

NUCLEAR SAFETY DIRECTORATE - BUSINESS MANAGEMENT SYSTEM		
TECHNICAL ASSESSMENT GUIDE THE SINGLE FAILURE CRITERION		T/AST/011
		ISSUE 001
Approved By: <i>R P Pape</i>	R P Pape	Issue Date: 2/10/00
Open Government Status: Fully Open		Review Date: 1/10/03

1. Purpose and scope

1.1 This Technical Assessment Guide (TAG) gives interpretation of NII's approach to the assessment of compliance with the single failure criterion (SFC) as set out in licensees' safety submissions, and as described in outline in NII Key Safety Assessment Principle P78. It contains *guidance* to advise and inform NSD inspectors in the exercise of their professional regulatory judgement. Comments on this guide, and suggestions for future revisions, should be recorded on the appropriate registry file.

1.2 A change in approach to the SFC was adopted in the 1992 SAPs which reflected international rather than traditional British practice. The effect of this change was to reduce the severity of the required SFC compliance test. The original NII safety assessment principles ^[2] contained two principles which addressed single failures, these are reproduced in **Appendix 1**. The first of the principles (no 31) was a general design objective, intended to test the vulnerability of the plant to any single failure, including failures of items whose main function was not directly related to safety. In the 1992 revision of the SAPs, new principles, which introduced the concept of defence in depth (P65), safety categorisation (P69), and a revised special case procedure (P70), permitted the deletion of the single failure design principle.

1.3 The second of these original principles (no 112) applied to protection systems, now redefined as *safety systems* in the revised SAPs, and required ^[3] that each protective (i.e. safety system) action should be shown to operate in the presence of any single failure. This principle was more restrictive than the internationally accepted version ^[4,5,6], and the decision was therefore taken during the 1992 review of the SAPs to adopt the more widely agreed SFC (Principle P78). The implication of this change was to move away from applying the SFC to an individual safety system, but instead to apply it to the totality of means of implementing a safety function.

1.4 It should be noted that, although the adoption of the internationally accepted version of the SFC is seen as a move towards harmonisation with other countries, there are still different national approaches to its interpretation. A comparison of the application of the SFC within CEC member states [7] has highlighted many of these differences, most of which stem from exceptions allowed in applying the SFC during maintenance outages at power, and for very infrequent faults. This document gives guidance on the objectives and the application of the SFC, principle P78.

2. SAPs addressed

2.1 The main SAP addressed is P78. Also relevant are SAPs P21, P22 and P178.

2.2 The SFC is intended to be used as a simple check to ensure that a minimum level of redundancy is incorporated into those safety systems provided to satisfy a safety function (P79). It is not in isolation sufficient to ensure an adequate reliability for any specific duty. To ensure this, a reliability analysis is required (P178) which takes into account the individual component reliabilities and associated maintenance procedures. The probabilistic safety analysis, in particular P41, also requires that "... information relevant to the requirements on the reliability, maintenance and testing of safety and safety related systems", is made available. This information may also have an influence on the redundancy requirements for a safety system or component.

2.3 Definitions

1) *Active Component:*

a component which has moving parts, or which requires an external input, such as electrical or pneumatic supply, actuation, or other mechanical movement in order to perform its function.

2) *Passive Component:*

a component which requires no external input and has no moving parts, but which may be subject to pressure, stress, temperature or fluid flow effects in performing its function.

3) *Safety system:*

a system which acts in response to a fault to prevent or mitigate a radiological consequence.

4) *Safety function:*

a specific purpose that must be accomplished for safety.

3. Relationship to licence and other relevant legislation

3.1 The primary licence conditions for which an assessments against the single failure principles are to be carried out are:

LC 14 (safety documentation);

LC 15 (periodic review);

LC 20(4) (modification to design of plant under construction);

LC 22(4) (modification or experiment on existing plant);
and

LC 27 (safety mechanisms, devices and circuits).

3.2 Other licence conditions for which the single failure principle is of relevance are

LC 23 (operating rules);

LC 24 (operating instructions); and

LC 28 (examination, inspection, maintenance and testing).

4. Advice to assessors

This guide mainly concentrates on the effects and implications of the SFC, rather than on the circumstances that should be considered in order to determine whether or not it should be applied. For guidance in these areas see **Ref 9** (T/AST/003), and in particular para 6.2 (4) and Appendix 1 of that guide.

4.1 Safety functions and safety systems

1) The safety case should contain a schedule of safety system provisions, from which the safety functions to which the SFC should be applied can be identified. A safety function is defined ^[4] as "*a specific purpose that must be accomplished for safety*". In order to achieve a safety function, one or more systems may be provided. Typical safety functions which need to be addressed include, in the case of a nuclear reactor:

- i) safe shutdown and maintenance of the sub-critical state;
- ii) residual heat removal;
- iii) containment.

2) For chemical plant, safety functions which may need to be addressed include:

- i) process and / or fission product heat removal;
- ii) containment;
- iii) personnel access control; and
- iv) criticality control.

3) A safety system is defined as "*a system which acts in response to a fault to prevent or mitigate a radiological consequence*". The safety schedule required by principle P178 should detail "*the extent of safety system provisions, their functions and required reliabilities*". It should be noted that safety systems encompass protection systems, safety actuation systems and safety system support features as defined in the principles, and may contain active or passive features, or a combination of both. They therefore form a basis for establishing those safety mechanisms, devices and circuits which are required under LC 27.

4) Typical examples of safety systems which may be

provided for the functions described above include, for power reactors:

- i) protection system;
- ii) shutdown system;
- iii) residual heat removal system;
- iv) emergency core cooling system;
- v) emergency power supply;
- vi) containment systems.

5) For chemical processing plant, and other nuclear facilities such as irradiated fuel storage, waste storage etc., safety systems include:

- i) protection system;
- ii) heat removal system;
- iii) ventilation / containment control;
- iv) emergency power supply;
- v) interlock systems.

6) The required safety functions must be capable of being achieved over progressing timescales, depending on the transient being considered and the initial plant status. This may therefore lead to a number of separate safety systems being provided, each of which has a specific input to terminating the fault. The systems listed above are only provided for guidance.

4.2 Single failure analysis

1) To show that the implementation of a safety function meets Principle P78 the safety case should include an analysis which addresses the following:

i) A fault schedule (required by P26), which, for each initiating design basis fault (as defined in P22), defines the safety functions required to terminate that fault sequence. External and internal hazards should also be considered as initiating faults (P122).

ii) A listing of the group(s) of safety systems which are provided to achieve each of the safety function(s) defined above in (i). These may comprise one or more systems, each of which is required to operate. Note that **each** of these 'systems' comprises all components that are necessary to achieve the safety function, including sensors, signal processing elements, actuators, and any supplies and services that are not fail-safe.

iii) The identification of the component failure modes which need to be considered within each system (or group of systems). Each component of the system, whether active or passive (see definitions), should be failed in turn and the system checked to ensure that it can still satisfy the required safety duty performance, and the safety function can be achieved. All modes of failure should be considered, for example, electrical short circuit, pipe burst, pipe blockage, valve mal-operation, etc.

iv) The potential for any component failure considered under (iii) above to cause consequential failures in other components of that system, or in any other system, by any means. Such failures and their consequences should be considered as part of the single component failure.

v) A demonstration that any non-safety systems (e.g. non-essential electrical supplies), which are permitted by principles 193 and 195 to be supplied via a safety system do not affect the capability of the system to meet the SFC, thus jeopardising

that safety system.

vi) The identification of any proposed maintenance or test procedures, including periods of overhaul and repair following breakdown or fault which would require a safety system (or part thereof) to be placed in a condition where it cannot perform its safety duty. The SFC should then be applied to this plant state to confirm whether the safety function can still be achieved.

vii) Demonstration that the reliabilities of redundant systems or components are broadly similar.

4.3 Exceptions

1) Where the analysis in **Section 4.2** shows that single failure in a safety system would prevent a safety function from being achieved and it is not reasonably practicable to provide further redundancy, a reasoned case should be provided by the licensee or the licence applicant for consideration. The following two conditions should be met in each case:-

i) the component cannot be caused to fail by the initiating event it is required to protect against;

ii) the reliability of the non redundant component under the relevant conditions can meet the safety requirement;

2) Additionally, other relevant factors to be addressed may include:

i) the severity of the consequences of failure to achieve the safety function;

ii) the ability of operators to recover from the failure in an adequate timescale;

iii) extremely high quality of a component in

relation to its duty;

iv) the time for which reliance is placed on the single component is short (e.g. up to one hour), and the PSA shows that the consequential risk is tolerable; and

v) whether or not the single component is active or passive - passive components generally being easier to justify.

4.4 Maintenance and testing

1) Where the analysis in **Paragraph 4.2 1) vi)** shows that the SFC cannot be met, the operating rules (or technical specifications) should require the plant to be shutdown or otherwise rendered in a safe state. Exceptions should not be permitted except where the following conditions are all met:-:

i) the outage time allowed by the operating rules / instructions is restricted both in terms of total time for the outage and the number of outages permitted in any fixed period;

ii) concurrent outages in other safety systems or trains do not affect the capability of the safety function to be achieved, or increase the probability of demand on the safety system; and

iii) a reliability analysis shows that the required average reliability of the system is attained, and the unreliability of performing the function is not excessive during the outage.

4.5 Application to rare events

1) The SAPs allow faults internal to the plant which have an expected frequency lower than about 10^{-5} per year to be excluded from the design basis (P21). Also, fault sequences with very low expected frequencies, typically 10^{-6} to 10^{-7} per year, need not be included (P22). This

does not imply that such faults, or fault sequences, should not be considered in the design. Instead, they should be treated on a case by case basis, with particular attention being given to their potential consequences. Allowance may then be made for the possibility that plant required to terminate the event or sequence may not need to be full "safety system" standards, on the basis that the lower the potential consequences the lower the standard that may be permitted. It therefore follows that whilst the application of the SFC should be considered for such cases, the criteria for exceptions (**Section 4.3**) may be further relaxed. For a more detailed review of these aspects see also **Ref 9** (T/AST/003), and in particular para 6.2 (4) and Appendix 1 of that guide.

4.6 Application to existing plant

1) The revised SFC is less restrictive than the earlier version. It therefore follows that for plant already assessed as satisfactory against the previous criterion, the assessment against the new criterion, P78, should be straightforward, and such plant should show compliance. In cases where a proposal is made to reduce the level of redundant systems, an in-depth analysis is still required, which addresses all the points described in **paragraphs 4.1 (6) to 4.4**.

2) For earlier plant not meeting the previous assessment standard, it is expected that compliance with P78 will also be easier to demonstrate. The same procedure (i.e. **paragraphs 4.1 (6) to 4.4**) should be followed, with particular attention being paid to the following:

- i) potential ageing effects reducing the reliability of active, and passive components;
- ii) system interactions between redundant safety trains (e.g. a single support feature such as essential electrical supply feeding two redundant trains);
- iii) test and maintenance procedures which may reduce the level of redundancy to a potentially unacceptable level.

Appendix 1. Extracts from 1979 issue of NII Safety Assessment Principles

A1.1 Principle No 31

The plant should be designed and operated in such a manner that no single failure should lead to a radioactive release or the occurrence of any direct radiation in excess of the requirements of principles 13 to 17. Where necessary, appropriate and adequate protection should be shown to be provided for the purpose of achieving this objective.

A1.2 Principle No 112

No single failure within the protection system should prevent any protective action achieving its required performance in the presence of any specified fault or external hazard initiating a demand on the protection system.

References

1. Safety Assessment Principles for Nuclear Plants (HSE 1992)
2. Safety Assessment Principles for Nuclear Power Reactors (HSE 1979)
3. Assessment Guide AG1 - November 1984 Draft
4. Code on the Safety of Nuclear Power Plants: Design (IAEA Safety Series 50-C-D Rev 1 pages 19-20)
5. Application of the Single Failure Criterion (IAEA Safety Series No 50-P-1, 1990)
6. IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems.
7. The Practical Application of Safety Principles to the Design of Safety Systems for NPPs (Report for EC Nuclear Regulator's WG, October 1992).
8. Safety Functions and Component Classification for BWR, PWR and PTR - IAEA 50-SG-D1 (1979).

9. T/AST/003 - Safety Systems.