not applicable, since the isolation valves are permanently locked in the open position and the system does not rely on mechanical actuation. Therefore, the review was focused on potential passive failures, particularly those related to fluid pressure boundary damage and flow path blockage due to mechanical failure.

The review indicated that leakage in isolation valves or piping would not significantly affect the overall system safety. Furthermore, it was found that the likelihood of passive failures can be further reduced by incorporating sufficient design margins, providing leak-prevention measures, and implementing periodic inspection and testing.

Therefore, rather than applying the same SFC approach used for active safety systems uniformly to passive safety systems such as the PCCS, a more reasonable review that reflects the system's unique characteristics and design objectives is necessary. Based on the PCCS case study, approaches for applying the SFC to passive safety systems were reviewed, and it is considered that further refinement will be needed through the development of interpretive criteria informed by probabilistic assessments and through empirical validation studies.

ACKNOWLEDGEMENT

This paper was supported by the Innovative Small Modular Reactor Development Agency grant funded by the Korea Government(Ministry of Trade, Industry and Energy, MOTIE) (No. RS-2024-00404240).

REFERENCES

[1] 10 CFR 50 App. A, "General Design Criteria for Nuclear Power Plant"
[2] U.S.NRC, "Single Failure Criterion", SECY-77-439, 1977
[3] APR1400 Design Control Document, Tier 2, Korea Electric Power Corporation (KEPCO) and Korea Hydro & Nuclear Power Co., Ltd. (KHNP.)
[4] U.S. NRC NUREG-0800, "Standard Review Plan Section 3.6.2, Determination of Rupture Locations and Dynamic Effects Associated with the Postulated Rupture of Piping", Rev. 3, 2016.
[5] U.S. NRC NUREG-0800, "Standard Review Plan Section Branch Technical Position 3-4, POSTULATED RUPTURE LOCATIONS IN FLUID SYSTEM PIPING INSIDE AND OUTSIDE CONTAINMENT", Rev. 3, 2016.
[6] U.S. NRC NUREG-0800, "Standard Review Plan Section 6.2.4, Containment Isolation System", Rev. 3, 2007.