IAEA-TECDOC-636

Manual on reliability data collection for research reactor PSAs

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

The IAEA does not normally maintain stocks of reports in this series. However, microfiche copies of these reports can be obtained from

INIS Clearinghouse
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

Orders should be accompanied by prepayment of Austrian Schillings 100,— in the form of a cheque or in the form of IAEA microfiche service coupons which may be ordered separately from the INIS Clearinghouse.

MANUAL ON RELIABILITY DATA COLLECTION FOR RESEARCH REACTOR PSAs
IAEA, VIENNA, 1992
IAEA-TECDOC-636
ISSN 1011–4289

Printed by the IAEA in Austria
January 1992

FOREWORD

Probabilistic Safety Assessment (PSA) is a matured tool for assessing safety of nuclear reactors. It has been widely applied to a number of nuclear power plants and over the past five years it has increasingly been applied to research reactor facilities as well. The IAEA has been actively promoting performance of PSA studies for research reactors. From 1986 to 1988 the IAEA undertook a Co-ordinated Research Programme (CRP) on PSA for Research Reactors which helped promote use of PSA and foster a broad exchange of information. Although the basic methodological approach in performing a research reactor PSA is understood, some unresolved issues, data availability being among them, still exist.

The availability of relevant reliability data was identified as one of the problem areas with research reactor PSA. To address the issue on the international level, the IAEA initiated a new CRP on "Data Acquisition for Research Reactors PSA Studies". The aim of the CRP is to develop a data collection system for research reactors and generate research reactor specific reliability data for use in PSAs.

To achieve comprehensive data collection on research reactors and to generate data which may be logically comparable, a set of precise definitions should be adopted. A set of definitions developed specifically for research reactors and covering classification of equipment and failure terms, reliability parameters, failure modes and other terms necessary for data collection and processing is presented in this document.

This document is being prepared in the framework of the above mentioned CRP on "Data Acquisition for Research Reactors PSA Studies". It is based on discussions during the first meeting of the CRP held in Vienna in October 1989 and during the second meeting held in Beijing, China, in October 1990. The principal author of the document is Mr. J. Hammer from the Paul Scherrer Institute in Switzerland. Selected sections have been prepared by other CRP participants: Mr. Li Zhaohuan, China; Mr.D.Winfield, Canada; Mr. J. Dusek and Mr.V.Stepanek, Czechoslovakia; Mr. H. Böck, Austria; Mr. H. Witt, Australia and Mr. Ha Anh Tran, Viet Nam. The project officers were Mr. Bojan Tomic from IAEA's Safety Assessment Section and Mr. F. Alcala Ruiz from the Engineering Safety Section of the Division of Nuclear Safety.

EDITORIAL NOTE

In preparing this material for the press, staff of the International Atomic Energy Agency have mounted and paginated the original manuscripts and given some attention to presentation.

The views expressed do not necessarily reflect those of the governments of the Member States or organizations under whose auspices the manuscripts were produced.

The use in this book of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of specific companies or of their products or brand names does not imply any endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

Limited availability of data specific to research reactors is of great concern when performing a PSA study [1]. While for commercial power reactors data collection has usually been an integral part of their operation and relevant data for PSAs was reasonably simple to acquire, data on research reactors has been rarely collected. To overcome the problem of data availability, the IAEA initiated the Co-ordinated Research Programme(CRP) on "Data Acquisition for Research Reactors PSA Studies" aiming to provide necessary data. For a comprehensive data collection which would generate adequate data for PSA purposes, a set of detail definitions is required.
The aim of this document is to provide definitions to be used in data collection which are derived specifically to cover research reactors. It contains all the definitions necessary to identify and group individual failures and definitions related to calculation of reliability parameters. The appendices to the document contain additional information on different reactor types, examples of data collection forms and coding schemes (referred to in computer code DES-Data Entry System) and statistical methodology used for data processing.
This is the first of a series of documents which are proposed to be published within the framework of the CRP. Subsequent documents will address other data related issues and ultimately provide a generic research reactor data base.

1.1. Scope

The definitions contained in this document apply to components used in the operating environment of research reactors and their associated research facilities. The examples of applicability have been provided by the users of a particular research reactor type. A set of commonly used definitions associated with data collection and processing is provided in this document. The list of components and associated codes in Appendix E is compiled on the basis of standard research reactor equipment typically considered in a PSA study.

1.2. Purpose

The purpose of this document is to provide a standard set of definitions for data collection on research reactor equipment and data processing to generate reliability parameters needed for PSA studies./1/.

Within the framework of the CRP, definitions as well as statistical methods and codes described in this document will be strictly followed in the preparation of the "Generic research reactors reliability data base", which will be the ultimate product of the CRP. Due to very specific definitions which may substantially influence reliability data, this document should be consulted before using any of the data generated within the CRP.

Finally this document is also intended to promote data collection on research reactors and related facilities worldwide by providing all the necessary definitions and appropriate examples to streamline the data collection and processing.

2. CLASSIFICATION OF RESEARCH REACTOR EQUIPMENT

The IAEA's Component Reliability Data Base (IAEA-TECDOC478,/2/) distinguishes more than 430 individual components and about 100 component groups. Even for smaller research reactors roughly 100 individual components are expected to be relevant to probabilistic safety assessment. All these components belong to one of 3 major categories:

- **mechanical (and electromechanical) components**
- **electrical components**
- **instrumentation and control equipment**

It is convenient to classify research reactor equipment (including the experimental facilities) into these categories.

2.1. Component categories

The **mechanical components** category includes typically the following component groups:

air compressor
pumps
piping and pool liner
valves
heat exchangers
HVAC equipment, ventilation systems
strainers, ion exchanger, and filters
control rod drive mechanisms
core support structure and related components
beam tubes and related equipment
fuel elements, fuel assemblies
reflector structure
incore irradiation devices
fuel handling equipment
D_2O-tank (reactor vessel calandria)
fuel storage containers
shielding and related equipment
lifting equipment, cranes, and elevators
building structures and structural components

The **electrical component** category includes usually the following component groups:

conductors and power cables
power transformers
motors and motor control units
power relays
batteries
uninterruptable power supply units (UPS)
inverters
motor generators
other electrical equipment related to electrical supply distribution
diesel generators

The **instrumentation and control equipment** category includes the following component groups:

sensors
transmitters
switches and control switches
annunciators, indicators and recorders
nuclear instrument channels
signal conditioning systems
computers and related equipment
other instrumentation and control systems

2.2. Component description

The component description defines the component in a way useful for the failure data collection. It includes at least the name, the type, the manufacturer, some main technical characteristics and the location within the facility.

2.3. Component boundary

The component boundary defines clearly all interfaces of a specific component to other components in the system with which it interfaces via hardware or software. In some cases (e.g. for new electronic equipment) the failure parameters at subcomponent levels (resistors, relays, semiconductors,...) are used to predict failure rates of components or subsystems. The procedure for this is well known and explained in detail in the US-MIL-Standards of electronic devices. In other cases failure data at higher levels (component or subsystem) is used as input data for reliability analysis of systems and for comparison with reliability allocation or prediction analysis. Therefore, an exact definition of component and system boundaries is necessary in order to clarify the application of equipment reliability parameters.

The component boundary definition is based on three criteria:

- a definition has to unambiguously describe the component
- a definition has to be compatible with the data which are being generated and for the applications of the data base user
- a definition has to be compatible with the component's documentation and operating features such as surveillance, operating, and test procedures, maintenance work orders, and spare part lists

Proper definition of component boundaries requires interface points with control systems, power supplies and support systems to be determined /3/. Failures occurring inside the component boundary are then accounted for in the component failure rates.

For the 3 component categories a set of general rules are listed below:

- **mechanical components**: the component itself plus any associated, dedicated auxiliary equipment (e.g. control circuits, protection and indication equipment) are within the component boundary. In addition, support systems, such as cooling systems, fuel systems (for diesels), and so on are within the component boundary.
- **electrical components**: for electrical components the same basic rules as for mechanical components applies. Local control and protection equipment as well as measurement devices attached to the component are within the component boundary.
- **instrumentation and control equipment**: the boundary definition for instrumentation and control equipment should include local cabling and connections but exclude process equipment.

According to these criteria the following examples are helpful for the definition of boundaries for a variety of different components. These definitions should be in a form that the constituent components or subsystems are discrete entities which are each mutually exclusive so that there are neither omissions nor overlaps. This is of utmost importance in the data collection, because double counting or omission of relevant piece parts can significantly influence a component's reliability parameter.

2.4. Examples for component boundary definitions

2.4.1. Centrifugal pump

Centrifugal pumps are often used in primary or secondary cooling circuits of research reactors. The subsystem (component) boundary of this type of pumps

clarifies all interfaces. As shown in figure 2.1. the subsystem 'centrifugal pump' consists of 5 components:

- pump
- motor
- power supply to the motor, including overload protection circuitry
- control equipment for the pump
- logic and instrumentation, such as indicators and actuators

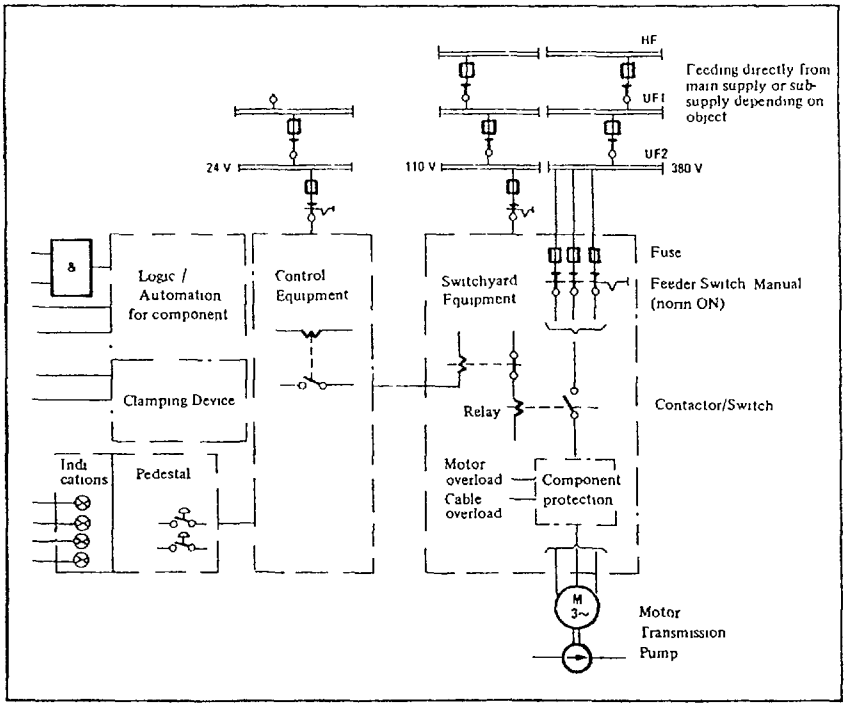

Fig. 2.1.: Physical boundary of a centrifugal pump

2.4.2. Motor operated valve

This type of component is used in the primary cooling circuit in higher power research reactors. The boundary of this component, similar to that of a pump, has interfaces to an electrical supply and control as well as to the piping. It consists of 5 subcomponents, as shown in figure 2.2. /4/:

- valve and adjacent mechanical components
- motor
- motor power supply and overload protection circuitry
- control equipment
- logic and instrumentation, such as indicators and actuators

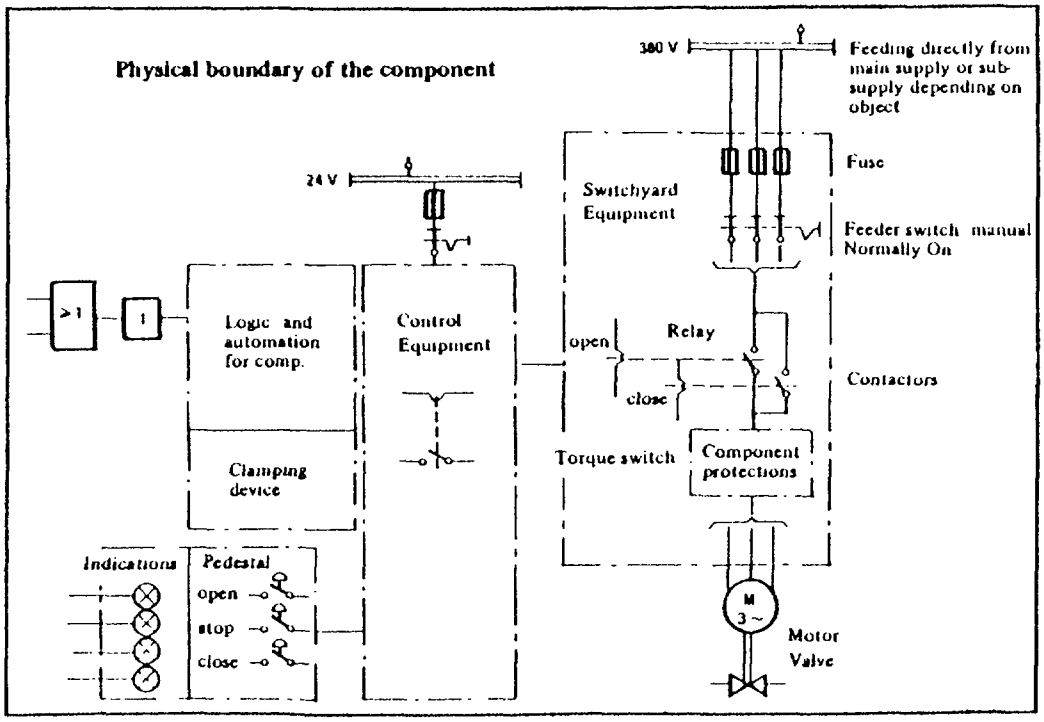

Fig. 2.2.: Physical boundary of a motor operated isolation valve

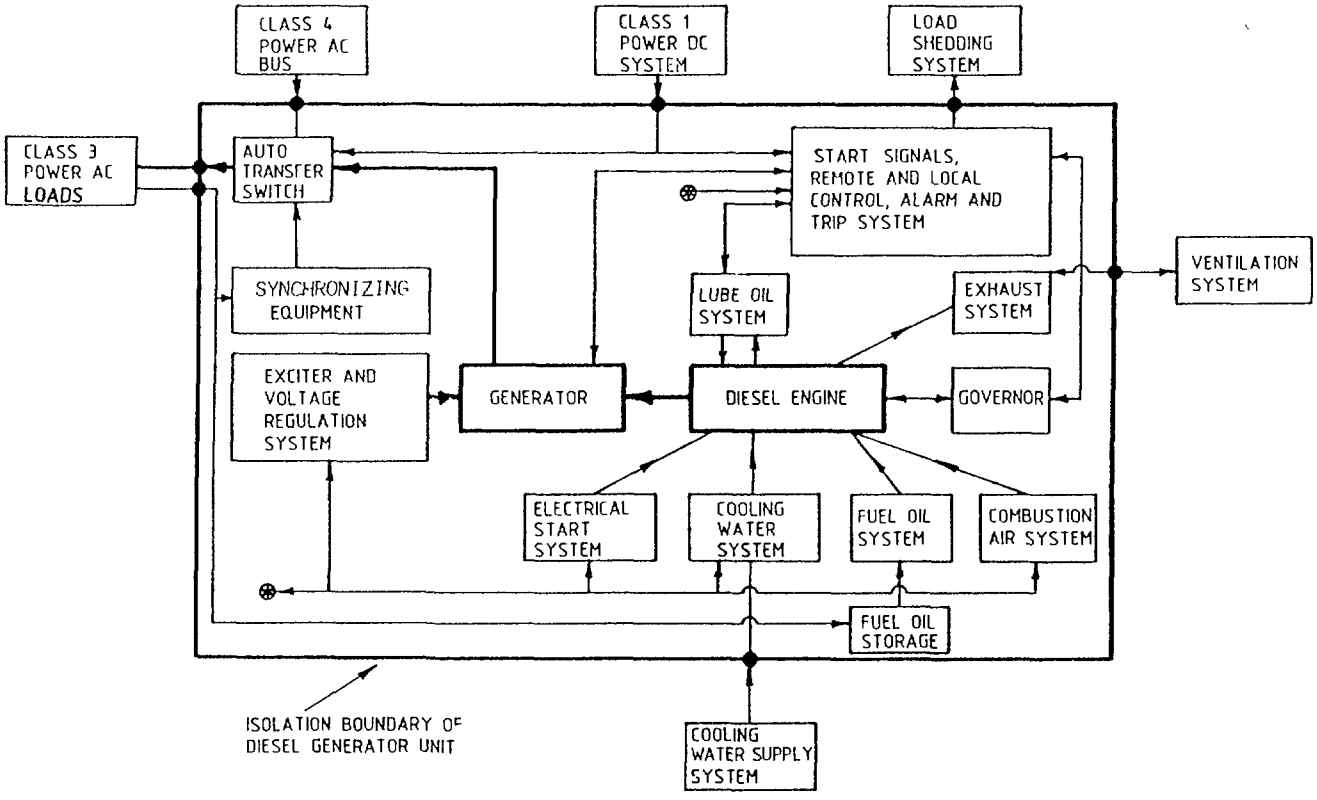

Fig. 2.3.: Physical boundary of a diesel generator /5/

2.4.3. Diesel generator

Diesel generators are usually part of the emergency power supply system of high power research reactors. The diesel generators are subsystems of the overall emergency power supply system. As shown in figure 2.3. /5/ the boundary of a diesel generator set defines the interfaces to the surrounding system. The set consists of:

- diesel engine, generator, and generator output breaker
- switchgear equipment with overload protection
- control equipment
- logic and instrumentation
- service systems (fuel, compressed air, coolant water, lubricant)

2.4.4. Sensors

Sensors used to measure parameters such as temperature, pressure, flow rate, level,...are widely used in all types of research reactors. A typical sensor (see figure 2.4.) consists of 2 parts:

- sensor and adjacent piping and mounting devices
- transmitter (usually an electronic device)

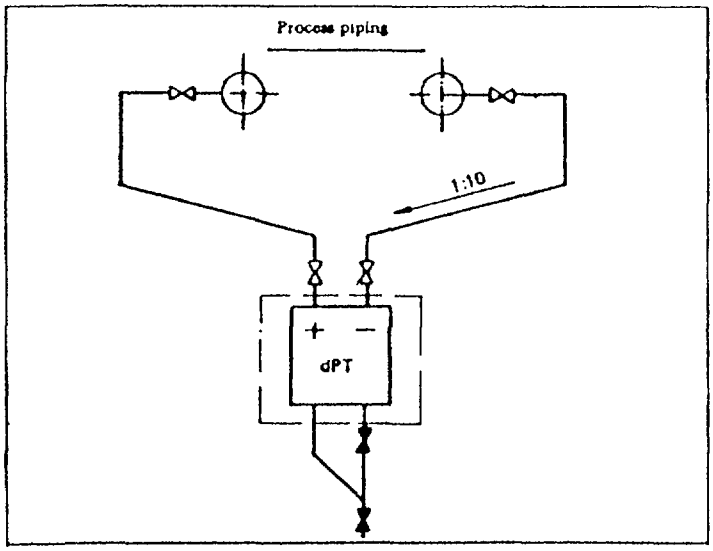

Fig. 2.4: Physical boundary of a pressure difference transmitter

2.4.5. Nuclear instrument channel

Nuclear instrument channels are a dedicated series of instrument components used to measure neutron flux. They consist of the sensor itself (e.g. ionization chamber, fission counter, self powered neutron detector) usually mounted in a guide tube and sometimes with dedicated power supplies. The signals are fed to various types of amplifiers. The boundary of a nuclear instrument channel is defined here to include the sensor, the power supply electronics and associated signal amplifiers.

3. DEFINITIONS OF COMPONENT RELATED TERMS

In probabilistic safety assessment (PSA) studies the detailed component type is the lowest hierarchial level, for which the reliability data are being provided. Components are different in size, design, characteristics, and specifications. To enable the classification of components in accordance to the PSA-study needs, the set of definitions of related terms (piece part, subcomponent, component, subsystem, system, item, equipment, device, set, assembly, element,...) is provided.

3.1. Piece Part

A piece part is the most fundamental component. It is defined as the lowest level of assembly, manufactured in accordance to engineering design drawings, and consisting of mainly one single material (aluminum, stainless steel, ceramic, plastic,...) sometimes with surface treatment and other minor details on it.

Examples of piece parts are:

(mechanical):	screw, spring, gasket, weld joint, seal, bearing, nut, bolt,...
(electro-mechanical):	winding of a relay, contact bin in a connector,....
(electrical):	graphite brush in a motor,...
(electronic):	jumper, wrapping post, printed board with no components on it,...
(sensor):	insulator ceramic in an ionization chamber,...

3.2. Component

A component is usually assembled from one or more piece parts. It is generally an off-the-shelf item procured by the system designer as a basic building block. It is that entity of hardware for which failure data are most generally collected and expected to be available. There are single part and multi part components:

3.2.1. Single part component

A single part component is a compact component which cannot be taken apart without destroying it, which would then prevent it from functioning in the required manner. This kind of subcomponent should be distinguished from typical piece parts as defined previously.

Examples of single part components are:

(mechanical):	vibration absorber, gridplate,...
(electro-mechanical):	hermetically sealed crystal can relay, small synchro motor, magnet valve, connector, switch...
(electrical):	fuse, lamp-bulb, ground fault circuit interrupter,...

(electronic): resistor, capacitor, diode, transistor, amplifier-chip,vacuum tube,...
(sensor): conductivity probe, fission chamber, self powered neutron detector,...

3.2.2. Multi-part component

A multi-part component consists of many items, single part components, or even other components and can be dismantled, repaired, serviced, examined, and recomposed without disabling its function. PSA-studies in general deal only with this multi-part components.

Examples of components are:

(mechanical): motor operated valve, pneumatic cylinder,...
(electro-mechanical): pump with transmission and motor, motor with gear, switch,...
(electrical): meter, transformer, battery,...
(electronic): power supply unit, amplifier and/or comparator module, counter/timer unit, digital indicator, fully assembled printed circuit board,...
(sensor): resistance temperature detector (RTD) with transmitter,...

3.3. Subsystem

A subsystem is a group of adjacent components which perform a specific task in a system.

Examples of subsystems are:
- Temperature control subsystem of main cooling system
- Electric starting system for diesel generator

3.4. System

A system is a collection of several components arranged to obtain a specified desired function. In general the system consists of a number of components and their associated control, auxiliary systems, and related protective devices.

Examples of systems are:

(mechanical): Ventilation system, pneumatic transfer system, movable reactor bridge, crane, beam port plug, primary coolant circuit, emergency cooling system, cooling tower,...

(electro-mechanical): control rod drive,...

(electrical): in-house power distribution, emergency lighting, star-delta connection,...

(electronic): reactor protection system, containment ventilation control,...

(sensor): logarithmic neutron flux channel with period meter, primary flow rate measurement system,...

4. DEFINITIONS OF OPERATIONAL RELATED TERMS

Operational related terms define the functional status of a component, a group of redundant components or a system during standby or operational periods.

4.1. Operation

4.1.1. Running

In general a running component is one which operates continually during the period of normal reactor operation.

Example: A centrifugal pump which runs during the period of reactor power operation is considered as a running component.

4.1.2. Functioning

As long as static components perform their specified purpose during the entire period of reactor operation, the operation mode is called "functioning".

Example: Nuclear instrument channel which operates during the normal reactor operation period, are considered as functioning.

4.1.3. Alternating (Periodic) operation

An alternating (periodically) operated component is defined as an item which periodically changes between standby and running operational modes.

Example: Air or gas compressors which operate according the consumption of the compressed gas, operate alternately between running and standby modes.

4.2. Standby

Any component or system which is not operating during normal reactor operation intended to change into running operation, upon demand is defined as a standby component or standby system. In general all standby components are required to operate in the event of a failure on a redundant component.

Standby, redundant components are frequently used to improve system reliability and availability. In case of failure of an operating component a standby component is (automatically) put into operation so that the operation of the system, containing redundant components, is not interrupted.

5. FAULT CLASSIFICATION AND DEFINITIONS OF FAILURE RELATED TERMS

5.1. Fault

A fault is any undesired state of a component or system.

Note: A fault does not necessarily imply a failure: for example, a pump may not start when required because its feeder breaker was inadvertently left open - a command fault.

5.2. Failure

A failure is defined as the loss of the ability of an item, a component or a system to perform its required function.

A failure is generally a subset of a fault. It represents an irreversible state of an item, a component or a system, such that it must be replaced or repaired in order to perform its design function. An item or component failure is always defined in relation to the system in which the item or component resides. For example, while a leak from the pipe might be considered as a system failure, a leak may be considered as a normal, or even required, state of a pump (pump packing gland leakage).

Failures can be divided into announced or unannounced failures by detection, into primary or secondary failures by induced cause, and into catastrophic, degraded or incipient by degree of damage.

The following subgroups of failures are representative for PSA studies for research reactors:

5.2.1. Announced (or revealed) failure

An announced failure (revealed or detected) is a failure which is detected at the instant, immediately after its occurrence. This type of failure is also named detected failure when it was discovered immediately after its occurrence.

Examples: fuse blown - fault signal recognized,
voltage drop - channel fault annunciated,...

5.2.2. Unannounced (or unrevealed) failure

An unannounced failure (unrevealed or undetected) is a failure which is not detected until the next test or demand occurs.

Examples: stand by dc-motor graphite brush broken,
connector on a dormant system: contact failure,
lamp bulb burns out,...

5.2.3. Primary failure

A primary failure is a so-called random failure. It does not result from external causes and it is considered to be independent.

Examples: failure on the isolation of an electro-motor,
pipe broken because of a welding defect,...

5.2.4. Secondary failure

A secondary failure occurs when a component is subjected to conditions which exceed its design specifications.

Examples: excessive voltage, high pressure, shock, vibration, high temperature, radiation,...

5.2.5. Common cause failure

Common cause failures affect multiple components, which may or may not be redundant and are caused by simultaneous failure of redundant components or by failure of some common influence such as a common support system, common location, etc. The common cause events that cause multiple failures are usually secondary events, or events which exceed the design envelope of the defective components, although in some cases failures of multiple components may be caused by similar manufacturing defects etc.

5.3. Failure unit classification

In general two failure categories are relevant in mathematical models for PSA studies: time related failures and failures on demand.

5.3.1. Time related failure

A time related failure is defined as a failure occurrence (e.g. per hour) of a component or system which is in the running or functioning mode of operation continuous operation (or function).

Example: A centrifugal pump fails to continue running

5.3.2. Failure on demand

A failure on demand is defined as a failure occurrence of a component or system when it is demanded to start operation or to change its present state.

Example: Motor driven valve fails to open/close when this is demanded.

5.4. Failure severity

Three types of failures severity are usually distinguished: catastrophic, degraded, and incipient. However, the PSA data base will usually contain catastrophic failures only, since other types of failures, not resulting in complete loss of a component's function are not as relevant and also usually poorly documented.

5.4.1. Catastrophic

The failure severity catastrophic (or critical) describes a failure which is both sudden and complete.

A catastrophic failure causes termination of one or more component's functions. Corrective action is required to restore component's function.

Examples of catastrophic failures are:

(mechanical): spring broken, welding in the primary cooling system broken
(electro-mechanical): relay of the reactor protection system failed,...
(electrical): reactor instrumentation power supply - fuse blown,...
(electronic): diode destroyed, thyristor breakdown,...
(sensors): thermocouple broken, ionization chamber short circuit,...

Note: The term "catastrophic" (critical) is only related to the system, component or item which failed. It has no direct relation to the status of the research reactor facility.

5.4.2. Degraded

The failure severity degraded describes a failure which is both gradual and partial. The equipment in question is still working but certain characteristics, which are not critical in respect to the main function of the component, have degraded.

The degraded operation of an item or system does not cease all its functions but compromises at least one specified function. The function may be compromised by any combination of reduced, increased or erratic outputs. In time, such a failure may develop into a complete (critical) failure.

Examples of degraded failure types:

(mechanical):	external leakage on the seal of a rotating pump, valve cannot fully open,...
(electro-mechanical):	control rod moves too slow,...
(electrical):	control rod magnet needs much more current as nominal,...
(electronic):	log. amplifier mis-calibrated,...
(sensors):	Geiger-Müller counter pulse pile-up,...

5.4.3. Incipient

The failure severity incipient describes an imperfection in the state or condition of an item, component, or system such that a degraded or catastrophic failure is imminent if corrective action is not taken.

Examples of incipient failure mode types:

(mechanical):	humidity in a gearbox, cracked welding,...
(electro-mechanical):	dust protection cap of a relay missing,...
(electrical):	lamp holder slightly defective so that the lamp replacement is difficult,...
(electronic):	resistor overheated - brown, ...
(sensors):	sensor housing corroded,...

5.5. Failure cause

The failure cause of a component or system is defined as an initiating event or a sequence of such events which prevent the component or system to perform its intended function.

The causes of a failure are the circumstances that activate or induce the failure mechanism. The so-called root cause of a system or a component failure may be located at some lower level subcomponent or piece part. In many cases, however, it will not be further evaluated. For reliability analysis purposes, information on the causes of a component or system failure is of qualitative significance only. Such information is useful for component/system design activities, repair strategies and for determining the common cause potential.

Examples: insufficient cooling, unsuitable ambient atmosphere, high gamma-radiation, vibration,...

5.6. Failure mechanism

The failure mechanism is defined as the mechanical, physical, chemical or other process which results in failure of an item, a component, or a system.

The failure mechanism is a process which changes the physical and/or functional characteristic of materials in a failed item. This involves the sequence of mechanical, electrical, physical, or chemical processes or a combination of these, which occur during the period in which the failed item changes from an operational (or standby) state to a failed state.

Examples: overheating, corrosion, ageing, radiation damage, mechanical stress, gas decomposition,...

5.7. Failure mode

A failure mode is the way in which an item, component or system ceases to perform its designated function. In other words it is a description of the failure which identifies that the functional requirements are no longer being met.

About 100 different failure modes were identified in different reliability data sources compiled in the IAEA-TECDOC-478, /2/. Such a high number of failure modes makes any failure rate comparison difficult and sometimes impossible. Therefore, a set of "generic failure modes" has been defined, covering practically all component failure modes accounted for in PSA-studies.

Each failure in a research reactor facility can be classified in one of these generic failure modes. The generic failure mode describes what the research reactor operator recognizes in case of a failure of a certain component or system. On the other hand, the failure mode of a component is being used to classify raw data for their use in reliability models. Therefore, data processing must clearly distinguish between the different failure modes observed. While failure causes or failure mechanisms are of concern to the component designer or repair specialist, failure modes are of interest to the system designer and the fault tree analyst.

6. DEFINITIONS RELATED TO THE FAILURE RATE

6.1. Failure rate

The failure rate is a numerical value which represents the probability of specified failures of a component per time unit. The all modes failure rate of a component is an aggregate of failure rates summed over relevant failure modes.

The failure rate $\lambda(t)$ of a system, subsystem or component is defined as

$$\lambda(t) = \frac{f(t)}{1 - F(t)}$$

where

f(t) ... the probability density for a failure of the device
1-F(t).. the probability that the device did not fail up to the time t

For many devices, the behavior of $\lambda(t)$ follows the classic bathtub curve: early in life the failure rate for such a device is high because of "wear-in failures" or failures arising due to poor quality assurance during manufacturing or installation. During the middle of the lifetime, failures occur at a rather uniform rate corresponding to random failures. Finally, late in life, $\lambda(t)$ begins to increase because of "wear-out failures".

6.1.1. Time related failure rates

Two time related failure rates are defined:

- Operating failure rate
- Standby failure rate

The failure rate for continuously operated equipment (called operating failure rate) is the expected number of failures of a given type in a given time interval (failures per hour, per year) - while the equipment is continuously in use.

Examples of failure rates of continuously operated components:

(electronic):	capacitor short circuit failures per million operating hours while under nominal voltage
(sensors):	self-powered neutron detector degraded current output failure per thousand full power days

The standby failure rate is the expected number of failures per time unit for those components which are normally dormant or in a standby state until tested or required to operate. Data representing standby failure rates is often not available in practice.

6.1.2. Failure on demand

Failures on demand is relevant to failures occurring on periodically or cyclically operated equipment. Failure on demand is the expected number of failures of a given type during a given number of operating cycles on demand when required to start, change state, or function.

Example of failure rates of demand operated components:

(electro-mechanical): relay contact failure per million switching cycles

6.2. Environmental conditions

In general, the failure rate of equipment depends on the environmental conditions. Therefore, these circumstances should ideally be taken into consideration in all data acquisition activities. However few data bases provide the environmental application factors needed to do this and they are generally only available for electrical and electronic components /6/.

The environmental application factor is a multiplicative constant used to modify a failure rate to incorporate the effects of other normal and abnormal environmental operating conditions.

Generic abnormal environmental conditions are:

(mechanical):	impact, vibration, high pressure, stress, grit, moisture,...
(thermal):	overtemperature, freezing, humidity,...
(electrical):	electromagnetic interference, contact with conducting medium, power surge voltage or current, short circuit,...
(radiation):	radiation damage, insulation failures, gamma heating, neutron activation,...
(chemical):	acidic corrosion, oxidation, chemical reactions, poisonous gases,...
(human-interaction):	students in the control room,...
(others):	missile hazards, explosion,...

7. DEFINITIONS RELATED TO THE CALCULATION OF RELIABILITY PARAMETERS

7.1. Operating time

The operating time is the accumulated time period during which an item, component or a system performs its intended function within specified limits.

7.2. Standby time

The standby time is the accumulated time period during which an item, a component or a system performs its intended function as standby equipment.

7.3. Outage time

The outage time is the time when equipment is not available for its specified service due to failure or maintenance. Outage times can be divided into three categories; out of service, restoration and repair.

7.3.1. Out of service time

The out of service time is the time required to identify the failure, analyze it, obtain spare parts, repair, and return the equipment to service, including planned delays.

7.3.2. Restoration time

The restoration time is the time period from the moment the failure is revealed to full restoration to operable state. It is the same as out of service time except that planned delays are excluded.

7.3.3. Repair time

The repair time is the time from when the failure is revealed, and includes the time to analyze the failure, prepare for repair, repair, test, qualify, and return the equipment to service. The repair time is, therefore, the time necessary to repair the equipment and restore it to operation or standby (this excludes all planned delays and waiting for spare parts and tools). The repair time is the same as the out of service time except for spare part waiting.

7.3.4. Active repair time

The active repair time is the time which is actually spent for the repair of an equipment.

7.3.5. Maintenance time

The maintenance time is defined as the time required to plan, administrate, and prepare for test or inspection, test or inspect, and return the component back to service.

7.3.6. Active maintenance time

The active maintenance time is the time spent for the maintenance (test, inspection,...) itself.

7.4. Population

The population is the total number of components which are observed.

8. FAILURE EVENT CHARACTERISTICS

Failures of a piece of hardware may be defined in functional terms as: the loss of ability to perform required functions. Failures of equipment may be defined technically in terms of definitive specification-parameters which were not met during established tests or inspections. Failures of complex systems may be defined in terms of system functions which are disabled or degraded by the failure. These failures may also be defined in terms of the degradation or loss of specific functions by the subsystem in which the failure occurred. In tracing a system failure to the lowest level of assembly or part involved in the failure event there will often be a chain of interrelated failure events - each of which had an effect upon another element in the chain.

8.1. Failure tracing

Failure tracing can be done through a cause-effect chain from the root cause of the failure to the failure effect on affected system. In general, failure tracing systems show a primary, independent root cause failure which initiated a series of events leading to the failure of the system. As a consequence of that primary failure one or more secondary failures are triggered. These dependent or contributing failures are directly or indirectly caused by the root-cause failure.

When discussing failure tracing it may be helpful to characterize failure causes as root-causes, contributing causes and immediate (direct) causes. A root-cause can be characterized as the basic or fundamental cause of a failure. Contributing causes follow root causes and lead up to an immediate cause. The immediate cause is what the failure mode precedes. Typical failure tracing is shown in figure 8.1.

8.2. Failure effects

The effects of a failure within a system may be propagated to higher and lower levels of assembly. But there exists a system design which prevent such propagation. For the discussion on the interrelation of failure modes and failure effects see NUREG/CR 2300, /7/.

In a typical system, failure of a piece part affects the function of the next higher level multipart component of which it is a part. This effect also initiates a failure mode at this level, and in turn becomes a failure mode at the next level, the subsystem and so on. Therefore, as failure modes and failure effects occur at successively higher levels, each failure effect may give rise to a new failure mode.

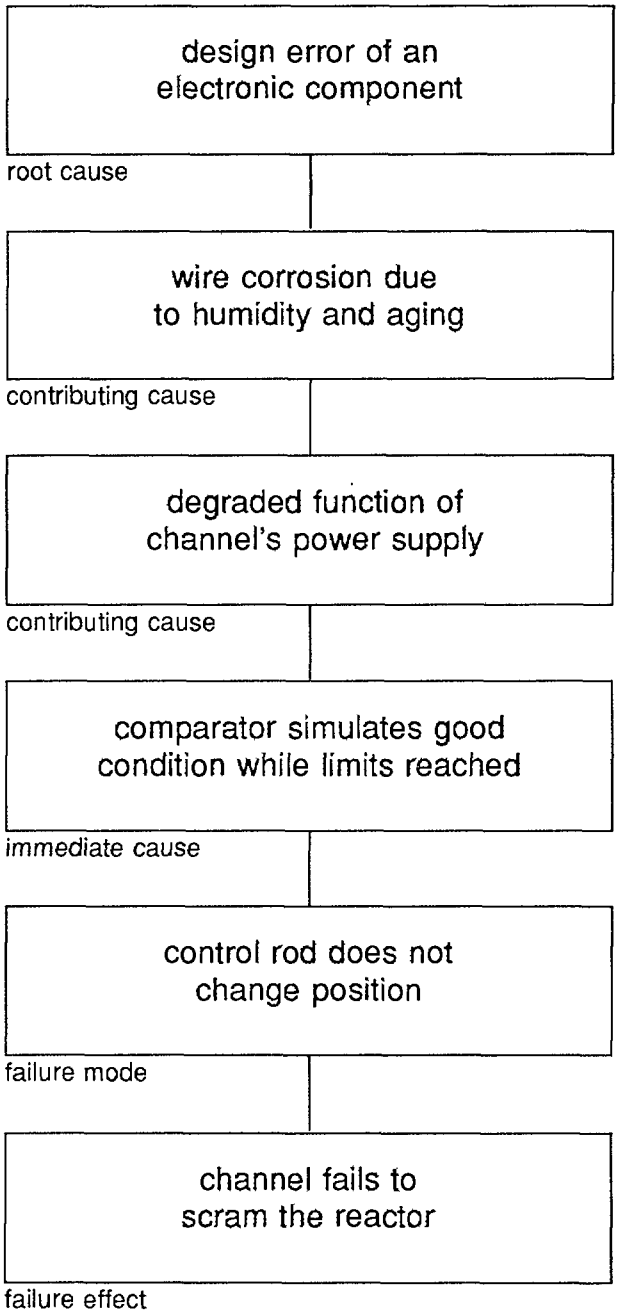

Fig.8.1.: Failure tracing; the example describes a defective filter capacitor in the power supply unit of a safety channel.

9. DATA ANALYSIS

9.1. Failure rate estimations

The raw failure data collected is analyzed to provide the various reliability parameters, as described below:

9.1.1. Failure rates

This parameter is applicable to components in an operating or running condition. In most cases, components are assumed to be in the useful life phase (i.e. having a time independent failure rate), that is, wear in, or wear out failures, which are time dependent are not included. In practice however it is not always possible to distinguish between these different phases.
All failures are therefore assumed to be time independent and the average failure rate λ is given by:

$$\lambda = \frac{n}{T} \qquad (1)$$

Where

- λ .... the total failure rate in occurrences per component operating time (i.e. hours)
- n .... the total number of observed failures of the component type
- T .... the total component operating time (i.e. hours).

For zero failures the average failure rate λ_0 is calculated as:

$$\lambda_0 = \frac{\chi^2(0.5,2)}{2T} \qquad (2)$$

Where χ^2 is the chi-square distribution, 50th percentile with 2 degrees of freedom, /8/.
Calculation of the associated confidence limits for λ is discussed in the Appendix D.

9.1.2. Failures per demand

As noted under section 6.1.2 this parameter is applied to components, usually in a standby operating mode, subject to periodic demands to start, change state or to function. The parameter, also termed the unavailability, is made up of two components called the demand unavailability Q_d and the standby unavailability Q_s respectively. The demand unavailability is given by:

$$Q_d = \frac{n_d}{d} \tag{3}$$

n_d ... the total number of observed failures to start, change state or to function on demand of the component

d .... number of demands, changes of state or functions.

For zero failures the calculation is the same as equation 2 with T being replaced by d.
For a standby component, the unavailability also depends, as well as on the number of demands, upon the time interval between testing or operation. This contribution to overall unavailability, due to testing, is called the standby unavailability Q_s. This is given by:

$$Q_s = \frac{\lambda_s / T_T}{2} \tag{4}$$

where

λ_s ... the standby failure rate in the dormant mode

T_T ... the average time between consecutive demands or tests on the component.

In practice however it is rare that standby failure rates λ_s are available. The factor of 2 indicates that, on average, the component is likely be in a failed state equal to half the average demand/test interval. The two unavailability contributions of equations (3) and (4) together are combined to provide the total unavailability (failures per demand) $Q = Q_d + Q_s$, of a standby component.

The use of Q, the failure on demand parameter, should be used with caution as the data base component test time may not correspond to that being used by the analyst. For the analyst to correct for this requires the data base to supply Q_d, λ_s and T_T, for a correction to be applied.

In the event that the data base does not supply the relevant test time T_T there will be an unknown uncertainty associated with the use of the data, quoted as failures per demand Q, as it may actually represent Q_d or $Q_d + Q_s$ and this should be recognized by the user.

Calculation of the associated confidence limits is discussed in the Appendix D /9/.

9.1.3. Mean time to repair, MTTR

The MTTR is calculated from:

$$MTTR = \frac{t_1 + t_2 + t_i + \ldots t_k}{k} \tag{5}$$

where t_i is the observed repair time of the ith failure and k is the number of failures for which the repair times were recorded.

9.1.4. Error factor

The error factor, EF represents a quantitative measure of the uncertainty associated with failure rates for different components and their failure modes.

Error factors are used in PSA for uncertainty analysis and defined here for the failure rates and failures per demand respectively as the ratio of the 95 percentile, λ_{95} or n_{d95} to the average failure rate λ or average number of demands n_d.

$$\text{EF (failure rates)} = \lambda_{95}/\lambda$$

or

$$\text{EF (failures per demand)} = n_{d95}/n_d$$

The calculation of λ_{95} and n_{d95} is discussed in Appendix D.

9.2. Failure rate scatter plots

Even when the data are collected in accordance with strict definitions and rules, and analyzed using the same statistical methods, reliability data for similar components may vary due to causes like design of a component, operating mode, maintenance practice etc. One of the ways to compare data in order to select the most appropriate ones for particular analysis is graphical presentation-scatter plots. By plotting the data points including uncertainty bounds for similar components and failure modes, ranges of data could be easily recognized. This approach in data presentation was utilized in the IAEA's TECDOC 508 "Survey of ranges of reliability data for PSA" /10/. As this type of presentation of data combing from multiple data sources has shown its obvious advantages, one of the scatter plots from TECDOC 508 is being reproduced here.

Figure 9.1 represent a scatter plot for normally standby motor driven pump, failing to start. 9 data points presented at the plot are representing 9 distinctive groups of motor driven pumps (different type,location,system etc). Most of the data points are plant specific. Some of the data points only median value is indicated, while for others mean, 95th and 5th percentile of the distribution is plotted.

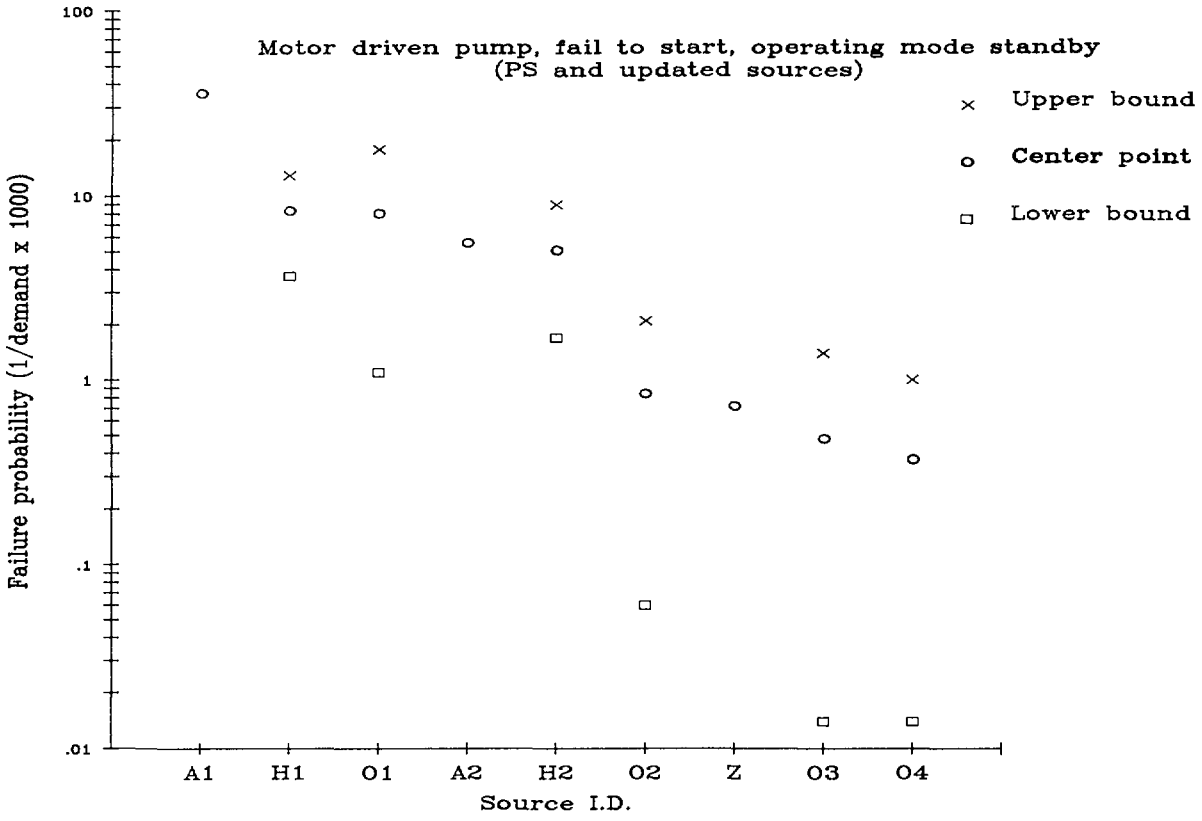

Fig. 9.1.: Example for a failure rate scatter plot

10. SPECIFIC DEFINITION OF GENERIC FAILURE MODES FOR RESEARCH REACTORS

These definitions are essentially the same as the generic failure modes for power plants, published in IAEA-TECDOC-478, /2/. The generic failure modes cover:

- safety related components
- non-safety related components and
- research reactor specific components

For each of the generic failure modes a detailed definition and an area of applicability for research facilities is provided. The effects of the observed failure and the failure mode code, used in data acquisition, complete the definitions. To facilitate the application of definitions in data acquisition work, examples are given for different research reactors (TRIGA, MTR, heavy water moderated - D_2O, WWR). A short description of research reactor types is given in Appendix A. Further details can be found in /11/.

Summary of failure mode codes:

Code	Failure Mode
B	Degraded
C	Failure to change position
D	Failure to remain in position
E	Failure to close
O	Failure to open
F	Failure to function
G	Short to ground
H	Short circuit
I	Open circuit
Q	Plug
K	Spurious function
R	Failure to run
S	Failure to start
X	Other critical Faults
Y	Leakage
J	Rupture
M	Control rod failure

10.1. Degraded

Description: Failure which causes the component not to perform its function in the expected manner, or the expected (designed) capacity but, which is not a catastrophic failure. This failure mode describes immediate as well as drift failures.

Applicability: Usually pertinent to instrumentation and control components, but not only.

Characteristic: Time related failure

Operation mode: Running, functioning or standby

Consequences: Degraded function

Failure mode code: B

General examples:
- temperature drift on logarithmic amplifier module in the reactor instrumentation
- ion exchanger in the purification circuit exhausted
- radiation monitor defective
- flow meter indicates for example 20% less flow as the real value
- reduction of battery capacity
- reduction of insulation resistance in an ionization chamber

TRIGA-examples:
- drift in compensation voltage supply for a compensated ionization chamber, low flow rate in the purification system,...

MTR-examples:
- decreasing of water level in comparing tanks, burn-up of uranium in fission counters,...
- decreasing of heat exchanger capability due to sand,

D2O-examples:
- butterfly valve in containment isolation system closes but does not fully seat (leak rate of up to 100 times building nominal leak rate may result but leakage far less severe than failure to close mode), emergency core cooling system pump works but at a lower than expected capacity due to partial blockage by debris,...

WWR-examples:
- indicator failure, filters fouling in purification circuit,...

10.2. Failure to change position

Description: Characterizes failure of components to move to a new required position.

Applicability: Usually pertains to components which perform their function by changing (moving) between discrete states (valves, breakers) or changing their state discretely, step by step, between several points (for example motor driven regulating valve).

Applicable to components which perform their function by moving from one state to the other but limited to the situations where the required final state is irrelevant or characterized by other means, or not defined.

Characteristics: Demand related failure

Operation mode: Functioning, periodical, alternating, or standby

Consequences: Failure to change state with command.

Failure mode code: C

General examples:

- one of six water level indicator stacks, fission chamber does not move in the middle of three positions
- flow rate regulating valve fails to change position (stacks due to corrosion)

TRIGA-examples:

- recorder stucks at a certain power level, transient rod shock absorber does not move into desired position,...
- frozen water level regulator in cooling tower
- flaps malfunction due to gear defect

D2O-examples:

- safety rod stuck in withdrawn position,...

WWR-examples:

- regulating unit sticks in intermediate position without further movement, fission chamber does not reach the working position, cart and shielding of the thermal column -sticks in intermediate position,...

10.3. Failure to remain in position

Description: Characterizes failures of components to remain in the required position.

Applicability: Usually pertinent to components which perform their function by changing state between two discrete states (valves, breakers, relay), or change state while regulating between two end points.

Typically used for two-state components which are required to remain in position during a mission time.

Characteristics: Time related

Operation mode: Periodical, alternating, functioning or standby.

Consequences: Change of state without command.

Failure mode code: D

General examples:

- flaps do not hold in closed position (normal operation, primary coolant flow at nominal level)
- pneumatic beam port mechanism moves without command in the opposite position
- contact in relay or breaker fails to remain closed

TRIGA-examples:

- motor operated valve in the secondary cooling circuit does not remain in position,...

D2O-examples:

- secondary circulator electrical contact does not remain closed (secondary circulator operates during normal operation and is required to continue to operate for some time after shutdown),...

WWR-examples:

- valve fails to remain in position during its mission time, beam port plug mechanism moves spontaneously due to a defect in the control unit,...

10.4. Failure to close

Description: Characterizes failures of a component to move to a new, closed position.
Subset of failure mode: fails to change position.

Applicability: Used for components which perform their function by moving from one state to another, but its definitive closing is necessary to complete the mission.

Characteristics: Demand related failure

Operation mode: Functioning or standby

Consequences: Failure to change state with command.

Failure mode code: E

General examples:
- motor driven valve cannot be closed
- beam port mechanism does not close
- security door remains open,...

TRIGA-examples:
- water filled beam port shutter fails to close because of loss of water
- fuel handling tool does not close properly
- shielding door of the thermal column cannot be closed completely,...

MTR-examples:
- pneumatically driven reactor hall entrance door does not close when requested,...

D2O-examples:
- containment isolation system butterfly valve remains open

WWR-examples:
- motor driven shielding gate fails to close at demand
- valve in the airway piping system fails to close...

10.5. Failure to open

Description: Characterizes the failures of a component to move to a new, open position.
Subset of failure mode: fail to change position.

Applicability: Used for components which perform their function by moving from one state to another when opening is necessary to complete mission.

Characteristics: Demand related failure.

Operation mode: Functioning or standby

Consequences: Failure to change state with command.

Failure mode code: O

General examples:
- emergency cooling valve remain closed, overpressure relief valve does not open at nominal overpressure,...

TRIGA-examples:
- thermal column door fails to open
- magnetic valve for the transient rod drive mechanism fails to open,...

MTR-examples:
- fire exit fails to open on demand,...

D2O-examples:
- guard line relay remains closed following de-energization,...

WWR-examples:
- valve (magnetic or motor driven) fails to open
- accident shower valve fails to open
- fresh air inlet valve fails to open at demand,...

10.6. Failure to function

Description: One of the general failure modes, applicable mainly to components which do not move (macroscopically) to perform their function, (battery, transformer, instrumentation and control equipment) or which have a complex function such as air-coolers, thyristors converters, etc. Failure to run does not adequately characterize the component failure mode in these cases.

Characterizes the failure of components to function in required manner either continuously or on demand.

Applicability: Used for components which perform their function without movement on a macroscopic level, and for components which are characterized by providing output given an input or a command (continuously in time).

This failure mode is also applicable (and being used) as a composite failure mode for a pump not able to perform its function (pump fails to start, run, or fails to accomplish the mission for any other reason)

Characteristics: Time related failure (operational or standby)

Operation mode: Functioning or standby but not running

Consequences: Loss of function of the component.

Failure mode code: F

General examples:
- electronic power supply or high voltage supply no output
- primary pump speed control (thyristor converter) out of order
- transmitter output remains constant regardless of the input signal,...
- incorrect calibration of indicator devices

TRIGA-examples:
- primary pump fails to function
- blower in the ventilation system fails to function,...

MTR-examples:
- period meter trip signal prevented due to complex electronic failure
- computation module does not change the output any more,...

D2O-examples:

- space conditioner system unable to provide cooling for duration of emergency,...

WWR-examples:

- ionization chamber fails to function due to decrease of the resistance of insulation
- rectifier (transformer,...) fails to function during its mission time,...
- acid leak or cracked pole connections on a battery

10.7. Short to ground

Description: Characterizes ground connections of any electrical component where electric current is isolated on a higher-than-ground voltage. Subset of failure mode short circuit.

Applicability: Applicable to all electrical, instrumentation, or control components which in any way conduct, transfer or modify electrical currents.

Used for components which are unable to perform their function or can cause disturbance to other equipment when isolation to ground is broken and a power to ground circuit is formed.

Characteristics: Time related failure

Operation mode: Running, functioning, or standby

Consequences: Loss of function of component.

Failure mode code: G

General examples:
- isolation defect on the HV-cable of the ionization chamber in the safety channel

TRIGA-examples:
- high voltage supply for the ionization chamber short to ground
- thermocouple for fuel temperature measurements short to ground,...

MTR-examples:
- cable isolation defect due to high gamma irradiation and humidity leads to short to ground,...

D2O-examples:
- terminals of emergency core cooling pump motor short to ground (possibly due to excessive moisture in plant room during LOCA,...

WWR-examples:
- battery short to ground due to isolation defect
- bus bars in power supply system have contact to ground

10.8. Short circuit

Description: Characterize connections between two or more conductors (or conducting materials) which are normally insulated.

Applicability: Applicable to practically all electrical, instrumentation and control components.

Used for components which are unable to perform their function, or cause disturbance to other equipment when insulation between two normally separated conductors disappear and a short circuit is formed.

Characteristics: Time related failure

Operation mode: Running, functioning or standby.

Consequences: Loss of function of the component.

Failure mode code: H

General examples:
- line to line fault in a distribution board, isolation defects

TRIGA-examples:
- inner connector defects at connectors related to radiation monitoring instruments,...

MTR-examples:
- short circuit due to an overheated indicator lamp in the ventilation control unit,...

D2O-examples:
- connection made across pins on a relay base or across a guard line terminal board

WWR-examples:
- failures in contact disconnections of relays or actuators,...
- bus bars in the mains power supply system short between two of the three phases
- short circuit in a battery cell
- puncture in a transformer winding

10.9. Open circuit

Description: Characterizes disconnection (insulation) of an electrical circuit. Opposite from short circuit.

Applicability: Applicable to practically all electrical, instrumentation, and control components.
Used for components which are disabled to perform their function when electric conductor becomes internally insulated.

Characteristics: Time related failure

Operation mode: Running, functioning or standby.

Consequences: Loss of function of component.

Failure mode code: I

General examples:
- connector defective, relay broken, thermocouple defect,...

TRIGA-examples:
- fuel temperature thermocouple broken, coaxial cable defect: inner conductor torn,...

D2O-examples:
- power supply connection to emergency core cooling pump open circuit (may be due to nuts in the terminal box vibrating loose and arcing causing failure of connection,...)

WWR-examples:
- Pt-100 sensor broken
- loss of contact connection at reactor protection relay
- bus bar loose contact due to un-tightened bolts

10.10. Plug

Description: Characterizes any means of preventing flow in a required direction not caused by normal operation of component.

Applicability: Applicable to most of the components through which of liquid/steam/gas flow is established or maintained. It is of particular interest to components whose internal parts can become loose and prevent normal flow (valves, pipes, tubes,...) or depositions can reduce flow below required level (filter, strainers, sieves,...).

Characteristics: Time related failure

Operation mode: Running, functioning, or standby

Consequences: Change of state without command, partial loss of function

Failure mode code: Q

General examples:
- purification system blocked

TRIGA-examples:
- plugging of filters in the purification loop, ventilation system filters plugged, aerosol monitor: filter plugged,...

MTR-examples:
- irradiation sample stacks in transfer tube
- partial blockage of the down-streaming coolant through the core,...

D2O-examples:
- pressure tapping line blocked (e.g. crud deposited in level sensing line)

WWR-examples:
- clogging of the purification circuit filter,

10.11. Spurious Function

Description: Characterizes failure of components to retain their current status, e.g. to change state without being called to. Complement to failure to remain in position.

Applicability: Applicable to components which perform their function by means other than by changing state between two distinctive states.

Used for components which perform their function by being in a certain (usually dormant) state, but failure will cause changing state (operation of component).

Characteristics: Time related failure

Operation mode: Running, functioning, or standby

Consequences: Change of state without command or as a consequence of external interference (electromagnetic noise).

Failure mode code: K

General examples:
- Spurious alarm on the radiation monitoring system

TRIGA-examples:
- Pulse rod drops down because of air pressure loss
- spurious interruption of circuit breaker

MTR-examples:
- Reactor scram because of a very short (150ms) line interruption (drop down)

D2O-examples:
- stand-by ventilation valve opens during building seal

WWR-examples:
- reactor scram due to malfunction of the reactor control system (e.g. period meter)

10.12. Failure to run

Description: Characterizes failure of a component to continue operation (usually rotating movement) during the required mission time.

Applicability: Applicable to all components which perform their function by continuous movement.

Characteristics: Time related failure

Operation mode: Running, functioning, or periodical.

Consequences: Loss of function.

Failure mode code: R

General examples:
- all kind of pumps when they fail to continue operation, blower in the ventilation system terminates operation because of V-belt defect

TRIGA-examples:
- primary cooling system pump stops running
- ventilation system blower motor stops

MTR-examples:
- electrical fan on the cooling tower fails to run

D2O-examples:
- emergency core cooling pump does not complete operational mission

WWR-examples:
- DC/AC motor generator set fails to continue running

10.13. Failure to start

Description: Characterizes the failure of components to start on demand.

Applicability: Applicable to all components which perform their function by starting and subsequently continuously moving (rotating).

Characteristics: Demand related failure

Operation mode: Standby, periodical, alternating

Consequences: Loss of function of component.

Failure mode code: S

General examples:
- emergency diesel engine does not start on demand

TRIGA-examples:
- air compressor for the pulse rod does not start when required, uninterrupted power supply fails to start on demand,...

MTR-examples:
- air compressor for pneumatic control of the ventilation system fails to start
- drain water sump pump fails to start,...

WWR-examples:
- core spray pump fails to start
- emergency blower fails to start,...

10.14. Other critical faults

Description: Characterizes also the failures that would cause the component to fail to function if demanded before repair.

Applicability: Summarizes all failures not covered by any of the other failure modes. Applicable to sensors representing sensor failures discovered prior to an actual demand.

Characteristics: Time related failure and failure on demand

Operation mode: Running, functioning, or standby.

Consequences: Loss or degradation of function.

Failure mode code: X

General examples:
- fuel cladding defects, core loading failure (start-up-accident), diesel fuel contamination,...
- pipe clog in sensor for flow rate measurement device
- leakage in a self-powered detector

TRIGA-examples:
- corrosion of tank internals
- deformation or elongation of fuel elements,...

MTR-examples:
- BeO-reflector element cladding defect,...

10.15. Leakage (external leak/internal leak)

Description: Characterizes a failure of component boundary to remain intact (to retain liquid). If the component performs another function, (e. g. pump) this failure will not necessarily prevent that other function.

Applicability: Applicable to all components which retain liquid or gas by any means including failures of check valves which prevent reverse flow. Not necessarily a catastrophic component failure. This failure mode sometimes overlaps with failure mode RUPTURE. It is not possible to strictly separate these two failure modes in all cases.

Characteristics: Time related failure

Operation mode: Running, functioning, or standby

Consequences: Loss of function of component (partial).

Failure mode code: Y

General examples:
- gasket defect on a water tank
- seal defects on pumps, tubes, and valves
- welding defects on pipe
- ionization chamber container leaking

TRIGA-examples:
- pneumatic transfer system core terminal leaking
- rotary specimen rack leaking,...

MTR-examples:
- leakage in a thermal isolation tube of an in-core irradiation experiment,...

D2O-examples:
- heavy water to cooling circuit leak
- containment isolation system water seal drain line leak
- leak in the helium system of the heavy water container,...

WWR-examples:
- leakage of a water storage tank, pump packing leaking
- leak in a small tube of the cooling flow measuring system
- leakage in a transformer housing

10.16. Rupture

Description: Characterizes a large break in liquid/steam/gas retaining boundary.

Applicability: Applicable to all components which retain liquid or gas by any means. It is always a catastrophic component failure. If the component performs some other function, not only to retain liquid (pump), this failure will completely prevent the component from functioning.

Characteristics: Time related failure

Operation mode: Running, functioning, or standby.

Consequences: Loss of function of component.

Failure mode code: J

General examples:
- rupture of principal pipe in the secondary cooling circuit
- severe rupture of fuel element cladding with fission gas release,...

TRIGA-examples:
- beam tube broken (flow more than 40 l/s),

MTR-examples:
- primary coolant pipe broken (flow more than 100 l/s)

D2O-examples:
- emergency core cooling pump case fracture

WWR-examples:
- integrity loss of the reactor vessel or the heat exchanger

10.17. Control rod failure

Description: Characterizes failures on the control rod and its related drive mechanisms.

This includes: failure to insert during normal shut-down or scram, failures during moves for reactivity changes, improper rod movement, mechanical defects on the rod, plates or blades,...

Applicability: Applicable to all research reactor reactivity control systems.

Characteristics: Time related failure

Operation mode: Functioning, or standby

Consequences: Loss of function of the system, change of state without command

Failure mode code: M

General examples:
- control rod position indicator defect or misaligned,...

TRIGA-examples:
- magnet defective - sticking
- absorber part of the pulse rod broken away,...

MTR-examples:
- control rod stucks

D2O-examples:
- uninitiated control rod withdrawal
- control rod broken,...

WWR-examples:
- clutch defect on the absorber drive mechanism
- absorber part of the control rod mechanically defective,...

REFERENCES

/1/ Application of Probabilistic Risk Assessment to Research Reactors, IAEA-TECDOC-517, IAEA Vienna, 1989.

/2/ Component Reliability Data for Use in Probabilistic Safety Assessment, IAEA-TECDOC-478, IAEA Vienna, 1988.

/3/ Data Summaries of Licence Event Reports of Pumps at US Commercial Nuclear Power Plants, NUREG/CR-1205, USNRC Washington DC, 1982.

/4/ J.P.Bento et al. Reliability Data Book for Components in Swedish Nuclear Power Plants, RSK, SKI Stokholm 1985.

/5/ Winfield D.J., Diesel Generator Reliability Study 1969-1985, AECL-9387, Chalk River, 1989.

/6/ IEEE Guide to the Collection and Presentation of Electrical, Electronic and Sensing Component Reliability Data for Nuclear Power Generating Stations, IEEE Std 500-1977 and 1988.

/7/ Probabilistic Risk Assessment Procedure Guide, NUREG/CR 2300, USNRC, Washington DC, 1983.

/8/ Kapur K.C., and Lamberson L.R., Reliability in Engineering Design, John Wiley & Sons, 1977, p. 254, 375.

/9/ Lipson C., and Sheth N.J., Statistical Design and Analysis of Engineering Experiments, McGraw Hill, 1973, p.88.

/10/ Survey of Ranges of Component Reliability Data for Use in Probabilistic Safety Assessment, IAEA-TECDOC-508, IAEA Vienna, 1989.

/11/ Directory of Nuclear Research Reactors, STI/PUB/853, IAEA Vienna, 1989.

APPENDIX A
BRIEF DESCRIPTION OF RESEARCH REACTOR TYPES

TRIGA

All of the TRIGA research reactors are open pool, light-water-cooled reactors using uranium-zirconium-hydride (UZrH) fuel. This fuel provides a reactor with a large, prompt negative temperature coefficient for inherent safety against reactivity accidents. As cladding material for the 36mm thick and 720mm, long fuel rods serves aluminum or stainless steel. The enrichment of U-235 is 20% (standard) and 70% (flip). The thermal neutron flux in a central irradiation position is in the range of $10^{13}cm^{-2}s^{-1}$ at full power.

The Mark I type has a configuration in which the reactor is placed at the bottom of the open cylindrical tank with the top of the tank at grade level. No beam ports and no thermal columns are available. The reactor core is a cylindrical configuration with an annular graphite reflector. The experimental facilities include a rotary specimen rack, a central in-core irradiation thimble, and a pneumatic transfer system. The thermal power level can be up to 1 MW with natural convection cooling.

A higher level of experimental capability was added by taking this same basic reactor design and constructing it within a shield structure above the floor level, allowing horizontal access to the core. This allows the construction of radial and tangential beam tubes as well as thermal columns.

The ultimate in experimental flexibility in low-power research reactors with inherent safety is the TRIGA Mark III design. In addition to extensive beamport facilities, this type incorporates a large exposure room and a large reactor pool with a movable reactor bridge. This reactor is water reflected and operates at up to 2MW with natural convection.

MTR

A material test reactor (MTR) is a light water moderated open pool reactor with forced cooling, operated at thermal power levels up to 15 MW. The thermal neutron flux in a central irradiation position is in the range of $10^{14}cm^{-2}s^{-1}$ at full power. As reflector material, beryllium elements are often used. The standard MTR fuel element contains 23 fuel plates, 1.3mm thick, 70mm large and about 600mm high. Today three types of U-235 enrichment are used in many MTR's: high enriched (90 and 93%), medium enriched (45%), and low enriched (20%).

The grid-plate is rectangular and holds 28 to 32 fuel elements for full power operation. The forced cooling streams downward through the plate type fuel elements. Many different pool designs are in use to cover all the experimental needs.

A typical MTR is equipped with radial and tangential beam tubes, used for beam port experiments. A wide variety of in core experiments is known for that reactor family.

Typical WWR research reactors are light-water moderated and cooled (continuous forced downward circulating) facilities with light-water and/or beryllium reflector. The reactor is installed in a zylindrical tank with a heavy shielding plate at the top. Their thermal power range is up to 15MW with average flux densities of $10^{13}cm^{-2}s^{-1}$. The core contains highly enriched (80% ^{235}U) IRT-M-type fuel elements.

The grid-plate contains 52 working positions with a square lattice pitch of 71,5mm. A typical loading contains 28 to 32 fuel elements, 11 control rod elements and 10 to 15 beryllium reflector elements. The rest is used for irradiation rigs.

The standard fuel element consists of four (or three) concentric tubes (square section, 69 x 69 mm). The active fuel lenght is 580mm. The meat is an AlU-alloy with 37wt% uranium. The wall thickness is 2mm; 0.4mm meat and 0.8mm cladding.

APPENDIX B
EVENT RECORD FOR THE TRIGA REACTOR VIENNA

This is the Event Record Form which was developed to support the data collection as well as the operation and maintenance activities of the TRIGA reactor operated by Atominstitut of the Austrian University in Vienna, Austria.

Next page(s) left blank

APPENDIX C
METHODOLOGY OF DATA EVALUATION

1. INTRODUCTION

A Probabilistic Safety Assessment (PSA) study has several levels of scope of which each is different in its degree of probabilistic character. The analysis of initiating events is heavily probabilistic since it involves predicting the success or failure of so many components in a reactor such as valves, pumps, and switches. Similarly, the use of source terms is associated with probabilities to calculate the off-site consequences. However, an analysis must be done on the phenomena and consequences associated with those rare accident sequences that might lead to undesirable outcomes.

Thus a PSA study is supposed to be a common work of nuclear scientists and engineers and of probabilists and statisticians. The methodology contained in this document serves as a guideline to the needs of probability theory and selected statistical methods, which are encountered in dealing with a PSA study. First two basic approaches towards counting probabilities are distinguished. Then such fundamental principles of simple statistical inference as are confidence intervals, testing statistical hypotheses, and the maximum likelihood method are outlined and illustrated. Attention is paid to some specific probability distributions that may appear in the reliability theory. Among them the role of the exponential distribution predominates. All these specific distributions are treated in such a way that a user of this methodology can apply them in a particular situation of the work on a PSA study.

2. PROBABILITY THEORY

Uncertainty analysis in a PSA study employs the probability in that probabilities are assigned to different sizes of changes which can occur. Such analyses utilize Bayesian approaches and sometimes classical statistical approaches.

The *classical statistics approach* requires recorded data to be available for which probability distributions are constructed. The probability distributions describe the likelihood of the data occurring in a series of repeated measurements. The likelihood refers not to a degree of belief but to repeated measurements.

From the constructed probability distribution for the sample of data related to a parameter, a classical confidence interval is constructed for the unknown parameter. The confidence intervals, determined for those parameters for which there exists recorded data, are then propagated through the PRA (Probabilistic Risk Analysis). The propagation yields confidence intervals for the PRA results. The confidence intervals are discussed along with other techniques of statistical inference in the next chapter.

The basic philosophy in the *Bayesian approach* is that all quantified uncertainties can be described in terms of probability distributions. The probability distribution describes the analyst's degree of belief in the correct value a parameter may be. The probability distribution can also describe the analyst's belief that a model is the correct model from a set of possible models.

In essence, the Bayesian methodology consists of the analyst first assigning *prior* probabilities for the parameters and models utilized in a PSA study, and for which uncertainties are to be quantified. The prior probability distributions are then updated with any recorded data using *Bayes theorem*. This theorem can be written as

$$P(X_i|Z_j)= \frac{P(X_i).P(Z_j|X_i)}{P(Z_j)} \qquad i=1,2,\ldots,n;\ j=1,2,\ldots,m$$

where $P(X_i)$ are *a priori* probabilities, $P(X_i|Z_j)$ and $P(Z_j|X_i)$ are *conditional* probabilities, and $P(Z_j)$ can be computed by the formula of total probability as

$$P(Z_j)= \sum_{i=1}^{n} P(X_i),\ P(Z_j|X_i)$$

The recorded data consists of times of equipment failure, human errors committed, or other measurements related to the parameter. The updated probability distributions are *posterior* distributions and are propagated through the PSA to obtain probability distributions for the outputs.

3. STATISTICAL METHODS

3.1 The principle of confidence intervals

One of the objectives of statistical analysis of data is to estimate unknown parameters of the probability distribution in the population from which a random sample originates. For reactor data the most valuable from the

practical point of view are interval estimates (i. e., we try to find such an interval that will include the unknown value of the parameter with a probability given in advance). Such intervals are called *confidence intervals*. The probability α $(0<\alpha<1)$ is called the *confidence level*, and it represents the risk that the interval will not include the true value of the parameter. Confidence intervals can be obtained by various methods. Generally, the shortest ones are preferred.

It will be sufficient for our needs to introduce confidence intervals for the expected value in a normal distribution. Such a $100(1-\alpha)\%$ confidence interval for the true value μ of a parameter is given by the probability

$$P\left(\bar{x} - \frac{s.t_{\alpha}(n-1)}{\sqrt{n}} \leq \mu \leq \bar{x} + \frac{s.t_{\alpha}(n-1)}{\sqrt{n}}\right) = 1-\alpha$$

where $\bar{x}$ is the mean of n observations, s is their sample standard deviation, and $t_{\alpha}(n-1)$ is the critical (percentage) value of the Student distribution with $(n-1)$ degrees of freedom, which can be taken from the table of these values.

The confidence interval in question is symmetrical around $\bar{x}$, and it is the shortest one of all intervals with the given confidence level. Sometimes *one-sided* confidence intervals are more desirable. Such a $100(1-\alpha)\%$ confidence interval for the true value μ follows rom the probability

$$P\left(\bar{x} - \frac{s.t_{2\alpha}(n-1)}{\sqrt{n}} \leq \mu\right) = 1-\alpha$$

This is the lower one-sided interval. The upper one is given by

$$P\left(\bar{x} + \frac{s.t_{2\alpha}(n-1)}{\sqrt{n}} \geq \mu\right) = 1-\alpha$$

3.2 Testing statistical hypotheses

One important question is whether one parameter in a probability distribution has or has not an anticipated value (e. g., the failure rate of a component). It is then useful to formulate a hypothesis of the value of this parameter and verify it by the means of available data (a random sample). The manner of verifying a hypothesis is called a *significance test*.

If a hypothesis is of the form $\theta=\theta_0$, it is called *simple*; otherwise, it is *composite*. A test procedure simply amounts to a rule whereby each possible set of values $(x_1,x_2,\ldots,x_n)$ is associated with a decision to accept or reject the hypothesis H_0 being tested. It is obvious that errors of two kinds may be committed in applying a statistical test:

1. Errors of Type I: rejecting H_0 when it is true.
2. Errors of Type II: accepting H_0 when some other hypothesis is true.

The probability of the error of Type I is

$$\alpha=P\{(x_1,x_2,\ldots,x_n)\in w\,|\,H_0\}$$

where w is the *critical region*, i. e., the n-dimensional region of points for which H_0 is rejected. Alpha is often made equal to 0.05 or 0.01, although other values can be used. To facilitate the construction of such tests, tables have been prepared for some standard cases. The probability α is called the *significance level* of the test.

The probability of a Type II error depends on the hypothesis H that is really true. It is equal to

$$\beta=1-P\{(x_1,x_2,\ldots,x_n)\in w\,|\,H\}$$

and is called the *operating characteristic* of the test with respect to H. The complement

$$P\{(x_1,x_2,\ldots,x_n)\in w\,|\,H\}$$

is the *power* of the test with respect to H.

The decision procedure for a test of H_0 is shown in this *table of decisions and errors*:

Hypothesis H_0	Decision	
	Accept H_0	Reject H_0
Is true	Correct	α
Is false	β	Correct

We note that if H_0 is true and is accepted, the decision is correct. If it is false but is accepted, the decision produces a type II error. If H_0 is true but is rejected, a type I error arises.

By decreasing the extent of w, we reduce the significance level α. This also results in an increase in the probability of a type II error. There thus exists a conflict involving reduction of the probabilities of the first and second types of error. To resolve this conflict we try to control the significance level and, subject to this control, to minimize β.

It a hypothesis is accepted, the experimenter may still not be willing to say that it is true. What he may say is that on the prescribed significance level he has not enough evidence from the obtained data to reject the hypothesis provided that it is false.

In our problems related to reliability theory we are interested in the application of the test procedure to a hypothesis regarding the size of a parameter considered to be the *expected value* in a *normal* distribution of measurements (observations).We choose α and state the hypothesis H_0: $\mu=\mu_0$. Then the statistic

$$t = \frac{\bar{x} - \mu_0}{s} \sqrt{n}$$

might be used as a criterion where $\bar{x}$ is the mean, s is the computed standard deviation and n is the size of the random sample available. If H_0 is true, the statistic t has the *Student t-distribution* with *(n-1)* degrees of freedom.

The hypothesis H_0 will be rejected on the significance level α whenever

$$\left| \frac{\bar{x} - \mu_0}{s} \sqrt{n} \right| . > {}_{\alpha}t\ (n-1)$$

where $t_{\alpha}(n-1)$ is the *100(1-α) percentage value* of the Student distribution, if we test it against an alternative hypothesis H_1; $\mu\neq\mu_o$. This is a two-sided test. In a similar way we would get one-sided significance tests.

3.3 The maximum likelihood principle

The *maximum likelihood principle* is a general method of estimation that selects that value of a parameter θ for which the probability of obtaining a given set of data (sample values) is a maximum.

To illustrate the method of maximum likelihood, suppose that $x_1, x_2, \ldots, x_n$ is a random sample from a population having the exponential distribution and that the parameter a in the probability density

$$f(x) = \frac{1}{a} \exp\left(-\frac{x}{a}\right)$$

is to be estimated. Since the *likelihood function* is

$$L = \left(\frac{1}{a}\right)^n \exp\left(-\frac{1}{a}\sum_{i=1}^{n} x_i\right)$$

differentiating $ln\ L$ instead of L, which is the same, with respect to a and putting this derivative equal to 0 gives

$$-\frac{n}{a} + \frac{1}{a^2}\sum_{i=1}^{n} x_i = 0$$

It follows that the maximum likelihood estimator of the parameter a of an exponential population is the mean $\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$.

Maximum likelihood estimators have the *invariance property* that if $\hat{\theta}$ is a maximum likelihood estimator of θ and the function given by $g(\theta)$ is continuous, then $g(\hat{\theta})$ is also a maximum likelihood estimator of $g(\theta)$.

3.4 Some specific dostributions in the reliability theory

3.4.1 The binomial distribution

The binomial distribution is the relevant probability distribution used to describe situation where an event will produce either of two outcomes, its occurrence or a failure to occur (e. g., a diesel demand will result in a successful start or in a failure-to-start).

The binomial density function describes the probability of obtaining k failures in n trials provided that the probability of failure in an individual trial is the same for all trials and that the outcome of one trial is independent of the outcome of any other trial. It can be written as

$$P_n(X = k) = p(k) = \binom{n}{k}\theta^k(1-\theta)^{n-k} \qquad k=0,1,2,\ldots,n$$

where θ is the probability of failure in any one trial. Obviously, $p(k) > 0$. Since these probabilities appear to be members of the binomial expansion of $[\theta + (1-\theta)]^n = 1$, the distribution is called *binomial*. The combinatorial coefficient is

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

The distribution function of the binomial random variable is given by

$$F(k) = \sum_i p(i) = \sum_i \binom{n}{i} \theta^i (1-\theta)^{n-i}$$

where we sum up over all nonnegative integers less than or equal to k.

Computing the binomial probabilities does not encounter difficulties if n is small. However, for large n, either tables of combinatorial coefficients or incomplete Beta functions or an approximation must be employed.

3.4.2 The chi-square distribution

If $X_1, X_2, \ldots, X_n$ are *independent* random variables, each distributed as a *unit normal* variable N(0,1), we use the symbol X^2 *(chi-square)* to denote the sum of their squares

$$X^2 = X_1^2 + X_2^2 + \ldots + X_n^2$$

This sum of squares is distributed as

$$f(x) = \frac{1}{2^{\frac{n}{2}} \Gamma\left(\frac{n}{2}\right)} e^{-\frac{x}{2}} \cdot x^{\frac{n}{2}-1} \qquad \text{for } x \geq 0$$

The parameter n is called the *number of degrees of freedom* and it is an integer. It can be related to the number of independent quantities remaining after estimating a parameter or fitting a distribution.

The expected value is

$$E[\chi^2] = n$$

a the variance can be obtained as

$$V[\chi^2] = 2n$$

The χ^2-distribution is positively skew. The frequency curve approaches symmetry as n increases.

Percentage values $\chi^2_n(\alpha)$ of the chi-square distribution such as

$$P\left(\chi^2_n > \chi^2_n(\alpha)\right) = \alpha \qquad 0<\alpha<1$$

are tabulated for several values of α (0.1; 0.05; 0.01) in statistical textbooks.

Example:

The usual assumption is that the time to failure of items running under or in operation has an exponential distribution.

If k is the number of failures and T is the run time of the item, then the lower and upper confidence limits P_L and P_U for the failure rate can be found in terms of percentage chi- square values:

$$P_L = \frac{\chi^2_{2k}\left(\frac{\alpha}{2}\right)}{2T}$$

$$P_U = \frac{\chi^2_{2k-2}\left(1-\frac{\alpha}{2}\right)}{2T}$$

where, e. g., α = 0.10 for 90 % confidence.

3.5 The exponential distribution

3.5.1 Introduction

If a random variable X has the probability density

$$f(x) = \begin{cases} a.\exp(-ax) & \text{when } x \geq 0,\ a > 0 \\ 0 & \text{when } x < 0 \end{cases}$$

it has an *exponential distribution*. We obtain for its cumulative distribution function

$$F(x) = \int_0^x f(t)dt = \begin{cases} 0 & \text{when } x < 0 \\ 1 - \exp(-ax) & \text{when } x \geq 0 \end{cases}$$

The exponential distribution is continuous and is especially important in reliability studies. Its mean value is $1/a$ and the variance is equal to $1/a^2$. Therefore only the mean value is sufficient to specify the parameter a and, thus, the entire exponential distribution.

If X is the lifetime random variable for a component, $E[X] = 1/a$ is the mean-time-to- failure for the component. However the probability of the component suriviving until its mean- time-to-failure is not 0.5 but 0.37 because

$$P\left(X > \frac{1}{a}\right) = 1 - F\left(\frac{1}{a}\right) = 1 - \left(1 - \frac{1}{e}\right) = 0.37$$

3.5.2 Distribution of the failure time

A large number of components are placed on life test at $t = 0$. At any time each component is either failed or in the operational state. We take the failure rate H for constant.

A random variable T is defined to characterize the failure time. The event $\{T = t\}$ means that a component fails at time t. Similarty, the event $\{T \leq t\}$ implies failure before or at time t. The distribution function of T can be derived in the form

$$F(t) = 1 - \exp(-Ht)$$

provided that the probability of failure during any small interval t is H t, independent of t.

Thus, T has an exponential distribution with parameter H.

3.5.3 Lifetime random variable for a system

We deal with a system that fails when any of its constituent components fails. Its survival probability expressed in terms of the distribution function F of the system's lifetime random variable T is

$$1 - F\left(t\right) = P\left(T>t\right) = P\left(\bigcap_{k=1}^{n} T_k > t\right)$$

where T_k is the lifetime of the k -th component.

This reflects the fact that, if the minimum of the lifetimes is greater than t, then all of them must be greater than t.

It seems reasonable to assume that the probability of system survival to time t is the product of the survival probabilities of the individual components. Hence the events $\{T_k \leq t \; ; \; k = 1, 2,...,n\}$ are independent and

$$1 - F(t) = \prod_{k=1}^{n} [1 - F_k(t)] = \prod_{k=1}^{n} [\exp(-H_k t)] = \exp(-Ht)$$

where H denotes the sum of H_k. So T has an exponential distribution

$$F(t) = 1 - \exp(-Ht)$$

Example:

Let T be the lifetime (in hours) of a certain reactor component. Assume$T$ has an exponential distribution with parameter $a = 0.001$. The manufacturer wishes to guarantee these components for T_0 so that $P(T > T_0) = 0.95$.

The distribution function is given by

$$F(t) = 1 - \exp(-at)$$

for t>0, where a = 0.001. Since

$$P(T > T_0) = 1 - F(T_0) = \exp(-aT_0)$$

we choose T_0 to make $\exp(-aT_0) = 0.95$. Hence

$$T_0 = - \frac{\ln 0.95}{a} = - 1000 \ln 0.95 = 51.25$$

3.5.4 A unique property of the exponential distribution

Suppose that no failure occurs in the interval $\langle 0,t \rangle$. What is the probability of continued survival in the interval $\langle t,trs \rangle$?

This is a question in *conditional* probabilities. We wish to determine $P(T>t+s \mid T>t)$, the conditional probability that these is no failure in the interval $\langle 0,t+s \rangle$, given that there is no failure in the interval $\langle 0,t \rangle$.

From the definition of conditional probability we have

$$P(T>t+s \mid T>t) = \frac{P[(T>t+s) \cap (T>t)]}{P(T>t)} = \frac{P(T>t+s)}{P(T>t)}$$

Suppose now that $F(t)$ is an exponential distribution with parameter $a>0$. Then

$$P(T>t) = 1 - P(T \leq t) = \exp(-at)$$

$$\text{Hence} \quad P(T>t+s \mid T>t) = \frac{\exp[-a(t+s)]}{\exp(-at)} = \exp(-as) = P(T>s)$$

In other words, if the picca of equipment survives in the interval $<0,t>$, then the probability of continued surival in the interval $<t,t+s>$ is equal to the probability of survival in the interval $<0,s>$ having the same length. That is, the probability of survival depends only on the length of the time interval and not on the age of the equipment.

Expressed in terms of the distribution function F, the property states that

$$\frac{1 - F(t+s)}{1 - F(t)} = 1 - F(s) \qquad \text{for all } t>0,\ s>0$$

It can be shown in the Probability Theory that exponential distributions are the only probability distributions with this property.

3.5.5 A standby - redundant system

We are concerned with a system containing standby redundancy, which is one way to increase reliability. Each component in such a system operates continuously until it fails. The failure is sensed and a standby component rreplaces the failed component immediately and automatically.

The failure time of the original component is represented by the random variable T_0, while the failure time for the standby component is describeed by T_1. Their marginal probability densities are the exponential distributions (k = 0,1)

$$f(t_k) = \begin{cases} H_k \exp(-H_k t_k) & \text{if } t_k>0,\ H_k>0 \\ 0 & \text{if } t_k \leq 0 \end{cases}$$

The failure tendencies of individual components define the failure tendency of the system only then when the length of time that the original component operates does not affect the length of time the standby component works properly, i. e., when T_0 and T_1 are *stochastically independent.*

A substantial point in this argument is that T_0 and T_1 are measured from the time each component is turned on, not from the time the system was turned on.

With the assumption of stochastic independence we obtain the joint density $(H_0 \neq H_1)$

$$f(t_0,t_1)= \begin{cases} H_0 H_1 \exp(-H_0 t_0 - H_1 t_1) & \text{if } t_0>0 \text{ and } t_1>0 \\ 0 & \text{elsewhere} \end{cases}$$

The system's lifetime T is simply the sum of the component lifetimes. The system reliability function $R(t)$ can be obtained by inte-grating the joint density over the region D_t :

It results in

$$R(t)=P(T>t)= \int\int_{t_0+t_1 \geq t} f(t_0,t_1)\, dt_0\, dt_1$$

$$= 1 - \int_0^t \int_0^{t-t_1} H_0 H_1 \exp(-H_0 t_0 - H_1 t_1)\, dt_0\, dt_1$$

$$= \frac{1}{H_0 - H_1} \left[H_0 \exp(-H_1 t) - H_1 \exp(-H_0 t) \right]$$

However, we newly define T_0 and T_1 to represent the failure times of the original and standby components as measured from time t=0 at which the system was turned on.

The joint probability density for T_0 and T_1 can be found with the aid of a conditional density. The marginal density for T_0 is identical to that for the lifetime of the original component since its failure time cannot be affected by that of a standby component.

Therefore

$$f_0(t_0)= \begin{cases} H_0 \exp(-H_0 t_0) & \text{if } t_0 \geq 0 \\ 0 & \text{if } t < 0 \end{cases}$$

The joint density for T_0 and T_1 can be determined if the conditional density of T_1, given T_0, is known as

$$f(t_0,t_1)= f_{1|0}(t_1|t_0).\ f_0(t_0) \qquad \text{if } f_0(t_0) \neq 0$$

It is assumed that the failure law of the standby component is the same as that for the original component, except for the value of the parameter. Since the standby component is not turned on until the original component fails, the failure time of the original component must be assumed in the sense of a condition. Thus

$$f_{1|0}(t_1|t_0)= \begin{cases} 0 & \text{if } t_1 < t_0,\ t_0 > 0 \\ H_1 \exp[-H_1(t_1 - t_0)] & \text{if } t_1 \geq t_0,\ t_0 > 0 \end{cases}$$

where the failure law discussed earlier is used.

Then the joint density results in ($H_0 \neq H_1$)

$$f(t_0,t_1)= \begin{cases} H_0\ H_1 \exp[-H_1(t_1 - t_0) - H_0 t_0] & \text{if } t_1 \geq t_0,\ t_0 > 0 \\ 0 & \text{if } t_0 < t_0 \text{ or } t \leq 0 \end{cases}$$

The marginal probability densities f_0 and f_1 for the times T_0 and T_1 are obtained by integrating the joint density $f(t_0,t_1)$.

In addition to f_0 introduced above we get

$$f_1(t_1)= \begin{cases} \dfrac{H_0 H_1}{H_0 - H_1} \left[\exp(-H_1 t_1) - \exp(-H_0 t_1)\right] & \text{if } t_1 > 0 \\ 0 & \text{if } t_1 \leq 0 \end{cases}$$

The joint and marginal densities serve well to computing probabilities. Thus, e. g., the system reliability, or the chance that the system survives to time t, is the probability $P(T_1 > t)$:

$$P(T_1>t)= \int_t f_1(x)\ dx$$

$$= \frac{1}{H_1 - H_0} \left[H_1 \exp(-H_0 t) - H_0 \exp(-H_1 t)\right]$$

Also relevant is the probability that the standby component lasts longer than the original one and that the original survives to time t. In order to compute it we have to integrate the joint density over the region D_t:

$$D_t = \{s;T_0(s)\leq t\} \cap \{s;T_1(s) - T_0(s)>t\}$$

$$P(D_t)= \int_0^t \int_{x+t} f(x,y)\ dy\ dx = \left[\exp(-H_1 t)\right].\left[1 - \exp(-H_0 t)\right]$$

3.5.6 The Weibull distribution

This probability distribution, which is especially useful in problems of life-testing and reliability, may be considered a more generalized form of the exponential distribution since it has 3 parameters and can be reduced to the exponential with the proper choice of them. These parameters determine its range and shape.

The probability density of the *Weibull* distribution is

$$f(x)= \frac{c}{b} \left(\frac{x-a}{b}\right)^{c-1} . \exp\left[-\left(\frac{x-a}{b}\right)^{c}\right] \quad \text{for } x\geq a,\ b>0,\ c>0$$

In general, it is easier to work with the cumulative Weibull distribution function

$$F(x)= 1 - \exp\left[-\left(\frac{x-a}{b}\right)^{c}\right]$$

The graph of $f(x)$ is bell-shaped (that is, unimodal) for c>1 and J-shaped (that is, a decreasing function of x) for 0<c<1. With a=0 and c=1, $f(x)$ becomes the probability density of the exponential distribution, as it has been introduced in Section 3.5.1, with a replaced by $1/b$.

The expected value of X is

$$E[X] = a+b\ \Gamma\left(1+\frac{1}{c}\right)$$

where Γ is the *gamma function.*

3.6 The log-normal distribution

The well known normal distribution is not applicable in PSA studies. Its probability density is non-zero also for negative values of a random variable. However, in PSA studies the random variable is a probability and it assumes only values from the interval <0,1>. And thus the *log-normal distribution* appears to be a suitable model for uncertainties.

In its simplest form, the log-normal distribution is that of the random variable X when the logarithm $ln\ X$ has a normal distribution with parameters μ and σ^2. We have for its distribution function

$$F(x)= P(X \le x)= P(\ln X \le \ln x)= \phi\left(\frac{\ln x - \mu}{\sigma}\right)$$

where ϕ is the tabulated distribution function of the normal variable (0,1).
Hence, the probability density is

$$f(x)= F'(x) = \frac{1}{x\,\sigma}\ \Phi\left(\frac{\ln x - \mu}{\sigma}\right)$$

where

$$\Phi(z)= \frac{1}{\sqrt{2\Pi}}\ \exp[-(z^2/2)]$$

is the probability density of the distribution N(0,1). Thus

$$f(x)= \frac{1}{x\sqrt{2\Pi}\ \sigma}\ \exp\left[-\frac{1}{2\sigma^2}\ (\ln x - \mu)^2\right] \text{ for } x>0$$

and $f(x)= 0$ otherwise

Opposite to the normal distribution, this frequency function is strongly asymmetric, its central part is shifted to the left and the right tale converges towards zero more slowly then in the case of the normal distribution.

The *expected value*

$$E[X]= \exp\left[\mu+(1/2)\sigma^2\right]$$

and the *variance*

$$V[X]= \exp(2\mu + \sigma^2)(\exp \sigma^2 - 1)$$

The *median* does not equal the mean value. The *error factor* of the log-normal distribution is a good model for those estimates of an expert that concern small probabilities where the order of magnitude is to be estimated.

If not $ln\ X$, but $ln\ (X-x_0)$ is normally distributed, the distribution of X has the same properties as those described above except that the expected value is increased by x_0.
Thus, we obtain a "shifted" log-normal distribution.

APPENDIX D
FAILURE DATA PARAMETER CONFIDENCE LIMITS

This Appendix discusses the methods used to calculate the 90% confidence interval limits on:

(a). failure-to-run/hour data and
(b). failure-to-start on demand data.

(a). Failure-to-run/hour

The usual approximation concerning the failure rate of components running in operation is to assume failures are occurring randomly at a constant rate per unit time. This means the time to failure has an exponential distribution.

With n as the number of failures and T as the operating time of the component, then the lower and upper confidence limits P_L and P_U for the failure rate are /9/:

$$P_L = \frac{\chi^2(\alpha/2, 2n)}{2T} \quad (1)$$

$$P_U = \frac{\chi^2(1-\alpha/2, 2n+2)}{2T} \quad (2)$$

where α = 0.10 for a 90% confidence interval and $\chi^2(\alpha/2,2n)$ and $\chi^2(1 - \alpha/2, 2n + 2)$ are the chi-square distribution, with degrees of freedom 2n and 2n + 2, obtained from standard tabulations with specified respective confidence levels $\alpha/2$ and (1 - $\alpha/2$), /9/.

The chi-square values are tabulated up to 100 degrees of freedom i.e. 49 failures. For data with more than 49 failures then the chi-squared approximation can be approximated as /9/:

$$\chi^2(5\%) = \frac{(-1.645 + \sqrt{4n-3})^2}{2} \quad (3)$$

and

$$\chi^2(95\%) = \frac{(+1.645 + \sqrt{4n-1})^2}{2} \quad (4)$$

As an example, the 90% confidence interval limits can be derived for a component failure-to-run data of 10 failures per 863 hours, which is an average failure rate of $1.2 \bullet 10^{-2}$/h.

The lower 5% confidence limit from equation (1) is:

$$P_L = \frac{\chi^2(0.05, 20)}{2 \cdot 863} = \frac{10.8}{1726} = 6.3 \cdot 10^{-3} \tag{5}$$

The upper 95% confidence limit from equation (2) is:

$$P_U = \frac{\chi^2(0.95, 22)}{2 \cdot 863} = \frac{33.9}{1726} = 2.0 \cdot 10^{-2} \tag{6}$$

Therefore, $6.3 \bullet 10^{-3} < 1.2 \bullet 10^{-2} < 2.0 \bullet 10^{-2}$ represents the average failure rate, with associated 90% confidence interval limits.

(b) Failure-to-start on demand

The binomial distribution /9/ is the relevant probability distribution function (pdf) used to describe the component demand failures when either of two outcomes, a successful start or a failure-to-start may occur. The binomial pdf describes the probability p of obtaining n failures from a sample size (in this case, number of demand starts) of d as:

$$P(n_d) = \frac{d!}{n_d!\,(d-n_d)!} \cdot p^{n_d} \cdot (1-p)^{d-n_d} \tag{7}$$

The lower confidence limit P_L for this distribution is /10/:

$$P_L = \frac{1}{1 + [(d-n_d+1)/n_d] \cdot F_L(\alpha/2, 2 \cdot (d-n_d+1), 2n_d)} \tag{8}$$

where F_L is the value of the F distribution for degrees of freedom $2(d - n_d + 1)$ and $2n_d$, and $\alpha = 0.10$ for 90% confidence.

The upper confidence limit P_U for this distribution is:

$$P_U = \frac{1}{1 + \frac{d-n_d}{n_d+1} \cdot \frac{1}{F_U[\alpha/2, 2(n_d+1), 2(d-n_d)]}} \tag{9}$$

where F_U is the value of the F distribution for degrees of freedom $2(n_d + 1)$ and $2(d - n_d)$.

As an example, the following 90% confidence limits can be derived for component failure-to-start/demand data of 61 failures/1390 demands, which gives an average failure/demand of $4.2 \cdot 10^{-2}$:

$$F_L = F_L[0.05, 2(1390 - 61 + 1), 122]$$
$$= F_L(0.05, 2660, 122)$$
$$= 1.26$$

$$F_U = F_U[0.05, 2(61 + 1), 2(1390 - 61)]$$
$$= F_U(0.05, 124, 2658)$$
$$= 1.23$$

Hence from equation (8)

$$P_L = 0.035$$

and from equation (9)

$$P_U = 0.054$$

Therefore, $3.5 \cdot 10^{-2} < 4.4 \cdot 10^{-2} < 5.4 \cdot 10^{-2}$ represents the average failure on demand with associated 90% confidence limits.

APPENDIX E
LIST OF COMPONENTS AND CODES

This is a proposed basis for a hierarchial coding system for research reactor components. The component codes used in IAEA-TECDOC-478, /2/, are composed from three capital letters. The first letter of the code specifies the principal component category.

Code Component Group

Mechanical Component Categories

F Piping
G Pool, grid plate, beam ports, D_2O-tank, storage containers
H Heat exchanger
O Control rods and drive mechanisms
P Pumps
Q HVAC and air handling equipment
V Valves
W Shielding and related mechanics
X Fuel elements, reflector
Y Strainers, filters, demineralizer
J Other mechanical equipment, lifting gear, structures, experimental setup

Electrical Component Categories

T Transformers
R Relays
M Motors
C Conductors
B Batteries and chargers
K Circuit breakers
E Other electrical equipment, electrical part of experimental installations
D Diesel generators, gas turbine driven generators

Instrumentation and Control Equipment Categories

A Sensors (ionization chamber, Pt-100 temperature sensor)
I Instrumentation (channels, reactor protection system)
L Transmitters
N Signal conditioning system, computers
S Switches
U Other I&C equipment, instrumentation for experiments

List of component groups

This listing of component groups and their codes as used in the IAEA reliability data base and the data entry system (DES) is recommended for all data collection activities at research reactors. The code consists of two capital letters: the first letter describes the main group, the second letter determines the group level. It is in alphabetical order for each major component category. Component group codes with the number symbol (#) differ from IAEA-TECDOC-478 in order to cover research reactor components.

Codes and groups for mechanical components:

	QA	Air cooler
	QB	Blower fan
	JE	Clutch
	QC	Compressor
	OC	Control rod
	OD	Control rod and drive mechanism
	OR	Control rod drive
	QD	Damper
	QF	Fan cooler containment
	YF	Filter
	FY	Gasket
	HX	Heat exchanger
	JH	Heater
	QV	HVAC unit annulus ventilation
#	JI	Irradiation facilities
	YT	Intake screen
	JL	Lube oil cooler
	FX	Orifice
	JP	Penetration
	FE	Piping expansion joint
	FN	Piping nozzle
	FR	Piping rupture diaphragm
	FS	Piping straight section
	FT	Piping tees
	FW	Piping welds
	PD	Pump diesel driven
	PM	Pump motor driven
	PT	Pump turbine driven
	PW	Pump without driver
	YS	Stainer
	JT	Tank
	JU	Turbine
	VA	Valve air operated
	VE	Valve explosive operated
	VH	Valve hydraulic operated
	VX	Valve manual
	VM	Valve motor operated
	VP	Valve piston operated
	VC	Valve set operated

VD	Valve solenoid operated
VW	Valve without operator

Codes and groups of components for electrical equipment:

BT	Battery
BC	Battery charger
CB	Bus
CC	Cable
KA	Circuit breaker
KG	Circuit breaker generator
KC	Circuit breaker molded type
EC	Converter
KS	Feeder (branch, junction)
KT	Fuse
EG	Generator
EH	Heater electric
EI	Inverter
MA	Motor
MS	Motor servo
MG	Motor generator
EB	Panelboard
EP	Power supply
ER	Rectifier
RW	Relay
RA	Relay auxiliary
RC	Relay control
RP	Relay power
RR	Relay protective
RT	Relay time relay
RY	Relay coil
RX	Relay contacts
TA	Transformer
TT	Transformer auto
TI	Transformer instrument
TM	Transformer main power generator or unit
TV	Transformer regulating
TE	Transformer station service including excitation
TX	Transformer station start and auxiliary
TU	Transformer substation
CW	Wire
DE	Diesel engine
DG	Diesel generator emergency AC
DT	Gas turbine driven generator emergency AC

Codes and groups for instrumentation and instrumentation equipment:

	UN	Annunciator
	NK	Computational module
#	NC	Computer
	UC	Controller
	UI	Indicating instrument
#	NO	Input/output device
#	NI	Interface
	UM	Manual control device
#	NP	Programmable logic
	AR	Radiation monitors
	UR	Reactor scram system
	AC	Sensor core flux
	AF	Sensor flow
	AL	Sensor level
	AP	Sensor pressure
	AT	Sensor temperature
	NS	Signal conditioning system
	NM	Signal modifier
	UE	Solid state device
	SD	Switch digital channel
	SF	Switch flow
	SL	Switch level
	SI	Switch limit
	SM	Switch manual
	SP	Switch pressure
	ST	Switch temperature
	SQ	Switch torque
	SC	Switch contacts
	LF	Transmitter flow
	LA	Transmitter flow ,level ,pressure
	LL	Transmitter level
	LP	Transmitter pressure
	LT	Transmitter temperature

Alphabetical list of components with component code

This component list combines the codes used in IAEA-TECDOC-478, /2/, with the coding of DES, the data entry system for data collection at research reactors. Component codes with star symbol (*) indicate typical research reactor equipment and should therefore be used with preference.

#	ARA	aerosol monitor
	QAA	air cooler
	UNA	annunciator
	UNS	annunciator module solid state, LED-, LCD-display
*	BTA	battery
	BTL	battery lead acid accumulator
	BTN	battery nickel cadmium accumulator
*	BCA	battery charger
	BCS	battery charger solid state
*	QBF	blower fan
	CBA	bus
*	CB2	bus 120V AC , 220V AC
	CB3	bus 380V
	CB6	bus 6kV
*	CBD	bus DC
*	CCP	cable power
*	CCS	cable signal (supervisory)
*	KAA	circuit breaker
*	KDC	circuit breaker DC
	KIA	circuit breaker indoor AC application
	KID	circuit breaker indoor DC application
	KIS	circuit breaker isolation, ground fault circuit interrupter
*	KRP	circuit breaker reactor protection
*	JEM	clutch mechanical
*	JEE	clutch electrical
*	QCI	compressor instrument air
*	NKA	computational module
*	OCS	control rod clustered silver, indium, cadmium control rod
	OCC	control rod cruciform, boron carbide control rods
*	OCR	control rod single control rod assembly
*	ORA	control rod drive
	UCA	controller
*	UCE	controller electronic
	UCP	controller pneumatic
*	QDA	damper
	QDM	damper manual(HVAC)
	DEA	diesel engine
*	DGA	diesel generator emergency AC
	QFV	fan containment ventilation fan
	QFH	fan cooler reactor building cooling unit
*	KSF	feeder (junction box)
	YFM	filter liquid, mechanical restriction

* UCF flow controller
* KTA fuse all voltage levels
* FYA gasket
* HXA heat exchanger
HXH heat exchanger U tube horizontal shell and tube
HXV heat exchanger U tube vertical shell and tube
HXB heat exchanger straight tube horizontal shell and tube
HXM heat exchanger straight tube vertical shell and tube
EHT heat tracing pipe heater
EHA heater air heater
EHP heater pressurizer heater
* QVA hvac unit auxiliary building
* QVB hvac unit battery room ventilation
* QVR hvac unit control room ventilation
* QVE hvac unit electric equipment area ventilation
* UIE indicating instrument electronic
* IAA instrumentation
* ICC instrumentation channel analog core flux
* ICF instrumentation channel analog flow
* ICL instrumentation channel analog level
* ICP instrumentation channel analog pressure
* ICT instrumentation channel analog temperature
* IDL instrumentation channel digital level
* IDP instrumentation channel digital pressure
YTS intake screen service water system
EIA inverter
EII inverter instrument
EIZ inverter static single phase
EIX inverter static three phase
JIR irradiation rig
* UEY isolating diode assembly
JLC lube oil cooler
* UMC manual control device pushbutton
* MAA motor
* MAC motor AC
MAI motor AC induction
* MSS motor servo
MGX motor generator
ARN neutron monitor
FXA orifice
* JPE penetration electrical
* JPP penetration piping
* FSS piping small, < = 1" diameter
* FS3 piping medium, 1" < diameter < = 3"
* FSM piping large, > 3" diameter
* FEA piping expansion joint
FNA piping nozzle
FNS piping nozzle spray
FSA piping straight section
FTA piping tees
JIP pneumatic transfer system

EPA power supply (instrumentation and control equipment)
* PWC pump centrifugal
PWB pump centrifugal horizontal flow 22-820 l/s
PWE pump centrifugal vertical flow 70-1900 l/s
PDA pump diesel driven
PMA pump motor driven
PTA pump turbine driven
* URS reactor scram system
* ERS rectifier static
* RWA relay
* RAA relay auxiliary
RCL relay control
RCA relay control AC
RCD relay control DC
* RPH relay power 300-460 A
* RPL relay power 40-60 A
* RRA relay protective
RRO relay protective overload protection
RRV relay protective voltage protection
* RTA relay time delay
RTB relay time delay bimetallic
RTP relay time delay pneumatic
RTS relay time delay solid state
* RYA relay coil
* RXA relay contacts
* ACA sensor core flux
* AFA sensor flow
* ALA sensor level
* ALR sensor level reactor water level
* APA sensor pressure
* APD sensor pressure difference
* ATA sensor temperature
* NCA signal comparator bistable
* NSA signal conditioning system for core flux, level, pressure, temperature general
* NMA signal modifier
* NMT signal modifier current-current transducer
NMP signal modifier current-pneumatic transducer
* NMV signal modifier current-voltage transducer
NMS signal modifier square root extractor
NMO signal modifier voltage-pneumatic transducer
* UEH solid state devices high power application
* UEL solid state devices low power application
* ECM static converter for reactor main coolant pumps
* YSF strainer / filter
* SDA switch digital channel pressure / vacuum, pressure, level
* SFA switch flow
* SLA switch level
* SIA switch limit
* SIE switch limit electronic
* SMA switch manual
* SPA switch pressure

* STA switch temperature
* SQA switch torque
* SCC switch contacts
* JTR tank storage RWST (refueling water storage tank)
* EBA terminal board
* TAA transformer
* TA2 transformer 220/120 V
* TA6 transformer 6kV/380V
* TIP transformer instrument potential
* TIC transformer (instrument transformer, current transformer)
* LFF transmitter flow
* LAA transmitter
* LLL transmitter level
* LPP transmitter pressure
* LXR transmitter pressure difference
* LTT transmitter temperature
* VWA valve angle valve
* VWB valve ball valve
* VWT valve butterfly valve
  VWP valve diaphragm
  VWG valve gate
  VWL valve globe valve
  VWN valve needle valve
  VWU valve nozzle valve
  VWJ valve plug valve
* VRA valve relief
* VSA valve safety
* VA1 valve air operated
  VAR valve air operated all systems except raw water return line
  VEA valve explosive operated
  VHA valve hydraulic operated
* VXA valve manual
* VMA valve motor operated
  VPA valve piston operated
* VCA valve self operated check
* VDA valve solenoid operated
* CWA wire
* CWC wire control circuit typical circuit, several joints

91-05771