EUROPEAN COMMISSION
DG-JRC – Institute for Advanced Materials
Joint Research Centre

DISCUSSION DOCUMENT ON RISK INFORMED IN-SERVICE INSPECTION OF NUCLEAR POWER PLANTS IN EUROPE

December 2000 ENIQ Report nr. 21 EUR 19742 EN

Approved by the Steering Committee of ENIQ

"The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national."

Directorate-General
Joint Research Centre

Published by the
EUROPEAN COMMISSION

Directorate-General
Telecommunications, Information, Industries and Innovation
L-2920 LUXEMBOURG

LEGAL NOTICE

Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of the following information.

Catalogue number: CD-NA-19742-EN-C

©ECSC-EEC-EAEC, Brussels – Luxembourg, 2000
Printed in the Netherlands

Contents

Foreword

The present work is the outcome of the activity produced in the framework of the EURIS Concerted Action (European Network for Risk Informed In-Service Inspection), funded by the European Commission, Directorate General Research. This document has been produced by using the EURIS final report after discussions and further elaboration that followed the subsequent meetings of the Task Group 4 on Risk Informed In-service Inspection of the European Network for Inspection Qualification (ENIQ). The document was therewith formally approved by the Steering Committee of ENIQ during the 19th Steering Committee meeting held in Petten on 12-12 December 2000.

The contributors to this document include: O.J.V. Chapman (OJV Consultancy Ltd.), K. Aubert (EDF Research and Development, France), R. Axelsson (Oskarshamn Nuclear Power Plant, Sweden), B. Brickstad (SAQ, Sweden), L. Fabbri (European Commission, Joint Research Centre Petten, The Netherlands), M. Garcia Heras (Tecnatom S.A., Spain), R. Gerard (Tractebel, Belgium), W Kohlpaintner (E.ON Kernkraft, Germany), D.P.J. Lidbury (AEA Technology, UK), H. Schulz (G.R.S., Germany), B.W.O. Shepherd (Mitsui Babcock, UK), J.B. Wintle (The Welding Institute, UK).

The Directorate General Research of the European Commission is particularly acknowledged for the funding of EURIS and for their permission to use the EURIS material for the production of the present document.

1.Background

Equipment at nuclear power plants (NPPs) is inspected periodically during service by non-destructive examination in order to provide information about its current condition and any damage, defects or degradation that may be present. In-service inspection, ISI, is a key tool in the management of NPP safety and is an important measure for the assurance of integrity and the avoidance of failure.

As is well known, many ISI initiatives, involving the non-destructive examination of nuclear plant components have been conducted at a European level through the development of many EU programmes (PISC I, II, III, Nordtest, NIL, DDT, etc.). These programmes provided evidence of the importance of performing inspection qualification in order to guarantee the proper fulfilment of inspection objectives. This concept was developed at European level by the European Network for Inspection Qualification (ENIQ), driven by the nuclear power plant utilities, which aims to co-ordinate in an efficient way the resources available within the European Union for inspection qualification. A point to note is that the regulators published a common position document on inspection qualification, which is in agreement with the ENIQ methodology.

Effective and reliable ISI is therefore possible in many situations. However, much effort is often spent in situations for which the probability of failure and its effects on safety have a very low impact. Besides, practical experience demonstrates that failures can often occur in locations where the inspection was never performed. As the costs of such effective inspections are very high, the effort must be targeted at situations that offer a significant risk to safety.

In most if not all European countries, inspection planning for passive components is developing from prescriptive codified practices backed up by stringent regulatory requirements. These codes specify the locations, frequency and methods of inspection based primarily on the type and safety category of the component. The philosophy of the inspection codes addresses the threats to integrity identified within the original design basis within the scope of a limited number of design safety categories.

The definition of risk is generally accepted as the product of the measure of the (generally undesirable) consequence resulting from an initiating event and the probability of that event occurring within a given period of time. In a NPP, structural failure of a component is clearly an initiating event that can give rise to risk.

Many year's experience of operating nuclear power plants is now available which has resulted in improved knowledge of the mechanisms of plant degradation and the locations within the plant that are most susceptible. Improved probabilistic safety assessments have increased the understanding of the safety significance of individual components in terms of the consequences of their failure. These developments are leading the nuclear industry to consider setting inspection priorities on the basis of risk.

Operators are recognising that this offers an opportunity to achieve the goals referred to earlier. Indeed this process has already begun in several countries. There is not yet,

however, a common consensus, within Europe on what the process of risk informed inspection is and how it should be implemented.

Defining the situation for risk informed inspection identifies the main aims and elements of the process. It recognises that this is an evolving technology that is building on different existing regimes of inspection planning that have jurisdiction within individual countries. In presenting the principles of risk informed inspection, no advocacy or criticism of any existing or evolving regime is implied. The information is presented for discussion with the aim of creating a common understanding of risk informed inspection within Europe.

Different initiatives based on risk assessment for developing inspection plans are currently conducted at a national level in many EU countries. However, none of the groups involved is now in the position to lead to an EU position on risk-informed ISI. For this reason, within ENIQ a group has been set up (Task Group 4) in order to help to homogenise the different activities on risk based ISI for nuclear reactor safety by promoting and rationalising a common position in the EU. This activity, which through ENIQ is driven by the utilities, has been complementary to the Task Group of RI-ISI set up by Nuclear Regulators Working Group (NRWG). Most of the members of ENIQ TG4 also joined the European Network of Risk -Informed in-Service Inspection (EURIS), funded by the Directorate General RTD of the European Commission, with the main objective of identifying and analysing all the main elements to be considered in a risk based decision making process for inspection planning. EURIS completed its work in February 2000.

2.Objectives

The objective of this work is to continue the work presented by EURIS and to develop a methodology for risk based assessment relevant to the needs of plant operators.
The methodology could then be used to identify safety-significant categories for power plant components, and to optimise the targeting of inspections whilst maintaining or even increasing the safety. The present document represents a first attempt in this direction and should be seen as a discussion document that represents the thoughts of Task Group 4 (TG4) of ENIQ.

3.Scope

In order to implement a programme of inspection, an inspection planning exercise should be undertaken to determine the locations, frequency and types of inspections required. Many years' experience of operating nuclear power plants is now available which has resulted in improved knowledge of the mechanisms of plant degradation and the locations within the plant that are most susceptible. Improved probabilistic safety assessments have increased the understanding of the safety significance of individual components in terms of the consequences of their failure. These developments are leading the nuclear industry to consider setting inspection priorities on the basis of the risk of failure.

In formulating a programme of inspection for a nuclear power plant, the plant is generally divided into active and passive components. An active component is one that performs an active functionality that is necessary for the operation of the plant

(e.g. a pump that circulates water around the circuit). A passive component is a component that constitutes part of the pressure boundary (e.g. a pressure vessel or pipe). This means that a pump is generally both an active component and a passive component. Its active role is to pump water but it may also be part of the pressure boundary and would therefore be a passive component.

Active and passive components have tended to be considered separately for the purposes of inspection planning since the inspection of active components relates to the maintenance of the moving parts and mechanisms. This discussion document is restricted to the inspection planning for passive components and the passive element of active components. Whilst structural supports do not constitute part of the pressure boundary, they can, if they fail, act to breach containment. These are, therefore, included within the scope of this report as passive components

Failure consequences are considered both in terms of plant safety and availability. The scope of the document is targeted at possible application within the member states of the European Commission. A review of the current state of development of risk informed in service inspection both in Europe and the USA is included in appendix 3.

4.Overview of the risk-informed methodology

4.1 Definition and measures of risk

The probability of structural failure is a function of plant operations and degradations that occur over a period of time. Its probability of failure can then be evaluated over this time. Evaluated in this way, the probability of failure is specified in terms of the prescribed period of time. In terms of plant risk, it is often more convenient to measured the probability per unit time (yr^{-1}). However, if the degradation mechanism is a wear out mechanism, such as fatigue, the probability of failure per year is not constant. The consequences of structural failure may be measured in terms of its potential damage to reactor core, damage to the health and safety of employees and the public, damage to the environment, and financial damage to the company resulting from lost production, replacement of equipment and other costs. Since risk is the product of the probability and consequence, the measure of risk is directly related to the consequence and is either a per year risk or a risk over some given time period.

The consequence resulting from an initiating failure event is generally itself a probabilistic process depending on a range of scenarios including further failures of equipment. A given consequence, for example core damage, therefore has a probability conditional on the initial failure. Probabilistic risk assessment is used to assess the probability of different consequences of a given component failure, and, conversely, allows comparison of the effect of different initial failures on the probability of a given consequence.

Despite this strict definition, risk is often assessed qualitatively without this formal factoring. In this situation, the risk is the combination of the qualitatively assessed likelihood and the consequences of failure and is often presented as an element within a likelihood-consequence matrix.

4.2 Causes of structural failure of passive components

Structural failure of a passive component in the pressure circuit of a nuclear power plant is any breach of the pressure boundary resulting in loss of coolant. Local failure preserving mechanical integrity is termed a leak while a more widespread failure is classified as a break. At any location there can be a range of failure modes.

Commonly, structural failure results from the component being in a physically deficient state as a result of material defects, damage, or degradation. Component deficiencies may be the result of inadequate design, manufacture and welding, and the degrading effects of normal service conditions. They can also be the result of initiating events that lie outside the design basis such as leaking valves or water chemistry excursions of multifunctional supports.

Components not in a deficient state can fail due to extreme conditions that may arise from errors in operation and maintenance or from external factors and environmental conditions. Blockage or restriction of flow may also lead to a failure. All these events contribute to the risk from structural failure. The total risk from structural failure is made up from the likelihood of all of these causes. Component inspection by non-

destructive examination (NDE) provides information about the existence of defects (e.g. flaws and cracking), damage (e.g. denting, gouging) or degradation (corrosion, erosion) but does not address other causes of failure. NDE and hence ISI, can only address these later situations and is therefore only one of the package of measures needed to manage the total risk from structural failure.

4.3 The basic principles in defining the situation for RI-ISI

Risk informed inspection is the development of a scheme of inspection on the basis of the information obtained from an assessment of the distribution of both the probabilities of failure and its consequence, of all the sites being considered within the scope of the scheme. The process must then combine these two distributions to identify the specific sites that constitute the greatest risk to the plant.

In evaluating the distribution of the consequence, see later, it is almost certainly going to be in terms of pipe sections or subdivisions of specific components. However, inspection must be targeted at specific sites and it is the probability of failure within a pipe section or vessel that is ultimately going to produce the detail required to specify the inspection programme.

When defining the situation it will be necessary to provide a detailed break down of the information about the degradation processes and the threats to integrity for the specific sites defined above. When considering these threats to integrity the situation should identify the relative importance of any leak before break argument, see later in sections 5 and 6 on the failure probability and the consequence. In this way the resulting inspection plan can not only target the high risk components, but can also be specifically designed to detect the potential degradation processes identified at a level and a time when fitness for service could be threatened.

In order for the inspection to meet its objectives to provide quality information about the condition of the plant, the combination of the inspection techniques, procedures and operators must have sufficient reliability. An unreliable inspection is of little value. Risk informed inspection has a strong link with inspection reliability and the processes of qualification that can be used to measure and assure that the probability of not detecting defects, damage or degradation of concern is sufficiently low.

4.4 Effect of inspection on the plant risk and feedback

The information gained from inspection increases the knowledge base about the condition of the components inspected and reduces prior uncertainty. This may change the estimate of probability of failure and hence the estimated plants risk. If the component is found to be in better condition than previously expected, then the estimated plant risk is reduced; if more damage, defects or degradation are detected than previously considered, then the estimated risk is increased. If this is to be done, then the potential gains or objectives of the inspection must be clearly laid out within the definition of the situation. This serves to reinforce the statements in the previous section on defining the degradation processes and the threats to integrity as well as the inspection capabilities with respect to these issues. This feedback of the results of inspection into the risk assessment is an essential part of the process.

Inspection by itself does not alter the actual risk or time of failure. Risk can only be reduced in real terms if aspects relating to component integrity are improved, for

example, by component repair or replacement or a change in operating conditions. Inspection data may be the initiator for actions of this kind. However, components found by inspection to be free from deficiencies serve to increase confidence in the total process of integrity management

4.5 Postulated threats to structural integrity

When evaluating the damage and degradation mechanisms that threaten a given site or component area, it may be possible to identify a known mechanism that, although not believed to be present, there is sufficient uncertainty about to consider its presence. Such a situation can be seen as a postulated threat. When defining the situation it is important to recognise such threats and to consider their possible impact on the risk assessment. If the impact is sufficient to warrant the inclusion of such sites in the inspection plan, it should be made clear in defining the situation that such sites are for a postulated degradation mechanism. It may be possible to carry out only a sample inspection for such situations but as before, the capability of the inspection must be assessed against the postulate and the objectives clearly stated in the situation definition.

4.6 Elements of a risk informed inspection programme

A risk informed inspection programme could be defined by using an assessment of risk to answer the following questions:

- What are the plant boundaries/components of the inspection planning?
- How is the probability of failure distributed about the components inspection sites?
- How is the consequence of failure for each of these sites to be evaluated?
- What criteria are to be used to select the locations?
- Which and how many locations are to be inspected?

It could be argued that having selected the sites for inspection, this constitutes the boundary of the ISI plan. Indeed, as can be seen in appendix 3, the current ASME XI code case to implement risk informed inspection in the US nuclear power industry stops at this point. However, the group believes that any ISI programme must go further and ask:

- When should these locations be inspected and with what frequency?
- What information is it necessary to obtain from the inspection?
- What methods of inspection are appropriate?
- What is the reliability of the methods to be employed?
- How will the information obtained be fed back to the plant safety and or availability assessment?

A final subsequent question, certainly within the European nuclear context, is:

- What value is added by inspection qualification?

In a risk informed approach the answers to these questions are determined from the information generated from the risk assessment process.

4.7 The process of risk informed inspection planning

The key steps in the process of risk informed inspection planning are given below. It is based around an assessment of the risk of failure and the development of an appropriate inspection plan.

- Formation of the RII assessment team
- Definition of the boundary of the equipment considered by the inspection planning
- Determination of the applicability of risk based inspection
- Identification of the information necessary to carry out the risk assessment
- Establishing the availability and gathering the information required
- Identification of credible types and causes of failure for each unit/component
- Assessment of the rates of degradation mechanisms and the probability of failure
- Assessment of the consequences of failure in terms of safety of personnel, loss of production, damage to plant environment etc
- Risk ranking of each unit/component or placement in a risk matrix
- Development of the inspection plan defining the inspection scope, methods, reliability and interval in relation to risk and fitness for service
- Feedback of information from the inspection and review of RII assessment

Risk informed inspection is a multidisciplinary team based activity. The team needs to be able to draw on the expertise of competent individuals with knowledge of the hazards, risk assessment, materials degradation and inspection techniques, plus staff with plant specific knowledge of maintenance and inspection, plant operation and process conditions. The RI-ISI programme needs to take account of its context within the overall risk management of the plant which may include other possible palliatives against the risk.

4.8 Quantitative versus qualitative

Whilst not strictly part of the process for defining the situation, the choice of quantitative or qualitative can effect the situation definition. This choice will almost certainly effect the area of inspection capability and possible feedback. Difficulties may occur in defining the inspection requirements in terms of what is significant, which will, within the European context, give rise to difficulties for inspection qualification and subsequent feedback to assess any findings be they positive or negative. It may be possible to overcome these problems by the extended use of the expert elicitation, see section 5.5. However if the inspection programme is to be complete, all the requirements concerning the definition of the situation must be completed in an achievable way.

4.9 Information to define the situation for risk informed inspection

The process of risk-informed inspection planning brings together four categories of information.

- Design specifications
- Historical plant operating data
- An assessment of consequences

- An evaluation of failure probabilities

The information (deterministic or statistical) within each category required to specify a risk-informed inspection depends on the approach adopted, but may include:

Design Specifications

- Defined boundaries of plant items to be considered for inspection planning
- Design and manufacturing records
- Deterministic design stress and fatigue analysis

Historical Plant Data

- Operational transient and condition monitoring data
- Plant failures and service experience data
- Pre-service and in-service inspection records
- Environmental conditions including temperatures, water chemistry and flow rates
- In-service degradation assessments (fatigue, SCC, erosion-corrosion, external effects)

Consequence Assessment

- Design safety class categorisation
- Detailed assessment of consequences (including PSA)
- Failure modes and effects analysis
- Cost analysis of component failure

Failure Probability Evaluation

- Expert assessments of the failure probability
- Generic component failure rates
- Component specific failure rates
- Frequency and probability size density of defects
- Distributions of material properties and degradation rates
- Full analysis of probability of failure

The availability and accessibility of this information will vary depending on the particular circumstances.

The relationship between these categories within the process of risk-informed inspection is shown in Figure 1 below. Following inspection, the results feed back into the historical database and may used in planning further examinations.

Figure 1: Definition of the Situation: General Scheme

5.Estimation of the failure probability

Within a normal PSA, failures are classified as primary, secondary or command faults, see reference 1. These classifications are defined as follows:

a) A primary failure, is defined as the equipment being in the non-working state for which the equipment is held accountable, and repair action on any components is required to return the equipment to the working state.

b) A secondary failure, is the same as a primary failure except that the equipment is not held accountable for the failure.

c) A command fault is defined as the equipment being in the non-working state due to improper control signals or noise and, frequently, repair action is not required to return the equipment to the working state.

For active equipment, all three failures are applicable, however, in terms of the responsibilities addressed through NDE, it is only the primary failure, which is of concern.

Thus, within the context of a risk informed in-service inspection (RI-ISI) programme, it is the engineers responsibility to identify the probability of failure i.e. breach of containment, of the structural component. This can then be used within the PRA to assess the relative risk significance of individual candidate inspection sites. Note that this estimate of the probability of failure must not include any reduction in the probability that could be attributed to any in-service inspection. This statement has implications in later sections when world data or plant experience is used to assess the probability of failure.

5.1 Probability of failure

As already defined in the introduction of this document, risk is defined as "probability of failure x consequence". The introduction of the probability of failure takes a consequence of failure and converts it into risk. However, if we are to use this concept as a ranking tool for different passive components, or sub elements such as welds, then we must be sure to differentiate the probability of failure of these different welds or components. If this is not done there is a tendency for the risk ranking to become a consequence ranking. What follows in this section is an overview of the different approaches to this problem.

5.2 Expert judgement

Probably the simplest solution to the above problem is to employ a group of experts to assess the probability of failure of the individual sub components and hence provide a ranking for them. Such a ranking could, in principle, be qualitative or even quantitative. In reality, it is more likely to be only qualitative although reference 2 did attempt to provide a direct evaluation of the probability of failure of pipe welds. The lessons learnt from reference 2, although never explicitly reported, was that such an exercise, unaided by any analytical models or extensive database, was impractical.

Viewed in isolation, the use of experts in a form of expert elicitation, appears very subjective, unordered and provides no way of auditing the outcome. As such it would seem to be of limited value. At the same time it would seem inconceivable that the probability of failure of any component or sub element of that component can be assessed without the use of experts! The use of experts, in some form of expert elicitation is therefore deferred until later, when it can be placed more in relationship with the data/analytical tools that might be used to support the exercise.

5.3 World data

When faced with the problem of how to evaluate the probability of failure for a structural component, it is natural to look to the literature or specific plant experience for data. There is however, a difficulty with this so called 'world data'.

Using the frequentist approach to the definition of a failure probability from this type of data would give:

$$Pf = Nf/N$$

Where Nf is the sum of all observed failures for a particular family of component, and N is the total operating year's experience for that family of components.

This single probability of failure is, in reality, a point estimate of the mean probability of failure. Such a probability is reasonably satisfactory for an overall PSA because on average, over a number of such components, this is truly the mean or expected value. However, this statistic tells us nothing about the variation of the probability of failure between individual components within the family of components. However, as already stated, if a true RI-ISI policy is to be implemented, it is necessary to determine the probability of failure of the individual components from within the family of components. That requires knowledge of how the probability of failure distribution is spread across the family of components and so the simple statistic as it stands is of little use in this exercise.

Clearly, however, such a statistic must be of value, as it represents a true historic estimate of the mean failure rate. Thus the question becomes, how is it possible to either break the data down to give a better representation of the variability of the failure probability across the population or to derive a methodology that allows such a break down to be made. In other words, how do we derive the distribution for the failure probability and how do we identify which sites fall into which areas of the distribution.

5.4 Degradation mechanisms

The most obvious way to break down the world data is to categories the failures into degradation mechanisms.

Extensive analytical and experimental efforts have characterised effects of numerous degradation mechanisms that operate in structural components. These mechanisms vary widely in terms of their potential effects. Some operate in numerous systems, structures and components over wide ranges of environments and stress levels.

Furthermore, as discussed in the previous section, it will only give a single point estimate of the probability of failure for each given mechanism. If it can be assumed that the distribution of the failure probabilities within a given mechanism is very small then this break down could be sufficient. This, unfortunately, is unlikely to be true. Thus whilst such an initial break down is extremely valuable, it is probably not sufficient and some estimate of the spread within a particular failure mechanism needs to be assessed. Appendix 1 gives a more detailed summary of the gathering and analysis of world data and demonstrates that deriving failure data in this form is not without its difficulties!

One way of estimating the spread about these mean values is to return to our discussion on the use of 'Expert Judgement'.

5.5 Expert judgement to support statistical data on degradation mechanisms

If we make the not unreasonable assumption that any expert used in such an elicitation, would have knowledge of the world data then we can think of an expert elicitation as an extension of the world data. This extension of the world data would bring into play an element of judgement based on the expert individual knowledge about the relative failure mechanisms together with anecdotal information that can be used for formulating an overall opinion of the probability of failure in a given situation. In this way the expert elicitation can build a picture of the probability of failure distribution that surrounds the simple statistic associated with a given mechanism of failure.

The reader will probably not be surprised to hear that the make up of experts in any panel to assess the product failure is a vitally important mix. Such a mix would need to include experts in the field of structural integrity, material properties, degradation mechanisms and not least, experts with knowledge of the operational and historical experience from the plant under investigation. This last group of experts/knowledge brings into sharp focus the plant feed back that will be discussed in later sections.

If such an expert panel has available to it a reasonably extensive database derived from both plant specific as well as world data, together with a meaningful statistical analysis, then such a process can prove very powerful in identifying the spread about the statistics associated with the analysis. At the end of such a panel session, it is reasonable to assume that individual sites will have individual probabilities of failure that provides the spread in the failure probability. Such a distribution would reflect the world data, the plants specific data, the operating loads/stresses, the degradation mechanism and the failure mode associated with that particular site. Thus, in principle, such a procedure could provide all the information required in terms of the probability of failure.

As stated at the introduction of this section, the final assessment of the failure probability must give due cognisance of any service inspection that may be inherent in the world data. Any effect must be removed from the final estimate.

5.6 Attribute models

There are basically two difficulties associated with the expert panel or expert elicitation. The first is associated with the nature of the expertise that is necessary.

Whilst it is possible to gather a group of experts in the required fields of expertise, what is required from the experts is how these separate technological fields interact to provide a probability of failure. Generally, experts can, within their individual field of expertise, rank between different situations as to which is the worst. Sometimes this can be quite adequate but often it is the interaction between different areas of expertise that is the key to the probability of failure. Clearly if there were just two of these areas, which we will now call attributes, and one potential site is ranked high for both then it is almost certainly worse than one that is ranked low for both! The problem arises when the rankings are mixed and especially when there are several attributes to be considered.

The second problem with an expert elicitation is associated with the inability to audit an expert elicitation. Clearly one can audit the credentials of each expert and ascertain that he or she does bring the relative expertise to the meeting. However, one can never audit an individual's thinking! Again, as in the previous paragraph, it is generally possible for the expert to lay down his or her thinking within a particular expertise or set of attributes but it becomes very difficult when mixed areas of expertise are combined at a single site.

One way of tackling this problem is via the concept of what are now generally referred to as attribute models. It is reasonable to suggest that there are probably four types of different attributes:

1) Those related to the material.
2) Those related to its physical shape.
3) Those associated with the environment.
4) Those associated with the loading.

M Thomas developed one of the earliest attribute models, see for example reference 3. This work was targeted at the probability of failure of nuclear pipe work and was derived from the published world failure data plotted against the non-dimensional parameter Qw, the equation given was:

$$Pf = (Qw + Qp) \times T \times B \times F \times \text{Correlation Constant}$$

Where Qw is the original non-dimensional constant against which the world data for pipe failures was correlated, this being given by:

$$Qw = DL/t^2$$

Where

D = Pipe diameter
t = Pipe wall thickness
L = Pipe length

The Qp was added to represent the proportion of failures contributed by the base material. This was derived from a brain storming on what was felt to be a relative ratio of defects in the welds to defects in the extruded pipe used for nuclear pipe weld. Thus Qp became:

$$Qp = DL/(50 \times t^2)$$

Finally T, B and F were added as factors to represent a peak stress reduction factor, a design learning curve and an ageing factor respectively.

This model was criticised because it did not contain any specific degradation mechanism. An attempt was therefore made by other authors to add factors for a full range of degradation mechanism.

The most serious criticism of this type of modelling lies in the fact that it does not, in its simplest form, include the considerable mechanistic knowledge that now exist on the degradation mechanisms and failure modes, that fundamentally underlay the probability of failure.

To introduce this knowledge into the assessment requires a sideways movement away from the use of world data into the application of probabilistic methods to these underlying mechanistic models. Such modelling is generally referred to as structural reliability modelling.

5.7 Structural reliability models

Structural Reliability Models (SRM) approach the problem of assessing the probability of failure of a component from an entirely different approach. Unlike the frequentist approach the SRM attempt to estimate the probability of failure in terms of:

1 A mechanistic understanding of the degradation mechanism.
2 A knowledge of the failure criteria.
3 An estimate of the projected loading conditions.
4 Uncertainty about the inputs to all of the above.

It can be seen that the first three elements above are the requirements for what is generally described as a 'deterministic analysis'. Indeed, it can argued that if ever a deterministic analysis can be carried out, for say fitness for purpose, an estimate of the probability of failure can be made by estimating the uncertainties about input values to the deterministic analysis. It can be seen that this type of estimate requires no historical data on failures in order to estimate the failure probability or rate into the future.

The principle difficulty with this type of analysis is that completeness can never be proven. That is to say, complete knowledge can never be proven. However, it should be born in mind that any so called deterministic analysis also suffers this problem. Likewise the frequentist also has the problem with respect to the historical data being used to forecast a future probability; witness the turkey that gathers data all through the year up until Christmas!

Thus to produce a SRM we must start from a deterministic based model of the degradation mechanism that includes the failure criteria. An understanding of the variability within the parameters of the model must then be gathered. Finally an estimate of the projected operational loading is required in order to complete the analysis. Note the difference in the data that is required between the modeller and the

frequentist. The modeller is looking for data about the random variables that are the constitute parts of his model, whereas the frequentist, who has no model, is simple looking for failures in a given population. The attribute model can be seen as attempting to occupy a half way house between these two extremes.

The full SRM can, however, be taken further than this basic estimate of the failure probability. It is quite possible, from a mechanistic understanding of the failure mechanism, to provide an estimate of the failure mode. The failure mode could, for example, be assessed against the probability of being a stable leak, an unstable plastic tearing failure, a fast brittle fracture etc. Since the consequence associated with each of these different failure modes is likely to be quite different, a truer assessment of the risk associated with the component can be estimated.

Within the field of interest of this document, two relatively simple examples of SRM are given in appendix 2

It can be seen from the example in appendix 2 that this form of analysis provides precisely the information necessary for a risk-based model. It separates the probability of failure such as to reflect what would seem to be a self-evident difference between the different examples. Thus, it would seem to follow that when coupled with the consequence, this methodology should provide a truer perspective of the relevant risk.

However, the difficulty with the analysis lies in the extensive knowledge that is required about the situation, being addressed; the applied transients, the crack growth, the failure criteria etc. A further area of concern regarding the failure of welds, is the start of life defects in the weld. Finally, there is the question of how the values used to describe these variability's could be validated?

The answer to this last question is that few if any of them can be fully validated! In reality we know there is always a degree of uncertainty and the objective of the probability analysis is to reflect this uncertainty in terms of the defect distribution and density, the crack growth distribution, the material toughness etc. If there were no uncertainty then we would be in a truly deterministic world where probability had no meaning. The determinist solution to this uncertainty about the variability within the parameters, is to add 'safety factors' to all the unknowns and simply argue that these then provide adequate safety. The 'safety factor' approach, therefore contains an implicit assessment of the uncertainty. Thus the only difference between a deterministic assessment and a probabilistic assessment is the explicit, rather than implicit, recognition of uncertainty!

Whilst the previous discussion between deterministic and probabilistic based assessments are of considerable value, the most difficult question to answer is the one already mentioned, that defeats both methodologies; that of completeness. It can never, by definition, be possible to prove completeness in a probabilistic space and so there is little point in attempting to do so. This question of the unknown, or 'Factor X' as it is sometimes referred to, is discussed later in section 9.

If a SRM is used to evaluate the probability of failure for a RI-ISI programme, it must be a best estimate probability of failure, based on the best available knowledge at the

time. It should contain no hidden safety factors or known pessimism's as these will distort the relative values, which in tern will distort the relative risk.

Earlier in this section it was shown that an SRM analysis of any given failure probability is independent of any form of statistically derived world data. At the same time in earlier sections of this chapter it was stated that the statistical estimate of the failure probability derived from the world data, represented a true historic estimate of the mean failure rate. Thus the question arises as to how the world data can, in some way, be integrated in to the SRM analysis?

The answer to this question is quite simply, no! Such data cannot be integrated in to the modelling because the SRM is, as we have already stated, based around mechanistic models and the uncertainties about these models and their input data, not statistical data on failures. It would be quite impossible, within a single SRM analysis, to simulate what could be termed an average or mean set of conditions that represented the world data situation. Thus the world data must be seen as a complementary assessment of the failure probability which can be used to possibly validate, or at least give confidence in, the SRM estimates. However, even this is not straightforward! The statistic derived from the world data derives from the full variety of conditions, environments, loads and whatever else influences the failure probability; the SRM, on the other hand, represents a very specific set of conditions. If the world data is to be used to in some way to validate the predictions of an SRM, the SRM must be run so as to represent the world data against which it is to be compared. An example of this is given in reference 4 and the figure from that paper is reproduced here as figure 2. This plot shows how the SRM predicts a failure probability ranging from the 'no-never mind' region of 10^{-8} and below all the way up as high as 10^{-3} whilst still being compatible with the estimated world data value of $8x10^{-5}$.

Histogram of over 1,000 pipe weld failures (all sizes) per year predicted by SSRA analysis

Mean value form analysis $\simeq 4 \times 10^{-5}$

Probability of failure/weld/year as assessed from the world data $\simeq 8 \times 10^{-5}$

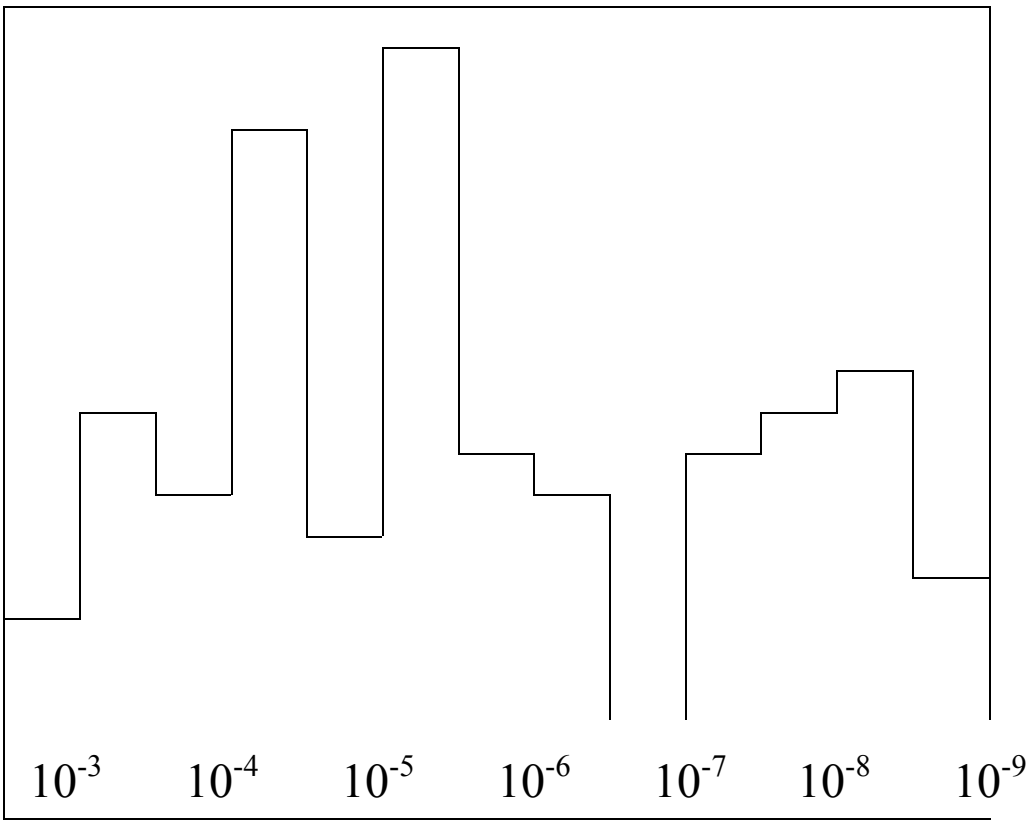


Figure 2: Probability of Failure per Weld per Year

5.8 Partial safety factors

The concept of partial safety factors has long been used in the design of such things as buildings. The partial safety factor approach is a simplified SRM. That is to say, that as with an SRM the basic concept is to assess the probability that the load will exceed the resistance to failure. The approach is a first order second moment method (FORM) where a reliability index β is estimated by in either a closed form or by an iterative numerical procedure. This reliability index is the minimum distance from the origin to the failure surface, expressed in normalised terms of all the variables involved. This can be done quite easily if for example the distribution of the load and the distribution of the resistance are normal. In such a situation the reliability index β can be uniquely described in terms of the means μ_L and μ_R, and standard deviations s_L and s_R respectively, as given by:

$$\beta = \frac{\mu_R - \mu_L}{\sqrt{s_R^2 + s_L^2}}$$

Characteristic values are often taken to represent upper bounds for distributions of load effects and lower bounds for distributions of resistance effects as follows:

$$C_L = \mu_L + n_L . s_L , \qquad C_R = \mu_R - n_R . s_R$$

Where n_L and n_R are the number of standard deviations above or below the relevant mean values of the distributions chosen to represent characteristic values.

Within the design space this methodology is used to optimise the design against different potential failure modes. In this way there are no unique individual safety factors that apply universally for any given failure mode, instead each design optimises its safety factor requirement over the specific failure modes it is subject to; hence the term 'Partial Safety Factors'.

At present the working group know of no efforts that have been made to adapt this methodology for use within a RI-ISI philosophy. However, it is known that at UMIST (University of Manchester) work in this field is being considered, see reference 5 and that ASME Section XI is also considering their possible impact, see reference 6.

5.9 Leak rate and leak before break assessment

This section has so far concentrated on the different methods that can be adopted in order to determine the probability of failure of a passive component. However, having determined the probability of failure, it would seem self evident that the level or rate of leakage was a crucial factor in determining the consequence of the failure, see section 6. A small leak may, of itself, pose little or no threat to the safety of the core. However, a small leak could result in a steam jet that could disable nearby safety equipment. To ignore this probability in favour of only a large leak could distort the risk analysis, see later under consequence analysis section 6. The most probable scenario, however, is that small leaks will not challenge core damage or offer any secondary risk. There is ever possibility that such a leak would be found before it progressed to a level that would either challenge the core directly or indirectly. Such a situation is generally referred to as 'leak before break' (LBB). The question then becomes, should LBB be recognized within a RI-ISI programme and if so can it be evaluated?

A principle argument for not crediting leak detection would be the assumption that this would mask important components or areas that warrant inspection to identify the degradation before failure. This argument pre-supposes that the principle value of ISI is to detect degradation mechanisms before they lead to failure and thus leak detection systems are only recognized as an additional mechanism that ensure defense-in-depth. Whilst, this attitude toward ISI is correct in the sense that inspection can only be concerned with the detection of degradation mechanisms before failure occurs. If the LBB situation is ignored in focusing limited inspection resources then an overall safety balance may be lost. The group believe that in introducing the concept of RI-ISI, there must be an explicit integration of all measures targeted against risk and that inspection is just one of the many tools. In order to optimise this total balance of risk

reduction, it is necessary to include all measures in the analysis that determines the focus for RI-ISI. Following this logic a LBB analysis is required to obtain as complete a picture of the risk distribution as possible for the following reasons:

1. The major contribution to the risk for core damage for high-risk locations is probably the rupture term (or possibly a large disabled leak) and not the term for small leak. For rupture, the leak detection capabilities play an important role.

2. If leak detection is neglected in the analysis, it presupposes that operators will ignore large leak rates over very long periods of time before rupture occurs. This is not realistic. Leak detection systems are active in the plant regardless of whether the components are selected for inspection or not. To ignore this would unbalance any risk analysis

3. If leak detection is ignored, and if no inspections are assumed, the probability of a rupture will approach the leak probability. If, from a starting initial surface crack, rupture is predicted to occur within the expected operating time of the plant, then there is nothing that will stop the crack from leading to a leak and to a rupture. Baring in mind that a major contribution to rupture is in most cases a crack, which grows with a sub-critical mechanism such as fatigue or stress corrosion, leading to wall penetration followed by further sub-critical crack growth until rupture occurs without detecting the leak. The non-LBB situation (immediate break at wall penetration) is a possible but rare event, which is supported by failure statistics. Thus unrealistically high estimates of rupture probabilities can be the result if leak detection is ignored. Then there will be less possibility to perform a realistic risk categorization and the selection procedure will be driven more by consequences than the actual risk for core damage.

Thus instead of ignoring leak rate detection completely, the group would recommended the use of adequate models for the estimation of leak areas and leak rates.

Any such analysis would have to take account of uncertainties arising from the complex crack shape following the wall penetration and uncertainties in the leak rate evaluation. All of the methods for determining the probability of failure discussed in this section could be adapted in one way or another, to derive the probability of a leak, as opposed to a rupture or fast failure. However, if LBB is to be employed, this question of the leak rate must be addressed. Any model attempting to evaluate the complex crack shape following the wall penetration and uncertainties in the leak rate evaluation would have to follow the SRM path or use simple judgment.

5.10 Summary of section 5

This section has shown that the evaluation of the probability of failure for use in a risk based methodology, must separate these probabilities in terms of the individual components or its sub elements. It puts forward the argument that a LBB analysis is required to obtain a complete picture of the risk distribution.

It has shown that the representation of the separation, or distribution of the basic failure probability, can vary from a simple qualitative measure such as High, Medium or Low, all the way through to a fully analytically based quantitative analysis of the

failure probability of each individual potential inspection site! The question then arises as to whether or not any single one methodology can be said to constitute the 'best current practise'?

The groups response to such a question is 'no'. That it is not believed that any single method can be seen to be universally correct for all situations and hence the best practice. At the same time it is not believed that within the European nuclear industry, a procedure that relies solely on the pontificate of a group of experts to arrive at a failure probability for each component/site, along with an estimate of the resulting leak rate, will be acceptable. Such a procedure would always be too controversial, in that it provides no auditable evidence of how the decision was reached, what factors were being considered, how possible interactions were considered etc.

The group also believe, that it is unlikely that the ongoing development of SRM, will, at least in the near future, be such as to provide a stand alone process for estimating the mire of failure mechanisms/criteria that will be required of a RI-ISI programme.

The above leads TG4 to conclude, that any best practice for determining the failure probability of the individual components/sites will inevitably be a combination of experts, global data, local data and modelling. However, the group believes that the most obvious area of development is that of the SRM analysis. As has already been stated in the text, it will probably never be possible to fully validate any given SRM, however much can be done to verify models one with another. Much can also be done to ensure that the mechanistic modelling behind the analysis is up to date with current model development. Likewise, sub-elements of these programs such as leak rates from defects, onset of unstable crack growth etc. can be checked against experimental data. If the absolute values from this type of analysis are to be accepted, there will need to be considerably more work carried out on comparing the model predictions with world data, despite all the difficulties highlighted earlier.

What is certain is any acceptable procedure will have to take account of the known facts, both globally and locally.

The group feels that since failure probabilities based on SRM type of analysis provides the essential mechanistically based link between any estimate of the failure probability and the actual degradation mechanism that is leading to, then such modelling must provide the fundamental tool for assessing the failure probability. It is, however, accepted that such models will inevitably include expert judgement to a greater or lesser extent and that such models may take the form of attribute models.

6.Analysis of failure consequences

A passive failure event is one involving leakage, rupture, or conditions that would disable a component's ability to perform its intended function. In general, the consequences of failure can be to safety, to the economic operation of the plant or to the environment. It is the purpose of the current document to consider those consequences with implications for safety and economics.

6.1 Nuclear safety

Considering first nuclear safety. Since core damage is the prelude to any nuclear release, be it contained within the nuclear site or not, then this would seem to constitute the most fundamental measure for nuclear safety. The normally accepted measure of core damage is the core damage frequency (CDF). However, core damage may occur with no loss of radiation either within the site or beyond it. Thus the next level of consequence would most logically be fission products release. The normal measure for this is the large early release frequency (LERF). Here, large early release refers to 'a radioactivity release from the containment involving the rapid unscrubbed release of airborne fission products to the environment. The large early release frequency is 'an estimate of the likelihood of a severe accident associated with a radioactive release from the containment occurring before the effective implementation of off-site emergency response and protective actions. Both of these measures evaluate the consequence as an event. The use of LERF would be directly in line with the consequence definition used by the UK Health and Safety Executive in their analysis of Canvey Island in the early eighties, reference 7. In both cases the consequence would be measured in terms of a probability i.e. the probability of core damage or the probability of fission product release. The difficulty with a probability measure is that it is just a probability! Whilst this probability can be combined with the failure probability to provide a risk, this does not, of itself, describe any variation in the severity of the event. Presumable, core damage can vary from minor to catastrophic, the probability does not differentiate unless we prescribe it so! Likewise LERF is the unscrubbed release of airborne fission products to the environment, but does this mean that fission product release in to the plant that would threaten workers is not a consequence of concern!

The next logical step in evaluating the nuclear safety consequence would be to break down the fission product release into levels of release, measured perhaps in terms of Iodine release. This would then provide a consequence measure scaled in levels of release with an associated probability. Such a break down would be in line with the UK HSE document on the tolerability of risk, reference 8. A final step in evaluating the nuclear safety consequence would be to further refine this analysis and estimate the collateral damage and potential loss of life and long term health hazard. A final break down to this level would then explicitly include the plant sighting.

6.2 Economic consequence

A simple measure of economic risk and consequence is 'equivalent plant outage'. This may be defined as the product of the fractional power loss and the duration of the power loss caused by a specific failure. Thus, a failure that causes a 10% drop from full power for 10 days will have same equivalent power outage factor as a failure that causes a complete loss of full power for one day. Equivalent plant outage looks at the

direct and indirect consequences of an event from the viewpoint of plant availability; equally, it is possible to address these more directly in monetary terms. For this it is necessary to establish a measurable consequence in monetary terms for plant availability. This is best expressed in terms of the consequential cost of repair and lost electrical production.

While economic models are in principle available to assess availability/cost aspects, in practice these consequences are usually determined on the basis of operating experience and expert judgement.

In contrast, in a qualitative risk assessment numerical values are not defined for the frequency or consequences of failure. Rather these parameters are placed into qualitative categories such as 'high', 'medium' or 'low', etc. Examples of both quantitative and qualitative assessments of risk and associated consequences will be discussed in what follows.

6.3 General principles of consequence evaluation

Central to the evaluation of the consequences of failure is an engineering analysis of the component or system. The most obvious tool to provide a quantitative assessment of the consequence for a RI-ISI programme is the well-established risk assessment, probabilistic safety analysis (PSA). Indeed it was the growing use of the PRA to assess nuclear plant safety that prompted the early work by Chapman and Balky to adapt its use to ISI.

A PRA provides a measure of consequence in terms of frequency of occurrence of different events, including the breach of containment integrity.

The inputs to a typical level 1[1]. PSA include:

- Plant familiarisation and information collection
- Identification of initiating events and pant damage states
- Plant systems modelling using event trees and fault trees
- Analysis of dependent failures and human performance
- Plant-specific reliability database development

The results of the PSA thus provide an in-depth understanding of plant behaviour because of the creation of interdependent logical plant behaviour models.

Historically, PSA's have addressed the failure of 'active' components (pumps, valves, etc.); more recently the scope has been enlarged to include the failure of 'passive' components, specifically through the consideration of pipe breaks. In order to use the PRA in this more expanded manner will involve an engineering analysis that includes assessment of the failure potential of the pressure retaining boundary and assessment of the resulting primary and secondary effects of any such failures.

In order to use the PRA, the plant must first be broken down in to sub divisions of areas that present the same consequence to the plant. For example, in the USA, where

[1] In a level 1 PSA consequence is considered in terms of core damage frequency (CDF); in level 2 and 3 PSA's consequence is considered in terms of large early release frequency (LERF).

the RI-ISI is only applied to pipe work, the plant pipe work is broken down in to pipe segments. A component segment is defined as a portion of piping for which a failure at any point in the segment results in the same consequence (e.g. loss of the system, loss of a pump train). A segment includes associated component structural elements between major discontinuities, such as pumps and valves.

Determination of the failure potential of a given plant segments must be based on consideration of degradation mechanisms, as well as anticipated loadings, flaw sizes, material properties, etc. The evaluation of associated consequences being based on a consideration of associated failure modes, and the primary and secondary effects that can result from a component failure. An example of the mapping between events and their secondary consequences for RI-ISI analysis is given in the following table, adapted from reference 9:

Event (Leak or Break)	Consequences
Leak	Effects from jet impingement
Disabling Leak or Full Break	Loss of system function
Disabling Leak (plant trip) or Full Break	Initiating event and or effects from flooding
Disabling Leak or Full Break	As above.
Full Break	As above plus effects from pipe whip

With reference to the above table, consideration should be given to the possibility of leaks resulting in failures of electrical components due to jet impingement. Similarly, disabling leaks and full breaks can lead to a loss of system function, flooding induced damage and initiating events. Full breaks can also lead to damage from pipe whip. Implicitly in the above table is the need for an assessment of small leaks as well as large. This in turn implies that a leak before break evaluation in the probability of failure analysis is required. Not to include these two different failure conditions would lead to a distortion of the consequence distribution.

In addition to the above secondary consequences, each segment failure may have one of the following **primary** types of impact on the plant:

- **Initiating Event Failures** when the failure is a direct cause of a reactor transient and may also cause the failure of one or more plant trains or systems
- **Standby Failures** when the failure causes the loss of a plant train or system but which does not lead directly to a reactor transient
- **Demand Failures** when the failure accompanies the demand for a train or system, e.g. as a result of loads associated with reactor start-up

Where the techniques of PSA have been used for the purpose of consequence evaluation, it is noted that the majority of such applications have not represented directly the failure of passive components. Clearly the best practise when evaluating the consequence for the failure of passive components, is to modify the PSA logic to include explicitly the impact of such failures. However, this is not a trivial undertaking. As a consequence the approach adopted in the USA is to introduce the

concept of the surrogate component. Here, the impact of a pipe failure is identified with some appropriate event already modelled in the PSA (note that in the USA only pipe failures are modelled for RI-ISI, see appendix 3). The authors of this document know of no evidence that has been presented to demonstrate that such an approach is either realistic pessimistic or optimistic. However, it is possible to cite circumstances were it could be argued that the surrogate approach might be optimistic. For example, the effect of a disruptive failure at a pipe to pump weld may not be well represented by assuming the pump to be the surrogate and representing the failure as that of the pump failing to deliver water! Not only is there the question of the lost water but the effect on the hydraulic equilibrium which may itself serve to disrupt the operation of some valves in the local vicinity.

Whilst re-iterating the early point that any best practice would be to model explicitly the effect of passive components within the PRA, it is accepted that for the present at least, this concept of the surrogate may well have to be used. It would seem necessary, however, in such situations to ensure, perhaps by an expert elicitation, that the surrogate analysis is felt to be as realistic as possible.

There are two important aspects of consequence evaluation where further comment is required: (a) locations outside of the containment, and (b) small leaks.

a) Locations outside of the containment

It is important to consider locations outside the containment. The reason for this is that ruptures in pipe systems outside the containment, together with malfunction of the closure valves, will drain cooling water from the RPV. This loss of coolant is not recovered via the condensation basin. The role of the containment barrier is thus compromised. Also, it is in general more difficult to detect small leaks outside compared with inside the containment. This may create problems because many PSA-studies only consider pipe breaks inside the containment.

b) Small leaks

Having evaluated the probability of small leaks it is important to consider these within the primary consequences. This may seem unimportant at first, since the consequence of a small leak is much smaller than that of a big rupture. But when it comes to evaluating risk (in which consequence is multiplied by the respective failure probability), the probability of a small leak probability is much larger than that of a large rupture. Therefore, it is not known beforehand which term in the risk evaluation is dominating, the small leak term or the rupture term. A consistent way of accounting for all possible events is to add the contributions to the risk from each of the categories as follows:

$$\text{Consequence from a given segment} = P(\text{small leak})*C(\text{small leak}) + P(\text{large leak})*C(\text{large leak}) + P(\text{rupture})*C(\text{rupture}),$$

where P = probability and C = consequence which must include secondary effects.

Brickstad, et al give examples of the evaluation of CDF in terms of the above equation in reference 10.

The discussion so far on consequence has revolved exclusively around the PRA that implies a quantitative analysis of the consequence. It is possible, however, to evaluate the consequence in a purely qualitative manner. Such an approach could use experts to assess the consequence of systems and then sub-systems down to the segment level as already discussed above. The complexity of a nuclear plant, with its multileveled safety systems and back up capability, would make such an exercise extremely difficult if not futile. Having said this it is interesting to reflect on the early categorisation of components in ASME Section III, which was carried out in precisely this manner. Fortunately there are no nuclear plants within the Europe Commission states, that do not have very detailed PRA's. These PRA's can then be used as a bases for an expert elicitation as to the consequence of failure of systems sub-systems and finally down to segments. The outcome of such an elicitation would then be the categorisation of plant segments in to consequence bands such as the simple three-levelled categorisation; high, medium or low categorisation.

6.4 Summary of section 6

Quantitative and qualitative methodologies for evaluating consequences of failure for use in RI-ISI and risk-informed maintenance have been described. These methodologies are focussed mainly on applications in the context of consequences for safety. Nevertheless, the essential principles upon which the methodologies are based have much in common and are sufficiently generic to be applicable to safety-significant components in general. Whereas the primary focus has been on safety, the evaluation of consequences can be expanded to include a consideration of plant availability. Here, the measurable consequence may be expressed in terms of the monetary cost of repair and lost electrical production during the unplanned plant outage.

7. Combining probability of failure and consequence to give risk

As stated several times already, the probability of failure for a given site must be combined with its consequence in order to determine the risk to the plant from that specific plant site. However for both the probability of failure and the consequence, two basic approaches have been put forward, namely the quantitative and the qualitative. The principles are the same for both approaches but a distinction may be made between the two.

7.1 Quantitative approaches to RI-ISI

In the previous section on consequence, much was made of the role the PRA would play in assessing the consequence. Indeed the PRA is itself a full quantitative risk based or risk informed process for evaluating of the plant. However, as also stated earlier it has, until now, been focused on the role of passive components to plant risk. Thus in a quantitative approaches to RI-ISI, an effort is made to determine or estimate the absolute values of annual failure probability and consequence of failure. The risk may be expressed as a single number being the product of the calculated annual failure probability (yr^{-1}) and consequential damage (e.g. core damage frequency). In this case, a criticality ranking of the components can be made in order of the evaluated risk that would be in terms of a probability of core damage.

The quantitative approach requires detailed mechanical information and is backed by calculations to determine numerically the failure probability and consequential losses. Probably the greatest challenge is in the evaluation of the probability of failure. As stated in the probability of failure section, the values used must represent an estimate relating to the specific site and not a global value.

As with any analysis the approach relies on the input data being accurate and all causes of failure being considered**.** Because this option provides an absolute measure of the risk it is sometimes criticised on the grounds of this absolute value. However, in terms of an inspection prioritisation process, it is the relative value between the risk, not the absolute value that is important. Thus, the absolute risk evaluated by this method can, if so desired, be put to one side and only the relative risk values used. But note, if absolute values are given for regulatory purposes, as for example in reference 8, this would seem to imply the use of absolute values here. The discussion in section 5 on the use of world data as a normalising value for passive failure would appear to play an important role

Clearly the quantitative analysis provides a ranking of the component/sites. However, this ranking is not a simple ordered ranking as it includes the relative risk between each site. This numerical risk ranking can be changed to a relative numerical ranking by simply dividing each individual site risk by the highest risk site. Thus every site has a relative risk equal to, or less than one. The best way to represent this information is in what could be referred to as a normalised risk-ranking plot. In such a plot the horizontal axis's is used to stretch out the ranking sites such that the highest risk site is on the left with descending ranking sites moving to the lowest ranked site on the furthest right of the plot. Thus the risk ranking is now be expressed as a form

of ‘Pareto diagram’ . Figure 3 is just such a plot for a set of fictitious data. However, the linear Pareto diagram is not generally sensitive enough and so figure 3 is re-plotted as a log/linear risk-ranking plot in figure 4.

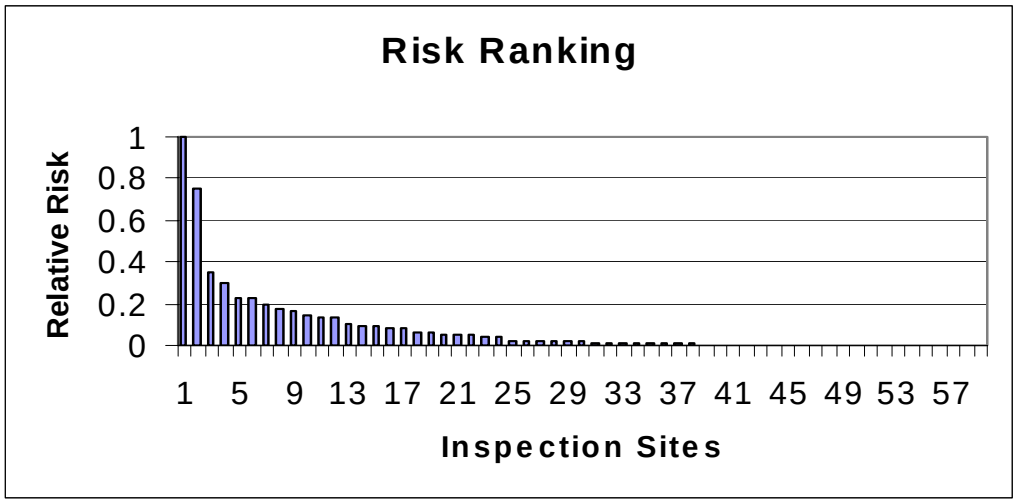


Figure 3: Linear ‘Pareto diagram’.

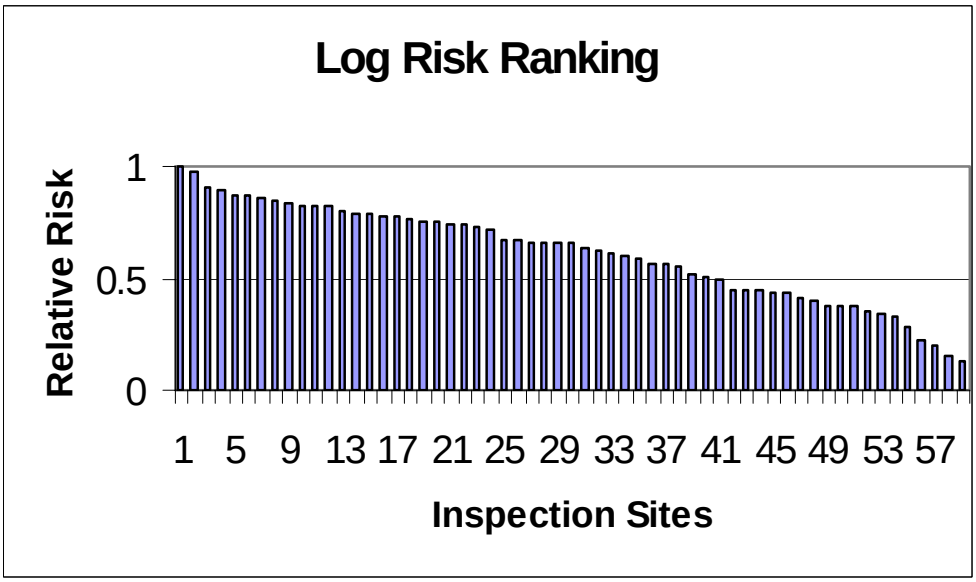


Figure 4: log/linear ranking plot.

Alternatively the data can be split into its two basic parameters, probability of the event and consequence to form what can be called a ‘Risk Plot’. The above data is plotted in this way in figure 5 below, note in this plot, both axes are on a log scale. This plot provides a clear picture of how the risk is distributed over the range of consequences.

Since the definition of risk is the product of the two parameters in this plot, then 45 degree lines on this log/log plot represents lines of constant risk. This representation

of the data means that the data is easily separated by lines of constant risk into bands of risk, thus clearly identifying groups of sites within different risk bands. In this example the high-risk sites can be seen to be distributed across the full range of the consequence

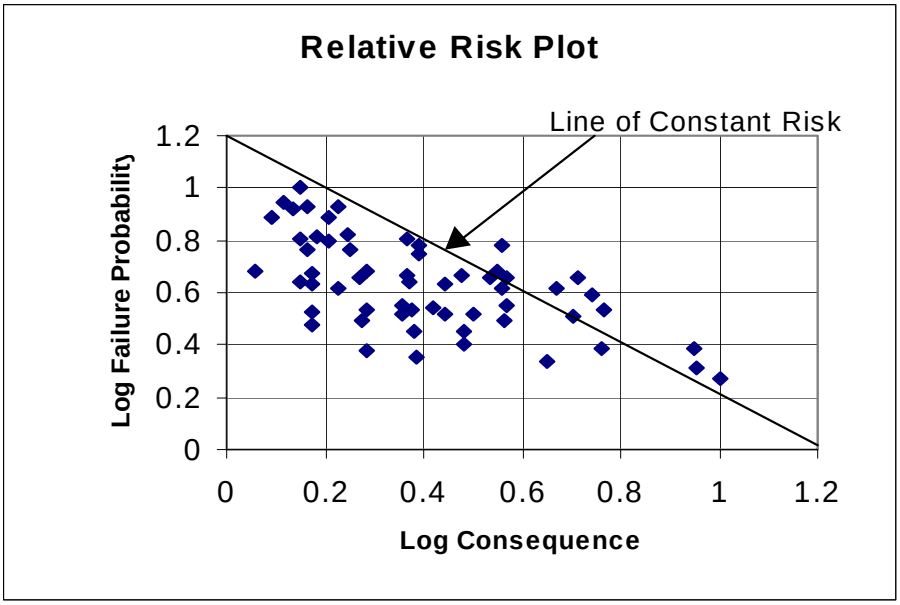


Figure 5: Relative Risk Plot.

.

7.2 Qualitative approaches to RI-ISI

In a qualitative approach to risk informed inspection, the two elements forming the risk, the likelihood and the consequences of failure, are not numerically evaluated in absolute terms, but are subjectively ranked (high, medium or low) or given a scoring on a arbitrary scale. Here, the risk is presented as the combination of failure likelihood and consequence allocated within bands on a likelihood-consequence matrix. Components presenting the same or similar risk may be grouped on the basis of a common likelihood-consequence combination.

The ways for assessing the ranking or scoring of a component vary according to the approach. Some approaches use an expert panel to make subjective judgement after discussing the issues. This approach relies on the engineering knowledge and experience of the panel. Other approaches are based on a scoring system from answering questions within a questionnaire. The lack of an absolute measure in this type of approach can belay or obscure the fact that just as with the quantitative approach, a realistic qualitative estimate relies on an extensive knowledge of the plant system, secondary consequences together with a understanding of the underlying causes of failure.

If a simple numerical scoring or ranking is used in the qualitative assessment then a of numerical ranking can be achieved as follows:

Score ten sites from 1 to 10 where 10 is the highest consequence of failure or probability of failure and 1 is the lowest.

Site	Consequence Score	Failure Probability Score	Risk	Site Risk Ranking
A	3	4	12	G
B	5	8	40	D &H
C	4	6	24	B
D	7	10	70	C
E	6	3	18	E
F	8	2	16	F
G	9	9	81	A
H	10	7	70	I
I	1	5	5	J
J	2	1	2	

This approach was experimented with in the UK for the Royal Naval Nuclear programme and in France, see for example reference 11. With this type of qualitative scoring it is possible to construct a form of risk plot as shown earlier. However, such a risk plot would be misleading because it is tempting to assume that 45 degree lines on such a plot would be lines of constant risk. This would not be the case in this situation because the scorings are not logarithmic.

If only a simple high, low, medium break down is used, then a rank of this kind is limited because there are only nine possible combinations. In this case the ranking can only be illustrated on a form of risk plot as shown in figure 6.

Probability of Failure				
	High	*High Low*	*High Medium*	*High High*
	Medium	*Medium Low*	*Medium Medium*	*Medium High*
	Low	*Low Low*	*Low Medium*	*Low High*
		Low	*Medium*	*High*
		Consequence		

Figure 6 Qualitative risk plot

Where *High Medium risk = Medium High risk*
High Low risk = Medium Medium = Low Medium etc.

In this type of plot it is always assumed that there is a direct equivalence between the consequence and probability ranking in terms of the risk. This then implies that the high, low, medium scoring is a logarithmic scale i.e. there is a factor of 10 between each range. This in turn implies that, in this example, the consequence range and the probability range covers three decades.

7.3 Choice of approach

The choice of either a qualitative or a quantitative approach is based on the level of detailed information available and the level of rigor and confidence required for regulatory acceptance. The nature of the simpler qualitative approach is that it can only act as an indicator of risk, and does not constitute a risk assessment. As a tool its best use is as simple screening method that can be used to identify the areas of highest risk and prioritise them for more detailed exercises.

The costs of undertaking a detailed quantitative analysis is, however, quite high and will need to be weighed against the potential benefits. In addition to this, finding correct and reliable data for all quantitative inputs can be difficult. As discussed earlier, information on such things as the density and size distribution of defects or the rate of stress corrosion cracking will be difficult to derive. For many situations, therefore, a phased manner of introduction may be appropriate. A significant benefit can be gained by first undertaking a qualitative assessment on a component level. This can then act as an initial screening process and once this is achieved an assessment analysis could be undertaken to see whether or not a more thorough quantitative analysis would be beneficial.

8.Gathering feedback from operation of plants

During the early stages of a component‘s life, non-destructive examinations (NDE) are often stipulated on the foundation of stress and fatigue analyses results based on specified design loads. But experience from operation of plants shows that design analyses are only of limited value for inspection planning. The primary reason for this is that the purpose of these analyses is to demonstrate only that stresses and end-of-life usage factors are within allowable limits. There is, therefore, a tendency for designers to use conservative loading and number of cycles stress levels in the evaluation of these design usage factors, as long as they can show the factors are meet. Furthermore, these highest stresses and usage factors may arise due to level B loading, which may never happened in a component’s life. As a result inspection locations based on these analysis may not be focused on areas of high failure probability or high risk. Hence, analyses with more realistic input data are required to adjust NDE-measures. In order to improve inspection planning not only realistic stress and fatigue levels are required, but also results from previous inspections and experience from operation of other plants have to be considered. Thus, “feedback“ is essential for ISI-optimisation. The following sections deal with the question; “which information from operation of plants is required for RI-ISI and in what form must this data be presented?”.

8.1 Basic data requirements for RI-ISI

As described in the previous chapters, within the RI-ISI approaches the optimisation of ISI programme is based on an evaluation of:

1 the probability of failures and
2 the consequences of failures.

Thus any data gathered to aid the optimisation of a RI-ISI programme must address one of these two evaluations.

Feedback information, such as failures occurred world-wide or failure frequencies can be drawn from literature or specific plant reports or from databases. Since this information reflects operational experience with failures it can only be used to deduce failure probability not failure consequences.

To address the question of consequence, feedback on plant modifications and operational changes will also be required. In this way an ongoing analysis of the plant risk assessment, or living PRA, becomes a necessity for a fully operational RI-ISI programme.

8.2 Requirements of data on failure probability

Several sources of information exist for the above data, unfortunately however, a review of these databases is outside of the scope of this work. However it is important to establish the fundamental requirements of any such data for use in a RI-ISI programme.
The data contained in such databases are often “world data“, which can only be used for assessments in a global sense and cannot be transferred directly to a specific plant. Many failures develop from coinciding influence factors which means they are

dependent on plant-specific design and operational factors. Sometimes not all the information that is necessary for the correct use of the data exists. Hence, the user of a database must establish the relevance of the data and whether or not the data are suitable for a given application. Appendix 2 from section 5.4 gives a more detailed account of assessing the failure probability from such data.
Operating experience shows often only a small number of events for a specific situation. The uncertainty is therefore considerable. On the other hand it is not always clear whether the data are found by a statistical analysis of operating experience or are derived from probabilistic fracture mechanics studies.

The conclusion is that the information contained within databases can be very helpful for a qualitative risk assessment, but a lot of additional information is required in order to get reliable plant specific results. Careful use of any databases is therefore recommended.

8.3 Required information from operation of plants

In order to improve the quality of risk assessment, lot of input information is required. Specifically, the following items has to be considered:

- type of system (primary circuit, feed-water system etc.)
- identification of failure modes (leak, disabling leak, break)
- degradation mechanism
- fault location within the component system
- geometric nature of site (pipe elbow or tee, terminal end vessel weld etc.)
- defect sizes and flaw distributions
- age of system/component
- structural element characteristics (butt welds, socket etc.)
- component material
- material properties (testified values)
- component design and operational stresses
- component support conditions
- expected usage factor (actual/design value)
- operating conditions (thermal cycles)
- mode of operation
- dynamic loads
- water chemistry
- sources of external corrosive attaches
- existing monitoring systems
- pre-service and in-service inspection results and repairs
- current ISI program, ISI drawings,
- results from post-inspection (e.g. metallurgy)
- plant operating experience (previous failures) and industry related failures.

8.4 Analysis of possible extensions of currently existing databases

From the previous section it can be seen that for a reliable risk evaluation detailed information is required, which is often not provided by the existing databases. The above list could be used to produce suitable guidelines to establish the specific

requirements that a “failure database” should satisfy. Additional benefit could be gained, if information on possible damages detected before failures is provided.

9.The unknown or ‘Factor X’

A persistent criticism of the risk-based methodology is that it does not address the ‘unknown’! Since the basic premise of a RI-ISI strategy revolves around an ability to identify where the maximum risk to the plant is focused, it would seem self evident that such a strategy could not be one that seeks to find the unknown. In terms of ‘Risk’ such an unknown situation can be considered as a virtual risk. This is because the risk cannot be identified or measured and compared with any other risk. It is instead, almost a personal perception that there is always this hidden risk and that if one looks hard enough one will eventually find! However, even this last logic is floored, since if we find a new risk, it then becomes a known risk, which simply leaves the unknown risk! In essence this becomes a question of completeness. How can we be sure, that our experience to date is such that our knowledge of the degradation mechanisms that apply to nuclear plant is complete. This returns us to the statements made in the introduction of this document, that the risk based philosophy is built on the extensive knowledge that has built up through the large number of operational years experience.

9.1 A virtual risk

Since the risk of the unknown is a virtual risk i.e. a question of our individual attitude or fears toward risk, our confidence in the experience to date etc. it is difficult, if not impossible, to fully satisfy such fears. What follows, therefore, is not a answer to such fears but a rational comparison between a RI-ISI strategy and any other strategy, involving the same inspection size, in terms of the ability to find an unknown situation.

It is first essential to establish the axioms of this discussion; these are relatively simple and can be stated as follows:

1. There is a prescribed boundary to the inspection scope.
2. The degradation/failure mechanism is not a postulational situation (see next section for discussion on postulated situations).
3. That the unknown degradation/failure mechanism can affect any site within the inspection boundary.
4. The probability of detecting the unknown degradation mechanism is the same for any given inspection, independent of the strategy.

With the above axioms in mind, consider the following problem:-

1. A bounded inspection volume consisting of ‘N’ possible inspection sites, where ‘N’ is exhaustive.
2. An unknown degradation/failure mechanism that effects ‘Q’ of these sites.

At the end of a risk assessment analysis there will exist a ranking list of the ‘N’ sites in terms of their risk to the plant. This ranking must be independent of the unknown degradation/failure mechanism because this unknown element played no part in evaluating the risk. Let ‘RS’ be the number of sites that are designated as risk significant i.e. the number of sites to be inspected using the risk-based philosophy.

The question now arises, "what is the probability that one of these inspections will occur at a site that has the unknown degradation/failure mechanism?"

If it is assumed that within a given inspection we do not inspect the same site twice, then the problem becomes a relatively simple statistical sampling problem without replacement. Such a problem is described by the hypergeometric distribution solution where:

$$\text{Probability of 'y' Successes From an inspection sample} = \frac{\binom{Q}{y}\binom{N-Q}{RS-y}}{\text{Size of 'HR' sites from a Total Population of 'N' sites}}$$

$$\text{The expected number of Successes} = \frac{RS * Q}{N}$$

The definition of success in the above, is the successful inspection of a site that contains the unknown degradation/failure mechanism. Thus if the number of inspection sites was 10% of the total population, then the expected number of successes would be 0.1 times the number of sites affected by the unknown degradation/failure mechanism.

This is, however, not the probability of detecting the unknown degradation/failure mechanism. If the unknown is a failure mechanism e.g.. some form of unknown material embritlement, then the inspection is not likely to provide any forewarning of the unknown problem! Likewise, if the degradation produces some form of cracking which has a morphology that is new to the data interpretation engineer, then the inspection capability will probably be very low. Indeed, experience has shown that until problems have full manifest themselves through failures the inspection capability has generally been very low.

Clearly everything in the above paragraph applies to any inspection programme because it is not possible to target any inspection technique against an unknown mechanism! Thus the only meaningful criterion to compare different site selection processes, is the criterion of successfully inspecting a site with the unknown degradation mechanism.

Using this criterion, consider an inspection where the sites are chosen purely at random. Assume R random sites are chosen. The unknown degradation mechanism must, by definition, be independent of the random selection process no matter what it is! Assuming, as before, that no site is inspected twice. This again leads to the hypergeometric solution where:

$$\text{Probability of 'y' Successes from an inspection sample} = \frac{\binom{Q}{y}\binom{N-Q}{R-y}}{\text{Size of 'R' sites from a Total Population of 'N' sites}}$$

$$\text{The expected number of Successes} = \frac{R * Q}{N}$$

Thus if the number of inspection sites R, was 10% of the total population, then the expected number of successes would be 0.1 times the probability that the unknown mechanism effected any given site. This is identical to the RI-ISI outcome and as can be see, if 'RS = R', the two equations are identical.

From the above it would seem clear that the probability of detecting an unknown degradation mechanism, at a single inspection period, is dependent only on the size of the inspection sample. This is simple because the unknown mechanism must be independent of the way of selecting the sites for inspection, be it risk based or any other!

Having set out the above case, it will be seen later in section 10.2.1 on the possible inspection of high consequence low failure probability sites, that a form of inspection against the 'unknown' can be a specified part of a RI-ISI programme!

9.2 The postulated situation

The preceding discussion on the unknown should not be confused with a 'postulated' degradation mechanism. In the postulated situation, a case is being put forward for a known degradation mechanism to exist, within the known loading or environmental conditions associated with the site. Thus, although it may be felt that this known degradation is not actually occurring, the mechanism cannot be ruled out at a high enough level of confidence. In this situation the inspection can be seen as a data gathering exercise. The objective of the inspection results being to provide confidence that the mechanism is indeed absent i.e. that the postulation is false.

The basic rules of the risk-based philosophy can still be applied in this situation. If it were possible to postulate a degradation process that could be present, it would seem reasonable to estimate some bounding levels by which this postulate would enhance the otherwise normal degradation. These bounds can be used to estimate an enhanced failure probability that can be combined with the consequence to see if the site becomes risk significant. This will then provide valuable information to help determine the required inspection capability and hence the inspection methodology and any necessary inspection qualification.

It is possible, however, that the work required to estimate the above probabilities and consequential risk may be difficult and costly. In such situation it may be more cost effective to simple carry out the inspection.

It must be remembered, however, that the primary objective of such an inspection is to identify if the postulate is true or false which takes us back to the comments in section 4.4 on reducing prior uncertainties. If the postulate were proved to be true, then the relative risk ranking of the site would change. However, if the postulate is shown to be untrue, then the site will return to its original risk ranking position, which one assumes is a none risk significant ranking. All that remains is to determine how much information is required from the inspection to test the postulate!

10. Definition of effective ISI programme, and qualification strategies based upon risk assessment

The determination of the probabilities of failures and consequences of failure makes it possible to rank the different structural elements in terms of risk. This risk ranking being achieved, the problem is now to use this information so as to most effectively address and consequently reduce this overall risk, be this measured in absolute risk or simply in relative risk. ISI is just one method of addressing the risk, design changes, operational changes, material replacement are other examples of the options available within a whole plant risk based philosophy. Clearly if one of the alternative options is chosen to address a given potential risk, then the ISI programme would need to be modified to reflect the changes and refocus the NDE effort to provide the maximum return for what is a considerable investment. This is what is meant by a living PRA.

10.1 General

Having defined the risk ranking against which the RI-ISI programme is to be targeted it is necessary to define an optimal inspection strategy. The definition of the strategy is not limited to the selection of the inspection locations, but must also provide the relevant input information for the qualification of the inspection. In other words, we must know precisely what we are looking for in each of these locations, but we must also account appropriately for unknown mechanisms. The group believes that the definition of an effective RI-ISI program should be based on the following principles:

1 concentrating limited and costly resources on systems and locations most relevant to plant safety and/or availability (i.e. the locations identified as corresponding to the higher risk);

2 identifying which damage mechanisms may be operative at specific locations, in order to select appropriate inspection methods and procedures for these damage mechanisms (defining the inspection objectives and input data).

The risk being defined as a combination of a probability of failure and of the consequences of this failure, the inspection strategy can only aim at reducing the probability of failure, by detecting in time a degradation of the equipment. Inspection has obviously no impact on the consequences of a failure. The present chapter lays out the general guidelines on inspection strategy as seen by TG4, whilst appendix 3 provides a review of the position in the USA and Europe.

10.2 Basic approaches to risk-informed in service inspection

Approaches based on traditional PRA's that focus on active component failures and include the passive failure probabilities as a single global value, will link the inspection back to the frequency of core damage or a large early release based on the system performance only. These approaches can not be considered as a true risk assessment based on the passive components.

Introducing the passive failure into these analyses, as described in this document, will provide a truer risk assessment but a risk still based on the system failure only. The introduction of the secondary consequences will provide the truest risk assessment based on the failure of passive components but again this is only in terms of the system performance. This system performance does not, however, consider the effects of support structures. It is possible, when considering the effects of an earthquake that support structures become the dominating failure. The addition of these structures and their effect of the pressure boundary would seem to complete the risk assessment of the passive components.

10.2.1 Selection driven only by risk

If a strict adherence to risk as the decider of where to inspect, two possibly undesirable situations may occur:

1 High probability of failures in situations of very low consequence may be deemed as acceptable because of a low risk.

2 Areas of very high consequence may be deemed acceptable because an accompanying low failure probability may again make the area, low risk.

The first of these two situations implies that whilst the direct risk contribution from low consequence areas may not be of concern, there is separate unacceptable level of failure probability for these areas. This belief would follow from a belief that the overall level of the passive plant reliability is indicative of the overall plant safety. Such a situation is easily catered for in the risk-informed ISI programme by stipulating an uperbound unacceptable failure probability. The inspection domain, within the risk plot, would then not be bounded by a constant risk line.

A first reaction to the second situation is then to follow exactly the same logic and specify an upper bound consequence that is not acceptable. The inspection domain within the risk plot would then simply include this area as well. It will be seen in a moment that there are difficulties with this last concept but first let us see how the above is represented on the risk plot shown in figure 5 of section 7.1. The boundary to the inspection area that follows from this approach is shown in figure 7.

In this plot, area A is the acceptable area. Elements, or inspection sites falling in area B are inspected because their risk to the plant is to high. Sites in area C are inspected because whilst they do not of themselves constitute an unacceptable risk, there is an accepted perception that failures of this frequency undermine the safety culture of the plant. Area D is inspected because consequences of this level are not acceptable.

However, as stated earlier, there is a difficulty associated with this last logic associated with area D. Inspecting sites in area B and C will drive the risk down in both cases toward the acceptable level. But inspection in area D cannot drive the site into the acceptable area because, as has been stated earlier, the inspection cannot affect the consequence. Thus it must be accepted, that if there is a consequence level that is deemed to be unacceptable, inspection cannot, of itself, correct any situation that is above this unacceptable consequence level. Thus inspecting sites in area D,

must have a different logic associated with it. One possible logic, is to argue in terms of the failure probability associated with any site that appears in this area.

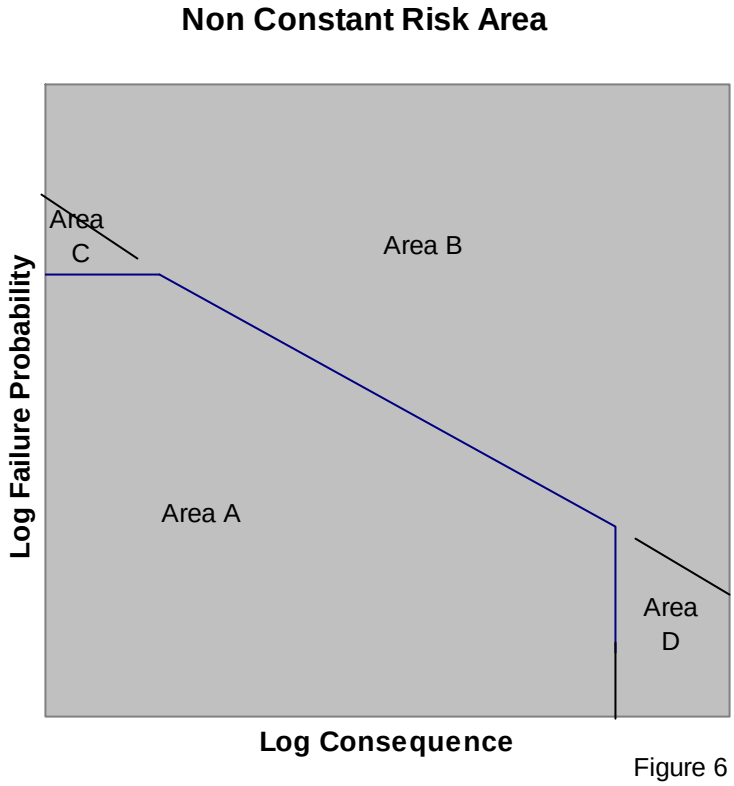


Figure 6

Figure 7. Non Constant Risk Area

In order for the risk to be low in area D, there must be a very low probability of occurrence associated with the very high consequence. This low probability of occurrence will derive from two separate probabilities. The first is the conditional probability that is a function of the safety system. That is to say, it is only possible to get into this area following a failure at the given site, if
and only if, a series of system failures occur after the initiating failure. In other words, the probability is not solely dependent on the probability of failure of the component itself. This situation is generally referred to as one with a
significant defence in depth behind the initiating event. The second situation is one were this defence in depth does not exist. The low risk is then dependent largely if not solely upon a very low probability of failure of the actual site itself. If one then agues, that it is impossible to derive any confidence in such a low failure probability, the ISI of such a site could be argued for on a defence in depth logic. This logic being as follows:

> *An analysis or assessment of the site has inferred a very low probability of failure of the site, which in tern makes the site none risk significant. However, there exist insufficient world experience to provide any significant level of confidence in this assessed low probability of failure! Thus the ISI provides an element of 'defence in depth' which cannot be provided by the system.*

From this logic, it can be seen that the inspection is not directly targeted at reducing the risk but at gaining confidence in the assessed risk. In this way such an inspection might well be considered as an inspection to cover an unknown degradation mechanism that could challenge the integrity of this component. Thus, within this RI-ISI it could be argued that an inspection for the 'truly unknown' is included.

10.2.2 Two different starting points to a risk analysis.

Since a risk analysis involves both the consequence and the failure probability this would suggest that the stating point, either consequence or probability, would not matter. Strictly this conclusion is true, however, in practice there can be a difference in the end result.

As stated earlier, a normal PSA based on active components, does not provide a risk ranking for the passive components within the system. If we consider an approach that starts from a traditional active component driven analysis this will identify the high consequence systems and sub-systems of the plant. These high consequence areas could then be broken down into possible inspection sites and the probability of failure of the individual sites evaluated. These can then be combined to produce a risk ranking that determines the inspection plan for the plant. However, such an initial screening, only screens out low risk sites from a purely system performance stand point. Such a screening may remove potential high risk sites within the passive component risk ranking, that derive there risk from a low system consequence but high failure probability. Such a procedure would, therefore, focus the inspection ranking into the medium to high consequence area of the risk plot. By doing these possibly medium-risk sites in the low consequence high probability of failure area of the plot could be missed. Thus whilst an existing PRA is an obvious and very efficient way to commence an initial screening, the above possible shortcomings should be guarded against.

An alternative approach is to start from 'known high failure probability sites'. This focuses attention primarily on the conditions that may give rise to defects and degradation during service and their time dependence. It also focuses attention on the extent and confidence in the knowledge to which these conditions are known or not known by applying appropriate conservatism within the assessment. This approach requires a considerable amount of information about the conditions at every weld or potential failure site and how these relate to the defect or degradation mechanisms. In reality such situations are often controlled by the most resent failure or potential failure hypothesis. Concentrating on the probability of failure first and then assessing the consequence associated with the high failure probability sites will tend to neglect the area of risk that are controlled by the high consequence element of the risk equation.

It will probably be impractical if not a simple waste of time to carry out a full analysis of both the probability of failure and the consequence for every potential site. Thus a mixture of both approaches will almost certainly provide the most economical way forward. Indeed the knowledge we have accumulated to date on failures and consequence will probably be sufficient to carry out an initial screening to eliminate the large number of elements within the plant that fall in the lowest risk category.

However, there is a final area of risk that the above does not address. This is that risk which derives from any secondary consequence of a passive failure. In order to protect against this risk, an extensive knowledge of the true geographical lay out of the plant must be achieved. Such knowledge will not reside within the normal system diagrams and will require a detailed walk through the site to identify potential effects.

10.3 Extent of the inspection and selection of inspection locations

The general principles for establishing the inspection programme are:

1 To focus the in-service inspection on the locations associated with the highest risk, where risk is defined as the "product" of the probability of failure and of the consequences.

2 Use qualified inspection techniques, adapted to the degradation mechanism, in order to maximise the potential for identifying, through NDE, component degradation prior to failure.

The group believes that the basic purpose of an in-service inspection programme is to decrease the plant risk by decreasing the probability of failure, inspection having obviously no impact on the consequences of a failure. However, as already discussed, within the definition of risk it is possible, indeed one will expect, to find high consequence sites with a low risk, area D in figure7. This would be due to the low probability of occurrence of the situation. If such situations occur were there is no defence in depth, i.e. there in only one barrier against fission product release, (typically the case for the Reactor Pressure Vessel), TG4 believe that inspections will be required even if the risk is deemed to be acceptable. Such an inspection would not be directed at further reducing the probability of failure, which by definition must already be low enough to identify the site as none risk significant compared with other sites but to provide confidence in the predicted failure probability. Such an inspection could be seen as insuring that no unexpected or unknown degradation appears.

At the other end of the range, it may be recommended to consider also location of low failure consequences and high probability, area C in figure 7. This is because any failure, even without serious consequences, reduces the overall confidence in the plant and may have a negative impact in the public opinion.

The group believes that simple common sense shows intuitively that an inspection strategy based on risk considerations should be an improvement as compared to the current strategy, largely based on the design stresses. The practical implementation and regulatory acceptance of a risk-based inspection strategy raises however the question of the required extent of the inspection. In other words, starting from the top elements in the risk ranking, we must define where, down this ranking list, it is justifiable to stop inspecting.

The risk procedure provides only a ranking of all the possible inspection sites in terms of the chosen consequence. Whilst it is self evident that the inspection should be concentrated on the top elements or inspection sites, in this risk ranking, there is nothing, inherent in the process that identifies where, down this ranking list, it is justifiable to stop inspecting. The view of the European Safety Authorities is likely to

be oriented towards some inspection programme that in some way maximises the risk addressed by the in-service inspection programme. Unfortunately, it follows from simple logic that the more locations that are inspected the greater the proportion of the risk that is addressed. Hence there is no maximum, the risk addressed is always a monotonically increasing function with the number of inspection sites.

The next section tries to present a rational methodology for identifying when to stop. Clearly it cannot be based on some local maximum in terms of risk reduction and so two possible situations are considered:

1. A relative ranking.
2. A relative risk plot.

Whilst both these cases are only relative, they require a quantitative evaluation of the risk in order to provide a criterion. A qualitative ranking can not be used in what follows.

10.4 The Relative Quantitative Ranking Criterion

Having derived a qualitative risk ranking, this is reduced to a relative numerical situation by simply dividing each individual site risk by the highest risk site. Thus every site has a relative risk equal to, or less than one. The need for a quantitative starting point is so that each site has a numerical ranking that reflects its relative and measurable difference from any other site.

The risk ranking can now be expressed as a form of 'Pareto diagram' as shown in figure 8. However, as stated in section 7.1, the linear Pareto diagram is not sensitive enough for our use and so figure 8 is re-plotted as a log/linear risk-ranking plot in figure 9. This takes up to the same point as described in section 7. The next step is to assess how a proposed inspection programme would affect this plot?

The effect of inspection on any given site can be taken as a relative reduction in the risk from that site. For example if, at the time of the inspection, the degradation process has reached a level where there is a 90% probability of it leading to failure and the proposed inspection has a 90% probability of detecting that level of degradation. Then, assuming the remedial action effectively reduces the probability of failure to zero, the probability of failure after inspection reduces from 0.9 to 0.09 i.e. a reduction of ten. To evaluate this reduction correctly requires integration over the full degradation range, however, the outcome must be some level of reduction in

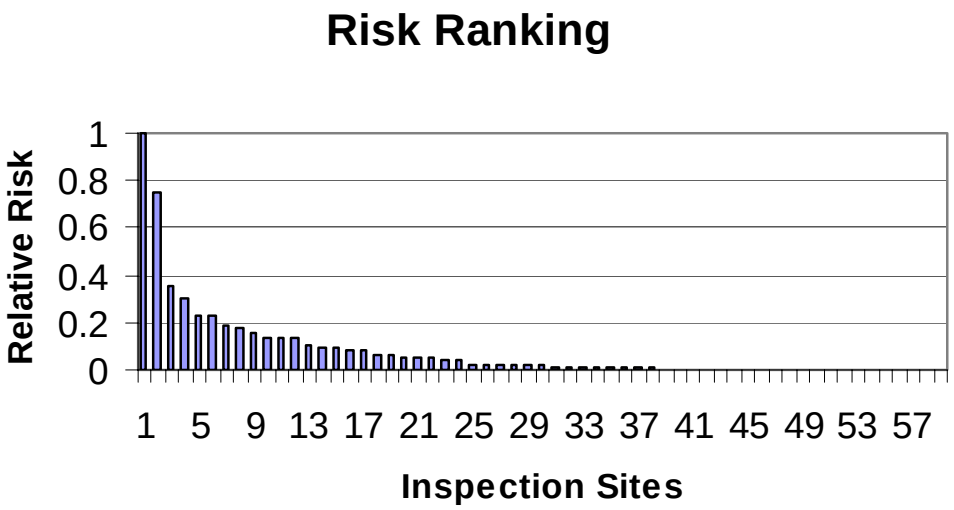


FIGURE 8 Linear Risk Ranking or Pareto Diagram

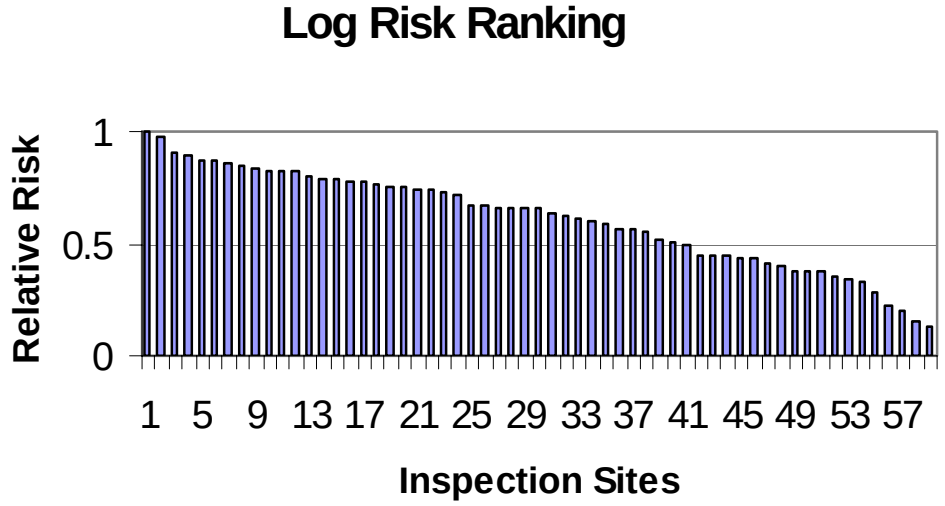


FIGURE 9 Log Risk Ranking

the probability of failure which can be seen in terms of the inspection capability. Just what level of reduction can be achieved is, of course, arguable. However, if it less than ten, one might argue that there is little point in the inspection in the first place? On the other hand, to argue that it could be of the order of a factor of one hundred could be optimistic. Thus a value of between ten and fifty might be considered as a reasonable value. Given the definition of risk, any reduction in the failure probability feeds directly to an equivalent reduction in the risk. Thus if the highest risk site, in the figure 8 Pareto diagram, is inspected, its estimated risk must be reduced to a value between 0.02 and 0.1. Likewise the second highest risk site would drop from 0.75 to

between 0.014 to 0.075 and so on down the Pareto diagram. This produces a new logarithmic risk ranking as shown in figure 10 were the inspection is taken up to the 19th ranked site.

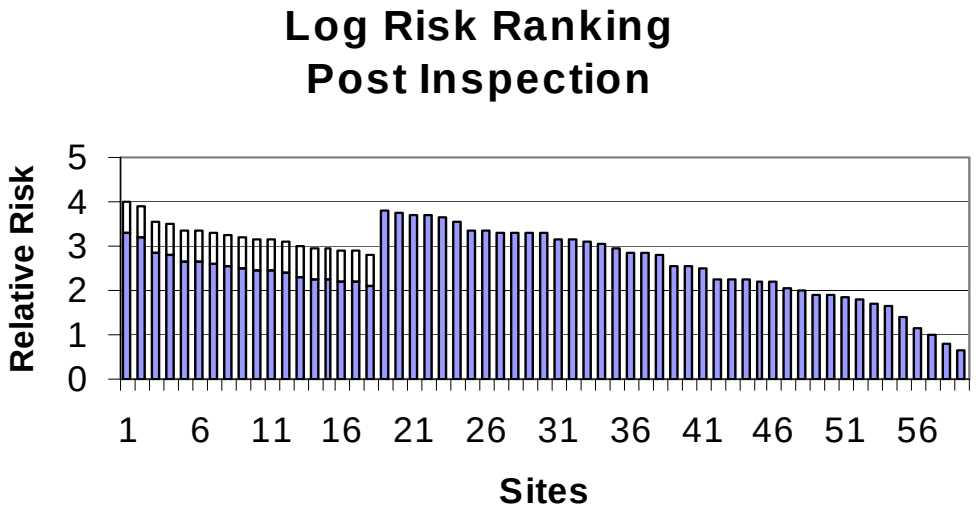


FIGURE 10 Log Risk Ranking Post Inspection
(White area represents uncertainty in inspection capability)

It can be seen from this plot that if the inspection efficiency is only 90%, to continue to inspect beyond the 19th site, is no longer to be addressing the highest risk sites!

The basic Pareto logic makes it clear that to continue inspecting beyond this site provides a rapidly decreasing return in risk reduction for the increased effort. It would, therefore, seem logical to stop inspecting beyond this point. Taking account of the possibly greater inspection capability and adding a small allowance for uncertainty in the ranking, then inspecting down to a relative risk, a factor of fifty to one hundred below the highest risk point, would seem to constitute a logical limit to the inspection programme. Figure 11 shows the effect, on this hypothetical example, of going down a factor of two decades from the highest risk site. This plot shows the original highest risked site again becoming the highest risk site even after inspection.

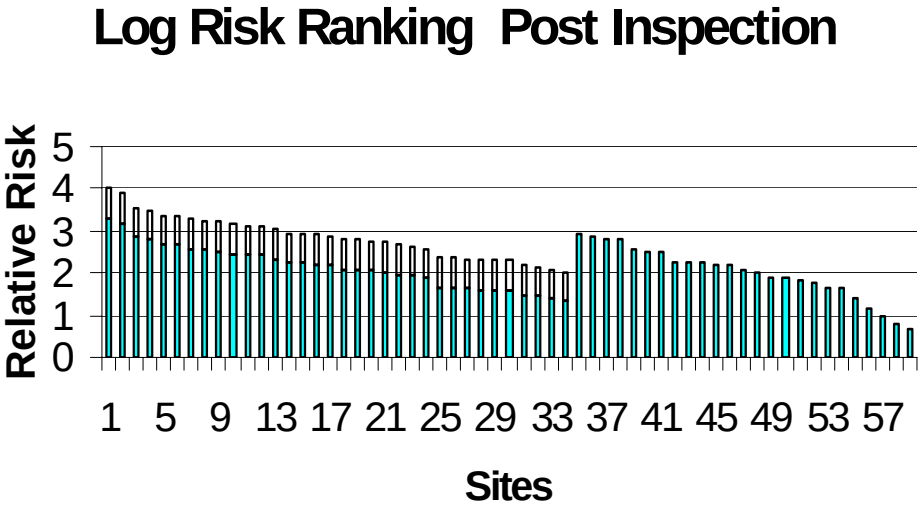


FIGURE 11 Log Risk Ranking Post Inspection

With this procedure, it is possible, for any assumed inspection capability, to identify the point were continued inspection would produce little reduction in total risk. If it can be assumed that a modern in service inspection can provide a 95% capability, then a reasonable criterion for setting the inspection cut off would seem to be, two decades below the highest risk site.

10.5 Consideration of ALARP and possible criteria for level of risk acceptance

Another aspect that must be taken into account in the nuclear power plant context is that of ALARP (As Low As Reasonable Practical). Increasing the number of inspection locations increases the dose received by the workers, causing a true risk to their health. The increase in real risk for the workers must be balanced against the potential decrease in risk for the public. The group believe that the use of the inspection ranking and the effect inspection has on the integrated plant risk can be used to investigate an acceptable dose/cost level to optimise these conflicting requirements.

It is also clear that in the present increasingly deregulated electricity market, utilities will only embark in a risk-informed in-service inspection approach either if it is a requirement of the safety authorities, or if it can be demonstrated that the cost-benefit aspects are favourable. We must therefore find an acceptable balance between a purely economic-driven approach and a purely safety-driven approach.

An attractive approach, that would complement the logic in section10.4, would be to compare the risk reduction, or even risk addressed[1], from a proposed RI-ISI with that from the current ISI programme in place at any given plant.. This means that high risk components shall be chosen for inspection that, together with the effectiveness of the

[1] The risk addressed is the risk from the proposed ISI sites. The risk reduction takes into account the effect of inspection capability/efficiency on the risk addressed.

ISI and the inspection interval, can be shown to generate a decrease in the total risk. The present selection rules of inspection locations being in many cases unrelated with the real risk, it should be possible to decrease the number of locations to inspect while at the same time decreasing the overall risk.

This implies a need to have a quantification of the risk, in order to evaluate the impact of the new inspection strategy as compared to the existing one. There is a rather large consensus in Europe on the need for quantitative probability of failure analysis.
There are cases, however, where the determination of the probability of failure is not feasible or meaningful, for example for phenomena that are difficult to evaluate accurately like high cycle thermal fatigue. In such case, a qualitative risk ranking (based in this case mainly on the consequences) is a more reasonable option. Qualitative arguments may then be used to justify that the Risk-informed inspection program results in a (non-quantified) improvement of the CDF.

10.6 Inspection qualification requirement

Within the European framework, ENIQ has developed a methodology, reference 12, for the qualification of inspection procedures, equipment and personnel for safety-significant components. Such a qualification will demonstrate the capability of detecting the type of defect that is relevant for the degradation mechanism that is acting at a given location. This implies that the inspection objectives and qualification requirements must be precisely defined as per the ENIQ requirements.

The use of qualified methods improves the inspection efficiency and is therefore more effective in reducing the probability of failure, which can be taken into account in the evaluation of the global effect of the risk-based program as compared to the "traditional" one. However, there is nothing specifically within the RI-ISI methodology that requires inspection qualification. Thus if the RI-ISI is being used against a purely commercial criteria, then the decision to qualify the inspection or not will rest with the utility management. TG4 would, however, recommend that even in these situations a level of inspection qualification be considered in order to ensure that the potential commercial gain from the inspection is to be realised.

In terms of a 'postulated' degradation mechanism then the information required for qualification must be based on the assumption that the postulate is true. However, in such situations it may be considered sufficient to provide only a 'statement of capability' of the inspection method (defining the size of cracks that can be detected), rather than a full qualification.

Defining the type of defect implies that the type of degradation mechanism acting at the location is known. As we have seen, this is not a problem for the postulated situation, however, this raises a serious question in terms of any inspection targeted at the "unknown". In section 10.2.1 a possible such situation could occur if inspection is carried out on a none risk significant component because of its high consequence. Since there is no known or postulated degradation mechanisms: how can we select an inspection method and define inspection and qualification objectives if we do not know what we are looking for?

There are two possible ways forward, one using a PRM the other a form of deterministic analysis known as 'defect tolerance'. However, both must be associated

with a measurable degradation such as crack growth. Within a PRM analysis it is very easy to increase the mean crack growth rate to identify a rate that would raise the failure probability and hence the component risk, to the unacceptable level. An inspection could then be introduced into the PRM that would identify the defect size that would need to be found by inspection in order to drive the probability back down again to an acceptable level. A similar approach can be adopted for the 'defect tolerance' approach. Here a postulated start of life defect could be used and the crack growth rate required to grow this postulated defect to failure could be evaluated. Given a time at which the inspection is to take place, then gives a defect size that needs to be found, at that time, for inspection qualification. Whilst both give a target size, since there is no plausible mechanism to cause this level of crack growth, no specific defect type could be given for the qualification. This requirement for inspection qualification would have to be agreed between the parties. In both of the above cases, it is more appropriate to consider a "statement of capability" of the inspection method (defining the size of cracks that can be detected), rather than a full qualification.

10.7 Strategies other than inspection

As stated in the introduction to this section, in-service inspection may not always be the most effective strategy to reduce the overall plant risk. Alternative methods can sometimes be more effective in this respect, and sometimes at a lesser cost. These alternatives must clearly be taken into account in the definition of an effective inspection strategy.

Some degradation mechanisms can develop suddenly and cause structural failures within time periods shorter than the proposed inspection intervals. Examples are excessive vibration fatigue and some extreme forms of thermal fatigue. New sources of vibrational stresses can develop from imbalances of rotating equipment or change in effectiveness of component supports. Thermal fatigue stresses from the mixing of hot and cold fluids can develop over the life of a plant from valves that begin to leak as a function of time. In these cases, a more effective strategy may be to monitor the systems for component vibrations, or for temperature conditions that indicate the development of thermal fatigue stresses.

Design or operational procedure modifications could be implemented in order to suppress active degradation mechanisms, reducing the need for inspections.

Continuous methods involving acoustic emission monitoring or leak monitoring can supplement or replace periodic ISI as a means for detecting the progress of degradation in component systems components. Such methods are particularly useful when concern becomes focused on a specific location where degradation is known to exist, and the objective is an early indication that the degradation is growing. This is particularly the case when it can be demonstrated that there is no risk of catastrophic failure, but leaks remain unacceptable. This LBB aspect of the risk analysis was discussed earlier in section 5.9.

Plant monitoring is an effective way of establishing the true plant usage. In this way uncertainty over the type and severity of the loading history seen by different segments of the plant can be largely eliminated. This in turn provides greater

confidence in the assessment of the failure probability. This knowledge seeking monitoring approach is widely used in German plants.

In-service inspection should also be understood in a wider sense than simply the detection of cracks or wall thinning. For example NDE can be used to follow-up on material degradation, like cast duplex stainless steel thermal ageing, for which non-destructive methods are emerging.

The above broader approach to addressing risk is not meant to be exhaustive, however, TG4 believes that these and possible other approaches should be an integrated part of minimising the overall plant risk.

10.8 Re- evaluation or feedback

The determination of an effective risk-informed program requires the development of a feedback procedure based on the risk ranking updating from plant changes affecting failure component probabilities or failure component consequences.

The affected portions of the risk-informed in-service inspection program shall be re-evaluated as new information affecting implementation of the program becomes available (component system design changes, plant PRA changes, plant operating changes, industry-wide failure notifications, prior examination results).

Of course, if a new type of degradation mechanism, previously unknown, is discovered, the whole risk ranking must be re-evaluated and the in-service inspection might need to be redirected to other locations. This active or living process is one of the strengths of the risk-informed approaches. It leads to an enabling process that is both flexible and responsive to emerging problems.

10.9 Summary of section 10

To summarise, the general principles guiding the definition of the inspection strategy are:

- To focus the in-service inspection on the locations associated with the highest risk, where the risk measure is decided by the interested parties.
- To use inspection techniques adapted to the degradation mechanism, in order to maximise the potential for identifying, through NDE, component degradation prior to failure.
- To use qualified inspection methods, which requires to define the type, position, size and orientation of the defect to detect

To consider also :

  - Locations where failures having very high consequences are not acceptable, even if their probability of occurrence is very low, when there is no defence in depth (typical example: the RPV).
  - Location of low failure consequences and high probability, (any failure, even without serious consequences, reduce the overall confidence in the plant)

- To define an inspection scope by taking into account both the safety and economic aspects.

- To consider alternative measures of identifying possible risk, like vibration or temperature monitoring, or leak detection.
- To consider other mitigating action to address the risk other than traditional inspection.

11. Conclusions

Task Group 4 believe that risk has always been an implicit factor in most, if not all, in-service inspection strategies. TG4 accepts, however, that the explicit separation of risk into its two elements of consequence and failure probability is new in the area of in-service inspection but that such a split is a natural progression against the background of modern probabilistic analysis. TG4 believe that the developments in the industries capability of assessing these two independent elements of risk has progressed to a stage that allows there explicate evaluation. As equally important as this technical capability, TG4 believe that the level of operational experience now available world-wide is such as to provide a firm practically based understanding of these two basic elements. The above leads TG4 to the positive conclusion that the explicit use of risk as a basis for determining in-service inspection strategy within the European nuclear industry is now a viable way forward. Furthermore, that the introduction of risk into the formulation of an in-service inspection programme has the potential of providing a win/win situation. By provide a better focused inspection programme this process should be able to better identify and hence address a greater percent of the plant risk than hitherto, thus providing a win situation for the European regulators in terms of improved overall plant safety. At the same time a focused programme should be able to eliminate non-productive costly inspection with the potential of an overall reduction in the cost burden for the operating utility. However, TG4 believes that within the European framework and in order to reap the greatest returns, the introduction of an inspection programme based on risk, is best achieved as part of a complete plant risk management process. Such a process should integrate the broad spectrum of possible actions/palliatives that can be used to address and reduce the overall plant risk. In this way TG4 believe that a common risk-based strategy based around commonly agreed best practices can be introduced within the independent regulatory jurisdiction that exist in the European countries.

12. Recommendations

The conclusions drawn above lead TG4 to recommend an integrated programme to develop the risk based philosophy for introduction within the European Community.

At the core of any such programme must be the development of the currently available probabilistic risk assessment (PRA) models. TG4 believes that the standards of current PRA's existing within the European countries is of a sufficiently high standard to form the basis of a risk informed in-service inspection (RI-ISI). Having said this however, TG4 believe work is needed to establish how well PRA models primarily directed at active component failures can be adapted via the surrogate concept, to handle the failure of passive elements. At the same time but over perhaps a longer time scale, the development of these PRA's to handle passive failures directly should be studied. TG4 would recommend the use of core damage frequency (PRA level 1) for statuary based safety risk assessments within the European Community. TG4 recognise that within a strict risk based process it is possible to identify areas of the plant where primary failure would lead to extreme consequences but whose evaluated risk would be acceptable. Such areas are those that have no defence in depth against a possible failure, known in the United Kingdom as areas that require an "incredibility of failure" analysis. TG4 recommend that such areas be recognised within any risk informed in-service inspection policy.

The second element of any passive component risk assessment lies with the derivation of a site by site estimate of the failure probability. TG4 believes that a mechanistic understanding of any proposed degradation mechanism lies at the centre of such an assessment. The development, verification and validation of structural reliability modelling (SRM) are therefore an important area of development. TG4 also believes that if a balanced passive risk assessment is to be carried out this should include a leak before break type of analysis. This in turn will require the ongoing development of leak rate evaluation and the uncertainties associated with such estimates. Whilst the difficulties associated with failure data has been highlighted in this document, TG4 accept that such data must play a substantial role in establishing the failure probability of passive components. Such data will also play an important role in the validation of SRM's as well as providing essential feedback for the updating of individual plant risk assessments. It is therefore important that work be done to both review all the data that currently exist and to see how successfully this data can be feed into the failure assessment as well as work to specify the form of data that could be collected in the future. TG4 also accept that even with the work referred to above, it is unlikely that a purely analytical process or even a combined analytical and data driven process will ever provide a total and comprehensive set of failure probabilities. This then implies that in many instances there will be a need to call upon expert judgement/elicitation to assess the probability of failure of the passive components. Work therefore needs to be carried out to ensure an agreed methodology/procedure for arriving at these probabilities.

Finally there are two questions of a more general nature. The first of these is on how the recommendations of ENIQ with respect to inspection qualification fit into any RI-ISI programme. The second is the question of the truly unknown or the virtual risk.

Whilst this form of risk has been discussed in this document, TG4 believe that more work is required to see how this form of risk can be addressed within any in-service inspection programme.

The ongoing work recommended above is summarised below as a set of bullet points:

- To investigate the extent and validity with which the surrogate procedure can be used for PRA's not targeted at passive component failures.
- Develop current PRA technology to include passive component failures.
- Establish a common approach to the verification/validation of structural risk assessment (SRM) models.
- Improve models to evaluate the leak rate and its variability from defects that breach containment but do not immediately cause catastrophic failure or fast fracture.
- Review the available databases on passive failures to evaluate their applicability to the RI-ISI process.
- Identify how future data can be better recorded to assist in both the updating of plant specific risk assessments and to aid in evaluating a form of generic failure probability.
- Review current methods of eliciting expert opinion for assessing site specific failure probabilities.
- Identify how the ENIQ inspection qualification process fits within a RI-ISI programme.
- Attempt to develop a strategy for dealing with virtual risk

Much of the work highlighted here is part of the ongoing technical development currently being carried out by the individual nuclear utilities and their technical support establishments. However TG4 believe that if a European risk based philosophy is to be developed a co-ordinated work effort is required to establish the best practices in terms of the above topics. Such a co-ordinated effort is, in the members of TG4 opinion, best lead by a combination of the already well established European Networks ENIQ and the European Commission.

References

1 E J Henly (1981), Reliability Engineering and Risk Assessment.

2 "Estimates of Component Rupture Probabilities for Nuclear Power Plant Components: Expert Judgement Elicitation" by Vo et al; Nuclear Technology, Volume 96 (3)

3 H M Thomas, Reliability Engineering 2(1981) 83-124

4 Page 23, "Industrial Application of Structural Reliability Theory"; ESReDA Safety Series No. 2; published by Det Norske Veritas 1998

5 UMIST Paper by Burdekin not yet published but should be by our publication time.

6 J M Bloom 'Partial Safety Factors (PSF) and Their Impact on ASME Section XI, IWB-3610'. 2000 ASME Pressure Vessel and Piping Conference, Seattle, Washington July 2000.

7 Canvey Island

8 HSE Publication ISBN 0 11 886368 1 'The Tolerability of Risk from Nuclear Power Stations'

9 RG 1.178. 'An approach for plant-specific risk-informed decision-making in-service inspection of piping' (for trial use), September 1998.

10 B Brickstad, et al. 'The use of risk based methods for establishing ISI priorities for piping components at Oskarshamn 1 nuclear power station', SAQ/FoU-Report 99/05, SAQ Kontroll AB, Stockholm, Sweden, November 1999.

11 Buchalet et al. 'A Tentative Approach to a More Rational Preparation of In-Service Inspection Programmes', IAEA-SM-218/39, 1977.

12 European methodology for qualification of non-destructive tests, second issue, EUR17299EN

APPENDIX 1

Problems associated with the use of field data to assess the probability of failure of passive components for use in risk analysis

As stated in the main text, for use in a RI-ISI policy, the estimated failure probabilities for the passive components must be broken down to separate failure probabilities for each potential inspection site. This means that a single point estimate of a general or global statistic, determined by simple adding all the known passive component failures together and dividing by an integrated total experience, will not service. Thus, it is a requirement of any RI-ISI analysis to break down the world data so that specific individual probabilities can be allocated to each inspection site.

A few seconds thought tells us that such a situation can never be achieved directly from the field experience of passive failures. Indeed, since by definition, the field experience is an historical observation and what is required here is a prediction of the future probability associated with different specific components, there would seem to be an almost fundamental logical inconsistency in the argument. Having said this however, nobody would deny that the field experience represents an historic record of the plant performance and must reflect the ongoing or expected performance into the future! Clearly then, whilst the field data will never lend itself up to the detail level required for the final RI-ISI assessment the data must be broken down into a fundamental categories. Three obvious categories spring immediately to mind, but there may well be others, these three are material, component and degradation mechanism. But, before going any further it must be recognised that even a simple break down like this presents problems. For whilst the three categories are exhaustive, they are clearly not independent! In this appendix, only a break down of the data into different degradation will be considered. It will be seen that even this simple break down presents its fair share of problems.

Breaking the data into degradation mechanisms

In order to break down the data into different degradation mechanisms, it is first necessary to define the different mechanisms. Having defined the mechanisms a set of attributes need to be associated with each mechanism in order to differentiate them one from another. These attributes need to be detailed enough to separate the degradation/failures, whilst at the same time being simple enough to implement! If not, then the ability to obtain meaningful data in sufficient volumes will become impractical. Table 1.1 is an attempt to illustrate the problem and perhaps act as a first attempt at what is required. What follows are notes on the analysis of this type of degradation specific data.

Table 1.1 Failure and Degradation Mechanisms

DEGRADATION MECHANISM	DEFINITION	ATTRIBUTES
Fatigue	The progressive permanent structural change in a material subject to repeated stresses having a maximum value less than the tensile strength of the material.	Characterised by incremental propagation of cracks until leak occurs. Indication by "breach marks".
Vibration Fatigue	The progressive permanent structural change in material subjected to repeated vibration, cavitation, slug flow and valve oscillations.	Generally starts from areas of stress concentration such as notches, sharp edges, grooves, etc.
Thermal Fatigue	The progressive permanent structural change in material subject to repeated thermal stress, transient ramps and shocks.	Caused by temperature changes acting against geometric restraints. High and low flow rates and cycles. Transverse fractures. Stratification of hot and cold layers of coolant and the classic mixing problem.
Erosion	A form of metal removal in which particles suspended in fluid flow at speed.	Causes severe wall thinning and gross failure, due to chemical composition, pH level, temperature, oxygen content, coolant velocity and turbulence.
Cavitation	A form of erosion which may include loss of material, surface deformation or changes in properties.	Formation and instantaneous collapse of innumerable tiny voids, or cavities within a liquid subjected to rapid and intense pressure changes. Damage similar to pitting corrosion except the pit surfaces tend to be rougher.
Creep	Time dependent strain occurring under stress.	Creep occurs in any metal or alloy at a temperature slightly above the re-crystallisation temperature of that metal or alloy.
Corrosion	Bulk corrosion in air, water or steam causes build-up of corrosion products, loss of material and activity transport.	These processes can lead to significant local wall penetration.
• Pitting Corrosion	Extreme localised corrosion caused by concentration cell that generally produces sharp defined holes where an area of surface becomes anodic.	Pitting can cause failure by perforation while producing only a small weight loss.
• Biological Influenced Corrosion	Corrosion initiates when steels are exposed to low flow or stagnant and wet environments. Forms films and deposits on metals and alloys exposed to wet environments.	Biologically induced corrosion processes in pipe work and other metallic portions of engineered systems can cause penetration and leakage through metal removal.
• Hydrogen Damage	A mechanical-environment failure process that results from the initial presence or absorption of excessive amounts of hydrogen in metals.	Can induce corrosion and subsequent cracking following high hot and cold temperature changes

Failure Probability Estimate for Different Degradation Mechanisms

The basic statistical or frequentist definition of failure probability gives us:

$$Pf = Nf/N$$

The first way of breaking this statistic down is to characterise the observed failures in to a set of mutual exclusive degradation failures e.g.:

$$Nf = Nf_{VF} + Nf_{EC} + Nf_{WH} + Nf_{TF} + Nf_{SC} + Nf_{CD} + Nf_{U/K}$$

where Nf_{VF} = failures from vibration fatigue
Nf_{EC} = failures from erosion-corrosion
Nf_{WH} = failures from water hammer
Nf_{TF} = failures from thermal fatigue
Nf_{SC} = failures from stress corrosion
Nf_{CD} = failures from construction defects
and $Nf_{U/K}$ = failures from unidentified mechanism

The unknown mechanism U/K is necessary to make the set complete.

The Pf can now be written as:

$$Pf = (Nf_{VF} + Nf_{EC} + Nf_{WH} + Nf_{TF} + Nf_{SC} + Nf_{CD} + Nf_{U/K})/N$$

$$= Nf_{VF}/N + Nf_{EC}/N + Nf_{WH}/N + Nf_{TF}/N + Nf_{SC}/N + Nf_{CD}/N + Nf_{U/K}/N$$

Each of the individual equations within this overall equation provides a true estimate, from the historical data, of the probability of failure from each of the individual failure mechanisms. Given this, it is tempting to assume that each of these probabilities represent the probability of failure given the particular mechanism associated with individual Nf values. Unfortunately this is not true! In order to derive the probability of failure given the mechanism is operative, the total number of operating years, N, must be subdivided in to the number of components years that were subject to each of the degradation mechanisms. That is, the single value N, must be broken down to give:

$$N_{VF}, N_{EC}, N_{WH}, N_{TF}, N_{SC}, N_{CD} \text{ and } N_{U/K}$$

It can then be argued that the ratio of the number of failures relative to a given degradation mechanism and the number of component years subject to that mechanism gives the conditional probability of failure for that mechanism i.e.

$Pf_{VF} = Nf_{VF}/N_{VF}$, (conditional failure probability from vibration fatigue)
$Pf_{EC} = Nf_{EC}/N_{EC}$, (conditional failure probability from erosion-corrosion)
$Pf_{WH} = Nf_{WH}/N_{WH}$, (conditional failure probability from water hammer)
$Pf_{TF} = Nf_{TF}/N_{TF}$, (conditional failure probability from thermal fatigue)
$Pf_{SC} = Nf_{SC}/N_{SC}$, (conditional failure probability from stress corrosion)
$Pf_{CD} = Nf_{CD}/N_{CD}$, (conditional failure probability from construction defects)

And $Pf_{U/K} = Nf_{U/K}/N_{U/K}$, (conditional failure probability from unidentified mechanism)

However, such a break down of the original family of components will almost certainly not be mutual exclusive i.e. one component may be suffering from two, three or even four of the degradation mechanism. Hence if the new-found conditional probabilities are summed, they will not come to the same value as the original overall estimate given by Nf/N.

This apparent incompatibility arises from the fact that we must consider the probability of the mechanism occurring. This is obtained by the ratio of the number of components affected by the specific degradation mechanism and the total number of components in the family; this then gives:

$$Nf/N = ((Nf_{VF}/N_{VF}) \times (N_{VF}/N)) + ((Nf_{EC}/N_{EC}) \times (N_{EC}/N)) + \text{etc.}$$

which returns us to the original probability of failure from the individual mechanism.

From the above it can be seen that if the world data is to be broken down in order to give attributes associated with different degradation mechanisms, then both the failure data and the accumulated experience must be subdivided in to these relative mechanisms.

Given that the data can be broken down so as to give the Pf values for the individual mechanisms, the original statement concerning the probabilities still holds. That is, each is only a point estimate of the failure probability and tells us nothing about the variability within this particular mechanism.

If this spread in the failure probability for all the given mechanisms is low relative to the difference between the mean values; then one can argue that these probability provide all that is required. However, if the opposite is true, then the distribution given by these individual failure probabilities is not truly sufficient for a RI-ISI application.

APPENDIX 2

Examples of Structural Reliability Models

As stated in the main text structural reliability models (SRM's) are models built up from a mechanistic description of the degradation mode being considered. The model then attempt to predict the failure probability for the specific situation being considered using a proposed or expected life duty and the uncertainties in the data that relate to the parameters within the mechanistic model. This make up of the SRM means that a 95% confidence statement can be given about the estimated failure probability. However, it should be realised that this confidence is a confidence associated only with the uncertainty in the data that makes up the mechanistic model, it does not address any uncertainty as to how well the modelling represents the actual field situation! The only way this confidence can be addressed is as suggested in the main text i.e. by using the models to predict known practical or representative field data, which takes us back to appendix 1?

In this appendix two examples are given of SRM analysis.

Example One

This first example is for a circumferential pipe weld subject to a well-defined fatigue life. This modelling was carried out using an SRM program known as "PRODIGAL" reference 2.1. The principle factors that were considered in this analysis are:

1. The initial probability of a weld fabrication defect (predicted by a subroutine in PRODIGAL that simulates the weld construction, including any build inspection, and then evaluates the probability of defects forming during this process)

2. The effect of a pre-service inspection (PSI) on the failure probability.

3. The effect of an in-service inspection (ISI) programme on the failure probability.

The idealised construction of the weld is detailed in figure 2.1. This idealised construction was obtained from the weld procedure and the expert knowledge of welding metallurgist derived from the sectioning of many similar welds. From an expert elicitation it was felt that typically a weld of this type would be constructed with approximately 30 weld beads, built up from one root pass plus nine layers as shown in figure 2.1. The weld was carried out in the shop and so access was considered to be good, as the weld is also a simple pipe butt weld, restraint was set to medium.

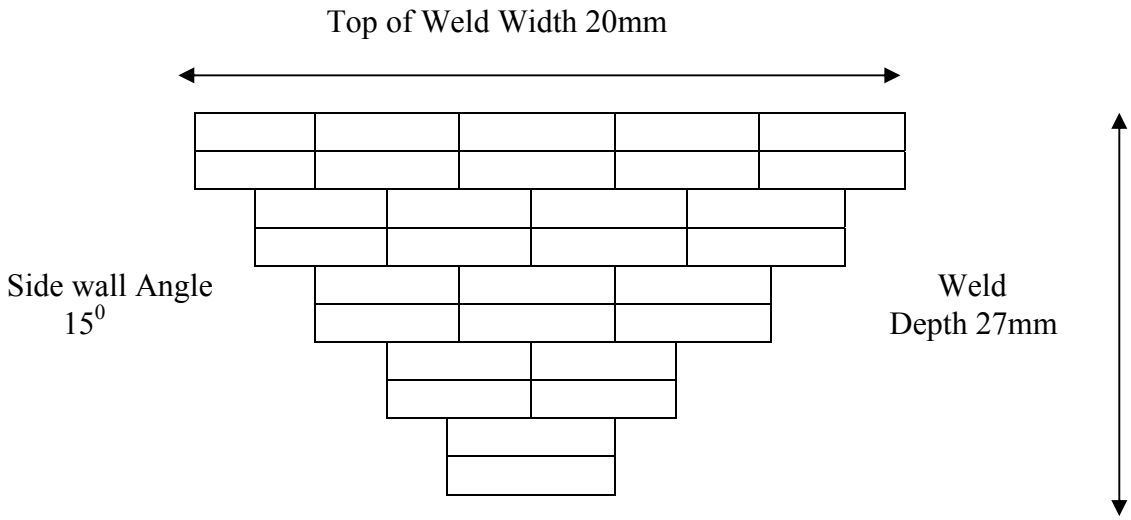


Figure 2.1 Idealised weld construction

IR = 160mm (15" OD Pipe)
Material = 508 carbon Steel
Process = Manual Metallic Arc IG Position
Single pass root

Pre – Service Inspection

The pre service or build inspection of the weld is described in the weld procedure as follows:

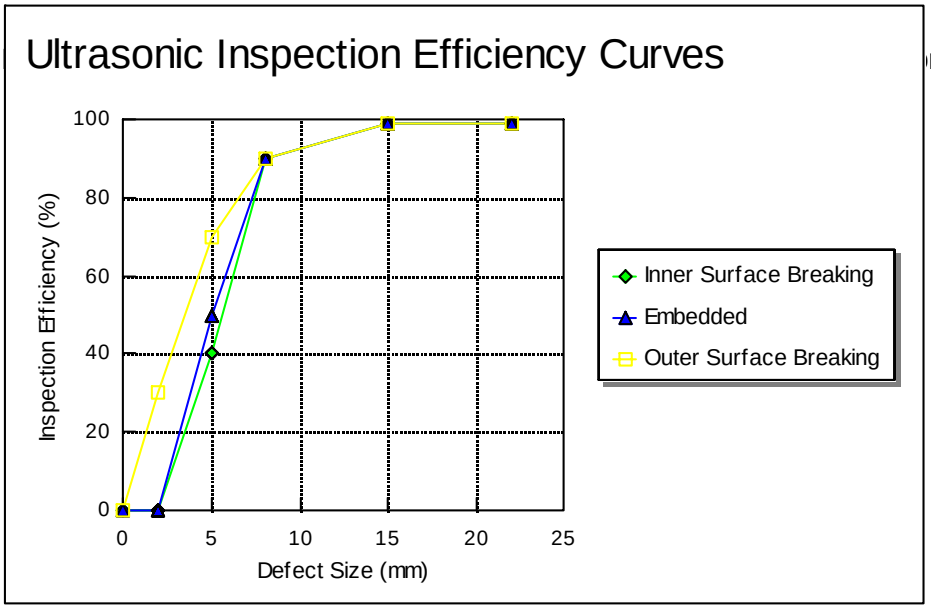
Dyepen on both surfaces of root (layer)
Dyepen on surface of completed weld
Isotopic inspection of completed weld
- SWSI film away
- IR 192

Predicted Start of Life Weld Defects

Defect Category	Predicted Rate of Occurrence	
	No PSI	**Inc PSI**
Inner Surface Breaking (1)	3.83×10^{-2}	8.6×10^{-4}
Embedded near Inner Surface (2)	5.25×10^{-1}	9.84×10^{-3}
Embedded Middle (3)	2.90	9.64×10^{-2}
Embedded Near Outer Surface (4)	2.59	6.04×10^{-2}
Outer Surface Breaking (5)	2.02×10^{-1}	1.43×10^{-4}

Assessment of Through Life - Quantification of In-Service Inspection

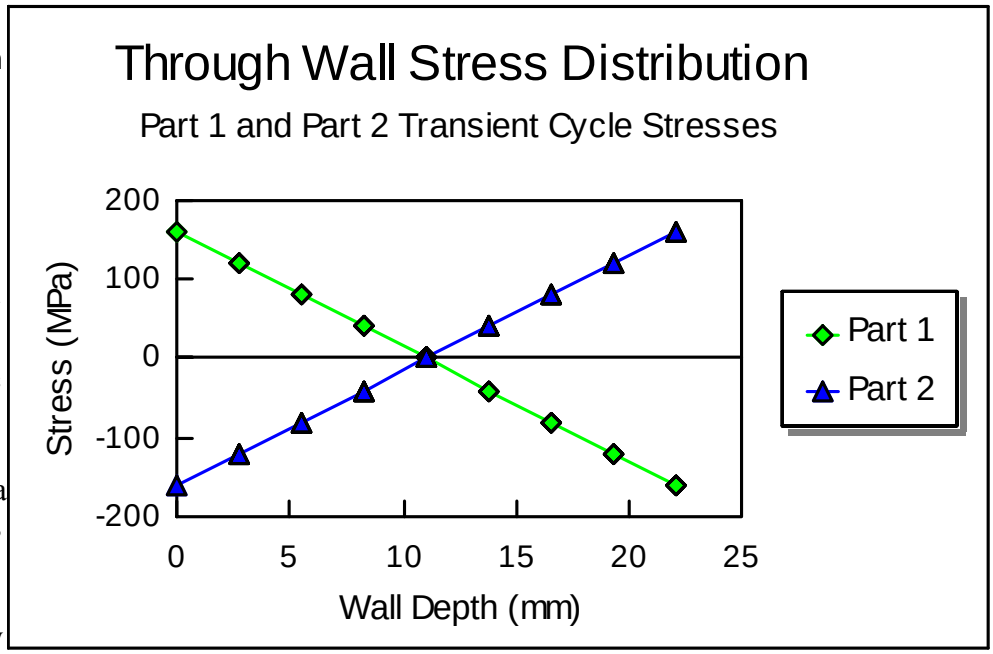
Ultrasonic inspection planned at half-life. This inspection is to be a fully validated inspection following the ENIQ recommended practices. Again an expert elicitation was held with inspection personnel and the inspection efficiencies shown in figure 2.2 were considered to be representative.

Figure 2.2 

Stress History

All stresses are based on linerarised through wall stresses as shown in figure 2.3. A pressure stresses of 100Mpa in the hoop direction and 50MPs in the longitudinal direction is also assumed.

Figure 2.3 Through wall transient stresses



The projected transient cycles were defined as follows.

ID	Cycle	Factor applied to Part 1		Factor applied to Part 2	
		Through Wall	Through Wall	Through Wall	Pressure
1	100	1.0	1.0	1.0	1.0
2	1000	0.8	1.0	0.8	1.0
3	10000	0.5	0.5	0.5	1.0
4	10	0	1.1	0	0

The factors are used to adjust the distributions shown in figure 2.3

End of life Failure Probabilities

Defect	Without PSI		With PSI	
	Without ISI	With ISI	Without ISI	With ISI
1	5.02×10^{-4}	1.49×10^{-5}	9.67×10^{-6}	2.79×10^{-7}
2	1.50×10^{-8}	1.48×10^{-9}	5.07×10^{-11}	7.83×10^{-12}
3	3.38×10^{-10}	3.47×10^{-10}	6.43×10^{-12}	7.12×10^{-12}
4	1.12×10^{-7}	1.82×10^{-9}	9.36×10^{-11}	1.11×10^{-11}
5	5.29×10^{-9}	9.94×10^{-11}	8.08×10^{-15}	3.51×10^{-14}
Total	5.02×10^{-4}	1.49×10^{-5}	9.67×10^{-6}	2.79×10^{-7}

Conclusion from this specific SRM analysis

With no PSI or ISI the predicted probability of failure is 5 x 10-4 a value that would compare well with that predicted from the world data for high quality welds. Simply carrying out a PSI, which could alternatively be seen as a high quality, independent acceptance inspection, reduces the probability of failure by a factor of fifty. The full PSI plus ISI, which could be applied to a risk significant weld, takes the probability down by three decades.

Such results can be seen as absolute values assessing the probability of failure of a pipe weld for an ISI programme or as purely relative comparisons to give an indication of the value associated with a proposed programme.

Second Example

The following example is taken from a pilot study that is published in Ref. [1]. For more details and the underlying model to evaluate failure probabilities, it is referred to the full report in [1] and the background report [2] that describes the structural reliability code PIFRAP. The damage mechanism in the example is IGSCC.

Geometry

Stainless steel pipe weld (By-pass) in the main circulation system to the BWR-plant Oskarshamn, unit 1 nuclear power station. The pipe weld is located inside the containment.
Outer diameter 114.3 mm, wall thickness 11.7 mm.
Stress corrosion cracks are oriented circumferentially in the vicinity of the weld.

Loading condition.

Internal pressure 7.0 MPa.

Primary membrane stress P_m = 15.4 MPa.
Primary bending stress P_b = 8.2 MPa.
Thermal expansion bending stress P_e = 4.2 MPa.
Primary bending stress at Safety Relief Valve blowdown P_{SRV} = 22.8 MPa. Frequency once a month.
Axial weld residual stress 182 MPa (local bending stress over pipe thickness).
No vibrations.

Material data at 288 °C
Yield stress of the austenitic stainless steel base material, 150 MPa.
Ultimate tensile strength, 450 MPa.
Fracture toughness for stainless steel submerged arc weld SAW, $J_R(\Delta a = 2 \text{ mm}) = 320$ kN/m.
Subcritical crack growth data for IGSCC in normal water chemistry conditions

$$\frac{da}{dt} = 4.5 \cdot 10^{-12} \cdot K^{3.0} \text{ mm/s}$$

with K in $\text{MPa}\sqrt{\text{m}}$. Plateau at da/dt = 5.63E-7 mm/s for K > 50 $\text{MPa}\sqrt{\text{m}}$.

Leak rate conditions
Crack face surface roughness 0.08 mm.
Pathway loss coefficient 0.282 mm^{-1}
Discharge coefficient 0.95.
External pressure 0.1 MPa.
Fluid temperature 288 °C.
Leak rate detection limit for shutdown requirement inside containment, 0.3 kg/s.

Inspection conditions
Year 0, 10 and 20: ISI with poor inspection efficiency.
Year 28, 34 and 40: ISI with ”good” inspection efficiency (qualified inspections) with model constants taken from **Simonen and Woo [3].**
Credit is taken for the latest inspection only (dependent inspections).
If a leaking crack is not detected by leak detection and an inspection occurs between leak and rupture, it is assumed that the crack is detected with the detection probability of 1.0.
Detected cracks are assumed to be repaired and will not further contribute to the failure probability.
Time in service since start of operation, t = 28 years.
Expected total time of operation T = 40 years.

	With leak detection No ISI	**Without leak detection No ISI**	**With leak detection With ISI**	**Without leak detection With ISI**
Rupture probability	0.948E-6	0.109E-3	0.572E-8	0.106E-6
Small leak probability	0.356E-3	0.356E-3	0.342E-4	0.342E-4

Table 1. Failure probability per reactor year

Table 1 shows the resulting failure probabilities for the particular weld at t = 28 years. They represent the mean value per reactor year, averaged for the remaining lifetime of the power plant. The small leak corresponds to leak rates well below 1 kg/s. Large leaks (up to 30 kg/s) will in these evaluations have the same probability as a rupture, ref [1]. Leak rate detection has only an influence on the rupture probabilities since the leak rate for the small leak probabilities are in general too small to be detected.

References

[1] Brickstad, B. et al, *The use of risk based methods for establishing ISI priorities for piping components at Oskarshamn 1 nuclear power station*, SAQ/FoU-Report 99/05, SAQ Kontroll AB, Stockholm, Sweden, Nov. 1999.

[2] Bergman, M, Brickstad, B. and Nilsson, F., A Procedure for Estimation of Pipe Break Probabilities due to IGSCC, *Int. J. Pres. Ves. & Piping* 74 (1997), pp 239-248.

[3] Simonen, F. A. and Woo, H. H., Analyses of the impact of ISI using a pipe reliability model, NUREG/CR-3869, USNRC, Washington D. C., 1984.

APPENDIX 3

Review of Risk Informed/based in-service inspection development in the USA and EC countries

A number of risk-informed approaches are evolving in the nuclear industry in different countries and these are now briefly reviewed. These approaches are state of the art and are the responsibility of the relevant national authorities. In making this review, no judgement on the adequacy of any individual approach is implied or intended, since all approaches have equal right within their jurisdiction. However, from this review, some common elements of the evolving processes for risk informed inspection can be identified as well as some considerable differences.

A3.1 US Approaches

Inspection requirements for nuclear components at US nuclear power plants are included in the *ASME Code Section XI*. Within this code the areas predominantly selected for examination are those associated with welds in the pressure boundary. It can be argued that the present ISI programme, as given by ASME Section XI, is already implicitly risk informed since it contains the two basic elements of risk. Consequence is incorporated through the ASME Section III categorisation of the plant components into three levels depending on the probability of a failure in a components leading to core damage. Probability of failure comes from the ASME Section XI stipulation to select sites having high stress or fatigue usage.

Risk-informed in-service inspections programs were initiated by ASME XI as an alternative to the current inspection programs. The progression from an implicit risk informed logic to an explicit risk informed logic, has been seen by many to be a natural progression. A principle difference, however, between the present code and the new risk-informed code, is not only the use of an explicit evaluation of risk but also that this risk is based primarily on the operational details of each specific plant rather than the design analysis.

Beginning in late 1988, a multi-disciplined ASME Research Task Force on Risk-Based Inspection Guidelines has been evaluating and integrating these technologies in order to recommend and describe appropriate approaches for establishing risk-informed inspection guidelines. This task force is comprised of members from private industry, government and academia representing a variety of industries.

The NRC, as part of the research effort, applied this technology in pilot studies of inspection requirements for both PWR and BWR plant systems. Later, it requested the ASME Research Task Force to make the risk-informed inspection process consistent with other Probabilistic Safety Assessment (PSA) applications.

ASME Section XI formed a Working Group on Implementation of Risk-Based Examination to begin making Code changes based on risk for inspection of passive, pressure boundary components. The first efforts of this group have been to develop Code Cases providing risk-informed selection rules for Class 1, 2 and 3 piping.

During 1997, the ASME Board on Nuclear Code & Standards approved **Code Case N-577** "*Risk-Informed Requirements for Class 1, 2 and 3 Piping, Method A, Section XI, Division 1*" and **Code Case N-578** "*Risk-Informed Requirements for Class 1, 2 and 3 Piping, Method B, Section XI, Division*". First one incorporates the methodology recommended by the *ASME Research Task Force* on Risk-Based Inspection Guidelines and evaluated in the *Westinghouse Owners Group (WOG)* plant application. Code Case N-578 incorporates the methodology developed by the *Electric Power Research Institute* (EPRI). The EPRI methodology was developed as an alternative to the WOG methodology due to the weaknesses shown for some PSA in US Nuclear Power Plants.

At the same time, the US NRC has been working to develop a framework for expanding the use of PSA technology in its regulatory activities to improve safety decision making, giving high priority to the activities that apply PSA technology and take into account risk insights. As part of this process, the NRC has published several Regulatory Guides to support changes in current in-service inspection and testing programs, technical specifications and quality assurance based on risk insights.

*Code Case N-577 (***WOG***)*

The present Code Case concerns Class 1,2,or 3 piping. The followed approach, normally refereed as WOG methodology, uses the PSA to divide the plant piping systems into *piping segments* where a failure has the same consequence as measured by core damage frequency. Each piping segment is then categorised as being of high or low *safety significance*. An assessment of degradation mechanisms and failure probability is used to determine the *failure importance* of each segment as being either high or low. This may be done by the judgement of an engineering sub panel or by the use of structural reliability models. A segment is deemed to have high failure importance if its probability of failure is greater than 10^{-4} per 40 year operating life. The final safety significance category in a 2 x 2 matrix is determined by an expert panel review using the PSA and deterministic and design insights.

More specifically, the presented methodology consists of the following elements:

1. Segment Definition (component with same consequence from the plant PSA point of view).

2. Consequence Evaluation. Assessment of consequences (direct and indirect) in terms of CDF and LERF.

3. Failure Modes and Failure Probability Estimation. Identification of the degradation mechanisms and loading conditions, in order to determine quantitatively the failure probability. Estimations based on probabilistic mechanic fracture codes are the best approach.

4. Risk Ranking Evaluation. Segments are categorised in two risk categories: *high safety-significant* and *low safety significant*. This process involves three phases:

- Application of PSA to calculate the total pressure boundary core damage frequency (CDF) and (LERF) (if possible) and importance factors.
- Integration of other deterministic considerations.
- Expert panel evaluation.

5. Structural Element Selection. Structural elements are selected for examination based on the safety significance of the segment (High and Low Safety Significance) and the failure importance within the segment (High and Low Failure Importance). The safety significance classification is based on the expert panel assessment, and the failure importance is based on the failure probability determined through probabilistic mechanic fracture codes.

HFI	OWNER DEFINED PROGRAM	SUSCEPTIBLE LOCATIONS (100%)
		STATISTICAL SELECTION PROCESS
LFI	ONLY SYSTEM PRESSURE TESTS AND VISUAL EXAMINATIONS	STATISTICAL SELECTION PROCESS
	LSS	HSS

The criteria for selecting the location for examination are the following:

- All susceptible locations classified as HSS identified as being likely to be affected by a known or postulated failure mechanism.
- HSS locations without known or postulated degradation mechanism will be selected through a statistical evaluation process.
- HSS locations with low failure importance will be selected through a statistical evaluation process.
- LSS locations identified as being likely to be affected by a known or postulated failure mechanism should be considered for examination in accordance with an Owner Specific Program. The impact on safety is small but may have a significant impact on availability.
- LSS locations with low failure importance will be only required to system pressure test and visual examination.

6. ISI Program.

HSS component structural elements should be examined according to the requirements of Code Case N-577.

LSS component structural elements do not require non-destructive examinations (NDE), they are only required to visual examinations and system pressure tests performed according to ASME Section XI.

Independently of the component segment classification, all ASME Code Class 1, 2 and 3 locations should continue to be visually examined for leakage in accordance with the system pressure test requirements of ASME XI.

The strength of the WOG approach is that it focuses inspection on the component segments that has been assessed by PSA to be critical to plant safety as defined by core damage probability. However, its weakness is that in preparing the PSA, assumptions have already been made about the probabilities of failure that have usually been based on generic data.

Code Case N-578 (*EPRI*)

This Code Case concerns Class 1, 2 or 3 piping. The proposed approach, usually referred as EPRI methodology, starts from a failure modes and effects analysis (FMEA) consisting of a consequence evaluation (direct and indirect) and an engineering review of the possible degradation mechanisms and associated failure modes. Component systems are divided into component segments that have the same degradation mechanism and the same failure consequence for a given mode of failure.

The component segments are then categorised into one of seven risk regions within a 4 x 3 risk matrix. This is according to their consequence category (high, medium, low or none), depending on the conditional core melt potential for a limiting leak/break size, and the degradation category (break, leak, none) depending on the maximum likelihood from industry experience and component failure data. The proportion of the welds of a given component segment to be inspected within a ten-year period depends on the risk region that it has been assigned.

More specifically, the presented methodology consists of the following elements:

1. System and evaluation boundary identification applied on a system-by-system basis.

2. Segments risk assessment. Each system selected is divided into component segments that have the same degradation mechanism and the same failure consequence.

3. Failures mode and effects analysis, consisting of a consequence evaluation (direct and indirect consequences) and degradation mechanism evaluation.

4. Risk evaluation. Component segments are grouped into three risk regions (High, Medium or Low) evaluating both the conditional core-melt potential for a limiting break size (Consequence Category) and the likelihood of a pipe break (Degradation Category).

The basic consequence-ranking philosophy that is considered in this analysis is the following:

<u>High Consequence</u>: Pressure boundary failures resulting in events that are important contributors to the plant risk, or pressure boundary failure that significantly degrade the plant's mitigating ability; Conditional Core Damage Probability CCDP > 10^{-4}.

Medium Consequence: Failures that do not belong to the High or Low rank; 10^{-6} < CCDP < 10^{-4}.

Low Consequence: Pressure boundary failures resulting in anticipated operational events, or pressures boundary failures that do not significantly affect the plant's ability; CCDP < 10^{-6}.

According to the degradation mechanism present, break potential categories (High, Medium, and Low) are assigned to each component segment, based on industry experience and component failure data. Thus, each component segment is included in a risk ranking (risk matrix) depending on its consequence category and degradation category.

Degradation Mechanism	Consequence Category			
	None	Low	Medium	High
Break	**7**	**5**	**3**	**1**
Leak	**7**	**6**	**5**	**2**
None	**7**	**7**	**6**	**4**

Pipe segments in the 1, 2, or 3 category are classified as High Risk, pipe segments in the 4 or 5 category are classified as Medium Risk and those segments in the 6 or 7 category are Low Risk.

5. Selection of inspection locations and examination methods. Identification of potential inspection elements within risk significant segments. Examination methods are determined based on degradation mechanisms.

Volumetric inspections are performed on those pipe segments included in the High and Medium risk regions. Low risk region pipe segments are only required to visual examinations and system pressure tests performed according to ASME Code Section XI.

The size of the sample for examination depends on the pipe segment risk category as follows:

- For categories 1, 2 and 3, a 25* percent of the welds on each category.
- For categories 4 and 5, a 10* percent of the welds on each category.

Code case N-560 – 2 (Ref. 6.3)

This Code Case is limited to the Class 1, Category B-J welds. It will be revised, in order to be consistent with CC N-577 and N-578. It will be split in two parts: N-560-1, which will include appendix I from CC N-577-1 ("ASME – WOG" methodology, and N-560-2, which will include appendix I from CC N-578-1 ("EPRI" methodology).
The important differences are that this Code Case may be applied to Class 1 systems only (where the expected benefits in terms of reduction of the required inspections are

* Since the ASME Code Case 578 is being revised these percentages may change.

the highest), and that it could even be applied to a single system, or a few selected systems. The extent of the inspection is as follows (CC N-560-2):
The examination program shall be based on a total number of examination zones consisting of not less than 10% of the Class 1, category B-J welds in each system, to be examined during each inspection interval.
The examination zones shall be selected from those component segments that fall into the highest risk group.
When this Code Case is applied to more than one Class 1 system, the selected examination zones may be distributed to concentrate examinations on higher risk systems.
The sequence of component examination established during the first inspection interval using the risk-informed process shall be repeated during each successive inspection interval. Modifications to the selected examination zones may be made based on relevant industry experience, changes in plant design or operation, new metallurgical knowledge or prior examination results.

A.3.2 France

The *French utility EDF* has devised a scheme for optimising the preventive maintenance and inspection of pipes and their supports. The method, called OMF Structures, uses risk-informed principles in order to select critical components where the preventive maintenance tasks should be located. The process takes due account of safety, availability and maintenance costs. The objective of the exercises is to identify critical components with regards to these three factors i.e. the components whose contribution to the risk justifies preventive maintenance.

The OMF-structures process consists of the following main stages:

1. Functional analysis (at the system level)
2. Consequence evaluation (FMEA) at the component segment level
3. Criticality analysis (FMECA) at the component level
4. Definition of preventive maintenance programmes
5. Preventive maintenance programmes and (or) corrective maintenance programmes

Consequence evaluation is performed by using existing PSA for active components and also deterministic criteria coming from operation analysis. When PSA is used, the consequence is measured by a quantitative indicator (FAR: "*Facteur d'Augmentation du Risque*"). This parameter is a measure of Defence in Depth. To estimate the FAR indicator, the impact of component segment rupture on initiating event occurrence and on mitigation function loss is taken into account. These effects can be direct consequences of the component segment rupture, or indirect consequences. Indirect consequences arise from damage to components that are located in the vicinity of the broken component segment and that are subject to spraying, jet impingement or pipe whip. Depending on the value of the calculated quantitative indicator, each segment/component is classified into safety significance categories (very safety severe, safety severe and not safety severe). A qualitative/deterministic approach based on knowledge of the accident response procedure and technical operation specification is used to assess the severity of the failure modes that are not modelled in the PSA.

The significant *failure modes* for the component segments considered in the OMF-Structures process are:

- External leak
- Loss of hydraulic characteristics resulting from a non-compensated leak
- Loss of hydraulic characteristics due to a blockage
- Loss of physicochemical characteristics
- Loss of thermal characteristics

Operating experience and degradation models are used to identify components where degradation mechanisms are likely to occur. Reliability models help to evaluate reliability indicators for each relevant {component, degradation mechanism}.

Considering the severity of the failure modes, and the potential for a degradation mechanism, a list of critical components is made out, as shown in the following table:

degradation mechanism	severity category			
	not severe		severe	very severe
relevant mechanism and high probability	I	I	IV	V
relevant mechanism and low probability	I	I	II	V
non relevant mechanism	I	I	II	III

critical

non-critical but very severe for safety

non-critical

non-critical

This classification into critical and non-critical components helps to make an initial decision between preventive maintenance (on critical components) and corrective maintenance (on non-critical components). For very safety severe components on which no degradation mechanism is relevant (either there is no active mechanism or the degradation kinetics of existing mechanisms are very low), the OMF-Structures process propose an inspection to confirm that no unknown or unexpected mechanism is active. Those inspections are not included in the scope of the Preventive Maintenance Program. They are done once during the plant life (after 10 or 20 years of operation at least) or every 10 years for the best.
The inspected locations and also the methods are related with the identified degradation mechanisms. The results of the degradation model (i.e. the degradation kinetics) help to define where and when to inspect. Generally, maintenance tasks must be applied to all components in a critical segment. But when the number of components to inspect is sizeable (for example welds in a pipe), it is possible to organise those components into a hierarchy according to the failure probabilities. Therefore, only a sample of the most critical components has to be inspected. As long as nothing is observed on the inspected components, the other non-controlled components should not fail.

For some degradation mechanisms, the existing inspection methods are not efficient enough because of the kinetics of degradation. The mechanism is so sudden that you cannot define correct time intervals for inspections. Examples are vibration and thermal fatigue. A solution can be design modifications (nozzles affected by vibrational fatigue for example) or operation conditions modifications (for thermal problems).

<table>
<tr><th rowspan="2">degradation mechanism</th><th colspan="3">consequence category</th></tr>
<tr><th>not severe</th><th>severe</th><th>very severe</th></tr>
<tr><td>relevant mechanism and high probability</td><td rowspan="3">corrective

maintenance</td><td rowspan="2"></td><td rowspan="2">Preventive Maintenance Program</td></tr>
<tr><td>relevant mechanism and low probability</td></tr>
<tr><td>non relevant mechanism</td><td colspan="2"></td><td>additional investigations</td></tr>
</table>

The last step of the method is to generate the future maintenance program by choosing the most suitable maintenance scenario for each area/piece of equipment. This final choice will be made at the same time as scenarios are grouped together at the most suitable equipment level. For structures with high stakes, this step may result in committing means designed to enrich the information used to make the final maintenance decision.
The stake of the maintenance optimisation process of the OMF-Structures method is more about improving safety (or at least keeping the risk at the same level) and bringing justifications to the French Safety Authorities than saving money.
The approach is complex because it requires a considerable amount of information about the operating conditions. Nevertheless this allows a precise identification of degradation mechanisms. This method is applicable to pipes and their supports, but it should be soon extended to tanks and heat exchangers.

A.3.4 Germany

In the *German KTA code* 3201.4 (class 1 components) and 3211.4 (class 2 and 3 components), the method, extent and intervals for in-service inspection are closely specified. At present, the German regulatory framework is fully deterministic and contains no scope for probabilistic analysis. However, this deterministic framework still has an implicit risk based logic because high stress/fatigue sites are singled out for inspection. There is close similarity here with the current ASME XI rules.

More specifically, the German approach is based upon the existing quality of a component or a system, the detailed knowledge of any potential damage mechanism as a result of operational loading and information about existing monitoring measures. For this purpose, the quality of the component after design and fabrication has to be assured *(basic safety concept),* and then has to be maintained during plant operation. This requires detailed operational control and monitoring of the plant and has to take into account of possible new elements (e.g., new loading or degradation mechanisms). Among the several factors that can account for deviations between the quality after design and fabrication and the actual state, changes of material properties (e.g. ageing) and fluid effects (water chemistry) are usually neglected. This because of the proper material selection during the design/fabrication phase, the knowledge on its long-term behaviour and the monitoring of water chemistry. Therefore the only factor

that can be responsible for a change in the system/component quality is the operational loading and cycles that have to be monitored during operation.

In order to get a clear understanding of the structural loading, stress and fatigue analyses have to be performed with measured operational loading. This leads to realistic stress levels and usage factors, which are much more suited for selection of inspection locations. Additionally, within the stress analyses not only stress intensity, necessary to show that the stresses are within the allowable limit, but also the principal stresses with their directions have to be calculated. Since at locations with prevailing compressive stresses there are lower requirements for NDE measures than in areas with tensile stresses. As is it well known the loading, which are of main interest regarding stresses and fatigue, are temperature transients. Therefore long-term surveillance of systems/components is heavily based on thermocouple instrumentation. If there is any loss of local integrity as a result of flaws either postulated or detected by ISI, calculation of crack growth on the basis of operational loading have to be performed. The main aim then is to show operational crack growth yields not to a critical crack size ("leak-before-break").

For ISI, representative sample of welds in high integrity components is normally selected. Results of stress and fatigue evaluations, together with information on previous NDE inspections are used to determine the extent and ranking for inspection and the appropriate NDE-measures. Besides, an additional class of inspection, generally referred to as "vagabonding" examinations, is called for in order to cover the unexpected, whereby the assessment of potential failure sites is based on engineering experience and judgement.

The number/locations of the welds to be inspected, and the frequency of inspections are determined by the ISI plans. For certain systems/components (e.g. primary circuit and connecting systems), KTA code has to be fully considered in the ISI-plans. There is no recognition yet of the benefit inspection qualification within the process. Inspection here is not tool to support the PSA, but to maintain integrity during plant operation.

The advantage of this approach is that it identifies the threats to integrity at the outset. Inspection programmes can be targeted at detecting specific defects or degradation mechanisms leading to the most appropriate methods and frequency for inspection. It also provides a clear feedback from the inspection results into future inspection planning. The avoidance of failures in-service is the primary objective. The difficulty of the approach is that it requires a considerable amount of information about the conditions.

A.3.5 Sweden

The approach to inspection adopted by *Swedish utilities* addresses all pressure retaining components and is aimed at finding defects. The approach recognises the design safety class but is not PSA orientated. A set of screening criteria (e.g. carbon content in austenitic components) is used to identify the potential degradation mechanisms for each weld and expert judgement applied to assess the probability of failure.

The Swedish Nuclear Power Inspectorate's Regulations use risk-informed principles in assigning components and parts of components to inspection groups A, B or C. This assignment takes into account the probability of cracking or other degradation in a specific component as well as the potential consequences of a failure. Structural components for which the resulting risk is highest are assigned to inspection group A; those for which the resulting risk is lowest are assigned to inspection group C. Inspection group B covers intermediate risk components.

All butt welds in the RPV and the internal surfaces of RPV nozzles and safe-end welds are assigned to group A and must be inspected at intervals not exceeding 10 years. Other pressure boundary components in group A, and 10% of components in group B, must be inspected at intervals necessary to ensure adequate safety margins with respect to failure. These intervals are based on considerations of damage tolerance. They are normally set with reference to the time estimated for a postulated defect to grow to the maximum extent for which adequate safety margins are considered to exist, when all potential damage mechanisms have been considered. Again, the interval between in-service inspections must not exceed 10 years. The inspection of components in group C must as a minimum comply with regulations of The Swedish Board of Occupational Safety and Health concerning the inspection of boilers, and suchlike.

The risk-informed principles are based on the assignment of components to inspection groups A-C on the basis of a damage index (I-III) and a consequence index (1-3). The damage index provides a measure of the likelihood of crack initiation or the occurrence of other damage mechanisms in a specific component. It is determined by the probable loads and environment in relation to the component's characteristic dimensions and material properties. The consequence index provides a qualitative measure of the likelihood that such damage will jeopardise the fuel, the containment leak tightness or lead to the discharge of significant amounts of radioactivity. It is determined mainly by the margin to prevent severe consequences were a failure to occur. The following table shows the resulting inspection groups:

		Consequence index		
		1	**2**	**3**
Damage Index	**I**	A	A	B
	II	A	B	C
	III	B	C	C

Qualification of non-destructive inspection systems includes all the equipment, procedures and the accompanying instructions, as well as the personnel. The qualification procedure follows in principle the ENIQ methodology.

While the initial approach in Sweden, described here above, is largely qualitative, there is a strong tendency now to go to more quantitative approaches, making a large use of the plant PSA's.

A.3.6 United Kingdom

The in-service inspection of *UK civil nuclear power plant* is subject to the general requirements of the UK Pressure Systems and Transportable Gas Containers

Regulations 1989 and their associated Guidance and Approved Code of Practice. In-service inspection is determined on much the same basis as conventional boiler plant. The Health & Safety Executive publication 'The Tolerability of Risk from Nuclear Power Stations' and its companion document 'Safety Assessment Principles for Nuclear Plants', clearly lays out a risk approach to the regulatory framework for nuclear plant. However a detailed risk analysis does not form part of the process. Special consideration is given to the reactor pressure vessels because of the lack of any physical defence in depth. Likewise, areas where problems have been identified are given special consideration.

For *UK submarine reactors*, developments in recent years have placed the selection of in-service inspection priorities on a fully quantitative risk basis. Calculations are carried out to determine the probability of failure of each component from identified degradation mechanisms, fatigue and initial defects. The calculated probabilities are modified by an expert elicitation before they are combined with assessments of core damage probability to provide a risk ranking. The detailed schedule of inspection targets the highest risk components but still contains a degree of speculative inspection of components where the consequences of failure are very high and there is little or no defence in depth.

A.3.7 Spain

The *Spanish Utilities* (UNESA) and the *Spanish Nuclear Safety Council* (CSN) are jointly developing a Risk-Informed In-service Inspection Piping Guide for applying, on a voluntary basis, the US Risk-Informed Methodology to the Spanish Nuclear Power Plants. The objective of the project is to issue a guide for risk-informed in-service inspection of piping, incorporating both the quantitative and qualitative methodology. With the US framework as basis this documents intends to extend the ASME XI scope in order to include other specific degradation programs, proposing also new examination frequencies, inspection methods, etc. The project is in its last stage, the validation of the guide through its application to two pilot studies. Currently, the quantitative methodology is being applied to the selected pilot plants, a PWR (Westinghouse design) and a BWR (General Electric design).

EUROPEAN COMMISSION

EUR 19742 EN 76 pages

Editors: O.J.V. Chapman and L. Fabbri

Luxembourg: Office for Official Publications of the European Communities

2000 – 76 pag. – 21.0 x 29.7 cm

Physical sciences

EN

Catalogue number: CD-NA-19742-EN-C

Copies of this ENIQ report can be obtained by writing to the following address:
L. Fabbri
JRC Petten Institute for Advanced Materials
P.O. Box 2 NL – 1755 ZG Petten
The Netherlands

ABSTRACT

The European Network on Inspection Qualification (ENIQ) has started a specific Task Group (TG4) with the main objective of developing a methodology appropriate to the European Plant Operators needs using the concept of risk and harmonising the different EU initiatives on this subject. This methodology should provide a framework for the European Plant Operators to develop a risk informed management strategy to optimise the plant inspection.

The present document represents a first attempt in this direction and should be considered as a discussion document that projects the general opinion of ENIQ TG4 on the issue of Risk Informed In-Service Inspection, and which covers all the main elements of the risk based decision making process. The integration of the above elements to form a single framework that encompasses plant inspection, maintenance and instrumentation to insure a cost efficient process of optimising the plant risk, will be the objective for a further document.