Safety Series No. 50-P-1

Application of the Single Failure Criterion

A PUBLICATION
WITHIN THE NUSS PROGRAMME

INTERNATIONAL ATOMIC ENERGY AGENCY, VIENNA, 1990
CATEGORIES IN THE IAEA SAFETY SERIES

A new hierarchical categorization scheme has been introduced, according to which the publications in the IAEA Safety Series are grouped as follows:

**Safety Fundamentals** (silver cover)

Basic objectives, concepts and principles to ensure safety.

**Safety Standards** (red cover)

Basic requirements which must be satisfied to ensure safety for particular activities or application areas.

**Safety Guides** (green cover)

Recommendations, on the basis of international experience, relating to the fulfilment of basic requirements.

**Safety Practices** (blue cover)

Practical examples and detailed methods which can be used for the application of Safety Standards or Safety Guides.

Safety Fundamentals and Safety Standards are issued with the approval of the IAEA Board of Governors; Safety Guides and Safety Practices are issued under the authority of the Director General of the IAEA.

An additional category, **Safety Reports** (purple cover), comprises independent reports of expert groups on safety matters, including the development of new principles, advanced concepts and major issues and events. These reports are issued under the authority of the Director General of the IAEA.

There are other publications of the IAEA which also contain information important to safety, in particular in the Proceedings Series (papers presented at symposia and conferences), the Technical Reports Series (emphasis on technological aspects) and the IAEA-TECDOC Series (information usually in a preliminary form).
APPLICATION OF THE
SINGLE FAILURE CRITERION
The following States are Members of the International Atomic Energy Agency:

<table>
<thead>
<tr>
<th>Afghanistan</th>
<th>Haiti</th>
<th>Paraguay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Albania</td>
<td>Holy See</td>
<td>Peru</td>
</tr>
<tr>
<td>Algeria</td>
<td>Hungary</td>
<td>Philippines</td>
</tr>
<tr>
<td>Argentina</td>
<td>Iceland</td>
<td>Poland</td>
</tr>
<tr>
<td>Australia</td>
<td>India</td>
<td>Portugal</td>
</tr>
<tr>
<td>Austria</td>
<td>Indonesia</td>
<td>Qatar</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>Iran, Islamic Republic of</td>
<td>Romania</td>
</tr>
<tr>
<td>Belgium</td>
<td>Iraq</td>
<td>Saudi Arabia</td>
</tr>
<tr>
<td>Bolivia</td>
<td>Ireland</td>
<td>Senegal</td>
</tr>
<tr>
<td>Brazil</td>
<td>Israel</td>
<td>Sierra Leone</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>Italy</td>
<td>Singapore</td>
</tr>
<tr>
<td>Byelorussian Soviet Socialist Republic</td>
<td>Jamaica</td>
<td>South Africa</td>
</tr>
<tr>
<td>Cameroon</td>
<td>Jordan</td>
<td>Sri Lanka</td>
</tr>
<tr>
<td>Canada</td>
<td>Kenya</td>
<td>Sudan</td>
</tr>
<tr>
<td>Chile</td>
<td>Korea, Republic of</td>
<td>Sweden</td>
</tr>
<tr>
<td>China</td>
<td>Kuwait</td>
<td>Switzerland</td>
</tr>
<tr>
<td>Colombia</td>
<td>Lebanon</td>
<td>Syrian Arab Republic</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>Liberia</td>
<td>Thailand</td>
</tr>
<tr>
<td>Cote d'Ivoire</td>
<td>Libyan Arab Jamahiriya</td>
<td>Tunisia</td>
</tr>
<tr>
<td>Cuba</td>
<td>Liechtenstein</td>
<td>Turkey</td>
</tr>
<tr>
<td>Cyprus</td>
<td>Luxembourg</td>
<td>Uganda</td>
</tr>
<tr>
<td>Czechoslovakia</td>
<td>Madagascar</td>
<td>Ukrainian Soviet Socialist Republic</td>
</tr>
<tr>
<td>Democratic Kampuchea</td>
<td>Malaysia</td>
<td>Republic</td>
</tr>
<tr>
<td>Democratic People's Republic of Korea</td>
<td>Mali</td>
<td>Union of Soviet Socialist Republics</td>
</tr>
<tr>
<td>Denmark</td>
<td>Mexico</td>
<td>United Arab Emirates</td>
</tr>
<tr>
<td>Dominican Republic</td>
<td>Monaco</td>
<td>United Kingdom of Great Britain and Northern Ireland</td>
</tr>
<tr>
<td>Ecuador</td>
<td>Mongolia</td>
<td>Britain and Northern Ireland</td>
</tr>
<tr>
<td>Egypt</td>
<td>Morocco</td>
<td>Ireland</td>
</tr>
<tr>
<td>El Salvador</td>
<td>Myanmar</td>
<td>United Republic of</td>
</tr>
<tr>
<td>Ethiopia</td>
<td>Namibia</td>
<td>Tanzania</td>
</tr>
<tr>
<td>Finland</td>
<td>Netherlands</td>
<td>United States of America</td>
</tr>
<tr>
<td>France</td>
<td>New Zealand</td>
<td>Uruguay</td>
</tr>
<tr>
<td>Gabon</td>
<td>Nicaragua</td>
<td>Venezuela</td>
</tr>
<tr>
<td>German Democratic Republic</td>
<td>Niger</td>
<td>Viet Nam</td>
</tr>
<tr>
<td>Germany, Federal Republic of</td>
<td>Nigeria</td>
<td>Yugoslavia</td>
</tr>
<tr>
<td>Ghana</td>
<td>Norway</td>
<td>Zambia</td>
</tr>
<tr>
<td>Greece</td>
<td>Pakistan</td>
<td>Zimbabwe</td>
</tr>
</tbody>
</table>
| Guatemala   | Panama | }

The Agency’s Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is “to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world”.

© IAEA, 1990

Permission to reproduce or translate the information contained in this publication may be obtained by writing to the International Atomic Energy Agency, Wagramerstrasse 5, P.O. Box 100, A-1400 Vienna, Austria.

Printed by the IAEA in Austria
September 1990
APPLICATION OF THE SINGLE FAILURE CRITERION

A Safety Practice

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 1990
APPLICATION OF THE SINGLE FAILURE CRITERION
IAEA, VIENNA, 1990
STI/PUB/819
ISBN 92-0-123790-1
ISSN 0074-1892
FOREWORD

In 1974 the IAEA established a special Nuclear Safety Standards (NUSS) programme under which 5 Codes and 55 Safety Guides have been produced in the areas of Governmental Organization, Siting, Design, Operation and Quality Assurance. The NUSS Codes and Guides are a collection of basic and derived requirements for the safety of nuclear power plants with thermal neutron reactors. They have been developed in a complex process which ensures the best possible international consensus.

This broad consensus is one of the reasons for a relatively general wording of the main principles and is sometimes a cause of problems in their application to the detailed design of nuclear power plants. The requirements, particularly those of the Codes, often need interpretation when applied to actual cases. In many areas national regulations and technical standards are available, but often even these do not answer all questions and only the practice used in applying certain rules fully reflects the outcome of the detailed consideration given to solving individual cases.

In order to present further details on the application and interpretation and on the limitations of individual concepts in the NUSS Codes and Safety Guides, a series of Safety Practice publications have been initiated. It is hoped that many Member States will be able to benefit from the experience presented in these books.

The present publication will be useful not only to regulators but also to designers and could be particularly helpful in the interpretation of cases which fall on the borderline between the two areas. It should assist in clarifying, by way of examples, many of the concepts and implementation methods. It also describes some of the limitations involved. The book addresses a specialized topic and it is recommended that it be used together with the other books in the Safety Series.
## CONTENTS

1. INTRODUCTION ................................................................. 1
   1.1. Background .............................................................. 1
   1.2. Objective ............................................................... 1
   1.3. Scope ................................................................. 1
   1.4. Structure .............................................................. 2

2. OVERVIEW OF RELATIONSHIP BETWEEN THE SINGLE FAILURE CRITERION AND RELIABILITY ........................................... 2
   2.1. Design for safety reliability ........................................... 2
   2.2. Failure types ......................................................... 3
   2.3. Single failure criterion ............................................... 4
   2.4. Testability ........................................................... 4
   2.5. Limitations of single failure criterion ............................. 5

3. APPLICATION OF THE SINGLE FAILURE CRITERION ............... 6
   3.1. Random failure considerations ....................................... 6
   3.2. System and component reliability with regard to random failures .. 13
   3.3. ‘Fail-safe’ design .................................................. 17
   3.4. Auxiliary services ................................................... 18

4. IN-SERVICE MAINTENANCE AND TESTING ............................. 18
   4.1. Equipment outage times ............................................... 18
   4.2. Test strategy ........................................................ 22
   4.3. Additional failure assumptions ...................................... 24

5. CONSEQUENTIAL FAILURES .................................................. 26

6. COMMON CAUSE FAILURES .................................................. 27
   6.1. General .............................................................. 27
   6.2. Common failure causes .............................................. 29
   6.3. Defence against common cause failures ............................. 31

7. EXEMPTIONS TO THE SINGLE FAILURE CRITERION ............... 36

8. SINGLE FAILURE ANALYSIS .............................................. 37
   8.1. General considerations ............................................... 37
   8.2. Objectives of the analysis .......................................... 37
1. INTRODUCTION

1.1. BACKGROUND

The IAEA Nuclear Safety Standards (NUSS) Code on Safety in Nuclear Power Plants: Design (Safety Series No. 50-C-D (Rev. 1), hereinafter called the Design Code), requires compliance with the single failure criterion in the event of any postulated initiating event (PIE) occurring at a plant (see paras 328–335 of the Code). The Design Code does not give the details of the interpretation of the criterion, in particular not for non-trivial applications. In the hierarchy of the IAEA Safety Series publications, the next level of detail after the Codes is represented by the Safety Guides. Since the single failure criterion is applicable to many systems in a nuclear power plant, the Safety Guides again cannot provide generic guidance on the application of the criterion.

In this situation, the present Safety Practice publication forms a synthesis of the various aspects of the application of the criterion to the typical reactor types in commercial use. It is intentionally placed at the hierarchical level of Safety Practices, which are intended to give practical examples of the implementation of certain safety requirements and for which the application of the content is not obligatory.

In most countries the application of the single failure criterion is not codified but a certain practice has developed which in fact varies little from country to country.

1.2. OBJECTIVE

The purpose of this publication is to provide interpretation of the single failure criterion in its practical application to the safety design of nuclear power plants.

1.3. SCOPE

During the development of this publication the actual practice of all countries with major reactor programmes has been taken into account. An interpretation of the relevant text of the Design Code is given in the light of these national practices.

The criterion is put into perspective with the general reliability requirements in which it is also embedded in the Design Code. Its relation to common cause and other multiple failure cases and also to the temporary disengagement of components in systems important to safety is clarified. Its use and its limitations are thus explained in the context of reliability targets for systems performance. The guidance provided applies to all reactor systems and would be applicable even to systems not
in nuclear power plants. But since this publication was developed to give an interpretation of a specific requirement of the Design Code, the broader applicability is not explicitly claimed. The Design Code lists three cases for which compliance with the criterion may not be justified. The present publication assists in the more precise and practical identification of those cases.

1.4. STRUCTURE

Section 2 of this publication deals with the purpose of the single failure criterion with respect to the safety of a nuclear power plant. It also shows where the criterion has its limitations.

The third section explains the difference between active and passive types of failure and the consequences of the failure characteristics for the application of the criterion. Examples are given of simple and more sophisticated component redundancy arrangements in a fluid system. The possibility of fail-safe designs and the role of auxiliary systems are also dealt with.

The following section, which is supported by an extensive appendix on various methods to determine allowable outage times for redundant components, treats the important case of the reduction of redundancy during in-service maintenance and repair actions in operating nuclear power plants. Different maintenance strategies are discussed.

Section 5 then considers that part of the definition of the single failure criterion which states that consequential effects of a single failure are to be considered as part of the failure.

Section 6 provides an introduction to the problem of common cause failures. While the single failure criterion may be satisfied by redundancy of identical components, the common cause failure of such components would nullify this redundancy.

Exemptions from the application of the criterion are related to failure occurrence probability in Section 7.

The methodology and the individual steps involved in a single failure analysis (SFA) are explained in the last section. A short commentary on the complementary use of probabilistic safety assessment (PSA) methods is also given.

2. OVERVIEW OF RELATIONSHIP BETWEEN THE SINGLE FAILURE CRITERION AND RELIABILITY

2.1. DESIGN FOR SAFETY RELIABILITY

The design of a nuclear power plant must be capable of coping with all identified postulated initiating events (PIEs) by ensuring that the required safety functions
can be accomplished with acceptable reliability for each PIE. A discussion on PIEs can be found in an appendix to the Design Code.

To achieve a high degree of confidence that the safety functions, if required, will be performed according to design intent, a number of measures are specified in the Design Code. Ensuring and maintaining adequate reliability of each safety function and of the systems and components provided to carry it out entail that three requirements be satisfied for the systems required to deal with a PIE:

(a) Maintaining the independence of these systems from the effects of the PIE;
(b) Minimizing the probability of failure of the components of these systems by adopting high quality standards and engineering practices for design, construction, operation and maintenance;
(c) Designing these systems to be tolerant to failures without loss of safety functions.

2.2. FAILURE TYPES

With respect to requirement 2.1(c), the types of failures that must be taken into account in the design of systems performing essential functions include random failures and common cause failures.

2.2.1. Random failures

A random failure is a failure whose occurrence is statistically independent of that of failures of other devices of the same type. Statistical variations in the material, the manufacturing process, the operating conditions or the maintenance and testing procedures may cause one device to behave in a different way from that of other devices of the same type. The cause of the random failure is not known prior to its occurrence.\(^1\)

2.2.2. Common cause failures

A common cause failure is the failure of a number of devices or components to perform their functions as a result of a single specific event or cause. The event or cause may be a design deficiency, a manufacturing deficiency, an operating or

---

\(1\) This definition of random failure has been phrased for specific use in the NUSS publications to highlight the characteristics that make it possible to distinguish random failures from common cause failures. The terminology used may be different from that employed in classical reliability theory.
maintenance error, a natural phenomenon, a man induced event, saturation of signals, a change in ambient conditions, or an unintended cascading effect from any other operation or failure within the plant. A common cause failure can, therefore, also be the failure of redundant components or devices intended to perform the same safety function. Principles for reducing the probability of common cause failures are discussed in Section 6.

2.3. SINGLE FAILURE CRITERION

To determine the degree of system or component redundancy, to ensure adequate reliability of the safety functions, the Design Code has introduced the single failure criterion. This is a deterministic criterion which specifies a simple design approach to obtaining a certain minimal redundancy of a system or of a group of items of equipment. It is based on the general experience that even components and equipment that are made to high standards of quality may sometimes fail to function, in a way and at a time that is random and unpredictable. The requirements making up the single failure criterion are given in paras 329–336 of the Code.

2.4. TESTABILITY

Implicit in the application of the single failure criterion is the requirement for testability of the systems and components to which this criterion is applied, since, otherwise, undetected failures would have to be taken into account in addition (see para. 323 of the Design Code and Section 4.3 of this publication).

The means of achieving this requirement depend on whether the failure is classified as active or passive. In practice, active failures are usually detected by the use of on-line testing and monitoring systems and procedures. The plant system configuration may have to be changed to make it suitable for the specific nature of the test and monitoring process.

In many cases the performance of these on-line tests requires a change from the normal configuration of the safety group\(^2\) involved. Practice has shown that the actions involved in changing from the normal configuration, performing the test and restoring the normal configuration add significant risks of human error. Special attention should be given to information systems, written procedures and training to reduce these risks.

Testing of passive components is usually performed by in-service or periodic inspection methods. These methods usually require that the plant be placed in a special shutdown mode and in some cases major components, such as reactor vessel internals, are removed to perform the inspection.

\(^2\) See definition on p. 8 of the Design Code.
2.5. LIMITATIONS OF SINGLE FAILURE CRITERION

The single failure criterion provides a simple and effective method that assists in the determination of the redundancy of systems or of components within a system so as to ensure the minimum required reliability of the safety functions. It should, however, be recognized that too literal an application of the criterion based on simple redundancy of safety features may not be appropriate in all cases.

The reliability of the safety functions should be commensurate with the expected frequency of occurrence of the PIEs whose effects they are called upon to prevent or mitigate. The higher the frequency of a certain PIE the more reliable should be the features which are provided to prevent the plant from reaching an unacceptable state. For PIEs with a relatively high frequency, a degree of system or component redundancy higher than that required by the single failure criterion may be needed. The opposite situation may also occur: for PIEs which are estimated to occur with an extremely low frequency, the reliability of the safety group may not need to be so high and even the simple redundancy required by the single failure criterion may become unnecessary. Such cases are indicated in para. 335 of the Design Code.

The decision process is aided by supplementing the single failure criterion with probabilistic evaluations to determine if there is a need for a higher degree of redundancy than that required by the criterion or to justify exemptions from meeting the criterion. Supplementary probabilistic evaluations can be either qualitative, based on estimated ranges of component failure probabilities, or quantitative, based on a detailed analysis of system unavailability. In some Member States, maximum unavailability limits for certain systems are established to ensure the reliability of the safety functions. The reliability of each safety function can also be confirmed by an overall probabilistic safety assessment (PSA).

Another aspect to be considered is the fact that the single failure criterion is only capable of dealing with random failures. Redundancy, which is the ultimate outcome of the application of the single failure criterion, may be defeated by common cause failures which are engendered by dependencies between components or systems. Guidance on a complete common cause failure analysis is outside the scope of this publication. However, to deal with common cause failures, other measures additional to the provision of redundancy must be taken, as explained in Section 6. Common cause failure analysis must also be carried out either to ascertain that the potential for common cause failures is sufficiently low or to determine appropriate means to cope with their effects.

Practices relating to the application of the criterion to undetectable failures are described in Section 4.
3. APPLICATION OF THE SINGLE FAILURE CRITERION

3.1. RANDOM FAILURE CONSIDERATIONS

A single failure is represented by a random failure and its consequential effects. Failures that occur as a result of a PIE are a part of the PIE and are additional to the assumption of the single failure.

The idea of a random failure can be applied to active as well as to passive devices, e.g. pipes, pumps, tanks, valves, wires, transistors, switches, motors, relays or solenoids. On the basis of the definitions of active and passive components used in various countries it is obvious that a tank is always considered a passive component. However, if mechanical movement is considered as the only defining feature, it is not obvious that a transistor or a solenoid are to be considered active. The definitions used in the NUSS programme (see pp. 4 and 7 of the Design Code) for active and passive components are broad but still leave some examples open to interpretation and therefore need further clarification.

A few examples may illustrate different types of random failures:

— An open circuit can be caused when a poor soldering point opens as a result of chemical (corrosion) or mechanical conditions (e.g. vibration);
— An intended switching process can be prevented when a relay sticks owing to reactions at the contact surfaces (e.g. adhesive corrosion);
— A pump may be hindered from running as a result of a blockage by a screwdriver that was inadvertently left in the fluid system after previous repair work.

The failure is arbitrarily assumed and is in principle applied to every safety related system or component with the exception of cases when as a result of extraordinary design and quality standards a failure is deemed not to be credible. According to the single failure criterion (paras 329 and 330 of the Design Code), a single random failure shall be assumed for each safety group incorporated in the plant design. Here, 'safety group' means that assembly of equipment which performs all actions required for a particular PIE in order that the limits specified in the design basis for that event are not exceeded. This implies that a single random failure is assumed not only in the front line safety system (safety actuation system) but also in the associated protection system and safety system support features, it being understood, however, that at no time during the single failure analysis is more than one random failure assumed to exist.

In principle, the application of the single failure criterion to individual safety systems, including associated protection system and safety system support features, is similar in all Member States. An example of a specific application is given in Sec-
tion 3.2.1 of ANSI/ANS-51.1 and ANSI/ANS-52.1. The relevant safety functions which require the application of the single failure criterion are:

— reactor shutdown
— emergency core cooling
— residual heat removal, and
— active containment.

Differences can be identified in the application of the criterion, especially for those functions which are required to be carried out in the long term after a design basis accident, e.g. containment hydrogen management (the NUSS Safety Guide No. 50-SG-D12 states that a single failure need not be postulated in the application of active measures if repair or substitute measures can be shown to be practical for hydrogen management).

3.1.1. Credibility of random failures

The concept adopted in the guidelines and practices of Member States, even if not explicitly stated in all relevant regulatory documents, does not require that every conceivable failure has to be assumed to occur in the application of the single failure criterion. Only credible failures are assumed. If the probability of a component failure is sufficiently small, as determined by reliability analysis, engineering judgement or other means, the failure may not need to be considered as credible.

The failure probability of many passive components during the period they are required to perform their safety function has been demonstrated to be sufficiently small as a result of stringent quality assurance during design and manufacture. Failures of those components need not be assumed in the application of the single failure criterion.

3.1.2. Passive failure

In the use of the single failure criterion, certain failures are defined as being passive. A passive failure in mechanical and fluid systems may be either the blockage of a flow path or failure of a component to maintain its structural integrity or stability so that it cannot provide its intended safety function. Examples of passive failures are:

— rupture of a pipeline or tank
— blockage of the containment sump by heat insulation material from the primary circuit.
Active components may also have passive failure modes that can prevent them from performing their intended function. Examples might be:

- rupture of the housing of a pump or a valve as a result of crack growth
- blockage of the flow path of a valve as a result of trash left in it during maintenance.

Electrical components also have failure modes that are passive in nature, such as short and open circuits in cables. In the application of the single failure criterion to power supplies or instrumentation and control sections of safety systems, no distinction between active and passive failure modes of components is made (see, for example, ANSI/ANS-51.1 and ANSI/ANS-52.1). Both active and passive single electrical failures must be considered.

Experience gained with operating nuclear power plants has shown that the likelihood of passive failures of mechanical components is generally much lower than that of active failures, especially when the passive components are designed, manufactured, tested and inspected (in-service) according to high quality standards (for example, ASME class 1). This fact is considered in the application of the single failure criterion to mechanical components in various national practices.

Typical passive failure rates are in the range of $10^{-8}$ to $10^{-7}$ per hour (figures derived mainly from safety related piping under continuous operation, i.e. the failure rate of welds and bends in piping with high quality design and fabrication, since they may be the only remaining weak points), while active failure rates range typically from $3 \times 10^{-6}$ to $3 \times 10^{-5}$ per hour.

To determine the maximum failure probability, the failure rate of a component must be multiplied by its test interval. (Further information with regard to unavailabilities and testing strategies is given in Section 4.) So if the test intervals are similar, the active failure modes dominate the system failure probability. If the required functioning time of the safety system is not long, for example less than one day, and the transient loads induced by putting a system into service are with sufficient margin part of the design basis for the system, the probabilities of passive failure modes are relatively low. Consequently, inadmissible plant damage states due to failures of such passive components are clearly of such low frequency that they are in the range of acceptable values. Therefore, from a probabilistic evaluation of the deterministic single failure criterion, passive failures of low probability may be reasonably discounted in the application of the criterion without substantially affecting overall systems reliability. To justify this procedure, extra high quality must be maintained during the whole service life of passive components. The possibility of ageing phenomena must be considered.

The approach adopted in Member States is reflected in the Design Code, which states that failure of a passive component designed, manufactured, inspected and maintained in service to an extremely high quality level need not be assumed in conducting the single failure analysis.
Certain passive failures could have severe effects on nuclear safety and result in more severe consequences than active failures. Examples are:

— Break of the pipeline from the containment sump to the ECCS pump. The entire water inventory for cooling the core might be lost during the recirculation phase of a LOCA in a PWR unless: (1) very high pipeline quality was maintained during its operational lifetime, allowing the pipe rupture to be considered as not credible, or (2) the pipe was installed inside another pipe (double pipe — in the event of rupture of the inner pipe the outer pipe serves as the pressure boundary) or (3) measures were provided to the operator to isolate the ruptured pipe section in time.

— Break of blowdown or relief pipe in a BWR. Such a failure would result in rapid overpressurization of the containment as a result of steam bypassing the suppression pool where it is condensed. The failure of these pipes must be made not credible by appropriate means.

Because of the severe consequences of such failures, a cautious attitude to their analysis is required. The use of PSA methodology in addition leads to a clear appreciation of the impact on safety in such cases. Failures with severe consequences must as a minimum be made very unlikely by appropriate quality conditions. If feasible, additional redundancy (e.g. the use of a double pipe) must be taken into account. To justify a passive failure being considered as incredible it must be demonstrated that the probability of the failure is extremely low by showing that the quality of the component is extremely high during its whole service lifetime. The high quality can be assumed if the requirements for the load spectrum, design, construction, choice of material, manufacture, testability, etc., and quality assurance programme of the component stipulated in the pertinent regulations are met. All these features are intended to ensure that the component is designed to cope with the maximum stresses anticipated during its operation with a sufficient safety margin and that this ability is preserved during service. Pressure vessels, water tanks and buildings are typical components for which the above considerations may be and are in fact applied.

The various national practices deal with most of the passive failures in a similar way. The single failure assumption is generally not applied to buildings, containment structures, support structures, large pipelines and the housings of pumps and valves or the reactor pressure vessel. Passive failure is normally restricted to a limited leak during the long term at flanges or pump and valve seals.

After some of the PIEs, e.g. a LOCA, the safety systems are required to function for an extended period of up to some months. During the long time period for which some systems are used after a PIE, possibly under additional adverse environmental conditions caused by the PIE (e.g. during the recirculation phase of a LOCA the pressure boundary of the ECCS must withstand the action of the coolant, which
probably contains radioactive substances and chemicals that may accelerate cor-
rosion), the likelihood of passive failures increases, being however, still smaller than
that of active failures. Therefore, passive failures are considered during the long
term unless they are also demonstrated to be of very low probability over such a
period. Failures that are discounted after appropriate justification are considered to
be incredible in terms of the application of the single failure criterion. Such cases
in which exceptions from the rule are assumed have to be clearly stipulated and justi-
fied in the safety analysis.

The above considerations have led to the definition of short term and long term
periods in the application of the single failure criterion to mechanical and fluid sys-
tems. The short term is commonly defined as that period of operation up to one day
following a PIE. In the design of the emergency core cooling and containment spray
systems, the short term is considered to be terminated after the system is transferred
from the injection to the recirculation mode. The long term is defined as that period
following the short term during which the system safety function is required. In the
application of the single failure criterion, a passive failure is not assumed during the
short term. During the long term a credible passive failure may be assumed.

The Design Code does not make use of the distinction between short term and
long term although this is a common practice in Member States. It states, however,
that if it is assumed that a passive component does not fail, such an approach shall
be justified for the total period of time after the PIE that the component is required.
For this purpose fatigue of such components (for example that due to temperature
cycling) during operation and specified in-service inspection needs to be considered.
Thus the total period of time that the components are required has an impact on the
assumptions to be made about their possible failures. The practice of many Member
States is to interpret this aspect of the single failure criterion in a balanced and
reasonable form.

3.1.3. Active failures

An active failure is a malfunction in the active part of a component. An active
failure in mechanical components could be due to:

- a failure of an item of equipment whose operation requires a mechanical move-
  ment by one of its components in order to carry out an operation on demand;
- an incomplete movement of an item of equipment with the consequence that
  the intended safety function is not fulfilled;
- a spurious action of a powered component originating within its instrumentation
  and control system (unless specific design features or operating restric-
  tions preclude such spurious action).

In some Member States, certain human errors are also considered as random
failures.
Examples of active failures are:

- failure of a pump or a fan to start;
- failure of a valve to reach its final position, i.e. an incomplete closure gives rise to a partial leak at the seating;
- unintended activation of a powered valve due to a faulty control signal;
- failure of a pump to function for a required period;
- in some Member States an activation at the wrong moment of an active component (for example, opening of a relief valve) by an operator if this activation is foreseen in the operating manual for this type of event, unless such activation is prevented by appropriate measures (e.g. interlocking). (Note: mistakes in the operating manual are not considered in the context of the single failure criterion but are considered as common cause failures.)

The probability of an active failure is normally too high for these failures to be considered as incredible. However, many Member States hold that the failure of an active component may be considered incredible if the proper active function of the component can be demonstrated in all credible situations and the component can be considered especially qualified for service.

The classification of components into active and passive is not always clear cut. For example, should the failure of the opening function of a simple swing type check valve be considered as an active or passive failure? In some Member States a failure of such a valve to open need not be considered as a single failure. In other Member States self-operating components (e.g. check valves) are considered to be active if the state of the component is changed during the given event sequence after a PIE. Therefore, opening or closing failures are considered to be active failures.

The reason for accepting that an opening failure of a simple non-powered valve need not to be considered as a single failure is that the failure probability is assumed to be very low, comparable with that of passive mechanical components, which generally are only assumed to fail in the long term. The failure rates for the opening function of check valves (mean value: $2 \times 10^{-7}$/h according to NUREG/CR-2815, PSA Procedures Guide), however, lie between the failure rates of active failures and those of passive failures (see Section 3.1.2).

To determine the maximum failure probability of the opening function of the check valve (which must be compared with the maximum failure probabilities of active or passive components), the test intervals have to be taken into account. On the assumption that the usual test intervals for active components are a few weeks, for passive components one to several years and for check valves about one year, the failure probability for the opening function of check valves is seen to be closer to the failure probabilities of active components than to those of passive components. Therefore, a careful examination of operating experience seems to be necessary before the opening failure of a special type of check valve is exempted from the
application of the single failure criterion. A conservative approach is to assume its failure to open in the single failure analysis.

The mean failure rate for the closing function of check valves is $2 \times 10^{-6}$/h. Consequently, a closing failure is considered to be an active failure. For instance, in the design of the isolation of BWR feedwater lines this aspect is taken into account by providing powered isolation valves in addition to the check valves. Thus, in the event of a feedwater line break outside the containment, isolation is possible by means of the powered valve despite the single failure of the check valve.

Pipe hangers are generally not considered to be active components although they change their state on demand, which in practice means that failures of pipe hangers could occur at most in the long term period after an accident. During this period, however, no extraordinary load conditions will occur, so that the failure is considered not credible in the context of the single failure criterion.

![Figure 1](image-url)

FIG. 1. Example of connections between injection system tank and pumps.
Electrical components include wires and cables, transistors, diodes, relays, batteries and motors. With regard to the single failure criterion, no distinction is made between active components such as diesels and passive components such as wires. A random failure is simply assumed on demand and dealt with like an active failure, i.e. it is assumed during either the short term or long term after an accident.

For powered components spurious action is considered and is regarded as an active failure. It is an unintended function of the component originating from a single failure within its instrumentation and control system. An example of a spurious action is the unintended energization of a powered valve to open or close. In the single failure analysis, the spurious action of a powered component may not need to be assumed if the spurious action is not credible (e.g. due to disconnection of the power supply from the component during operational states).

It is recommended that human failures be considered in the context of the single failure criterion as long as they can reasonably be restricted to a single incorrect or omitted action by an operator attempting to perform manipulations in accordance with prescriptions in the operator’s manual in response to an initiating event. It is impossible to take into account the manifold actions an operator could perform without being demanded. They must be taken care of by proper information displays, the provision of operating manuals and operator training.

3.2. SYSTEM AND COMPONENT RELIABILITY WITH REGARD TO RANDOM FAILURES

The basic measures used to achieve reliability for coping with random failures are:

- redundancy
- independence
- fail-safe design and
- appropriate auxiliary services.

3.2.1. Redundancy

A proper redundant design does not only require the redundancy of a few components but the fulfilment of the single failure criterion by the total system. The schematic examples below illustrate different system designs for identical safety functions with regard to the application of the single failure criterion. The figures

---

3 Guidance on the reliability of systems and the design measures outlined here can also be found in the Safety Guides 50-SG-D3, 50-SG-D4, 50-SG-D5, 50-SG-D6, 50-SG-D8, and 50-SG-D13.
An injection system with $2 \times 100\%$ pumps takes its coolant from one water storage tank. The possible connections between the tank and the pumps may be as shown in Fig. 1.

In the case of Fig. 1(a), the active failure of a valve to open leads to a failure of one train. The safety function of this system is still fulfilled. The same is true for Fig. 1(b). (If the throughput capacity of the pipe in the undisturbed leg is sufficiently high the total system still has a $2 \times 100\%$ capacity.) However, the failure of the suction pipe and tank outlet pipe must be made not credible by design, e.g. there must be low stress, minimum number of welds, etc.

In the case of Fig. 1(c), the powered valve must be in an open state under stand-by conditions. A closed valve which would not open as a result of an active failure would lead to a loss of the whole system. Furthermore, it must be ensured that spurious actions or erroneous operator actions which could lead to the closure of that valve are avoided.
A more complicated example with regard to a redundant design and the application of the single failure criterion is represented by the pneumatic pilot valves in a scram system of a BWR (Fig. 2).

The pilot valves are activated by the reactor protection system, which is built up in three trains (2 out of 3 logic). Train 1 controls valve 1, train 2 valves 2 and 3, and train 3 valve 4. This arrangement does not lead to a scram despite a spurious action in one train owing to the 2 out of 3 logic. It fulfils its function even when a single failure is assumed. During tests the arrangement is switched to a 1 out of 2 logic.

3.2.2. Independence

The reliability of systems can be improved by preventing the propagation of failures by applying the following principles for independence in design.

— Maintaining independence among redundant system components;
— Maintaining independence between system components and the effects of PIEs; for example, a PIE must not cause the failure or loss of a safety system or safety function that is required to mitigate that event;
— Maintaining appropriate independence among system components of different safety classes;
— Maintaining independence between items important to safety and those not important to safety.

Independence is achieved in the design of systems by using functional isolation and physical separation.

*Functional isolation* is used to reduce the likelihood of failure of connected systems resulting from normal or abnormal operation or failure of any component in the systems. Design provisions to prevent these interactions may include such devices as buffer amplifiers, optical isolators, cable shields and internal mechanical structures in the instrumentation and control systems, and isolation provisions at the interfaces of fluid systems.

*Physical separation* and proper layout of plant components can provide increased assurance that independence will be achieved, particularly in relation to certain common cause failures. The possibilities include:

— separation by geometry (distance, orientation, etc.)
— separation by barrier, and
— separation by a combination of the above.

The choices of means for separation will depend on the PIEs considered in the design basis, e.g. the effects of fires, chemical explosions, aircraft crashes, missiles, flooding, temperature, humidity, etc.
FIG. 3. Schematic diagram of DC emergency power supply.
Certain areas in the plant tend to be natural centres of convergence for equipment or wiring of various degrees of importance to safety. Examples of such centres are containment penetrations, motor control centres, cable spreading rooms, equipment rooms, control rooms and the plant process computers.

Physical separation of individual system trains aims mainly at prevention of the simultaneous failure of more than one train, for example as a result of unforeseen local conditions. So, as mentioned above, it is particularly effective for the prevention of certain common cause failures. Physical separation also helps to mitigate the consequences of events such as fires or internal flooding, which might be caused by a single initiating failure.

By functional isolation, the impact of a single failure in one train of a redundant system on another train of this system is avoided. Figure 3 shows an example of a redundant system with a good degree of functional isolation.

For the electrical emergency power supply of safety systems, loads are fed from two DC trains (batteries). If there is a single failure in one train of the DC power supply system, the power supply of the corresponding DC loads is ensured by the other train. A failure of two trains due to a single failure, for example a short circuit in one train which could cause an overload in the second, is prevented by adequate decoupling by diodes to ensure independence of the two trains. (With an appropriate number of trains the DC power supply system can deal not only with the single failure but also with a simultaneous outage for repair which is required in some countries.)

3.3. 'FAIL-SAFE' DESIGN

As a supplement to the basic requirements for selection and use of reliable equipment, it is a desirable feature of safety system design that the more probable modes of failure should increase the probability of a safe condition. It should, however, be recognized that a failure considered to be in the safe direction for a particular mode of plant operation may turn out to be less safe in some other mode of operation. Consideration should be given to making use of predictably 'fail-safe' features of safety system component failure modes, or to incorporating in the reactor design such features as natural circulation shutdown cooling, or the use of gravity

---

4 'Fail-safe' is a term used by many Member States as a conventional abbreviation for the situations described in this text. The quotation marks identify the use of the term in this book with this qualified meaning. The term 'preferred mode of failure' is sometimes used instead. It should be noted that it is not possible to design equipment such that all its modes of failure would lead to a safe condition of the nuclear plant in the absence of deliberate action to ensure safety.
or stored energy (for example in pressurized gas) to move components of a safety actuation system. However, where such practice is applied, safety requirements must still be met if failure can occur in less probable but credible failure modes.

Where practicable, the principle of 'fail-safe' should be incorporated into the design of systems and components important to safety for the nuclear power plant, i.e. if a system or component should fail the plant would pass into a safe state without a requirement to initiate any actions.

In the example depicted in Fig. 2, the pneumatic pilot valve should be chosen such that in its unactivated condition it is in the scram mode. A failure in the power supply would thus be in the safe direction. Similarly, the hydraulic pilot valve would be of a normally closed type such that in the event of failure of the air supply the valve would close and scram the reactor.

3.4. AUXILIARY SERVICES

Auxiliary services necessary to maintain a safe state of the plant may include electricity, cooling water, compressed air or other gases, means of lubrication, etc. Auxiliary services that support equipment forming part of a system important to safety shall be regarded as part of the system important to safety and their reliability must be commensurate with the reliability of the system.

To achieve the required reliability, auxiliary services should also be designed with adequate redundancy and should incorporate features to prevent any malfunction from adversely affecting safety. If, for example, cooling of the independent divisions of a protection system is required and is provided only by a non-redundant air-conditioning system, any failure in the air-conditioning system could adversely affect the entire protection system. An appropriate level of reliability, achieved, for example, by using sufficient redundancy, is therefore necessary.

4. IN-SERVICE MAINTENANCE AND TESTING

4.1. EQUIPMENT OUTAGE TIMES

4.1.1. General

The design of systems and subsystems aims at certain reliability targets commensurate with the importance to safety which the system function has in the overall plant design. As required in the Design Code (para. 322), the design has to ensure
that structures, systems and components can be tested, maintained and possibly repaired while ensuring that the functional reliability stays within the intended limits.

In many cases the testing or maintenance of a component or system requires a change in the configuration. An example might be the maintenance of a pump for which the pump has to be isolated from its connecting piping, drained and possibly disassembled. During this operation part of the system is inoperable and the availability of its function is reduced. The Design Code requires that this temporary reduction in safety function availability due to outage be taken into account (para. 346).

A certain reduction of system availability may be acceptable. The remaining reliability of the system function decreases with the outage duration and this section considers ways to specify admissible time periods for such outages.

It should be noted, however, that there are cases in which the problem of reliability reduction during testing or maintenance operations can be avoided.

4.1.2. Possible measures to limit reliability reduction

The need to perform maintenance may be taken into account at the design stage while still fulfilling the single failure criterion in the following ways:

- Some systems can be maintained on line.
- In some systems equipment can be put out of service for a relatively long time without unacceptable consequences (e.g. the spent fuel pool cooling system) provided the time to repair the equipment and return it to service in this case is sufficiently short that subsequent loss of some of the remaining part of the system would not result in unacceptable consequences.
- The systems which are required in all the plant states (e.g. component cooling system) or which are inaccessible when the plant is operating but are in service when the plant is shut down (e.g. the residual heat removal system installed in the reactor building) may be designed with an increased redundancy or with a diverse system providing functional backup.

As regards tests, it may be acceptable in the case of LWRs, for example, to have sufficiently long intervals between the tests so that they can be implemented partly or totally when the plant is shut down and the system is not required to be available.

Another case concerns equipment and systems which can be tested without making them unavailable to meet their safety functions. This is true of electrical systems which can be tested on-line, of self-testing in electrical circuits, and of mechanical or electrical systems which automatically go back into operation, if required, following a PIE (an example is the reactor protection system where a channel is automatically put in a safe state during a test; an adequate safety level during the test is maintained but the probability of spurious actuations is increased).
4.1.3. Permissible outage times

In the context of the single failure criterion, the basic requirements concerning permissible maintenance, test and repair times should be considered. They can be summarized as follows:

(a) If during maintenance, test or repair work, the assumption of a single failure would lead to a failure of the safety features, these activities are only permissible within a relatively short period without special measures being taken (e.g., replacing the function or rendering its operability superfluous). In most cases the time involved in the maintenance, test or repair procedure is so short as to preclude any significant reduction of the reliability of the safety feature concerned. Various methods (including probabilistic) can be used to determine an admissible outage period.

(b) If the resultant reliability is such that the safety feature no longer meets the criteria used for design and operation, the nuclear power plant shall be shut down or otherwise placed in a safe state if the component temporarily out of service cannot be replaced or restored within a specified time (stated in the technical specifications).

(c) Maintenance procedures on safety features over a longer period, during which the component concerned is not operable, are only admissible without special measures if in addition to the maintenance a single failure can be assumed without preventing the safety feature from fulfilling its safety function or if another available system can adequately replace the impaired function.

(d) Even if the single failure criterion is fulfilled during the maintenance procedure, the time for this procedure should be reasonably limited.

(e) A PSA can be used to define the maintenance and repair times (time from the detection of the failure until the completion of the repair procedure), as well as the inspection concept. If this is done, the maintenance procedures should be defined so that they do not reduce the reliabilities of the safety features below the value required for the relevant PIEs and so that the probabilistic safety criteria, if established, are met.

Several methods can be used for the determination of permissible outage times. Important parameters are the degree of redundancy of the components or systems and the failure rate. The final goal is always the performance of a certain safety function, not primarily the availability of a particular component. The determination of the required degree of redundancy has to take this into account. It allows, therefore, not only for parallel trains of identical configuration but also for other systems which could perform the same function. On the other hand, the failure rate refers to the full length of the train, comprising also essential auxiliaries up to the point where they may branch off from a common part of the system (for example, the tank in Fig. 1(a)). Both qualitative and quantitative probabilistic methods may be used in the determination of the outage time. They may be limited to a reliability analysis of a
certain system in the configuration where a component or a full redundant train is taken out for maintenance. Such analysis may also take into account periodic testing by which the system is confirmed to be properly operable.

Other methods may take a broader perspective by including the likelihood of initiating events and plant operating conditions or even by relating the effect of component outages to an incremental increase of core melt probability by a quantitative PSA of the plant. All these methods have advantages and disadvantages in relation to the necessary effort they involve and the precision and completeness of the results. One feature is common to all of them. A judgement has to be passed regarding the acceptable reduction in system availability or increased potential core melt frequency or similar consequences.

The limitation of outage times (if no additional measures are taken) in connection with the application of the single failure criterion leads to slightly different procedures in different Member States.

Generally, the length of permissible outage times is required to be very short in the case of a two train system which would be reduced to a single operational train by the outage. A typical example of such a case is the maintenance or repair of a containment isolation flap. In this case a necessary repair must be started immediately after a deficiency has been discovered, the functionality of the other flaps must be checked and if the admissible repair time might be exceeded, measures must be taken which either replace the function of the flap (in particular closing the penetration concerned by another flap) or render its operability superfluous (e.g. shutdown of the plant or stopping fuel handling). Depending on the relevance of the system concerned and the national practice, the permissible outage times range from a few hours to a few days, with an average length of about one day, depending on which method is used (see Appendix).

For system outages which would result in a system with at least two redundant trains (including diverse systems) the permissible outage times without compensating measures can be longer, but are still limited. Such outage times may be in the range of weeks or months or even last until the following planned plant maintenance or refuelling shutdown.

The result of these considerations should be reflected in the technical specifications in terms of equipment outage times. All the methods described above must be considered as an aid to the elaboration of the technical specifications, which are in fact the results of discussions between the designer and the regulatory authorities. Other important considerations taken into account are, for example, the anticipated duration of maintenance, the feedback of experience and so on.

Taking into account the need for reliability of safety systems and the desire for high operational availability, some countries consider it necessary in ensuring plant safety to require, along with the single failure criterion, additional redundancy for some specified safety functions in order to be able to cope with both ongoing maintenance or repair work and a simultaneous single failure. This requirement leads to
an n + 2 degree of redundancy, for example 4 × 50% or 3 × 100% redundancy concepts. Another method used in many countries is to increase the redundancy of active components (e.g. pumps, valves) which require the most frequent maintenance. This leads in general to a 4 × 50% or a 4 × 100% redundancy concept for such components.

It should also be noted that some countries as a result of probabilistic considerations introduce further equipment in addition to the single failure criterion requirements. This increases the level of redundancy of some safety groups required to cope with the relevant PIEs.

The question of common cause failure must also be considered, as described in Section 6. The advantage of applying these concepts is not only a higher reliability of the safety systems but also a higher availability of the plant, because in the event of longer lasting repair activities additional measures such as power reduction or plant shutdown are not necessary. The choice between the possibilities is then also an economic matter; the investment costs must be compared with the anticipated savings connected with the improved availability of the plant.

4.2. TEST STRATEGY

The methods described above have shown that the reliability of a system is not only a matter of the degree of redundancy but also a matter of the test strategy. The maximum unavailability of a system decreases, for example, with decreasing length of the test interval. On the other hand, very short test intervals are unacceptable for practical reasons with regard to operation, total test outage times and possible adverse effects due to testing. Such adverse effects relate to wear and potential deterioration of components by the repeated testing. During testing the configuration of the system has often to be changed in order to isolate a component from the remainder of the system or to connect it to a test loop. After the test the original configuration of the system has to be restored. All these operations may give rise to errors (e.g. forgetting to open a closed valve or to unlock a bypassed alarm), especially if such tests are done routinely. Such errors may completely ruin the reliability of a system by making it inoperable. Thus optimal test intervals and procedures must be identified with regard to the operational possibilities and hazards.

Another aspect to be considered in the test strategy of redundant systems is staggered testing. With staggered testing, redundant trains are tested not all within a very short period of time but one after another at regular intervals. With this method all redundancies are tested once within the same period as with the unstag-gered testing scheme. The staggered testing scheme reduces the period of time that a common cause failure can exist before detection. This test procedure is especially important for the detection of common cause failures since it gives information more frequently on the behaviour of a ‘typical’ part of the total system.
Figures 4 and 5 show the unavailability of a 1 out of 2 system and a 2 out of 4 system as a function of $\lambda \tau$, i.e. the failure rate $\lambda$ of one train times the test interval $\tau$. The figures show clearly the increase of unavailability with increasing $\tau$. In Fig. 4, which represents the simultaneous test of all trains, the clear advantage of the 2 out of 4 arrangement in terms of lower unavailabilities can be seen. In Fig. 5, which is based on staggered testing of the trains, the difference between the two curves seems to have disappeared. The apparent increase of the unavailability is due to the different definition of the test interval $\tau^*$, the interval between two successive tests in the staggered procedure.

Although the advantage of a 2 out of 4 system seems to have disappeared, there is still an important difference in unavailabilities for low values of $\lambda \tau^*$. This range, however, is the essential range for practical applications since with $\lambda = 10^{-5}$/h and a monthly test interval ($\tau^* = 700$ h) the resulting $\lambda \tau^*$ equals about $7 \times 10^{-3}$. If the approximation which is inherent in the theoretical model is ignored, the 2 out of 4 system has some advantage even with this testing strategy.
The above discussions are based on a simplified procedure in which only independent events are considered in calculating the unavailability of redundant systems. However, the influence of dependent failures must be taken into account. The effects of and the possible countermeasures against these dependent failures are described in Section 6.

4.3. ADDITIONAL FAILURE ASSUMPTIONS

As explained above, systems important to safety must be tested and maintained in a reliable condition. In order to test systems or components successfully for the detection of potential faults they have to be designed appropriately.

A failure that does not cause an alarm or cannot be detected by specified tests shall be considered as undetectable and must therefore be assumed to exist at any time. The requirement is thus essentially equivalent with the one that systems shall be properly testable. The probability of such an undetected failure increases with
time and could be relatively high during the last years of the plant operation. Accord-
ingly, a system having an undetectable failure possibility cannot be considered to be as reliable as one without an undetectable failure possibility. Therefore, by a re-
design of the system or the test scheme, identifiable undetectable failure possibilities should be eliminated. If an identifiable undetectable failure possibility is not elimi-
nated, the failure must be assumed in addition to the single failure when applying the single failure criterion. According to some national regulations, identified undetectable failures may be shown to be not credible or to have a very low probabil-
ity of occurrence. This may be demonstrated by a rigorous analysis.

If identified undetectable failure possibilities remain, the designs can be characterized as follows:

— A simple $2 \times 100\%$ design (active and passive components) with identified undetectable failure does not fulfil the single failure criterion,
— $4 \times 50\%$ and $3 \times 100\%$ designs or designs using diverse redundant systems fulfil the single failure criterion with one identified undetectable failure that is not a common cause failure.

There are very few cases known where identified undetectable failures are not avoided in a plant so that this requirement serves essentially as pressure on the designer to ensure that no such failure types exist, i.e. to make the system fully testable. The principle may also be understood to call for the further development of those methods which may allow early failure detection (e.g. acoustic emission).

The term 'undetectable failure' or 'non-detectable failure' is also used in other documents, such as IEEE Std 379, IEEE Std 603 or RCC-E. For example, IEEE Std 603 requires that:

"The safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions which cause or are caused by the design basis event requiring the safety functions."

Another example of requirements which should be mentioned in this context exists in a national technical nuclear standard for the reactor protection system (KTA 3501). An unidentified ‘systematic failure’ (which may be a design error, a wrong set point or even a common cause failure) has to be assumed to occur in one of the two initiation channel groups (giving the initiation signals from two diverse physical process parameters) in addition to any single failure in the other channel group. This requirement was introduced because the reactor protection system is very complex and comprises a large variety of different components.

---

5 See Bibliography.
5. CONSEQUENTIAL FAILURES

Although some PIEs and single failures as well as consequential effects of PIEs and consequential effects of single failures may be similar or even identical, these events or event sequences have to be distinguished for a proper application of the single failure criterion. Similar events with similar immediate consequential effects are, for example, leaks in a pipe with a loss of coolant and the corresponding environmental effects. But a single failure with its consequences has to be considered on the basis of a plant configuration which is affected by the PIE. For example, the gross leak of an accumulator of the ECCS as a PIE leads to a loss of coolant within the containment and the environmental consequences have to be taken into account when considering the cooldown of the reactor. That same leak as a single failure after a medium size LOCA as PIE would lead to a reduction of the ECCS capacity in addition to the environmental consequences from the LOCA and leak.

Consequential failure effects of a single failure can be very different. Examples are:

(a) When during an event sequence a pump of the service water system or closed cooling water system fails, all equipment connected to this train of the service water system is expected to fail.

(b) The situation may be worse, if, for example, by a failure in one train in the service water system (e.g. a break of a line) a reactor transient is caused. If, in addition to the failure in the first train, a single failure is assumed in the second train of the service water system, then the effectiveness of the heat removal from components and systems important to safety has to be examined. In addition, the ability of such systems to work under increased temperature loads has to be checked.

(c) Power plants of older design, which in some exceptional cases have one diesel generator, would experience a station blackout if the diesel generator fails as a single failure following a loss of grid as a PIE. Thus an examination is necessary to determine if all relevant safety functions for this event sequence can be performed without AC power (e.g. residual heat removal via an emergency condensor of very large capacity).

(d) A consequential effect of a loss of a scram tank due to a single failure is a prolongation of the scram time. Consequently, it must be determined whether the prolonged scram time is still sufficiently short for coping with all relevant accidents.

(e) As a consequence of a single failure an aggravation of an event sequence is possible. If, for example, one of the pressurizer safety or relief valves of a PWR remains stuck open owing to a single failure, special operating modes (hot stand-by) are not possible.
Consequential environmental conditions caused by a single failure have to be considered, in particular if in the long term period single failures of passive components are taken into account. Not only could loss of coolant be a consequential effect but flooding of areas or an increase in humidity and temperature could also result.

6. COMMON CAUSE FAILURES

6.1. GENERAL

The established principles of the single failure criterion have been an important feature of nuclear power plant safety, but there are limits to the benefits of identical redundancy as the method of complying with this criterion. It can reasonably be argued, and operational experience supports the arguments, that complete independence of redundant items is practically unattainable, and therefore the safety benefits of redundancy of identical items are limited.

If total independence of the redundant components and the trains of a system is assumed, an arbitrary low failure probability of that system could be achieved by simply adding redundancies. This can be seen from the equation for the probability of failure of a system having \( n \times 100\% \) redundancy:

\[
P(\text{system failure}) = [P(\text{train failure})]^n
\]

The train failure probability is less than 1, so that as \( n \) increases, the system failure probability decreases. If the train failure probability is \( 10^{-2}/\text{demand} \), which is achievable in practice, and \( n = 4 \), the system failure probability according to the equation is \( 10^{-8}/\text{demand} \). The experience gained with engineering systems indicates that such a very low failure probability would be almost impossible to achieve in practice. Actual values tend to stay above \( 10^{-4}/\text{demand} \) irrespective of any increase in identical redundancies. The model underlying the equation is obviously too simple.

Dependence (coupling) exists between items because of their physical form (hardware) and because of external influences to which they are subjected during their lifetime. Both the physical form and the causal influences can be common to the redundant items so that a single influence can cause multiple failures and therefore limit the assumption of complete independence.

For identical redundant items there will be some degree of dependence and there are various methods available to minimize or optimize that degree. There will be limits to what can be achieved in practice and it might be necessary, depending
FIG. 6. Recognition of limitations.

on the system, the plant and the particular reliability requirements, to make a major change from identical redundancy to diversity and other measures effective against common cause failure. As previously indicated, common causes of failure are coupled to redundant items because of their common identical characteristics and the most effective way in which this can be avoided is to make them different (diverse).

The sequence for finding an acceptable solution to problems related to the application of the single failure criterion is as shown in Fig. 6.

There are three main categories of dependencies in relation to the single failure criterion and they usually have different degrees of significance in safety analysis:

(1) Dependencies between PIE and a system in the associated safety group
(2) Dependencies between systems in a safety group
(3) Dependencies between components within one system of a safety group.

Diversity is usually applied of necessity to defend against the first two categories, primarily because of the diverse functional or other requirements of the
various systems. Although the reliability requirements related to the third category will not be as stringent, there can still be a need to diversify components within a system.

6.2. COMMON FAILURE CAUSES

The possible common failure causes can be classified, for example, as shown in Fig. 7. Common cause failure data collected and analysed in various studies have clearly indicated that the problem is predominantly caused by errors and deficiencies in human performance. Design and maintenance have been shown to be the most significant contributions to common cause failures, with operation errors also being a problem of concern. Construction errors and environmental influences have, for most data samples, not made a significant contribution.

It is important to distinguish between different types of multiple failures with common causes. The different types are as follows (not considered here is a sequence of failures which are independent or whose dependence is not recognizable, e.g. operator errors after an accident or during accident management activities):

*Multiple failure due to human related cause.* A failure of more than one component that occurs as a result of a single specific cause, which may be a deficiency

![Classification of common cause failures.](image)
in design, manufacture, installation, operation or maintenance of the components or systems. Examples are the incorrect calibration of limit switches; sticking of reactor scram system relays due to the use of wrong coil insulation material that spreads on the contacts; and choice of the wrong material for pump bearings so that all similar redundant pumps fail to perform their required function.

*Multiple failures due to environmental effects.* Multiple failures of redundant items can be caused by tolerance limits of common environmental conditions being exceeded. Examples of such conditions are high vibration levels, high or low temperatures, high humidity, high radiation levels and corrosive atmospheres.

*Multiple failures due to an energetic event with widespread effects.* The failure of several components can be caused by events external or internal to the plant, such as an earthquake, airplane crash, fire or flooding. These events are capable of having an adverse effect on the proper operation of redundant (identical or diverse) components or systems necessary to ensure the safety functions, not only locally but also over a relatively large area. These events can also be defined as PIEs. Consequently, if the probability of occurrence of such events so justifies, they are taken into account at the design stage, and, if necessary, additional measures have to be implemented to protect the systems necessary to ensure the safety functions. Flood barriers and seismic qualification are examples of such measures.

It has been recognized that causes of dependent multiple failures do not always affect all of the redundant parallel trains of a system. Sometimes all are affected but not at the same time. The available data clearly indicate that some channels can survive for a considerable time a common cause that has affected other channels.

Generally, any human task that is carried out to a common specification, instruction or procedure will affect all items subject to it, for example, design specifications, drawings, test specifications and maintenance procedures. If errors exist in such documentation then failure of all items can be caused. This kind of dependence therefore represents the strongest possible coupling between redundant items and defence against such dependencies relies on quality only, with no diversity involved.

For many other causes the coupling is weaker and random. For example, a maintenance worker, although working to common correct procedures, might make a mistake on two channels, thus causing failures, but correctly perform the task on others. Similarly, different maintenance personnel working to the same procedures on identical items of equipment could cause some failures whilst other items will not be affected. However, more obscure strong coupling could exist in maintenance equipment used by one worker that would affect all channels that are worked on, or two or more workers could have received common training that would provide strong coupling causing all channels to fail. Common supervision could have similar effects.

Environmental effects could be similar to those of human errors in that multiple failures could be caused, but one or more channels could survive. For example,
a high temperature environment could cause two channels to fail, only weaken a third, but have no effect on a fourth, because of the applied defences.

6.3. DEFENCE AGAINST COMMON CAUSE FAILURES

The avoidance of common cause failures is of vital importance in the design and operation of systems important to safety. Therefore, everything practicable must be done to prevent them from occurring, or at least to minimize their frequency of occurrence and their effects on the systems. There should be a general awareness of common cause failure problems, their causes and the defence against them at each stage: design, manufacture, installation, commissioning, operation and maintenance. An overall defensive strategy against common cause failures is a valuable means of ensuring high reliability in systems important to safety.

In the defence against common cause failures, quality, segregation and diversity are of fundamental importance. There are two basic forms of preventing common cause failures in a system: either the causal influences on the system can be reduced, or the ability of the system to resist those influences can be increased. The reduction of causal influence can be related to all the classified causes of failure shown in Fig. 7 and the overall defensive strategy can be as shown in Fig. 8.

\[ \text{Defence} \]

\[ \text{Internal system resistance (hardware)} \]

\[ \begin{align*}
\text{Quality} & \\
\text{Diversity} & \\
\text{Segregation} & 
\end{align*} \]

\[ \text{External causal influence reduction} \]

\[ \begin{align*}
\text{Environment} & \\
\text{Human activities (software)} & \\
\end{align*} \]

\[ \begin{align*}
\text{Quality} & \\
\text{Diversity} & \\
\text{Quality} & \\
\text{Diversity} & 
\end{align*} \]

*FIG. 8. Common cause defence structure.*
6.3.1. Quality

High quality will generally increase the reliability of both individual items and complete systems. The various aspects of quality and quality assurance which have an influence particularly on the occurrence of common cause failures are discussed in the following paragraphs.

Quality assurance

Quality assurance provides discipline in the design, manufacture, installation, commissioning and operation of systems important to safety. It thus assists in minimizing common cause failures due to human errors and also in maintaining the designed reliability of the system. It ensures that components and materials of adequate quality are initially specified and that the environmental conditions to which the components are subjected are considered in the specification. It also ensures that valid inspections and tests are performed on the system during construction, commissioning and operation. The review of the system design prior to manufacture and installation may be part of a quality assurance programme for the design process. As a result of a thorough review of the system design, common cause failures and other weaknesses can be identified during the design stage.

Proven design and standardization

This method of defence utilizes operational experience. If proven standard components can be used they should be preferred over innovative designs, provided that it has been demonstrated that they are not prone to common cause failure under working conditions. Design changes and innovations may introduce common cause failure possibilities into the system. The systematic examination of previous failures could help in finding a design that is acceptably immune to common cause failures.

Environmental control

The environment within the boundary of the system should be controlled in such a way that the actual degree of adverse environmental conditions cannot serve as an origin of common cause failures. Whether the environments for redundant items are different, similar or identical, their nature must be identified. There are two general causal types:

- extremes of the normal environment, for example of temperature or humidity, or vibration or radiation levels
- energetic events such as plant fires or aircraft crashes.
Defence against environmental causes is not solely the responsibility of the designers; the plant operations and maintenance staff must also help to ensure the continued quality of the environment.

**Environmental qualification**

Qualification programmes must confirm that the equipment is capable, throughout its operational life, of performing safety functions while subject to the actual environmental conditions existing at the time of need. More detailed discussions of the principle and its application to various systems and components are presented in the following IAEA Safety Guides: 50-SG-D3, 50-SG-D8, 50-SG-D11, 50-SG-D12, 50-SG-D13 and 50-SG-D14.

The programmes must include administrative controls of design, manufacture, operation and maintenance activities.

**Fail-safe design**

A further means of reducing the consequences of failures is the principle of fail-safe design. This principle is stated in the Design Code as being necessary 'where practical' (para. 343). This technique is in many cases a well established defence against single failures and it is also relevant to common cause failures (see Section 3.3).

**Operational interfaces**

A frequent cause of failures is human action at interfaces with systems and equipment and their controls. The incorporation of specific design features to improve the man–machine interaction and thereby reduce the probability of human error is therefore important. Examples of specific design features are given in Safety Guides 50-SG-D3, 50-SG-D8 and 50-SG-D11.

Although most of these principles apply to the plant–operator interfaces, at least equal importance should be given to the maintenance interactions. Interlocks to prevent inadvertent action are another means of human error rate reduction.

**Operating and maintenance procedures**

Well prepared procedures are a defence against common cause failures in the operation and maintenance of a nuclear power plant. Procedures exercise direct and indirect influence on safety system performance and thus can cause common cause failures if not properly prepared. If operating personnel are provided with comprehensive, concise, unambiguous and detailed procedures and they submit to the discipline of these procedures, common cause failures due to human errors will be minimized.
A common cause failure in a reactor protection system preventing it from forming the actuation signal for the shutdown movement of the control rods as a result of an anticipated transient requiring reactor scram could result in severe plant damage. This kind of event, known as anticipated transient without scram (ATWS), needs special consideration which takes into account the national regulations. In most countries design provisions are made to keep the transient within acceptable bounds even if ATWS is not considered as a design basis event.

**Staff quality**

Complementary to the operational interfaces and procedures referred to above is the quality of human performance. Some of the attributes relevant to the reduction of human error rates are basic ability, training, experience and safety awareness. The latter should include awareness of common cause failure problems and the particular requirements for redundant systems design, construction, operation or maintenance.

The potential for human error is not solely associated with the lower echelons of the staff structure, but can also emanate from management and supervisory activities. Quality assurance is an essential requirement for all human activities in order to reduce error potential and increase the recovery possibilities following an error.

**Stress margins**

Any item or system must endure extrinsic environmental stresses and also intrinsic stresses imposed by its functional operation (fluid pressure, temperature, electrical voltage, mechanical load, etc.). Adequate margins should be allowed between applied stresses and the design strength of the item so that statistical variations cannot lead to failure.

6.3.2. **Segregation**

The main purpose of segregation is to provide and maintain independence between redundant components by locating them so that a common influence cannot cause failure of all of them. This is achieved by either spatial separation or protective barriers, or both. Such segregation may be between redundant items or between them and sources of potential environmental influences. Segregation might be regarded as a form of diverse location and environment. For example, cables and instrument racks of redundant protection system channels can be located in separated cable channels and rooms having independent ventilation and fire protection systems so that adverse environmental conditions within one train have no effect on equipment in other trains. Guidance relating to physical separation is given in Safety Guides 50-SG-D2, 50-SG-D3, 50-SG-D7 and 50-SG-D13. A special case of this principle
is the provision of a supplementary control point; guidance on this is given in Safety Guides 50-SG-D3 and 50-SG-D8.

6.3.3. Diversity

In addition to quality, there is a need for adequate diversity in human activities, environment and hardware. If designers, constructors, operators and maintenance personnel, and the environment in which the equipment operates, have something in common with each other, then common failures will definitely exist. If there is any diversity within the influences listed then the likelihood of common cause failures will be reduced.


Functional diversity is commonly applied in the protection systems which initiate safety actions related to such areas as pressurizer pressure, containment pressure or ECCS actuation. These require entirely different technologies and engineering in design, construction, operation and maintenance. Functional diversity is also employed for heat removal, through the use of an auxiliary feedwater system or reactor coolant injection system.

Equipment diversity implies the use of different kinds of components in redundant trains. The difference may originate, for example, from the manufacturing process, material selection or principles of operation. For example, relays from different manufacturers may be used in different channels of a protection system. Or relay techniques may be employed in one channel and semiconductors in another. An example of equipment diversity applied to the emergency feedwater system is the use of both motor driven and steam driven pumps.

Human diversity may be applied by using separate teams for the design, manufacture, operation and maintenance of redundant items. This procedure would limit the human error. It is very unlikely that all the teams would commit the same error.

Diversity could also be implemented through the use of auxiliary equipment associated with human activities or in the operational procedures used.

Another form of diversity used in some cases is limited time diversity of maintenance by way of staggered preventive maintenance and testing, with possible consequential diversity of staff as a result of shift working.
7. EXEMPTIONS TO THE SINGLE FAILURE CRITERION

According to para. 335 of the Design Code, non-compliance with the single failure criterion may be justified for:

— very rare PIEs,
— very improbable consequences of PIEs, or
— withdrawal from service for limited periods of certain components for purposes of maintenance, repair or periodic testing.

This statement is in line with the relation between the frequency limit for a plant damage state, the frequency of an initiating event and the reliability of all the systems that are provided for dealing with this initiating event (safety group). If the frequency of the initiating event is very near to or even below an established acceptable frequency limit for the unacceptable plant damage state (for example core melt) there is no need to have very reliable safety system(s) for such an event sequence. Therefore the single failure criterion does not need to be considered for very rare PIEs or very improbable consequences of PIEs.

For internal PIEs and external impacts having a very low probability of occurrence (such as certain aircraft crashes or explosion shock waves) or the coincidences of independent events each having a low probability of occurrence, there is no need to postulate either a simultaneous occurrence of a single failure or a simultaneous repair outage.

Very rare events are usually not considered to be design basis accidents. The design requirements therefore also differ. ANSI/ANS-51.1 and ANSI/ANS-52.1 present a value based on an optional probabilistic analysis approach, namely $10^{-6}$/reactor-year on a best estimate basis, which suggests the order of magnitude for the frequency of very rare events for which no single failure criterion compliance would be required. This is about the order of magnitude which seems to be internationally acceptable.

To decide whether, for example, an external impact can be considered as being a rare event, the following factors based on risk considerations must be taken into account:

— frequency of site dependent events, including possible impacts,
— overall design of the plant.

To generalize the above examples, in principle those events which do not belong to the design basis are considered to be rare. Because of the possibility of severe consequences, countermeasures have often been provided in order to cope even with some of these events. However, application of the single failure criterion to the systems for dealing with these events beyond the design basis is not normally required.
8. SINGLE FAILURE ANALYSIS

8.1. GENERAL CONSIDERATIONS

A single failure analysis (SFA) must be performed to assess compliance with the single failure criterion and associated requirements. An SFA must be performed as part of the total safety analysis of the plant and its design. As discussed in Section 2, the single failure criterion is one of several elements of the deterministic design process that is used to achieve adequate plant safety. Within the deterministic process reliability analyses may be used to demonstrate that certain postulated failures need not be considered in the application of the single failure criterion. A total plant PSA is an independent methodology for assessing plant safety. For compliance with the Design Code, a PSA cannot be used in place of an SFA. A PSA may be used to complement the SFA, particularly to cope with PIEs linked mainly to common cause failures.

8.2. OBJECTIVES OF THE ANALYSIS

In the analysis for ensuring that the safety functions of a nuclear power plant can be performed under all credible conditions which will be encountered in operation, single random failures of components and systems which are credible are considered. Concurrent random multiple failures generally do not need to be analysed as part of the deterministic process, because the reliability levels of the components and systems are kept so high as to render such concurrent multiple failures not credible. If performed, a PSA would assess such failures. The repair times may be adjusted (see Section 4) so that the repair of a single failed item or system is completed before another component or system can fail. Thus, at any stage of operation of the plant the existence of more than one failure is not assumed under the single failure criterion.

The Design Code therefore stipulates that a single failure shall be assumed to occur and analysis be performed sequentially, taking into account the failure of each element of an assembly and ensuring that the safety functions required can still be performed. This analysis is generally known as a failure modes and effects analysis. A single failure can affect the performance of a large part of the system in which it occurs or it may cause other consequential failures. Any such failure, including the consequential failures, has to be taken as a single failure for the purpose of the analysis, which has to continue until all assemblies and all credible failures have been considered.

The second requirement in SFA is to perform the analysis in a well balanced manner, keeping in mind the idea of credibility. Artificial combinations of events
without due regard to the likelihood of occurrence of the single failure in combination with a PIE should be avoided.

In brief, the objective should be to comply with the requirements of the Design Code and not to include events or combinations of events which have extremely low probabilities.

8.3. SINGLE FAILURE ANALYSIS PROCEDURE

The procedure for an SFA is as follows:

1. The relevant PIEs in the design basis which need the safety function to keep the plant safe have to be identified. The probabilities of occurrence of the PIEs have to be determined. If they are credible, the consequential effects of the PIEs have to be determined.

2. The safety functions, the safety systems and supporting features that are required to cope with the PIEs (for example control rod insertion, closing of containment isolation valves) have to be determined. These include alternative success paths through which the safety function could be satisfied.

3. A single failure must be assumed in the system as required by the Design Code. The consequences of the single failure must be determined.

4. It has to be shown that the safety function can still be performed.

5. In the determination of the consequences, compliance with the requirements for independence within safety groups must be established. The process would include verification that safety groups have no shared equipment or points of vulnerability, as far as practicable.

6. If the independent redundancies and trains of the required systems have been identified as single failure proof, the systems do not need further detailed analysis for potential failures under the single failure criterion.

7. If in exceptional cases the single failure criterion is not met, then the design is modified to meet the criterion, or, if justifiable, an exemption is established. It then has to be ensured that the reliability of the systems is maintained at a very high level by proper in-service inspection, maintenance and operating procedures so as to render their failure during service not credible.

8. If a single failure could prevent adequate reliability of a safety system, it has to be ensured that other systems are available to prevent unacceptable consequences.

9. In the application of the single failure criterion the detectability of failures is implicitly assumed. However, there may be failures which cannot easily be detected by testing or revealed by alarms or anomalous indications. The systems have to be analysed for such non-detectable failures. The preferred course would be to redesign the system or the test schemes to make the failures easily detectable. If that is not possible, it has to be assumed that the identified
undetectable failures have occurred and then a single failure has to be assumed in addition. It has to be ensured then that safety functions can be performed under these circumstances.

(10) Operator actions prescribed for the event sequences of concern have to be identified. The consequential effects of single random incorrect or omitted prescribed operator actions have to be analysed. It has to be ensured that under these circumstances the safety functions will be performed.

(11) In some Member States, the single failure criterion is not applied when one train of redundant trains is out of service owing to testing or maintenance. In such cases, the allowable out of service times that ensure the required reliability have to be determined.

(12) Analysis of common cause failures is normally not included in an SFA. Credible common cause failures have to be assessed separately, either by deterministic measures, PSA or a combination of both. Sufficient independence and diversity are to be incorporated to provide reasonable assurance that safety functions can be performed in the event of common cause failures.

8.4. IMPLEMENTATION CONSIDERATIONS

In an SFA, certain portions of the safety systems require special consideration. The following paragraphs include potential areas of concern in which particular care must be taken to ensure that the single failure criterion has been properly met.

Interconnections between redundant safety trains (through devices such as isolation valves in fluid systems or data loggers and test circuitry in electrical systems) are areas where independence could be lost. These interconnections must be analysed to ensure that no single failure can cause the loss of a safety function. The means for isolating the redundant trains must be analysed for single failures that would lead to the loss of a safety function.

Interconnections between safety systems or components and non-safety systems or components (such as isolation valves or lines connecting sensors to process systems) are also areas where independence could be lost. These interconnections must be included in the SFA.

System logic is of particular importance in an SFA since it is here that redundant trains and redundant actuator circuits may be brought together. The analysis must verify that no single failure in the system logic will cause failure in the trains or actuation circuits which would cause loss of the safety function. The single failure criterion does not invoke coincidence (or multiple channel) logic within a safety group; however, the application of coincidence logic may evolve from other criteria or considerations to maximize plant availability or reliability.

Those actuators designed to fail in a preferred mode upon loss of power must be analysed to ensure that no single failure (such as that which would cause power
to be maintained incorrectly on the actuator system terminals) can cause a loss of any required safety function.

Those actuators designed to apply power when protective action is required must be analysed to ensure that no single open circuit, short circuit, or loss of power can cause loss of a safety function.

The complete actuator system, which can encompass pneumatic, mechanical, electrical and hydraulic parts, must be analysed for failures that might affect the ability of the system to meet the single failure criterion. Particular attention must be paid to ensuring that failures in mechanical portions of actuators do not cause electrical failures in redundant equipment and that electrical failures do not cause mechanical failures in redundant equipment.

Power supplies have the potential for causing loss of safety functions in several ways and particular care is needed to identify all possible failures, their consequences and their effects on safety functions. An electrical power supply malfunction resulting in a high voltage could cause failures (such as transistor failures) in redundant trains. Similarly, a pneumatic or hydraulic power supply malfunction resulting in a change in pressure could cause failures (such as a diaphragm failure) in redundant safety trains. The single failure analysis must assess the entire power supply system, including devices which may supply non-safety loads. Further guidance may be found in the Safety Guide 50-SG-O8.

Any auxiliary supporting features which are required for proper operation of any safety function to which the single failure criterion is applied shall be included in the SFA as part of the system that provides the function. For example, when a portion of a system providing a safety function is dependent on the availability of cooling water, lubrication or a controlled environment, failure of the auxiliary supporting system becomes a potential violation of the single failure criterion unless it can be shown that failure of the supporting system would not result in loss of the safety function when required.

8.5. OTHER CONSIDERATIONS

Non-safety electrical systems (for example, test lines or circuitry) which are coupled in some manner to safety electrical systems to which the single failure criterion is applied must be examined to establish whether any failure within these systems can degrade the safety electrical systems to which they are coupled. If they can degrade any portion of the safety electrical systems to the point of failure, the SFA of the safety electrical system must include consideration of those failures.

The potential for system actuation due to single failures must be examined to determine whether such actuation would constitute an event with unacceptable safety consequences. For any such actuation identified as being unacceptable, the single failure criterion must be met (that is, the safety systems must not initiate the actuation
as a result of any single detectable failure in addition to all identified non-detectable failures in the systems).

Where reasonable indication exists that a design which meets the single failure criterion may not provide adequate reliability, reliability analysis of the safety system must be performed to help identify additional design features to achieve adequate reliability.

8.6. RELIABILITY AND PROBABILISTIC SAFETY ANALYSIS

A reliability analysis of safety systems may be performed to demonstrate that certain postulated failures need not be considered in the SFA. The reliability analysis is intended to eliminate consideration of PIEs and failures that are not credible; it must not be used in place of the SFA but may be used to complement, augment or support an SFA.

When a reliability analysis is used, the probability of the combination of the PIE plus a single failure must be based on best estimate values.

In some Member States, PSA methods employing event tree or fault tree analysis are used to confirm the reliability, separation and diversification goals specified for the design.
Appendix

EXAMPLES OF METHODS FOR THE DETERMINATION
OF PERMISSIBLE OUTAGE TIMES

The mathematical treatment in the following examples is simplified and does not deal with a combination of diverse systems with different failure rates in parallel trains. The overall concept is based on the following ideas:

(a) The failure probability of a single component depends on its failure rate and increases linearly with time $t$.

(b) After a test has shown that the component is available, the failure probability is zero (neglecting any possible time independent contribution to the unavailability).

(c) The maximum failure probability $P_{\text{max}}$ of a component which is periodically tested increases linearly with the test interval $T$.

(d) For a redundant system the failure probability depends on the failure rate $\lambda$ of each redundant train, the time $t$ and also the degree of redundancy. For example, for a 2 out of 4 system, the failure probability $P(t) = 4(\lambda t)^3$, $t$ being the time since the last test, and $P_{\text{max}} = 4(\lambda \tau)^3$, $\tau$ being the length of the test interval.

(e) The failure probability of a system increases with the total outage time of one or more single trains of that system within a specific time period, for example, the test interval.

(f) If the same safety function can be fulfilled by more than one system, the admissible outage time shall be considered with regard to all of these systems.

METHODOLOGY

Some of the possible methods for the determination of admissible outage times are explained below.

The first method uses a defined relation between the failure probabilities of the degraded and non-degraded systems. The maximum failure probability $P_{R, \text{max}}$ of a system of which some parts are under repair or test during an outage time $T_R$ must not exceed a factor $f$ times the maximum failure probability of the non-degraded system $P_{\text{max}}$ within a specified period. This means that:

$$P_{R, \text{max}}(T_R) \leq f \cdot P_{\text{max}}$$

---

6 The failure rate of the component may change with time, as a result, for example, of ageing. This aspect is not taken into account here.

7 The test interval is the time between two tests.
For \( f \), a value of 5 may be used. A simple example shows how a maximum acceptable outage time \( T_{R, \text{max}} \) can be derived from this method.

Let us assume that a 2 out of 4 system is degraded to a 2 out of 3 system by the repair of one train. Thus, during the outage time \( T_R \) the failure probability of the remaining system is:

\[
P_R(T_R) = 3(\lambda T_R)^2
\]

and since

\[
P_R(T_R) \leq f \cdot P_{\text{max}} = f \cdot 4(\lambda T)^3
\]

it follows that the maximum admissible outage time

\[
T_R = 2\tau \sqrt[3]{f \lambda \tau / 3}
\]

If \( \tau = 700 \text{ h} \), \( \lambda = 10^{-5} / \text{h} \) and \( f = 5 \), then \( T_R = 151 \text{ h} \) (6.3 days).

The second method is as follows. For a time span \( T \) between two repair or maintenance outages much larger than a test interval, the failure probability of the system, which for a certain part \( x \) of this time span is degraded due to outages, is compared with the limit value of \( f \) times the failure probability of the non-degraded system (with \( f \) being different from the value in the first method). If the time span \( T \) is significantly greater than the test interval the mean failure probability of the system with the repair outages and of the undisturbed system may be compared rather than the instantaneous failure probabilities.

This second method can be illustrated by a simple example. For the non-degraded system (2 out of 4) the mean failure probability is given by:

\[
\bar{P} = \frac{1}{\tau} \int_0^\tau P(t) \, dt = (\lambda \tau)^3
\]

For a system that is degraded to a 2 out of 3 system for a longer period than the test interval the mean failure probability is approximately (see Fig. 5):

\[
\bar{P}_R = \frac{1}{\tau} \int_0^\tau P_R(t) \, dt = (\lambda \tau)^2
\]

If the system is degraded for a part \( x \) of the total time period considered, its failure probability during the total time span \( T \) is:

\[
x \cdot \bar{P}_R + (1 - x) \cdot \bar{P}
\]

The above mentioned requirement leads to the condition

\[
x \cdot \bar{P}_R + (1 - x) \cdot \bar{P} \leq f \cdot \bar{P}
\]
FIG. 9. Schematic representation of failure probability as a function of time for a system with several redundancies, one of which is out for repair up to time $T_R$.

and from this, the maximum $x_{\text{max}}$ during which the system might be degraded can be determined.

The situation is illustrated by Fig. 9 (it should be borne in mind that $\lambda \tau \ll 1$). If $\tau = 700 \text{h}$, $\lambda = 10^{-5}/\text{h}$, and $f = 5$, then $x_{\text{max}} = 0.028$.

The third method prescribes a more pragmatic procedure which is under discussion in one Member State. It indicates a more qualitative and systematic way to approach the problem. The method:

— is based on operational experience
— takes into account the necessary reliability of the systems concerned with regard to PIE frequencies and a limiting frequency for inadmissible plant damage states
— considers the fact that for short outage times the risk involved in unchanged further operation of the plant can be lower than that of precautionary measures such as plant shutdown.

The essential parameters of this method are as follows:

(a) The frequency of the most probable PIE for which the system concerned is provided to deal with. The frequency of the PIE is characterized by one of five
special event classes $E$, which are defined in the following way (numerical frequency ranges can be assigned to each class):

$E = 1$ — normal operation
$E = 2$ — anticipated operational occurrences
$E = 3$ — events which cannot be excluded within the lifetime of the plant
$E = 4$ — events which are taken into account in the design basis as limited cases
$E = 5$ — very rare events.

(b) The degree of redundancy $k$ of the resultant safety feature. This means the degree of redundancy of the system configuration with one or more trains out for maintenance (and additionally trains of an alternative system which could fulfil on demand the same safety function). The degree of redundancy is defined as follows:

$k = 0$ — no redundancy available during the maintenance or repair procedure, i.e. a single failure in the system cannot be dealt with
$k = 1$ — 1 redundant train available during the maintenance or repair procedure, i.e. a single failure in the system can be dealt with
$k = 2$ — 2 redundant trains available.

The sum of $E$ and $k$ is a combined parameter for the qualitative determination of admissible outage times.

Let us suppose the permissible outage times are $O_1$, $O_2$, $O_3$, $O_4$, where $O_1 \leq O_2 \leq O_3 \leq O_4$. The assignment of values of a few hours to $O_1$, days to $O_2$, weeks to $O_3$ and months to $O_4$ corresponds to the estimated reduction in reliability of real systems or component configurations for such times. Table I indicates how the values of $E$ and $k$ combine to determine the outage.

<table>
<thead>
<tr>
<th>$E$</th>
<th>$k$</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td>$O_1$</td>
<td>$O_2$</td>
<td>$O_3$</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>$O_1$</td>
<td>$O_3$</td>
<td>$O_4$</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>$O_3$</td>
<td>$O_4$</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td>$O_4$</td>
</tr>
</tbody>
</table>
Although there should not be an outage in the case \( E = 2, k = 0 \), the short outage time \( O_i \) is allowed for this case because alternative measures (e.g. power reduction or shutdown) might lead to more adverse conditions than the slight decrease in reliability involved. The case \( E = 3, k = 0 \) is taken slightly more conservatively than the scheme might suggest. Since the scheme is only concerned with admissible outage times for safety features that are provided for coping with PIEs it does not include \( E = 1 \).

In the event of a need for short time maintenance or test operations of one of the operational trains while one train is out for a long term repair, the resultant redundancy conditions have to be taken into account in using the scheme.

The qualitative probabilistic basis for Table I is the reduction of the frequency of the PIE with increasing event class number and an increase in the system reliability with increasing degree of redundancy. This means that for a constant value of the sum \( (E + K) \) the product of PIE frequency and system unavailability is to a first approximation constant. Consequently, the admissible outage times are assumed to be the same for constant \( (E + K) \).

This approximate philosophy may be somewhat refined for any actual application, e.g. with regard to possible outage time ranges. But in principle it presents a pragmatic method with a probabilistic background.

The fourth method tried or used in some Member States consists in the examination of the outage time variation effects on the result of a PSA. An acceptable outage time for equipment is that time period which does not significantly change, for example, the probability of a core melt. One Member State uses a target which can be stated as follows: the acceptable outage time for equipment does not lead to a core melt probability higher than \( 10^{-7} \)/year.

EVALUATION

The essential differences between the four methods are:

— Methods 1, 2 and 4 are based on quantitative reliability analysis, whereas method 3 takes account of qualitative results.
— Methods 1 and 2 consider only the reliability of the safety feature concerned, whereas methods 3 and 4 also consider the frequency of the related PIE.

Compared to the other methods, the third method has the following features:

— it is easily carried out
— it also takes into account the PIE frequency
— the result is affected by two uncertainty bands (PIE frequency and system reliability)
— it has lower precision
— it leads to long outage times for safety features with many redundancies and for safety features provided for rare events.
The fourth method is the most precise and most elaborate because: it takes into account the actual safety function of diverse systems; it requires a knowledge of the detailed design and thus is most useful for standardized series of plants; it can also take into account the possibility of very rare events.
BIBLIOGRAPHY


ELECTRICITE DE FRANCE, Principes généraux de conception et d'installation, Extrait du RCC-P 1300 MWe, Révision 2, Règle I.3.a, Paris (1985).

General provisions for ensuring the safety of nuclear power plants at the design, construction and operational states, At. Energ. 54 2 (1983).


CONTRIBUTORS TO DRAFTING AND REVIEW

Amano, F. 
International Atomic Energy Agency

Bonechi, M. 
Atomic Energy of Canada Ltd, Canada

d’Ardenne, W. 
General Electric Co., United States of America

Dastidar, P. 
International Atomic Energy Agency

Edwards, G.T. 
United Kingdom Atomic Energy Authority, United Kingdom

Fischer, J. 
International Atomic Energy Agency

Gallagher, J. 
Westinghouse Electric Corporation, United States of America

Kakodkar, A. 
Bhabha Atomic Research Centre, India

Komsi, M. 
Imatran Voima Oy, Finland

Kraut, A. 
Gesellschaft für Reaktorsicherheit, Federal Republic of Germany

Kus, J.P. 
Electricité de France, France

Nguyen, C. 
Institut de protection et de sûreté nucléaire, France

Working Group Meeting
Vienna, Austria: 20–31 July 1987

Technical Committee Meeting
Vienna, Austria: 29 August–2 September 1988
LIST OF NUSS PROGRAMME TITLES

It should be noted that some books in the series may be revised in the near future. Those that have already been revised are indicated by the addition of '(Rev. 1)' to the number.

1. GOVERNMENTAL ORGANIZATION

50-C-G (Rev. 1) Code on the safety of nuclear power plants: Governmental organization

Safety Guides

50-SG-G1 Qualifications and training of staff of the regulatory body for nuclear power plants

50-SG-G2 Information to be submitted in support of licensing applications for nuclear power plants

50-SG-G3 Conduct of regulatory review and assessment during the licensing process for nuclear power plants

50-SG-G4 Inspection and enforcement by the regulatory body for nuclear power plants

50-SG-G6 Preparedness of public authorities for emergencies at nuclear power plants

50-SG-G8 Licences for nuclear power plants: content, format and legal considerations

50-SG-G9 Regulations and guides for nuclear power plants

2. SITING

50-C-S (Rev. 1) Code on safety of nuclear power plants: Siting

Safety Guides

50-SG-S1 Earthquakes and associated topics in relation to nuclear power plant siting

50-SG-S2 Seismic analysis and testing of nuclear power plants

50-SG-S3 Atmospheric dispersion in nuclear power plant siting

50-SG-S4 Site selection and evaluation for nuclear power plants with respect to population distribution

1988

1979

1979

1980

1980

1982

1982

1984

1988

1979

1979

1980

1980

53
3. DESIGN

50-C-D (Rev. 1) Code on the safety of nuclear power plants: Design 1988

Safety Guides

50-SG-D1 Safety functions and component classification for BWR, PWR and PTR 1979

50-SG-D2 Fire protection in nuclear power plants 1979

50-SG-D3 Protection system and related features in nuclear power plants 1980

50-SG-D4 Protection against internally generated missiles and their secondary effects in nuclear power plants 1980

50-SG-D5 External man-induced events in relation to nuclear power plant design 1982

50-SG-D6 Ultimate heat sink and directly associated heat transport systems for nuclear power plants 1981

50-SG-D7 Emergency power systems at nuclear power plants 1982

50-SG-D8 Safety-related instrumentation and control systems for nuclear power plants 1984

50-SG-D9 Design aspects of radiation protection for nuclear power plants 1985

50-SG-D10 Fuel handling and storage systems in nuclear power plants 1984
<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>50-SG-D11</td>
<td>General design safety principles for nuclear power plants</td>
<td>1986</td>
</tr>
<tr>
<td>50-SG-D12</td>
<td>Design of the reactor containment systems in nuclear power plants</td>
<td>1985</td>
</tr>
<tr>
<td>50-SG-D13</td>
<td>Reactor cooling systems in nuclear power plants</td>
<td>1986</td>
</tr>
<tr>
<td>50-SG-D14</td>
<td>Design for reactor core safety in nuclear power plants</td>
<td>1986</td>
</tr>
</tbody>
</table>

### 4. OPERATION

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>50-C-O</td>
<td>Code on the safety of nuclear power plants: Operation</td>
<td>1988</td>
</tr>
<tr>
<td>50-SG-O1</td>
<td>Staffing of nuclear power plants and the recruitment, training and authorization of operating personnel</td>
<td>1979</td>
</tr>
<tr>
<td>50-SG-O2</td>
<td>In-service inspection for nuclear power plants</td>
<td>1980</td>
</tr>
<tr>
<td>50-SG-O3</td>
<td>Operational limits and conditions for nuclear power plants</td>
<td>1979</td>
</tr>
<tr>
<td>50-SG-O4</td>
<td>Commissioning procedures for nuclear power plants</td>
<td>1980</td>
</tr>
<tr>
<td>50-SG-O5</td>
<td>Radiation protection during operation of nuclear power plants</td>
<td>1983</td>
</tr>
<tr>
<td>50-SG-O6</td>
<td>Preparedness of the operating organization (licensee) for emergencies at nuclear power plants</td>
<td>1982</td>
</tr>
<tr>
<td>50-SG-O7</td>
<td>Maintenance of nuclear power plants</td>
<td>1990</td>
</tr>
<tr>
<td>50-SG-O8</td>
<td>Surveillance of items important to safety in nuclear power plants</td>
<td>1990</td>
</tr>
<tr>
<td>50-SG-O9</td>
<td>Management of nuclear power plants for safe operation</td>
<td>1984</td>
</tr>
<tr>
<td>50-SG-O10</td>
<td>Core management and fuel handling for nuclear power plants</td>
<td>1985</td>
</tr>
<tr>
<td>50-SG-O11</td>
<td>Operational management of radioactive effluents and wastes arising in nuclear power plants</td>
<td>1986</td>
</tr>
</tbody>
</table>

### 5. QUALITY ASSURANCE

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>50-C-QA</td>
<td>Code on the safety of nuclear power plants: Quality assurance</td>
<td>1988</td>
</tr>
<tr>
<td>50-SG-QA1</td>
<td>Establishing of the quality assurance programme for a nuclear power plant project</td>
<td>1984</td>
</tr>
</tbody>
</table>
50-SG-QA2  Quality assurance records system for nuclear power plants  1979
50-SG-QA3  Quality assurance in the procurement of items and services for nuclear power plants  1979
50-SG-QA4  Quality assurance during site construction of nuclear power plants  1981
50-SG-QA5 (Rev. 1)  Quality assurance during operation of nuclear power plants  1986
50-SG-QA6  Quality assurance in the design of nuclear power plants  1981
50-SG-QA7  Quality assurance organization for nuclear power plants  1983
50-SG-QA8  Quality assurance in the manufacture of items for nuclear power plants  1981
50-SG-QA10  Quality assurance auditing for nuclear power plants  1980
50-SG-QA11  Quality assurance in the procurement, design and manufacture of nuclear fuel assemblies  1983
SELECTION OF IAEA PUBLICATIONS RELATING TO THE SAFETY OF NUCLEAR POWER PLANTS

SAFETY SERIES

    1982
49  Radiological surveillance of airborne contaminants in the working environment
    1979
52  Factors relevant to the decommissioning of land-based nuclear reactor plants
    1980
55  Planning for off-site response to radiation accidents in nuclear facilities
    1981
57  Generic models and parameters for assessing the environmental transfer of radionuclides from routine releases: Exposures of critical groups
    1982
67  Assigning a value to transboundary radiation exposure
    1985
69  Management of radioactive wastes from nuclear power plants
    1985
72  Principles for establishing intervention levels for the protection of the public in the event of a nuclear accident or radiological emergency
    1985
73  Emergency preparedness exercises for nuclear facilities: Preparation, conduct and evaluation
    1985
75-INSAG-1  Summary report on the post-accident review meeting on the Chernobyl accident
    1986
75-INSAG-2  Radionuclide source terms from severe accidents to nuclear power plants with light water reactors
    1987
75-INSAG-3  Basic safety principles for nuclear power plants
    1988
77  Principles for limiting releases of radioactive effluents into the environment
    1986
79  Design of radioactive waste management systems at nuclear power plants
    1986
81  Derived intervention levels for application in controlling radiation doses to the public in the event of a nuclear accident or radiological emergency: Principles, procedures and data
    1986
84 Basic principles for occupational radiation monitoring 1987
86 Techniques and decision making in the assessment of off-site consequences of an accident in a nuclear facility 1987
93 Systems for reporting unusual events in nuclear power plants 1989
94 Response to a radioactive materials release having a transboundary impact 1989
97 Principles and techniques for post-accident assessment and recovery in a contaminated environment of a nuclear facility 1989
98 On-site habitability in the event of an accident at a nuclear facility: Guidance for assessment and improvement 1989
103 Provision of operational radiation protection services at nuclear power plants 1990

TECHNICAL REPORTS SERIES

155 Thermal discharges at nuclear power stations 1974
163 Neutron irradiation embrittlement of reactor pressure vessel steels (being revised) 1975
189 Storage, handling and movement of fuel and related components at nuclear power plants 1979
198 Guide to the safe handling of radioactive wastes at nuclear power plants 1980
200 Manpower development for nuclear power: A guidebook 1980
202 Environmental effects of cooling systems 1980
217 Guidebook on the introduction of nuclear power 1982
224 Interaction of grid characteristics with design and performance of nuclear power plants: A guidebook 1983
230 Decommissioning of nuclear facilities: Decontamination, disassembly and waste management 1983
237 Manual on quality assurance programme auditing 1984
239 Nuclear power plant instrumentation and control: A guidebook 1984
<table>
<thead>
<tr>
<th>Year</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1984</td>
<td>Qualification of nuclear power plant operations personnel: A guidebook</td>
<td></td>
</tr>
<tr>
<td>1985</td>
<td>Decontamination of nuclear facilities to permit operation, inspection,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>maintenance, modification or plant decommissioning</td>
<td></td>
</tr>
<tr>
<td>1986</td>
<td>Manual on training, qualification and certification of quality assurance personnel</td>
<td></td>
</tr>
<tr>
<td>1986</td>
<td>Methodology and technology of decommissioning nuclear facilities</td>
<td></td>
</tr>
<tr>
<td>1986</td>
<td>Manual on maintenance of systems and components important to safety</td>
<td></td>
</tr>
<tr>
<td>1987</td>
<td>Introducing nuclear power plants into electrical power systems of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>limited capacity: Problems and remedial measures</td>
<td></td>
</tr>
<tr>
<td>1987</td>
<td>Design of off-gas and air cleaning systems at nuclear power plants</td>
<td></td>
</tr>
<tr>
<td>1988</td>
<td>Manual on quality assurance for computer software related to the safety</td>
<td></td>
</tr>
<tr>
<td></td>
<td>of nuclear power plants</td>
<td></td>
</tr>
<tr>
<td>1989</td>
<td>Design and operation of off-gas cleaning and ventilation systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td>in facilities handling low and intermediate level radioactive material</td>
<td></td>
</tr>
<tr>
<td>1989</td>
<td>Options for the treatment and solidification of organic radioactive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>wastes</td>
<td></td>
</tr>
<tr>
<td>1989</td>
<td>Regulatory inspection of the implementation of quality assurance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>programmes: A manual</td>
<td></td>
</tr>
<tr>
<td>1989</td>
<td>Review of fuel element developments for water cooled nuclear power</td>
<td></td>
</tr>
<tr>
<td></td>
<td>reactors</td>
<td></td>
</tr>
<tr>
<td>1989</td>
<td>Cleanup of large areas contaminated as a result of a nuclear accident</td>
<td></td>
</tr>
<tr>
<td>1989</td>
<td>Manual on quality assurance for installation and commissioning of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>instrumentation, control and electrical equipment in nuclear power</td>
<td></td>
</tr>
<tr>
<td></td>
<td>plants</td>
<td></td>
</tr>
<tr>
<td>1989</td>
<td>Guidebook on the education and training of technicians for nuclear</td>
<td></td>
</tr>
<tr>
<td></td>
<td>power</td>
<td></td>
</tr>
<tr>
<td>1989</td>
<td>Management of abnormal radioactive wastes at nuclear power plants</td>
<td></td>
</tr>
<tr>
<td>IAEA-TECDOC SERIES</td>
<td>Title</td>
<td>Publication Year</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>225</td>
<td>Planning for off-site response to radiation accidents in nuclear facilities</td>
<td>1980</td>
</tr>
<tr>
<td>238</td>
<td>Management of spent ion-exchange resins from nuclear power plants</td>
<td>1981</td>
</tr>
<tr>
<td>248</td>
<td>Decontamination of operational nuclear power plants</td>
<td>1981</td>
</tr>
<tr>
<td>276</td>
<td>Management of radioactive waste from nuclear power plants</td>
<td>1983</td>
</tr>
<tr>
<td>294</td>
<td>International experience in the implementation of lessons learned from the Three Mile Island accident</td>
<td>1983</td>
</tr>
<tr>
<td>303</td>
<td>Manual on the selection of appropriate quality assurance programmes for items and services of a nuclear power plant</td>
<td>1984</td>
</tr>
<tr>
<td>308</td>
<td>Survey of probabilistic methods in safety and risk assessment for nuclear power plant licensing</td>
<td>1984</td>
</tr>
<tr>
<td>332</td>
<td>Safety aspects of station blackout at nuclear power plants</td>
<td>1985</td>
</tr>
<tr>
<td>341</td>
<td>Developments in the preparation of operating procedures for emergency conditions at nuclear power plants</td>
<td>1985</td>
</tr>
<tr>
<td>348</td>
<td>Earthquake resistant design of nuclear facilities with limited radioactive inventory</td>
<td>1985</td>
</tr>
<tr>
<td>355</td>
<td>Comparison of high efficiency particulate filter testing methods</td>
<td>1985</td>
</tr>
<tr>
<td>377</td>
<td>Safety aspects of unplanned shutdowns and trips</td>
<td>1986</td>
</tr>
<tr>
<td>379</td>
<td>Atmospheric dispersion models for application in relation to radionuclide releases</td>
<td>1986</td>
</tr>
<tr>
<td>387</td>
<td>Combining risk analysis and operating experience</td>
<td></td>
</tr>
<tr>
<td>390</td>
<td>Safety assessment of emergency electric power systems for nuclear power plants</td>
<td>1986</td>
</tr>
<tr>
<td>416</td>
<td>Manual on quality assurance for the survey, evaluation and confirmation of nuclear power plant sites</td>
<td>1987</td>
</tr>
<tr>
<td>424</td>
<td>Identification of failure sequences sensitive to human error</td>
<td>1987</td>
</tr>
<tr>
<td>425</td>
<td>Simulation of a loss of coolant accident</td>
<td>1987</td>
</tr>
<tr>
<td>443</td>
<td>Experience with simulator training for emergency conditions</td>
<td>1987</td>
</tr>
<tr>
<td>Page</td>
<td>Title</td>
<td>Year</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>444</td>
<td>Improving nuclear power plant safety through operator aids</td>
<td>1987</td>
</tr>
<tr>
<td>450</td>
<td>Dose assessments in NPP siting</td>
<td>1988</td>
</tr>
<tr>
<td>451</td>
<td>Some practical implications of source term reassessment</td>
<td>1988</td>
</tr>
<tr>
<td>458</td>
<td>OSART results</td>
<td>1988</td>
</tr>
<tr>
<td>497</td>
<td>OSART results II</td>
<td>1989</td>
</tr>
<tr>
<td>498</td>
<td>Good practices for improved nuclear power plant performance</td>
<td>1989</td>
</tr>
<tr>
<td>499</td>
<td>Models and data requirements for human reliability analysis</td>
<td>1989</td>
</tr>
<tr>
<td>508</td>
<td>Survey of ranges of component reliability data for use in probabilistic safety assessment</td>
<td>1989</td>
</tr>
<tr>
<td>510</td>
<td>Status of advanced technology and design for water cooled reactors: Heavy water reactors</td>
<td>1989</td>
</tr>
<tr>
<td>522</td>
<td>A probabilistic safety assessment peer review: Case study on the use of probabilistic safety assessment for safety decisions</td>
<td>1989</td>
</tr>
<tr>
<td>523</td>
<td>Probabilistic safety criteria at the safety function/system level</td>
<td>1989</td>
</tr>
<tr>
<td>525</td>
<td>Guidebook on training to establish and maintain the qualification and competence of nuclear power plant operations personnel</td>
<td>1989</td>
</tr>
<tr>
<td>529</td>
<td>User requirements for decision support systems used for nuclear power plant accident prevention and mitigation</td>
<td>1989</td>
</tr>
<tr>
<td>540</td>
<td>Safety aspects of nuclear power plant ageing</td>
<td>1990</td>
</tr>
<tr>
<td>542</td>
<td>Use of expert systems in nuclear safety</td>
<td>1990</td>
</tr>
</tbody>
</table>

**PROCEEDINGS SERIES**

<p>| STI/PUB/566 | Current nuclear power plant safety issues                                               | 1981 |
| STI/PUB/593 | Quality assurance for nuclear power plants                                             | 1982 |
| STI/PUB/628 | Nuclear power plant control and instrumentation                                        | 1983 |
| STI/PUB/645 | Reliability of reactor pressure components                                             | 1983 |</p>
<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>STI/PUB/673</td>
<td>IAEA safety codes and guides (NUSS) in the light of current safety issues</td>
<td>1985</td>
</tr>
<tr>
<td>STI/PUB/700</td>
<td>Source term evaluation for accident conditions</td>
<td>1986</td>
</tr>
<tr>
<td>STI/PUB/701</td>
<td>Emergency planning and preparedness for nuclear facilities</td>
<td>1986</td>
</tr>
<tr>
<td>STI/PUB/716</td>
<td>Optimization of radiation protection</td>
<td>1986</td>
</tr>
<tr>
<td>STI/PUB/759</td>
<td>Safety aspects of the ageing and maintenance of nuclear power plants</td>
<td>1988</td>
</tr>
<tr>
<td>STI/PUB/761</td>
<td>Nuclear power performance and safety</td>
<td>1988</td>
</tr>
<tr>
<td>STI/PUB/782</td>
<td>Severe accidents in nuclear power plants</td>
<td>1988</td>
</tr>
<tr>
<td>STI/PUB/783</td>
<td>Radiation protection in nuclear energy</td>
<td>1988</td>
</tr>
<tr>
<td>STI/PUB/785</td>
<td>Feedback of operational safety experience from nuclear power plants</td>
<td>1989</td>
</tr>
<tr>
<td>STI/PUB/803</td>
<td>Regulatory practices and safety standards for nuclear power plants</td>
<td>1989</td>
</tr>
<tr>
<td>STI/PUB/824</td>
<td>Fire protection and fire fighting in nuclear installations</td>
<td>1989</td>
</tr>
</tbody>
</table>
HOW TO ORDER IAEA PUBLICATIONS

An exclusive sales agent for IAEA publications, to whom all orders and inquiries should be addressed, has been appointed in the following country:

UNITED STATES OF AMERICA UNIPUB, 4611-F Assembly Drive, Lanham, MD 20706-4391

In the following countries IAEA publications may be purchased from the sales agents or booksellers listed or through major local booksellers. Payment can be made in local currency or with UNESCO coupons.

ARGENTINA Comisión Nacional de Energía Atómica, Avenida del Libertador 8250, RA-1429 Buenos Aires
AUSTRALIA Hunter Publications, 58 A Gipps Street, Collingwood, Victoria 3066
BELGIUM Service Courrier UNESCO, 202, Avenue du Roi, B-1060 Brussels
CHILE Comisión Chilena de Energía Nuclear, Venta de Publicaciones, Amunategui 95, Casilla 188-D, Santiago
CHINA IAEA Publications in Chinese:
China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing
IAEA Publications other than in Chinese:
China National Publications Import & Export Corporation, Deutsche Abteilung, P.O. Box 88, Beijing
CZECHOSLOVAKIA S.N.T.L., Mikulandska 4, CS-116 85 Prague 1
FRANCE Office International de Documentation et Librairie, 48, rue Gay-Lussac, F-75240 Paris Cedex 05
HUNGARY Kultura, Hungarian Foreign Trading Company, P.O. Box 149, H-1389 Budapest 62
INDIA Oxford Book and Stationery Co., 17, Park Street, Calcutta-700 016
OXford Book and Stationery Co., Scindia House, New Delhi-110 001
ISRAEL Heiliger & Co. Ltd., 23 Keren Hayesod Street, Jerusalem 94188
ITALY Libreria Scientifica, Dott. Lucio de Biasio "aeiou", Via Meravigli 16, I-20123 Milan
JAPAN Maruzen Company, Ltd, P.O. Box 5050, 100-31 Tokyo International
PAKISTAN Mirza Book Agency, 65, Shahrrah Quaid-e-Azam, P.O. Box 729, Lahore 3
POLAND Ars Polona-Ruch, Centrala Handlu Zgranicznego, Krakowskie Przedmiescie 7, PL-00-088 Warsaw
ROMANIA Illexim, P.O. Box 136-137, Bucharest
SOUTH AFRICA Van Schaik Bookstore (Pty) Ltd, P.O. Box 724, Pretoria 0001
SPAIN Díaz de Santos, Lagasca 95, E-28006 Madrid
SWEDEN AB Fritz's Kungl. Hovbokhandel, Fredsgatan 2, P.O. Box 16356, S-103 27 Stockholm
UNITED KINGDOM HMSO, Publications Centre, Agency Section, 51 Nine Elms Lane, London SW8 5DR
USSR Mezhdunarodnaya Kniga, Smolenskaya-Sennaya 32-34, Moscow G-200
YUGOSLAVIA Jugoslovenska Knjiga, Terazije 27, P.O. Box 36, YU-11001 Belgrade

Orders from countries where sales agents have not yet been appointed and requests for information should be addressed directly to:

Division of Publications
International Atomic Energy Agency
Wagramerstrasse 5, P.O. Box 100, A-1400 Vienna, Austria