APPLICATION OF THE SINGLE FAILURE CRITERION TO THE ADVANCED CANDU REACTOR (ACR)

C. Nie, A. H. Stretch, P. Santamaura, D. Wright, B. Lekakh
Atomic Energy of Canada Limited (AECL)
Mississauga, Ontario

Abstract

The Single Failure Criterion (SFC) is intended to address random failures by providing a measure of redundancy to ensure adequate reliability of important safety functions.

In the traditional CANDU design practice, this is achieved by having two sets of systems that can perform the essential safety functions to satisfy a probabilistic safety goal, supplemented by implementation of redundancy in the special safety systems, comprising shutdown systems 1 and 2, the emergency core cooling system, and the containment system.

To facilitate licensability in international markets, and to be consistent with international standards and practices, the accepted approach of applying the SFC within systems or groups of systems that perform the important safety functions required for the design basis events has been adopted.

This paper provides an outline of how the SFC is applied to the ACR design.

Keywords: Single Failure Criterion, Limiting Single Failure, Failure Mode and Effects Analysis (FMEA), Advanced CANDU Reactor™* (ACR)

1. Introduction

The single-failure requirement was formulated in the mid 1960s by the US Atomic Energy Commission as a regulatory requirement for nuclear power plants in the form of General Design Criteria (GDC). It was first applied to the plant protection system (the system that senses abnormal conditions and initiates mitigating actions in light water reactors), and then to the emergency core cooling system.

The objective of the Single Failure Criterion (SFC) is to address random failures, and thus to provide reliability of important safety functions required for design basis accidents. This is achieved through the redundant design of important safety functions. These functions are implemented by safety related systems; each safety related system may have redundancy, or redundancy may be achieved with two or more single-train safety related systems.

Under the framework of the traditional CANDU safety design and analysis [1], the intent of SFC is implemented by having two sets of systems (e.g. Group 1 and Group 2), which

* ACR™ (Advanced CANDU Reactor™) is a trademark of Atomic Energy of Canada Limited (AECL).

perform the essential safety functions to satisfy a probabilistic safety goal. This approach is supplemented by the provision of redundancy in each special safety system [2] [3] [4] to satisfy a reliability target for the mitigating safety functions. A probabilistic safety assessment and reliability analyses confirm that the required reliability of safety functions to satisfy the safety goals for the plant are provided.

The ACR design builds on the proven technology of existing CANDU plants and on AECL's knowledge base acquired over decades of nuclear power plant design, engineering, construction and research. The primary objectives of the ACR are enhanced safety and licensability in international markets, and cost reduction. To facilitate licensability in international markets, the widely recognized approach of providing redundancy by application of the SFC within certain safety related systems that perform essential safety functions for design basis accidents has been adopted.

This paper outlines how the SFC is applied to the ACR design, including the interpretation and application of the SFC, specific rules on the assumption of single failures, and methodologies for performing single failure analysis and identifying limiting single failures assumed in the design basis event analysis.

2. Single Failure Criterion

The term "single failure" is defined as a random failure (e.g., a single component failure) concurrent with its consequential effects, in addition to an initiating event, that results in the loss of capability of a component to perform its function.

Theoretically, the single failure could occur prior to, or at any time during, the event.

Simply stated, the SFC is a requirement that a safety related system must be capable of performing its intended safety functions for a design basis event assuming a single failure within the system or in an associated system that supports its operation.

This application of the SFC leads to hardware redundancy (e.g., two or more trains) in specific safety related systems to ensure that the systems can respond to the challenges with adequate reliability, and to establish safe end states with acceptable safety margins.

3. Application of Single Failure Criterion

In the ACR design, the SFC is applied to certain safety related systems or components used to accomplish important safety functions required for design basis events, such as the heat transport system isolation and over-pressure protection, reactor shutdown, decay heat removal from the reactor core, emergency core cooling, containment isolation and containment cooling.

Any consequential and/or coincident failures specified by the required design basis event analysis assumptions are considered in addition to the single failure. For example, if a reactor trip or turbine trip is a direct consequence of the design basis event, loss of the normal power supply may be considered as a consequential failure of that design basis event due to disruption of the grid following a turbine trip during the event.

Examples of the ACR safety related systems that will be subject to the SFC are:

- Shutdown systems
- Emergency core cooling system
- Containment cooling system
- Containment isolation system
- Safety related Class I/II/III power supply system
- Safety related service water systems

Single Failure Analysis for Design

Application of the SFC is complicated by the intricacies of various fluid and electrical systems, their interrelationships, and their supporting auxiliaries. Furthermore, there is a need to identify the events and associated assumptions that must be considered during application of the SFC. This involves a systematic search for single failure points and their effects on the performance of safety functions. The objective is to identify design weaknesses that could be overcome by increased redundancy, or the use of alternative procedures. This is achieved in the ACR design through the following process, called Single Failure Analysis (SFA):

1) Identification of Safety Groups

   For each design basis event, the following steps apply:

   i) Determine the safety functions (e.g., reactor shutdown, reactor core cooling, and containment isolation) required to cope with the design basis event;

   ii) Identify the protective actions at the system level (e.g., rapid insertion of control rods, closing of containment isolation valves, safety injection) that are available to accomplish each required safety function identified in Step i);

   iii) Identify the safety groups used to accomplish each required safety function.

   Here, safety group is defined as a given minimal set of interconnected components, modules, and equipment that can accomplish a safety function. This may be a safety related system, or a portion of the system.

2) Design Assessment for Single Failure

   For each safety group identified in Step 1), a Failure Mode and Effects Analysis (FMEA) is conducted to determining how a component can fail and what the consequences would be if it should fail.

   i) A single failure is assumed in the group, and the consequences of the single failure are determined. It must be shown that the safety function (e.g., rapid insertion of control rods, closing of containment isolation valves, safety injection) can still be performed.

   ii) In determination of the consequences, the independence of the safety group is verified by observing that there are at least two safety groups having no shared equipment or points of vulnerability (e.g., valves, pumps, relays, switchgear, buses, power sources, cooling water).

   iii) Once independence is established, redundant capability exists to perform the safety function. It follows then that, for the purpose of satisfying the SFC, it

is not necessary to consider further the potential for failures within the redundant parts.

Not all hypothesized failures need to be considered in the SFA. Only those failures judged to have a credible likelihood of occurrence are assumed. This justification may be achieved by reliability analysis, operating experience, engineering judgement, or a combination thereof. The SFC application should be commensurate with the expected frequency and consequences of the challenge to plant safety. Examples are given below to illustrate the ACR positions on failure modes to be considered in the SFA. Active and passive failures

The failures considered in the single failure analysis include both active failures (such as failure of a powered valve to move to its correct position, or failure of a pump, fan or diesel generator to start) and passive failures (such as leakage of safety related system piping or blockage of the process flow path of a safety related system).

In dealing with active or passive failure, a time frame, long term or short term is determined. During the short term, the single failure is limited to an active failure. Generally, the short term is that period of operation up to 24 hours following an initiating event. During the long term, assuming no prior failure during the short term, the single failure can be either active or passive.

For example, for the emergency core cooling system, only an active failure is assumed during the short-term emergency coolant injection mode following a loss of coolant accident; while during the long-term recirculation cooling mode, either an active failure or a passive failure is assumed.

- Electrical Components

  For electrical components, no distinction is made between active components such as diesels, and passive components such as wires. A random failure is simply assumed on demand or during the mission period and dealt with as an active failure. Therefore, a single failure is assumed to occur at any time.

- Passive failures

  Passive failures applied to fluid systems during the long term include the degradation of pump or valve seals, or a moderate-energy piping crack and resulting leakage. The rationale for applying this type of failure is the recognition of the relatively extended periods that the systems must operate during the long term following a design basis accident associated with a pipe break. No other passive failures are required to be assumed because of sufficiently small probabilities of combination of other types of passive failures with a design basis accident.

- Undetectable Failures

  An undetectable failure that does not cause an alarm or that cannot be detected by specified tests or inspections is assumed to exist at any time.

- Fluid System Isolation Devices

  The SFC is applied to the actuation of interface barriers or isolation devices for the pressure integrity of fluid systems to ensure that loss of fluid via an interfacing

system will not impair the ability of the safety-related system to perform its safety functions.

When determining the loss of fluid, the closure time of open valves, the leak tightness of closed valves, and the limitation of losses due to flow restrictions are evaluated. The loss of fluid is assessed for the full duration of the event.

- Exemptions

  Based on international practice, exemptions are normally granted for the following single failures:

  - Where the proper active function of a component can be demonstrated despite any credible condition, then that component may be considered exempt from active failure. Examples of such component functions may include opening of rupture discs and opening of simple swing check valves.
  - When one train of a redundant safety-related system or its safety supporting systems is temporarily rendered inoperable due to short-term maintenance, as allowed by the technical specifications for the plant, a single failure need not be assumed in the other train.

    However, action is required according to the plant Technical Specification, to return the plant operating mode to a safe condition within a specified time. The specified time to take action, as a temporary relaxation of the SFC, depends on the overall system reliability considerations.

4. Limiting Single Failures

Due to a single failure, a change to the event consequences is possible; therefore, the safety analysis for design basis events would be carried out with an assumption of a limiting active single failure (LSF) in safety-related systems. The LSF is a single failure that exists in the safety groups, and has the worst impact on the performance of the required safety function (i.e., due to which, the event consequence is worst).

The LSF is identified by the following process:

- Determine the event sequence being analysed;
- Determine the safety group for each safety function required for the event;
- Define the analysis objectives for each safety function;
- Identify the potential single failures existing in the safety groups required for each safety function;
- Determine the effects of identified single failures on the performance of each safety function;
- Select the LSF for each safety function, based on the worst impact on the safety function's performance (i.e., due to which, the event consequence is worst). This justification may be done either by the past experience or sensitivity analysis.

5. Comparison with the IAEA and US Requirements

The ACR SFC practice meets the IAEA requirements. Consistent with the requirements of the IAEA standards [6] [7] [8], the SFC is applied to important safety functions

required for a design basis event in the ACR design. The SFA is applied to the ACR design to assess compliance with the SFC; only credible single failures are considered in the SFA, and the worst (or limiting) single failure is assumed in the design basis event analysis.

The ACR SFC practice is consistent with US practice [9] [10] [11]. This provides high system reliability through the provision of redundancy in systems that are designed to perform a safety function. The SFA will show that at least two independent safety groups exist to accomplish each required safety function. In addition to other conservative assumptions, a limiting single failure is assumed for each safety function being analysed in the design basis accident analysis in both the ACR design and the US practice [12].

6. Conclusions

Under the ACR safety assessment framework established by the ACR Safety Basis [5], the internationally accepted SFC was adopted by the ACR design that provides a systematic approach for implementing the SFC, including the extent of application, the specific rules for assuming single failures, and the methodologies for performing SFA and identifying the LSF in the design basis event analysis.

The ACR SFC practice provides an acceptable level of redundancy in specific safety related systems that perform important safety functions required for design basis events, when used in conjunction with the reliability targets based on the probabilistic safety assessment to satisfy the safety goals for the plant.

7. References

[1] CNSC Draft Regulatory Guide, “Requirements for the Safety Analysis of CANDU Nuclear Power Plants”, C-006 (Rev. 1), September 1999.

[2] CNSC Regulatory Document R–7, ‘‘Requirements for Containment Systems for CANDU Nuclear Power Plants’’, February 1991.

[3] CNSC Regulatory Document R–8, ‘‘Requirements for Shutdown Systems for CANDU Nuclear Power Plants’’, February 1991.

[4] CNSC Regulatory Document R–9, ‘‘Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants’’, February 1991.

[5] M. Bonechi, H. Johal, Z. Bilanovic, V. Lau, C. Xu, and C. Nie, “Safety Basis of the Advanced CANDU Reactor”, paper presented at 25th Annual CNS Conference on Nuclear Energy – Meeting the Challenge, Toronto, 2004.

[6] IAEA Safety Requirements NS-R-1, “Safety of Nuclear Power Plants: Design”, Vienna 2000.

[7] IAEA Safety Guide NS-G-1.2, “Safety Assessment and Verification for Nuclear Power Plants”, Vienna 2001.

[8] IAEA, Safety Practices 50-P-1, “Application of the Single Failure Criterion”, Vienna, 1990.

[9] USNRC, "Code of Federal Regulations, Title 10, Part 50, Appendix A: General Design Criteria for Nuclear Power Plants", January 1998

[10] ANSI/ANS, "Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems", Standard No. 58.9-1981.

[11] IEEE, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems", Standard No. 379-2000.

[12] US NRC RG 1.70, Revision 3, "Standard Format and Content of Safety Analysis Report for Nuclear Power Plants," November 1978.