The UK Nuclear Industry Good Practice Guide To:

**Design Basis Assessment
(DBA) Schemes**



This Nuclear Industry Good Practice Guide was produced by the Safety Case Forum and published on behalf of the Nuclear Industry Safety Directors’ Forum (SDF).

**Issue 2 – March 2020**

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Issue Number** | **Revision Date** | **Changes** |
| Issue 1 | April 2018 | Initial Publication |
| Issue 2 | March 2020 | Update due to time lapse. Incorporation into new SDF Template. |
|  |  |  |

It is recognised that – through the experience of using this Guide – there may be
comments, questions and suggestions regarding its contents.

In the first instance, any such comments should be sent to all of the following:

safetycaseforum@awe.co.uk

Author: Tony Rice (Rolls-Royce)

Contributions have been provided through the Safety Case Forum
by all participating members, particularly:

Alec Bounds (LLWR)

Helen Boyer (UKAEA - Culham)

This document was reviewed and approved by the Safety Case Forum
of the Safety Directors’ Forum.

# Foreword

This Safety Case Forum guide considers the formulation and use of Design Basis Assessment (DBA) Schemes within a safety case framework.

One of the aims of the Safety Case Forum, which reports to the Safety Directors Forum, is to share knowledge, processes and practices between the organisations involved in the civil and defence nuclear industries. All have a common goal to provide fit for purpose safety cases in the most efficient manner possible.

The general purpose of DBA schemes is to provide a simple and useable tool to guide which hazards should be subject to full design basis assessment requiring robust demonstration of fault tolerance and protection to prevent adverse consequences. This includes guidance on where safety measures are required. In the context of this guide, hazard means any event, fault, failure, or action that may lead to unintentional exposure of people to a radioactive dose.

A comparative analysis of DBA schemes used within the industry was carried out as part of the Safety Case Forum. This identified that the DBA schemes and the guidance that support them have been derived separately and in many varied ways. This can be expected due to the variance in the hazards and complexity at different sites. A fully standardised DBA scheme for use throughout the industry is not practicable or sensible to implement.

However, identification of common themes or principles on the basis of DBA schemes provides an opportunity for consistent understanding across the industry and is the basis of this Safety Case Forum guide.

The guide covers the three high level factors to be considered in forming a DBA scheme and its underlying guidance, namely: Definition of the Initiating Event Frequency (IEF) to be used as an input to the DBA scheme; Definition of unmitigated consequence to be used as an input to the DBA scheme; Guidance on the derivation of the DBA scheme and its boundaries in order to place hazards into broad groups of importance.

The following guiding principles have been formulated in relation to determining the Initiating Event Frequency for use in a DBA scheme:

1. Initiating Event Frequencies do not need to be assessed where fault sequences can be excluded from DBA on the basis of low unmitigated consequences.
2. The Initiating Event Frequency is the summation of the frequencies of the failures/initiators and any combined conditions in the absence of safety measures that lead to the potential unmitigated dose consequences.
3. The Initiating Event Frequency should be determined on a best-estimate basis.
4. Where Initiating Events lead to the same fault condition, therefore protected by the same safety measures, grouping of the events should be considered, with their frequencies summed for the purposes of the DBA. Salami slicing or over aggregation should be avoided.

The following guiding principles have been formulated in relation to determining the unmitigated consequences to be used against initiating events in a DBA scheme:

1. Unmitigated consequences do not need to be assessed where fault sequences can be excluded from DBA on the basis of low initiating event frequency.
2. The unmitigated radiological consequences of a fault or accident evaluated should assume all safety measures are absent or fail to operate, with the exception of passive features.
3. For unmitigated consequences, only the overall dose related to the IEF needs to be conservative, not all inputs.
4. For unmitigated consequences, the credibility of coincidental failures of normal operation safety features and controls, particularly where highly revealed, should be considered in assigning the consequence for use against the Initiating Event in the DBA scheme.

The following guiding principles have been formulated in relation to forming a DBA scheme:

1. A staircase approach should be used in a DBA scheme;
2. The cut-off frequency for Initiating Events within the DBA region of the scheme should be
1E-5 per year;
3. The cut-off consequence within the DBA region of the scheme should be 1mSv for public and 20mSv for workers;
4. The adoption of a Low Consequence Methodology for areas below the DBA region cut-off consequence should be considered;
5. Where there is a range of high and low consequence hazards and a range of frequencies, the adoption of at least two DBA regions, with a sound basis, should be considered within the DBA scheme;
6. Where the consequence, or initiating frequency of hazards, are close to the boundary of a higher region within the scheme, the confidence levels of the inputs should be examined, and where there is significant uncertainty, consideration should be given to moving to the higher region;
7. For areas outside of the DBA region, consideration should be given to provide less restrictive guidelines on protection, rather than no guidelines, as part of the overall DBA scheme;
8. The DBA regions, when used to provide quantitative targets for safety measures, should have appropriate guidance to ensure that the safety measures when combined with the initiating event frequencies will lead to a mitigated risk outside of the DBA region.
9. The DBA regions, when used to provide quantitative targets for safety measures, should be derived on a sound basis, taking into account the target safety measure pfd and an overall fault sequence frequency target based on the potential accumulation of numerous fault sequences.
10. The DBA regions and guidance, when used to provide quantitative targets for safety measures, should always be treated as guidance to inform ALARP, rather than mandatory design requirements for the number of safety measures and associated pfd targets.

The derivation and explanation of these guidelines is provided within this guide.

## Safety Directors’ Forum

In a sector where safety, security and the protection of the environment is, and must always be the number one priority, the SDF plays a crucial role in bringing together senior level nuclear executives to:

* Promote learning;
* Agree strategy on key issues facing the industry;
* Provide a network within the industry (including with Government and regulators) and external to the industry;
* Provide an industry input to new developments in the industry; and,
* To ensure that the industry stays on its path of continuous improvement.

It also looks to identify key strategic challenges facing the industry in the fields of environment, health, safety, quality safeguards and security (EHSQS&S) and resolve them, often through working with the UK regulators and Government, both of whom the SDF meets twice yearly. The SDF members represent every part of the fuel cycle from fuel manufacture, through generation to reprocessing and waste treatment, including research, design, new build, decommissioning, care and maintenance and waste disposal. The Forum also has members who represent the Ministry of Defence (MoD) nuclear operations, as well as “smaller licensees” such as universities and pharmaceutical companies. With over 25 members from every site licence company in the UK, every MoD authorised site, and organisations which are planning to become site licensees, the SDF represents a vast pool of knowledge and experience which has made it a key consultee for Government and regulators on new legislation and regulation.

The Forum has a strong focus on improvement across the industry. It has in place a number of subject-specific sub-groups looking in detail at issues such as radiological protection, human performance, learning from experience and the implementation of the new regulatory framework for security. Such sub-groups have developed a number of Good Practice Guides which have been adopted by the industry.

## Safety Case Forum

This Guide has been produced by the Periodic Review Forum, a workstream of the Safety Case Forum, which is in turn a sub-group of the SDF.

The Safety Case Forum was established in June 2012 and brings together a wide range of representatives of nuclear operators, from all the Licensees and Authorisees across the UK, including:

* Civil, commercial and defence activities;
* Design, operation and decommissioning of nuclear facilities;
* Research facilities.

The purpose of the Safety Case Forum is to provide guidance that is useful to, and will benefit the widest possible range of UK nuclear operators.

Such guidance is not mandatory, nor does it seek to identify minimum standards. It aims to provide a tool kit of methods and processes that nuclear operators can use if appropriate to their sites and facilities.

These guides are intended to improve the standardisation of approach to the delivery of fit-for-purpose safety cases, while improving quality and reducing the cost of production. They are designed to cater for all stages of a facility’s life cycle and for all processes within that life cycle.

This includes any interim, continuous and periodic safety reviews, allowing for the safe and efficient operation of nuclear facilities.

When using the information contained within these guides, the role of the Intelligent Customer shall always remain with the individual nuclear operator, which shall retain responsibility for justifying the arguments in their respective Safety Cases. The ONR and the Defence Nuclear Safety Regulator are consultative members of the Safety Case Forum.

The following companies and organisations are participating members of the Safety Case Forum:

   

  

  

  

   

  

  

Safety Case Forum Guides are available on the Nuclear Institute Website;

<http://www.nuclearinst.com/SDF-safety-cases>

**Disclaimer**

This UK Nuclear Industry Guide has been prepared on behalf of the Safety Directors’ Forum by a Technical Working Group. Statements and technical information contained in this Guide are believed to be accurate at the time of writing. However, it may not be accurate, complete, up to date or applicable to the circumstances of any particular case. This Guide is not a standard, specification or regulation, nor a Code of Practice and should not be read as such. We shall not be liable for any direct, indirect, special, punitive or consequential damages or loss whether in statute, contract, negligence or otherwise, arising out of or in connection with the use of information within this UK Nuclear Industry Guide.

This guide is produced by the Nuclear Industry. It is not prescriptive but offers guidance and in some cases a toolbox of methods and techniques that can be used to demonstrate compliance with regulatory requirements and approaches.

**Contents**

[Foreword 3](#_Toc30069531)

[Safety Directors’ Forum 5](#_Toc30069532)

[Safety Case Forum 5](#_Toc30069533)

[1. Introduction 10](#_Toc30069534)

[1.1 Context 10](#_Toc30069535)

[1.2 Purpose of a DBA Scheme 10](#_Toc30069536)

[1.3 Scope of the Guide 11](#_Toc30069537)

[2. Initiating Event Frequencies 13](#_Toc30069538)

[2.1 Introduction 13](#_Toc30069539)

[2.2 Definitions 13](#_Toc30069540)

[2.3 Calculation of Initiating Event Frequency 14](#_Toc30069541)

[2.4 Exclusions 16](#_Toc30069542)

[2.5 Application of Conditions to IEFs 17](#_Toc30069543)

[2.6 Initiating Event Frequency Summary 17](#_Toc30069544)

[3. Unmitigated Consequences 19](#_Toc30069545)

[3.1 Introduction 19](#_Toc30069546)

[3.2 Definition 19](#_Toc30069547)

[3.3 Interpretation of ‘Passive Safety Features’ 19](#_Toc30069548)

[3.4 Appropriate Conservatism 19](#_Toc30069549)

[3.5 Consideration of Multiple Co-incident Failures 20](#_Toc30069550)

[3.6 Hazards not Suitable for Unmitigated Consequence Assessment as Part of a DBA Scheme 22](#_Toc30069551)

[3.7 Unmitigated Consequences Summary 23](#_Toc30069552)

[4. DBA Scheme Guidance 24](#_Toc30069553)

[4.1 Factors to Consider in a DBA Scheme 24](#_Toc30069554)

[4.2 Staircase or Gradual Approach to DBA Region 24](#_Toc30069555)

[4.3 Low Frequency Cut-Off for the DBA Region 25](#_Toc30069556)

[4.4 Low Consequence Cut-Off for the DBA Region 26](#_Toc30069557)

[4.5 Number of DBA Regions 27](#_Toc30069558)

[4.6 Hazards Adjacent to DBA Region Boundaries 29](#_Toc30069559)

[4.7 Treatment of Areas Outside of the DBA Region 29](#_Toc30069560)

[5. Extended Use of DBA Schemes for Quantitative Guidance 31](#_Toc30069561)

[6. Summary 34](#_Toc30069562)

[7. Glossary 36](#_Toc30069563)

[8. References 37](#_Toc30069564)

[Appendix A: ONR SAPs Target 4 Guidance 38](#_Toc30069565)

[Appendix B: Example DBA Schemes 41](#_Toc30069566)

**Figures**

[Figure 1: Initiating Event within Fault Sequence illustration 13](#_Toc30069567)

[Figure 2: ONR SAPs Target 4 DBA Scheme 38](#_Toc30069568)

[Figure 3: DBA Scheme A 41](#_Toc30069569)

[Figure 4: DBA Scheme B 42](#_Toc30069570)

[Figure 5: DBA Scheme C 43](#_Toc30069571)

[Figure 6: DBA Scheme D 44](#_Toc30069572)

[Figure 7: DBA Scheme E 45](#_Toc30069573)

[Figure 8: DBA Scheme F 46](#_Toc30069574)

# Introduction

## 1.1 Context

This Safety Case Forum guide considers the formulation and use of Design Basis Assessment (DBA) Schemes within a safety case framework.

One of the aims of the Safety Case Forum, which reports to the Safety Directors Forum, is to share knowledge, processes and practices between the organisations involved in the civil and defence nuclear industries. All have a common goal to provide fit for purpose safety cases in the most efficient manner possible.

It is seen as beneficial for the organisations to be aware of what each other do, through comparative analysis, and to identify areas where guidance can be provided. This guidance can help individual organisations to determine how their methodologies compare, which can provide confidence in their approaches or help understand where any disparities are and to inform when reviewing/updating methodologies. This aids in demonstrating to internal and external approving authorities that the organisation producing the safety cases is aware of relevant practice elsewhere and these have been considered when forming the methodologies.

Duty holders are expected to develop their own methods for defining the scope of DBA tailored to their specific circumstances. A comparative analysis of DBA schemes used within the industry was carried out as part of the work by the Safety Case Forum. This identified that the DBA schemes and the guidance that support them have been derived separately and in many varied ways. This can be expected due to the variance in the hazards and complexity at different sites.

It is not the aim of this guide to form a single fully standardised DBA scheme to be endorsed for use throughout the industry, as this is not seen as practicable to implement, given the large range of different types of facilities and operations and challenges posed. It is not considered that a ‘single DBA scheme fits all’ is appropriate.

However, identification of common themes or principles on the basis of DBA schemes provides an opportunity for consistent understanding across the industry and is the basis of this safety case forum guide.

## 1.2 Purpose of a DBA Scheme

The general purpose of DBA schemes is to provide a simple and useable tool to determine which hazards should be subject to full design basis assessment requiring robust demonstration of fault tolerance and protection to prevent unmitigated consequences. In the context of this guide, hazard means any event, fault, failure, or action that may lead to unintentional exposure of people to a radioactive dose. This includes guidance on where safety measures are required. DBA guidance is provided in the Office of Nuclear Regulation (ONR) Safety Assessment Principles (SAPs), as discussed in Appendix A. Examples of DBA schemes from the comparative analysis are presented in Appendix B.

In general, a safety case framework consists of two main areas: DBA which takes a conservative approach to demonstrating fault tolerance and robust protection against hazards; complemented by Probabilistic Safety Assessment (PSA) which evaluates the best estimate of risk. Both of these assessments can provide an input into a demonstration that risks are As Low As Reasonably Practicable (ALARP), along with other factors such as good practice.

While PSA may be carried out on all hazards to a very low frequency cut-off, DBA is normally carried out on significant hazards only. A DBA scheme can be used to determine which hazards are significant and therefore required to be subject to DBA.

A DBA scheme uses the Initiating Event Frequency (IEF) and unmitigated consequences of hazards to effectively guide where the most effort is required in demonstrating protection. The scheme allows hazards to be placed into broad groups of importance in terms of unprotected radiological risk, and provides proportionate guidance for these groups.

Importantly, the scheme is also used to define which hazards do not need to be subject to DBA due to low frequency, low consequences or a combination of both.

The DBA scheme can be used to assess an existing facility to determine how the design and operation compares against DBA requirements, which can inform where there are potential areas where ALARP improvement studies should be focussed, complementing PSA.

However, it is often most effectively used during early stages of a design to inform on the relative importance of hazards present, and providing guidance on where robust protective measures are required.

The DBA scheme and its underlying guidance can be expanded to include numerical targets for safety measures and their probability of failure on demand (pfd). Safety measure pfds can also be provided through other design basis assessment means such as within the categorisation and classification process or other robust design approaches against safety principles or directly from PSA.

The design and safety case are influenced by the DBA scheme that is used and the underlying guidance that supports them, as it identifies the need for protective safety measures and mitigation safety measures, and ultimately input and presentation of the DBA within safety cases and application of ALARP studies, e.g. for shortfalls.

It is important to emphasize that the DBA scheme provides a tool for guidance only on the numbers of safety measures required. This should not be used to form absolute requirements, and other factors such as PSA and principles should always be considered as part of an ALARP demonstration.

## 1.3 Scope of the Guide

This Safety Case Forum guide provides discussion and guidance on the common themes and principles on the use of Design Basis Assessment (DBA) Schemes.

The guide covers the three high level factors to be considered in forming a DBA scheme and its underlying guidance, namely:

1. Definition of IEF to be used as an input to the DBA scheme (Section 2);
2. Definition of unmitigated consequence to be used as an input to the DBA scheme (Section 3);
3. Guidance on the derivation of the DBA scheme and its boundaries in order to place hazards into broad groups of importance (Section 4);
4. Guidance on the extended use of the DBA scheme for quantitative guidance (Section 5).

The guidance in the sections needs to be considered as a whole, rather than individually, as they are interrelated. For example, consideration of the unmitigated consequences first may remove the requirement to derive an IEF at all. The size of the risk bands presented in the DBA scheme used will also determine the accuracy needed in assigning an IEF or consequence, as these will be typically in broad ranges of at least a decade.

The collated guidelines for a DBA scheme are presented within the Summary in Section 6.

This guidance takes account of Target 4 and associated commentary from the ONR SAPs, reproduced in Appendix A, which represents the guidance produced by the regulator for their inspectors. This guidance also takes account of the comparative analysis carried out, with descriptions of the types of schemes that have been used in industry presented in Appendix B, noting that it is expected that duty holders develop their own methods rather than use the SAPs.

# Initiating Event Frequencies

## 2.1 Introduction

A main input into any DBA scheme is the Initiating Event Frequency (IEF) that leads to the unmitigated consequences. The approach to defining the IEF could have a large bearing on the inclusion or not of a fault sequence within DBA, and on the guidelines for protective safety measures.

A consistent understanding of the IEF methodology to be used in a DBA scheme across industry is desirable, such that all DBAs are formulated based on similar assumptions. A cross-industry comparison of guidelines and practices has been made in order to draw up a consistent, high level approach for application independent of the variation of the detailed DBA scheme that may be used.

Note, before developing IEFs, the associated consequences and the DBA scheme regions and its underlying guidance should be considered to inform the required level of accuracy of the IEF for DBA purposes. IEFs do not need to be assessed where fault sequences can be excluded from DBA on the basis of low unmitigated consequences.

## 2.2 Definitions

Within the Nuclear Industry, an Initiating Event can be defined as that part of a fault sequence which, if not prevented from developing further, could result in non-negligible radiological consequences to the public or workforce.

More broadly, an Initiating Event represents a fault condition which results in an unplanned departure from a normal operational state into an unsafe state, requiring some safety measure(s) to prevent or mitigate the consequences to arrive at a safe, controlled state. It is not necessarily the first chronological initiator as it may require combined initiators or initiators combined with conditions. More than one initiator may lead to the Initiating Event. This is illustrated in Figure 1, below.



Figure 1: Initiating Event within Fault Sequence illustration

There may be several Initiators, each of which individually could cause the Initiating Event fault condition, namely:

1. A failure of a control system;
2. A failure of plant;
3. An operator error;
4. A procedural error.

Internal and External hazards may also be initiators, though may be treated separately as they may cause a number of fault conditions simultaneously.

A Condition is a circumstance that is required in combination with the Initiator for the Initiating Event fault condition to arise. Therefore, the IEF is the product of the Initiator(s) and the associated conditional probability.

The IEF is therefore the summation of the failure frequencies of the set of Initiators, accounting for any Conditional probabilities.

In summary, an Initiating Event consists of a failure/initiator resulting in:

1. An unplanned departure from a normal operational state;
2. Which may also require detrimental circumstances/conditions;
3. In the absence of safety measures;
4. Which gives rise to the potential for non-negligible unmitigated radiological consequences.

The IE frequency definition in this guide is applied to the initiating fault of the plant or item that normally maintains control of the source of the radiological hazard and the conditions related to the fault for the potential to lead to radiological consequences.

There may be other co-incidental factors unrelated to the initial fault that may affect the potential unmitigated consequence and these are discussed as part of the assessment of unmitigated consequences in Section 3 of this guide.

## 2.3 Calculation of Initiating Event Frequency

2.3.1 Identification of Initiating Events

Appropriate hazard identification is an important step in overall DBA, though not the focus of this guide. Initiating Events are primarily derived from the hazards identified in Fault Schedules based upon information drawn from Hazard Logs/Lists.

Since an Initiating Event is defined as that part of a fault sequence which, if not prevented from developing further, could result in non-negligible radiological consequences to the public or workforce, the Initiating Event Frequency should be identified as the point at which non-negligible radiological consequences are inevitable without intervention from safety measures. As the input to the DBA scheme is based on a per year basis, the IEF should be annualised.

2.3.2 Grouping of Initiators into Initiating Events for DBA

Where Initiators lead to the same Initiating Event fault condition, and therefore will be protected by the same safety measures, they may be grouped, and their frequencies summed for the purposes of the DBA. This could be for a reactor plant where the initiators of electrical failure, mechanical failure and operator could all lead to failure of a pump and loss of flow, which is the loss of the normal duty means of maintaining control of core temperature. The initiators can be combined to one Initiating Event of loss of flow due to pump failure.

It is also possible to group a number of separate Initiators, e.g. if pump failure and an inadvertent valve closure all lead to loss of flow, the IEF may be based on all causes of loss of flow if the fault condition and safety measures are the same. However, if the safety measures are different for the pump failure and valve failure, then they should not be grouped.

Where Initiating Events are grouped, the most significant consequences should be used as part of the DBA. As the events lead to the same unsafe state then any differences in consequences should be minor and have no effect on DBA. If there are significant differences in consequences, then grouping may not be appropriate.

Careful consideration should be given to the grouping to ensure appropriate DBA is carried out:

1. Failure to group initiators sufficiently could mean that the guidance on safety measures from the DBA scheme is underspecified. There is the potential for a significant Initiating Event frequency to be effectively subdivided into multiple component or sub-component fault frequencies to the extent that the DBA requirements for Safety Measures is reduced/removed as the individual frequencies are decreased ('salami slicing'). This could result in insufficient DBA carried out and potential decrease in fault tolerance and risk reduction.
2. Conversely, over aggregation of initiators with different fault progressions could result in over estimation of requirements for safety measures and/or the lack of clarity on which safety measures protect against which initiating events. This would also result in an unclear basis for the DBA.

The grouping of initiators should therefore be targeted to ensure this is at the highest appropriate level while ensuring the demand on specific safety measures is clear.

2.3.3 Data for Initiating Event Frequency

The IEF should be determined on a best-estimate basis if practicable except for natural hazards, where a conservative approach should be taken to take account of data and model uncertainties when defining low frequency extreme events.

In determining the IEF from component failure data, there is a hierarchy of preferred information sources depending on availability which is generally:

1. Site specific plant data;
2. Item specific data from similar applications;
3. Generic reliability data;
4. Engineering judgement/expert elicitation.

A best estimate frequency would ideally be the most accurate value of the frequency derived from operating experience and/or test data, noting that the accuracy with which an IEF can be estimated will therefore improve as operational experience increases.

Data from the Manufacturer can also be useful in selection of the most appropriate generic data and in informing engineering judgement. In application of this data, care is needed to ensure that the data is relevant and that failure modes and environmental conditions of the item are representative. Also, data from each source should be reviewed and considered so that the most appropriate data is selected. Whilst plant specific data may be the most representative, it will be limited to the lifetime of plant operation. Comparison of plant/item specific data with generic/manufacturer supplied data and the impact on the derived IEF can be used to put such data into context, and can also provide useful insight with respect to the operating environment and the effect on performance and implications for maintenance/inspection requirements.

If there is insufficient or inadequate data to be able to derive a best estimate value, a reasonably conservative value should be derived using engineering judgement based on advice from relevant subject matter experts, such as human factors. This would particularly be applicable where it is necessary to make use of generic data for an item. Where early stage conservatism is applied, this should be revisited and refined over time.

For assessing human error probabilities, direct operating experience can be used, e.g. based on event reporting of operator errors, if sufficiently robust information exists. As this is not always available, an appropriate human factors technique such as HEART (Human Error Assessment and Reduction Technique) or THERP (Technique for Human Error Rate Prediction) or consultation with a Suitably Qualified and Experienced Person (SQEP) in Human Factors is recommended. Where procedures and operations are already very well established, such that their failure is very unlikely, a case could be made to consider this in the Human Error Probability (HEP) selection process to reflect credibility. For actions incorporated in the IE frequency, care should be taken to avoid giving credit in the selected HEP for undefined global measures such as training or supervision where this cannot be demonstrated, or unspecified recovery actions, since such requirements would ideally be derived from the results of the early DBA in order to be implemented to decrease the IEF.

Historical failure data i.e. observed failures over time can be used to predict future failures on the basis that the same pattern of failure continues into the future. This requires appropriate assessment to ensure applicability. Where no historical failures are recorded some conservatism should be used to reflect uncertainties and appropriate sensitivity analysis carried out.

2.3.4 Short Term Duration Initiating Events

For assessing events which are of relatively short duration or infrequent activities (such as maintenance activities, short term decommissioning activities or where disconnection of safety measures is required to carry out essential repairs), application of an annualised IEF by assumption of continuous operation would be a conservative approach. This would ensure that, for example, during a repair of an emergency cooling system, failure of the feed system would be assessed for continuous operation or during entry to a tented area failure of the room ventilation would be assessed for continuous operation. This would enable demonstration of the robustness of the plant using DBA without any consideration of time at risk.

For very short duration or one-off activities, or for some hazard types such as fire, application of an annualised IEF may be considered too conservative. It may be more appropriate to make an ALARP argument to demonstrate identification of appropriate and robust safety measures taking into account the short period within the DBA. In these circumstances, sensitivity studies could be carried out to determine the importance of this aspect.

For demand related faults, the DBA IEF could calculate the probability of a fault on demand based on the number of operations i.e. for a dropped load the IEF could be calculated by multiplying the probability of the fault on demand by the number of lifts carried out per year. This should be considered on each case to ensure it is not introducing additional conservatism into the assessment.

## 2.4 Exclusions

No credit should be claimed for a reduction in the IEF due to operation of safety measures, including the safety measure equipment and administrative controls. Where failures or unintended operation of equipment not qualified for specific accident conditions could exacerbate the consequences, or otherwise make the fault more severe, this would need to be assumed within the DBA.

No credit is generally claimed for facility occupancy in determination of the IEF for DBA which should represent failure of the normal control of the radiation source, but occupancy may be considered in assigning the appropriate unmitigated consequence as discussed in Section 3 if this requires a co-incident failure.

## 2.5 Application of Conditions to IEFs

As discussed in Section 2.2, the probability of specified ‘Conditions’ should be included in the IEF. Conditions are required in order for the failure/initiator to lead to dose consequences. The caveat is that these ‘Conditions’ must not be safety measures. This is in line with the best estimate approach to avoid potentially putting overly onerous requirements on design basis assessment guidance for safety measures, which may skew the design and operation of a facility.

An example of a ‘condition’ is an operating parameter such as the operating temperatures at the point of the failure/initiator which is applied as the starting point of a temperature excursion, where dose consequences will only occur if the operating temperature is at an infrequent or abnormal condition. Also, the application of an operational buffer for the maximum number of elements to be in a store, which is below the store capacity, can be accounted for within the IEF.

Another example of conditions is to account for the probability of recovery to a safe state using the normal duty control system, without any claims on safety measures. This could be where there is a partial loss of feed to a cooling system, where the normal control system or operator can compensate by reducing the power or duty required to maintain a normal operation state of the plant. This is where these recovery actions will occur for reasons other than safety and is in line with the best estimate approach.

If using this approach, any conditional probabilities applied which are not due to chance (e.g. number of a particular type of operations per year or steady state recovery actions) should be clearly listed in the safety case and need to be substantiated or managed to ensure these are not invalidated.

There may be a case for some conditions which are truly random and cannot be controlled, being assigned a probability in the IEF calculation. For example, the probability of a dropped load impacting exactly a vulnerable area of a plant leading to a fault condition, rather than an area with no consequences. These would have to be argued on a case by case basis if accounting for in the IEF to be inputted into the DBA scheme to determine if this needs to be subject to full DBA assessment.

Independence should be shown between the condition and the initiators under consideration. Control measures on the condition may need to be justified specifically in the safety case. The sensitivity of the safety assessment to the condition should be examined to establish its safety significance.

## 2.6 Initiating Event Frequency Summary

In terms of forming a DBA scheme, the following guidance principles have been formulated in relation to determining the Initiating Event Frequency:

**Guideline**: Initiating Event Frequencies do not need to be assessed where fault sequences can be excluded from DBA on the basis of low unmitigated consequences.

**Guideline**: The Initiating Event Frequency is the summation of the frequencies of the failures/initiators and any combined conditions in the absence of safety measures that could lead to the potential unmitigated dose consequences.

**Guideline**: The Initiating Event Frequency should be determined on a best-estimate basis.

**Guideline**: Where initiating events lead to the same fault condition, therefore protected by the same safety measures, grouping of the events should be considered, with their frequencies summed for the purposes of the DBA. Salami slicing or over aggregation should be avoided.

# Unmitigated Consequences

## 3.1 Introduction

The second main input into any DBA scheme is the unmitigated consequence. There are a number of factors that should be considered when defining the unmitigated consequence to ensure the DBA is appropriate and representative of the fault sequence.

A consistent understanding of the application of unmitigated consequences to be used in a DBA scheme across industry is desirable such that all DBAs are formulated based on similar assumptions. A cross-industry comparison of guidelines and practices has been made in order to draw up a consistent, high level approach for application, independent of the variation of the detailed DBA scheme that may be used.

Note; before developing unmitigated consequence, the associated IEFs and the DBA scheme regions and its underlying guidance should be considered to inform the required level of accuracy of the consequences for DBA scheme comparison. Consequences do not need to be assessed where fault sequences can be excluded from DBA on the basis of low frequency.

## 3.2 Definition

This definition of unmitigated consequences given in the 2014 ONR SAPs is considered appropriate:

*“The potential radiological consequences of a fault or accident evaluated assuming all safety measures are absent or fail to operate. This excludes passive safety features such as walls, or pipes, unless the fault or accident affects that feature”.*

The unmitigated radiological consequence should apply to an “unprotected” plant. For clarity the term “all safety measures” is interpreted as a protective safety system, a safety related system or administrative procedures that respond to the Initiating Event fault condition and returns the plant to a safe state (as shown in Figure 1 in Section 2.2).

The above definition of unmitigated consequences on its own is not enough; some guidance is required to amplify the definition.

## 3.3 Interpretation of ‘Passive Safety Features’

The phrase ‘passive safety features’ generally refers to Structures, Systems and Components (SSCs) that are robust and without moving parts, and would not be challenged by the initiating event. An example of a passive safety feature is a concrete wall that will continue to provide shielding in the fault scenario if independent of the fault, and therefore should be accounted for in assessing the potential unmitigated consequences. Similarly, a vessel that normally contains liquor can provide containment of released material and could be a passive safety feature. These features should be items that are part of the plant design, rather than specific safety measures added against a fault. Electrical, electronic or programmable electronic SSC would not count as a passive safety feature.

This approach includes an implicit safety claim on the passive safety feature which should be justified within the safety case.

## 3.4 Appropriate Conservatism

To support DBA, appropriately conservative dose calculations should be carried out. All inputs and assumptions into the dose calculation should be considered and justified. It is important to note that only the overall dose needs to be conservative, not all inputs. This includes the source term, dispersions and occupancies [Ref. 1].

The approach to defining the unmitigated consequence can have a large bearing on the inclusion, or not, of a fault sequence within DBA and the guidance on safety measures. Excessive conservatism could lead to an overly conservative design that may skew the design and/or introduce safety features that cause hazards in themselves. Ensuring that the basis of the consequences is understood, and the factors and assumptions are justified should be an important part of the DBA, rather than reverting to an onerous over-conservative approach. There should be an appropriate understanding of the uncertainties within the assessment of unmitigated consequences, rather than applying unspecified conservative safety margins. An understanding of any cliff-edges should be demonstrated.

In some circumstance, differences in the assumptions can change the unmitigated consequences from no consequence, to very high consequences needing several barriers, e.g. dependent on the threshold used for defining an unsafe state that could cause a radiological release. For example, the consequences can change significantly based on the use of criticality criterion, thermal limits, or, the withstand of barriers in determining if an unsafe state is reached where potential radiological release/exposure can occur.

Similarly, assumptions on the dose assessment from a release/exposure can have a significant effect on the magnitude of the consequence. A specific example is exposure durations. The longer that an exposure to radiation or contamination goes on, the higher the unmitigated dose will be. Judgement is required when defining a limit to exposure duration. Specific advice on worker exposure durations is given in the published SCF Guide on ‘Conservative exposure duration for unmitigated worker doses in design basis analysis’. This follows the principle of what is reasonable to consider within design basis derivation to avoid over-conservatism in the unmitigated consequences. In other cases, for example an ongoing release from a stack, the specific characteristics of plant operation will need to be considered.

Unmitigated consequences should only be assessed in-line with the scope and basis of the safety case. Typically, malicious acts that could cause increased consequences are excluded from safety cases, being addressed elsewhere, and therefore should not be assumed as part of the consequences.

Additionally, some consequences can be excluded simply on the basis of what is reasonable. For example, if an operator drops a sample bottle, and liquid leaks out, it is expected that doses from direct radiation and from any airborne contamination would be assessed; it is not expected that dose from the operator though ingestion (drinking) of the spilt radioactive liquid would be assessed. This would be inappropriate conservatism.

## 3.5 Consideration of Multiple Co-incident Failures

The IEF definition in Section 2 is applied to the initiating fault and conditions for the plant or item that normally maintain control of the source of the radiological hazard, thus potential for unmitigated consequences. However, in many circumstances, the probability of the full worst-case unmitigated consequences being realised will only occur if there are co-incident failures and therefore the consideration of these is required as part of assigning the consequences for the Initiating Event fault condition for use against the DBA scheme.

In line with the unmitigated consequences definition, this should be on the basis that the specific safety measures are not present. However, also assuming the potential for initiating events occurring combined with coincidental failures unrelated to the safety measures can result in over onerous design basis assessment. Co-incident failures can be accounted for in the IEF used for the DBA, but this can be complex to discuss multiple unrelated failures within the IEF. Given this, it may be decided to demonstrate that coincidental failures of safety features related to day to day activities are not assumed when assessing unmitigated consequences as part of the DBA assessment.

Therefore, the overall unmitigated fault sequence needed to reach the unmitigated consequences should consider the frequency of any assumptions on co-incident failures in the assignment of appropriate unmitigated consequences to an initiating event. Sequences with very low expected frequencies need not be included in the DBA. Judgement should be exercised in this regard, but for high hazard facilities, a fault sequence frequency of 1E‑7 per year would be a typical cut-off when applying design basis techniques.

For example, on a release of hazardous material in a controlled area, the credit taken for the operator wearing an air-fed suit or not would result in significantly different unmitigated consequences for the same fault condition IEF. If air-fed suits are always worn in a specific area that requires crossing a barrier, unmitigated consequences can be determined based on an air-fed suit being worn. This recognises that for sites where air-fed suits are worn, the importance of wearing an air-fed suit in such an area is well established as part of normal duty controls, such that assuming failure to do this is not considered credible or reasonable. Therefore, the unmitigated consequence would take credit for the air-fed suit being operational. The requirement for the air-fed suit may not be directly attributed a result of DBA, but its importance will be considered as part of the normal operation controls, allowing the DBA to assess hazards in the area on a more realistic basis, including appropriate categorisation and classification.

Similar considerations can be applied on whether to assume failure of ventilation extract. Ventilation extract is not always regarded as only a safety measure, as for some facilities it is used as a dose reduction measure claimed for planned work, thus forming part of normal duty controls and categorised as such. A fault occurring within the facility where ventilation has also failed would require a coincidental failure, as long as appropriate measures are in place to confirm that the ventilation system is operational and effective. In practice, failure of ventilation extract can be revealed to control room operators, and depending on facility procedures, it is expected operations would be ceased if the ventilation extract fails, or that the facility would be evacuated having ‘made safe’. Therefore, it would not be credible or reasonable to assess the unmitigated consequence assuming ventilation becomes ineffective independently and coincident at the time of the initiating event due to very low frequency.

Another potential consideration is the presence of personnel in unauthorised locations that would have a significant effect on the unmitigated consequences. An example is for radiation exposure hazards where high dose rates would only occur in these prohibited areas, as passive safety features such as concrete structures would significantly reduce the consequences outside of them. The measures in places to control access to these areas, rather than chance or time at risk, would have to be assessed to ensure that it is not credible or reasonable to assume occupancy at the time of a fault.

However, if the initiating event in the facility also affects the safety function of, say the air-fed suit or ventilation extract, then failure must be assumed when assessing unmitigated consequences.

Faults of air fed suits, ventilation extracts or entering prohibited areas can initiate separate fault sequences in their own right, and if this will lead directly to dose consequences should be considered appropriately. However, this should not be considered co-incident with the plant faults, which should be treated within the unmitigated consequences of the plant fault initiating event as discussed above.

It is recognised that measures such as ventilation can be regarded as a mitigating safety measure in relation to an initiating fault elsewhere in the facility where the ventilation is not part of the normal control system. For example, if used to support a higher decontamination factor for a containment barrier than if the extract is not working. If in this case, only local operations would be stopped due to ventilation failure, then it should not be claimed for unmitigated consequences for faults in others areas of the facility where operations would not be stopped due to ventilation failure.

## 3.6 Hazards not Suitable for Unmitigated Consequence Assessment as Part of a DBA Scheme

There are a number of hazards where it can be difficult to have a simple IEF to unmitigated consequence relationship for use as part of the DBA scheme. These instances include:

1. Faults that do not lead to immediate consequences;
2. Hazards that have complex series of conditions between the original initiator and the potential unmitigated consequences such as fire;
3. Catastrophic structural failures unrelated to any defined operational faults.

In some cases, faults might not have any immediate consequences, but result in the potential for consequences sometime in the future. This can be difficult to assess unmitigated consequences against an IEF in any meaningful manner compared to more direct fault conditions and therefore not suitable to input in a DBA scheme. Therefore, complementary approaches to demonstrate robust DBA will be required rather than use of the DBA scheme.

For example, loss of a reactor chemical treatment system, which keeps the plant pH and oxygen content within specification, will have no short-term consequences, but could lead, if undetected for a long period of time to structural integrity issues and a fault condition. Although an IEF for loss of the treatment system can be assigned, relating this to a consequence with an appropriate conditional probability can be difficult as there will be detection and recovery. Where this is the case, there isn’t an easy way to address this type of issue within a DBA scheme, and comparison with numerical DBA criteria may be inappropriate. Therefore, it is important that appropriate deterministic assessment of long-term-issues is provided, separate but complementary to the DBA scheme assessment of direct short-term faults. For example, these should be considered appropriately within the normal operation substantiation, with appropriate actions and operational constraints and limits generated on loss of these systems.

A leak-to-ground may also be considered to be a fault without immediate consequences therefore not suitable for input into a DBA scheme. The long-term consequences may be environmental, or if the ground is later excavated by workers, an uncertain worker dose might result. Relating the IEF to a consequence with an appropriate conditional probability would be difficult, thus comparison with DBA criteria may again be inappropriate and alternative approaches to assessment would be required. A leak-to-ground is clearly a negative consequence that needs to be avoided and assessed in the safety case and/or environmental case. Appropriate good engineering design features and any appropriate safety measures should be identified, preferably ones that prevent the leak in the first place. This would be backed up by engineering substantiation and appropriate examination, inspection, testing and maintenance.

There are a number of faults that will not lead directly to a radiological dose, but may affect safety measure functionality. As these cannot be measured directly in immediate dose terms, typical DBA criteria cannot be applied directly, but these faults can be assessed as part of confidence in the protection. Similarly, unintended relocation of a substantial quantity of radioactive material within the facility which places a demand on the integrity of the remaining physical barriers may not lead to a direct dose but the safety case should consider the confidence in the physical barriers and safety measures that prevent such relocation.

Other hazards can also be difficult to apply a meaningful assessment against typical DBA criteria. For fire hazards, IEFs at source can be formulated, e.g. for a small electrical fire. However, assigning a meaningful unmitigated consequence can be challenging, as if truly unmitigated this would lead to a major fire and severe consequences. Assessing all potential sizes and locations of fire for IEFs and assigning conditional probabilities for consequences can become unwieldy within a DBA scheme. Similarly, intrinsic structural failures of cranes and buildings with no external influences such as a natural event or operational fault conditions, e.g. snagging, can become difficult to assign IEFs related to specific consequences. Therefore, complimentary approaches to DBA may have to be considered rather than use of the DBA scheme.

## 3.7 Unmitigated Consequences Summary

In terms of forming a DBA scheme, the following guidance principles have been formulated in relation to determining the unmitigated consequences:

**Guideline**: Unmitigated consequences do not need to be assessed where fault sequences can be excluded from DBA on the basis of low initiating event frequency.

**Guideline**: The unmitigated radiological consequences of a fault or accident evaluated should assume all safety measures are absent or fail to operate, with the exception of passive safety features.

**Guideline**: For unmitigated consequences, only the overall dose related to the IEF needs to be conservative, not all individual inputs.

**Guideline**: In assessing unmitigated consequences, the credibility of coincidental failures of normal operation safety features and controls should be considered, particularly where highly revealed, when assigning the consequence for use against the Initiating Event in the DBA scheme.

# DBA Scheme Guidance

## 4.1 Factors to Consider in a DBA Scheme

The general purpose of DBA schemes is to provide a simple and useable tool to determine which hazards should be subject to full design basis assessment requiring robust demonstration of fault tolerance and protection to prevent unmitigated consequences. This is by classing hazards into nominal risk regions and developing guidance on broad expectations for protection or mitigation for hazards within these regions.

Duty holders are expected to develop their own methods for defining the scope of DBA tailored to their specific circumstances. A comparative analysis has been carried out, which indicates a representative range of design basis schemes that have been used by duty holders along with the baseline of Target 4. These are included in Appendix B within Figures 3 to 8 along with accompanying notes on the regions. Target 4 of the SAPs from Appendix A has been used as a baseline and is overlaid in all of the design basis schemes.

The comparative analysis identified that the DBA schemes and the guidance that support them have been derived separately and in many varied ways. This can be expected due to the variance in the hazards and complexity at different sites.

It is not the aim of this guide to form a single fully standardised design scheme to be endorsed for use throughout the industry, as this is not seen as practicable to implement, given the large range of different types of facilities and operations and challenges posed.

However, from the comparative analysis, identification of common themes or principles on the basis of formation of the DBA schemes provides an opportunity for consistent understanding across the industry. Guidance has been formed on the factors to consider when forming a DBA scheme and discussion on the underlying principles to apply.

The areas of guidance for consideration when developing a scheme can be split into the following areas:

1. Staircase or gradual approach to DBA region;
2. Low frequency cut off for the DBA region;
3. Low consequence cut off for the DBA region;
4. Number of DBA regions;
5. Treatment of faults adjacent to DBA region boundaries;
6. Treatment of areas outside of the DBA;

These are discussed in turn within the following sub-sections.

The extended use of DBA schemes for quantitative guidance is discussed in Section 5.

## 4.2 Staircase or Gradual Approach to DBA Region

DBA should be a graded approach, where high frequency and high consequence hazards are treated separately to low frequency/consequence hazards to ensure a proportional approach. This is carried out by plotting the IEF against the unmitigated consequence on DBA schemes (graphs) which have defined regions to group the hazards into significance bands.

In applying a graded approach, standard applications to define the boundaries regions would be in the form of a curve, sloped line, or staircase.

Although ideologically, a curve provides the exact correlation of frequency and consequence to a single common point, target 4 and the general approach used throughout industry has been to use a staircase approach to defining the DBA region.

The use of a curve or sloped line would indicate exactness about the ability to provide a frequency of a hazard, or the calculation of an unmitigated consequence to specific points. This is an unrealistic expectation as the reality is that the frequency and consequence estimates provide confidence in the region where the initiating event lies. The use of a staircase is a more pragmatic approach, as this allows hazards to be placed into broad groups to allow distinction between significant hazards and those of lower significance, with use of at least decade-wide bands.

The advantage of using a staircase approach is that it removes the need to be precise in forming frequencies. Hazards can be assigned to a band of frequency, e.g. between 10-2 and 10-3 per year, rather than detailed definition. A similar argument applies to the unmitigated consequences, where bands simplify the level of analysis required.

This can be of particular importance during early stages of a design programme, e.g. in requirement setting or concept stages, where the detailed design of equipment or exact potential consequence cannot be derived sufficiently. At these stages, potential hazards can be placed into bands of consequence and frequency relatively quickly, using experience and read across as appropriate. This can be used to provide guidance to the design by ascertaining what is expected to be a DBA event and the number of safety measures required.

If assessing an older facility as part of a periodic review of safety, which may not have been assessed to the latest DBA scheme guidance, this also provides the same advantage in that a relatively quick assessment can be carried out.

The staircase approach can also lead to less sensitivity as the bands are much broader and simplistic, therefore most hazards will be clearly within a specific band and less sensitive to small changes in frequency and/or consequence.

The following guidance is provided.

Guideline: A staircase approach should be used in a DBA scheme.

## 4.3 Low Frequency Cut-Off for the DBA Region

As discussed in Appendix A, the SAPs state that all faults with initiating events below
1E-5/yr are excluded from the DBA region, except natural hazards which should use an IEF of <10‑4 per year. There is general agreement from the SAPs with all of the schemes (bar one) used in industry.

This use of 1E-5/yr is well established practice as a cut-off for DBA and therefore no more detailed derivation of this definition is considered necessary.

Initiating Events with frequencies below these values need not be subject to full DBA analysis, but the risk should still be considered and demonstrated to be ALARP using other methodologies, such as PSA. This is discussed further below in Section 4.7.

There is no upper bound for frequency in terms of the DBA scheme to ensure that all Initiating Events can be assessed. However, the use of the DBA scheme can be used to highlight hazards where there are high initiating event frequencies (e.g. >1/yr) leading to demand on safety measures which can be fed back into the design process and operation. Event frequencies of this significance could be considered as expected in normal operation in a year, rather than a fault condition, and therefore designed out if possible, or further prevention should be considered, rather than through protection only.

The following guidance is provided.

Guideline: The cut-off frequency for Initiating Events within the DBA region within the scheme should be 1E-5 per year.

## 4.4 Low Consequence Cut-Off for the DBA Region

Although a DBA scheme can be formed to cover all events that lead to a radiological consequence, it is usual to have a cut-off to delineate where the consequences become so low such that DBA would be disproportionate.

The SAPs Target 4 uses 1mSv public and 20mSv worker as the low consequence cut-off as explained within Appendix A, relating to the legal limits for normal operation exposure. This is considered to be the maximum dose cut-off that should be used within a DBA scheme, as any higher dose cut-off would suggest that exposure above normal operation limits would not need to be examined in the DBA.

However, in examining the design basis schemes currently used in industry, it is noticeable that most extend the low consequence below the Target 4 limits. This can be from directly extending the cut off in the DBA region to a lower limit,
e.g. 0.1mSv for the public, or through the introduction of a Low Consequence Methodology (LCM) region.

In general, the extending of the region has been due to a concern that events just outside the DBA region can still lead to a significant risk estimate, either as single events or cumulatively, therefore provision of safety measures is required when subject to PSA and ALARP demonstration. This can be due to higher frequencies associated with low consequence hazards, especially where best estimate assessments do not change the consequences significantly, which are then compared against the very low BSO targets.

The advantages of extending the DBA schemes below the Target 4 limits is to ensure guidance is in place for this relatively large area such that risks are reduced before the requirement to perform a full PSA. It should be exceptional for a hazard that meets the DBA scheme guidance to have a risk from PSA that is not ALARP.

To carry out a full PSA can require considerable detail on the design and analysis to be carried out to determine the consequences and can be difficult where there is low design maturity. As such, any significant risk in this region below the DBA cut-off, may only become apparent late in the design process with greater impact on rework required.

In addition, there can be a stark crossover, where within DBA the design is expected to be robust against events through engineering controls with safety measures provided. However, just below this line, though a noticeable consequence in comparison with legal limits, the engineering may not have to be robust and no safety measures required.

Inclusion of guidance on hazards below the Target 4 limits within the DBA scheme can provide a framework early in a project to inform the design and also provide a simple means to measure and present the safety case associated with these hazards. There are two means of providing this guidance, extending the DBA areas to lower consequence areas, or the adoption, as many have, of a Low Consequence Methodology area.

The extension of the DBA area, although at first seems a simple step to take, in practice does not allow any distinction between the requirements on providing fully justified safety measures for areas within Target 4, with those areas that are of smaller consequence. For many hazards with low consequences, e.g. minor spillages, releases, it can become disproportionate to provide fully engineered safety systems, where other administrative controls would be sufficient to lower the risk to ALARP levels.

It is therefore considered appropriate to maintain the DBA region in line with the Target 4 delineation.

The introduction of separate Low Consequence Methodology area within the DBA scheme, but outside the DBA region, provides an opportunity to provide more appropriate guidance for low consequence areas, distinguished from those hazards within the DBA region. This can include guidance on instances where a safety measure may be recommended, though this may not have to be to the same level of robustness as within the DBA region, or where administrative controls can be appropriate. This can be used to demonstrate robustness of a design or process and can effectively eliminate the need for PSA to be carried out if the hazard can be argued as negligible risk on qualitative grounds.

The Low Consequence Methodology area within the DBA scheme should be derived appropriate to the site. A lower consequence band should be selected, based on a level where it is considered the dose would be noticeable enough to be of concern compared to normal operation, for example 0.1mSv (public) and 2mSv (workers). For frequency, it can be considered proportionate to only define this area for frequent faults only. For example, this could be any fault sequence with a frequency in the range 1 to 1E-3/yr, in line with low frequency cut-off used within Target 4 of the SAPs for low consequences faults, as discussed in Appendix A. Below this, the combination of frequency and low consequence is unlikely to challenge the BSO. These boundaries may be extended if it is intended to use the LCM in place of PSA.

The following guidance is provided.

Guideline: The cut-off consequence within the DBA region of the scheme should be 1mSv for public and 20mSv for workers.

Guideline: The adoption of a Low Consequence Methodology for areas below the DBA region cut-off consequence should be considered.

## 4.5 Number of DBA Regions

The purpose of the DBA scheme is to classify hazards into nominal risk regions and developing proportionate guidance on broad expectations for these regions. The DBA scheme should therefore have a number of separate DBA regions to enable graded and proportional guidance to be provided.

In its simplest form, the DBA scheme could have two regions, such as Target 4 of the SAPs, with no further delineation other than within or out of the DBA region. This has a single dividing line between a DB region where protection is required, and an effective DB0 region, where no explicit requirement for safety systems is required out with separate PSA and ALARP considerations. In the DBA region the protection systems would then be assessed against other principles such as single failure criterion, i.e. the plant is tolerant to failure within a safety measure.

For sites that have a relatively small set of hazards, or the hazards are only in a small range of consequences, it is considered that direct use of DBA scheme only to determine what is within the DBA region is reasonable, without the necessity to create a scheme with different regions that will never apply to the facility.

However, based on the currently used DBA schemes, most duty holders considered that additional guidance and delineation was required to aid design and safety assessment and to aid safety case presentation. This can be reflected in the potential variance of plants and types of hazards, or complexity of the safety cases where more up-front guidance helps provide a more useful framework.

The most common approach is to further delineate the regions within the DBA region, nominally termed DBA1 and DBA2 region, as well as a DB0 region for those hazards outside the DBA region. This allows separate guidance to be provided for those hazards within the DBA that are high frequency/consequence compared to those that are closer the DB0 region.

It is intuitive that to ensure each hazard is reduced to a comparable risk, the hazards in the DB2 region in the scheme should have additional protection compared to hazards in the DBA1 region which are nearer the DBA0 region. For example, for the same consequence band, an additional safety measure is appropriate for higher frequency events, e.g. with IEFs of 10-2 per year, compared to initiating events at the edge of design basis frequency, i.e. near 10-5 per year, to achieve a comparable level of risk.

Also, it can be postulated that, from experience, high frequency events with high unmitigated consequence are generally found to require additional safety measures to meet other targets such as the risk BSL/BSO and to provide ALARP demonstration. Therefore, providing two DBA regions provides a more graded approach to DBA and can provide clearer proportional guidance.

For the DBA2 regions, schemes either advise that two independent safety measures should be provided, or there must be explicit demonstration of the single failure criterion.

Below the DB2 region, schemes either advise that one safety measure should be provided, or that provision should be considered in line with the ALARP principle.

It is also possible to develop a DBA3 region if very frequent/high consequence hazards exist.

As a variation, some schemes have introduced DBA+ regions. This is where it is expected that it should be treated as the higher DBA region, however if it can be shown that a passive or other highly reliably safety system is in place, then one safety measure may be appropriate in line with the ALARP principle.

The number of DBA regions should be derived based on the site-specific requirements and understanding of the hazard spectrum for the site. A clear argument should be provided on the demarcation of the boundaries and why this is appropriate. This can be through direct experience from the specific site operations. For example, there is little point in developing a DBA2 region if the site characteristics mean that high frequency/high consequence hazards do not exist. Also, the guidance associated with the DBA regions may differ on consideration of the number of hazards that may exist within a region.

It should be expected that the DBA scheme and the associated guidance should ensure that the safety measures provide protection such that the consequence is prevented in preference. If this is not fully possible, then the guidance should require the consequence to be mitigated by the safety measure(s) to below an acceptable level, e.g. the very low consequence BSO as shown on Target 4. Only the design basis safety measures should apply when judging design basis success for prevention of consequences or appropriate mitigation. Safety related systems or other features included due to broader considerations should not be included. Credit for these should only be part of the PSA.

Generally, the DBA scheme and the associated guidance should be based on the principle that the safety measures when combined with the initiating event frequencies, will lead to a mitigated risk that is as a minimum outside of the DBA region. Therefore, it is possible to consider whether the fault sequence frequency that takes account of safety measure failures, if it were placed on the DBA graph, would result in a location on the DBA scheme outside the DBA region. This can be in addition to the PSA where safety measure failure is considered to demonstrate that the safety measures are effective in lowering risk.

This last point introduces the potential for quantitative guidelines for safety measures within the DBA scheme, which can also be the basis for the derivation of the DBA regions. This extended use of DBA schemes to have a probabilistic element is discussed more in Section 5.

The following guidance is provided.

Guideline: Where there is a range of high and low consequence hazards and range of frequencies, the adoption of at least two DBA regions with a sound basis should be considered within the DBA scheme.

## 4.6 Hazards Adjacent to DBA Region Boundaries

As DBA can be used as an exercise to rank hazards, rather than exhaustively calculating frequencies and consequences, care has to be taken when an event lies just outside the DBA line, or between two DBA regions (e.g. DBA1 or DBA2 boundary).

For items just outside the relevant boundary, the level of confidence should be examined. In these cases, greater understanding of the uncertainties should be looked at.

If there is high confidence, then items should not be artificially moved to the higher DBA region. For example, if it is known that the unmitigated consequence assessment methods manage the degree of conservatism such that it is an upper bound. Similarly, if the initiating event frequency is based on actual operating experience, rather than generic data, then it will have high confidence.

However, where significant uncertainty exists, then consideration should be given to treating the hazard as if in the higher DBA region to ensure a robust DBA that will not be subject to later challenge. Alternatively, appropriate sensitivity analysis should be carried out.

Extra justification may be required to show that a hazard with high consequences is beyond design basis on low frequency grounds, e.g. just below <10-5/yr, as this can often be beyond operating experience and therefore rely on more qualitative demonstration.

The following guidance is provided.

Guideline: Where the consequence or initiating frequency of hazards are close to the boundary of a higher region within the scheme, the confidence levels of the inputs should be examined, and where there is significant uncertainty, consideration should be given to moving to the higher region.

## 4.7 Treatment of Areas Outside of the DBA Region

As part of the overall safety case, consideration still needs to be given to areas outside of the DBA region (e.g. initiating events just beyond 10-5 with high consequence). These areas are normally considered as part of the PSA only.

However, as a tool to help inform design, especially in early stages, rather than stating that no safety measures are required for hazards outside the DBA region, it may be prudent to provide additional guidance on the provision of safety measures in this area, possibly included within the overall DBA scheme and associated guidance. This is not to meet DBA requirements, but as a design and safety case aid as part of the DBA scheme to provide extended guidance.

This is in recognition that once safety measures are accounted for as providing protection of hazards within the DBA region, it can lead to these other hazards becoming dominant if unprotected and therefore become the focus of ALARP considerations. The PSA may not be carried out at sufficient detail until later in the design process for this to be highlighted.

Recognising that these are outside the DBA region, the guidance should be pragmatic and be less restrictive on the basis of the safety measures. For example, the safety measure could be justified on a best estimate basis only, since it is to de-risk the PSA only.

This can also aid demonstration that the plant is robust to cliff edges in terms of safety measure provision without relying on PSA which could show that risk is low due to time at risk rather than robust design.

In terms of hazards that are just below the Target 4 area, the Low Consequence Methodology should be considered as discussed in Section 4.4.

The following guidance is provided.

**Guideline**: For areas outside of the DBA region, consideration should be given to provide less restrictive guidelines on protection, rather than no guidelines, as part of the overall DBA scheme.

# Extended Use of DBA Schemes for Quantitative Guidance

A number of duty holders have extended the use of DBA schemes to provide quantitative guidance for probability of failure on demand of safety measures. The quantitative approach can also be done through the categorisation and classification process linked to the DBA scheme to assign Cat A, B or C safety measures with pfd targets and Safety Integrity Levels (SILs) for electronic equipment. Other duty holders address the safety measure pfd exclusively in a PSA context. This Section discusses the option to extend the use of the DBA scheme for quantitative guidance for probability of failure on demand of safety measures.

Section 4.5 discussed that the number of DBA regions should be derived based on a clear argument on the demarcation of the boundaries and why this is appropriate.

One method to deriving the DBA scheme is through a quantitative approach. The DBA scheme guidance can be expanded to include numerical targets in terms of numbers of safety measures and their probability of failure on demand (pfd). The approach anticipates any numerical risk assessment using PSA, with the intent that meeting the DBA scheme guidance would ensure that the numerical risk criteria will also be met.

This quantitative approach is beneficial for a facility that merits this level of analysis to support a new or complex design or to inform the design before the safety measures are even designed.

The derivation of DBA regions can have a basis in mathematics and provide a quantitative output as guidance to designers and to assess the final design against within the safety case. To be an informative tool, underlying assumptions on the robustness of the safety measures claimed in order to meet the DBA regions can be generated against an overall fault sequence target for each sequence.

The advantage of this approach is that it results in the development of very simple guidelines directly from the DBA scheme for use in the design process or assessment of existing facilities. This comes in the generic forms of:

For an initiating event with a frequency of (X) with an unmitigated consequence of (Y), then (No. of) safety measures should be provided, each with a pfd of (Z), to meet the DBA fault sequence target.

**OR**

For an initiating event within the DB(X) region, then (No. of) safety measures should be provided, each with a pfd of (Z).

The DBA guidance can be based on ensuring that once the safety measure(s) are accounted for on a deterministic basis, as well as preventing the consequence, that fault sequence of the initiating fault and failure of the safety measures would have a frequency that would be outside the DBA region. The DBA fault sequence target for use should be formulated with consideration of the site and number of hazards.

An approximate mathematical model can be built up based on the appropriate safety measure pfd for all initiating events and unmitigated consequences to form the DBA regions. This should recognise that for lower doses, fatality risk factors can be applied (the probability of early death having received a specified dose) and can be accounted for in determining the overall sequence success. It may be appropriate once at lower consequence bands, to provide an argument basis for the regions, rather than strictly using a mathematical model, to reflect the decreasing significance of low consequence hazards in general.

In designing or assessing safety measures, the number of safety measures and the reliability is measurable against the selected DBA fault sequence target. The pfd of safety measures can be estimated using fault tree analysis and compared against a target pfd. This can be done early in the design and provide a feedback loop into the process.

As an example, if you have an initiating event with a frequency of 1x10-2 per year with an unmitigated consequence of >1Sv, then this is within the DBA region. It should be expected that once the safety measure(s) is accounted for on a deterministic basis, the frequency should be outside of design basis, i.e. <10-5 /yr. This would mean that the safety measures on a quantitative basis would at least have a 1x10-3 pfd or better to achieve this.

If the guidance is based on a generic safety measure pfd of 10-2, then this would suggest that on a quantitative basis, two safety measures would be required to move the fault sequence out of the DBA region, i.e. within the DBA2 region.

Taking this example, to move out of the DBA region, this would result in:

For an initiating event with a frequency of (10-2) with an unmitigated consequence of (>1Sv), then (2) safety measures should be provided, each with a pfd of (10-2), to meet the DBA fault sequence target of <10-5 /yr.

**OR**

For an initiating event within the DB(2) region, then (2) safety measures should be provided, each with a pfd of (10-2).

Due to rounding-up in the staircase grouping, a combined safety measure pfd of <10-3 could also be set, but provision of a safety measure(s) with a low pfd (0.1) to meet the fault sequence target should be discouraged in-line with robust design safety principles. This is to ensure that the DBA guidance is not met by ‘paper bag’ safety measures with poor reliability.

If safety measures were designed generally to meet a <10-3 pfd, then only one safety measure would be required to move out of the DBA region, i.e. within a DBA1 region.

For an initiating event with a frequency of (10-2) with an unmitigated consequence of (>1Sv), then (1) safety measures should be provided, with a pfd of (<10-3), to meet the DBA fault sequence target of <10-5 /yr.

**OR**

For an initiating event within the DB(1) region, then (1) safety measure should be provided, with a pfd of (10-3).

If there are a large number of fault sequences in a facility, then it may be appropriate to extend the fault sequence target to anticipate the collation of numerical risk assessment using PSA. The design could meet the DBA guidance, but the addition of 10’s or 100’s of fault sequences could still lead to a high PSA risk against the challenging low frequency BSOs, depending on the degree of difference between deterministic and best estimate assessment (salami slicing effect). Therefore, rather than aim for <10-5 per year to move out of the DBA region, the use of, for example, 10-6 per year would introduce a more conservative target to provide margin, or where there are numerous faults in a consequence band, 10-7 per year could provide additional margin. This would increase the target number of safety measures. The extension of the target fault sequence frequency can then be fed into the mathematical basis to decide on the number of safety measures required.

For the example, for a revised 10-7 per year target with a generic safety measures pfd of 10-2, this would result in a DBA3 region:

For an initiating event with a frequency of (10-2) with an unmitigated consequence of (>1Sv), then (3) safety measures should be provided each with a pfd of (10-2) to meet the DBA fault sequence target of 10-7 per year (or combined target of 10-5)

**OR**

For an initiating event within the DB(3) region, then (3) safety measures should be provided, each with a pfd of (10-2).

As can be seen, the guidance on the safety measure numbers is heavily influenced by the choice of pfd and DBA fault sequence target and needs balanced consideration by the specific duty holder. If using the higher generic pfd for safety measures (e.g. 10-2), this can lead to a DBA3 region, where it can be challenging to provide full independence between the measures due to common cause failures and appropriate guidance should be provided on these areas. From experience within industry where the quantitative approach has been used, the setting of the lower pfd targets (10-3) to avoid a DBA3 region is more practicable such that focus is on redundancy and diversity within a safety measure where required to meet the pfd, rather than independent measures.

To provide further flexibility, a DBA region can be further divided to allow credit where safety measures that are more reliable than the generic target pfd are available, e.g. passive safety measures. In order to prevent skewing of the assessment by only assuming the basic pfd, then DB+ regions can be introduced. This is where the guidance can state that either a high reliable safety measure is required, or two normal reliability safety measures should be provided.

One caution in using this approach is that the number of safety measures and associated pfd should always be treated as guidance only to inform ALARP rather than mandatory requirements for the design. The failure of a safety measure to reach the assumed pfd, or the failure to meet the overall fault sequence frequency should not be regarded as a fixed requirement and used only as a potential basis for further examination of the design and operation as part of ALARP, where the PSA should also be taken into account.

The following guidance is provided.

**Guideline**: The DBA regions, when used to provide quantitative targets for safety measures, should have appropriate guidance to ensure that the safety measures when combined with the initiating event frequencies will lead to a mitigated risk outside of the DBA region.

**Guideline**: The DBA regions, when used to provide quantitative targets for safety measures, should be derived on a sound basis, taking into account the target safety measure pfd and an overall fault sequence frequency target based on the potential accumulation of numerous fault sequences.

**Guideline**: The DBA regions and guidance, when used to provide quantitative targets for safety measures, should always be treated as guidance to inform ALARP, rather than mandatory design requirements for the number of safety measures and associated pfd targets.

# Summary

This guide provides advice on how to approach the formation of a Design Basis scheme for the use in nuclear facility safety cases. This has been formed taking into account a comparison analysis of schemes used in industry at present.

Guidance principles that can be followed for the use of DBA schemes have been generated for the inputs of IEFs and Unmitigated Consequences, as well as the formation of a DBA scheme layout.

The following guiding principles have been formulated in relation to determining the IEF for use in a DBA scheme:

1. **Initiating Event Frequencies do not need to be assessed where fault sequences can be excluded from DBA on the basis of low unmitigated consequences.**
2. **The Initiating Event Frequency is the summation of the frequencies of the failures/initiators and any combined conditions in the absence of safety measures that lead to the potential unmitigated dose consequences.**
3. **The Initiating Event Frequency should be determined on a best-estimate basis.**
4. **Where initiating events lead to the same fault condition, therefore protected by the same safety measures, grouping of the events should be considered, with their frequencies summed for the purposes of the DBA. Salami slicing or over aggregation should be avoided.**

The following guiding principles have been formulated in relation to determining the unmitigated consequences to be used against initiating events in a DBA scheme:

1. **Unmitigated consequences do not need to be assessed where fault sequences can be excluded from DBA on the basis of low initiating event frequency.**
2. **The unmitigated radiological consequences of a fault or accident evaluated should assume all safety measures are absent or fail to operate, with the exception of passive features.**
3. **For unmitigated consequences, only the overall dose related to the IEF needs to be conservative, not all individual inputs.**
4. **In assessing unmitigated consequences, the credibility of coincidental failures of normal operation safety features and controls should be considered, particularly where highly revealed, when assigning the consequence for use against the Initiating Event in the DBA scheme.**

The following guiding principles have been formulated in relation to forming a DBA scheme:

1. **A staircase approach should be used in a DBA scheme;**
2. **The cut-off frequency for Initiating Events within the DBA region of the scheme should be 1 E-5 per year;**
3. **The cut-off consequence within the DBA region of the scheme should be 1mSv for public and 20mSv for workers;**
4. **The adoption of a Low Consequence Methodology for areas below the DBA region cut-off consequence should be considered;**
5. **Where there is a range of high and low consequence hazards and range of frequencies, the adoption of at least two DBA regions with a sound basis should be considered within the DBA scheme;**
6. **Where the consequence or initiating frequency of hazards are close to the boundary of a higher region within the scheme, the confidence levels of the inputs should be examined, and where there is significant uncertainty, consideration should be given to moving to the higher region;**
7. **For areas outside of the DBA region, consideration should be given to provide less restrictive guidelines on protection, rather than no guidelines, as part of the overall DBA scheme;**
8. **The DBA regions, when used to provide quantitative targets for safety measures, should have appropriate guidance to ensure that the safety measures when combined with the initiating event frequencies will lead to a mitigated risk outside of the DBA region.**
9. **The DBA regions, when used to provide quantitative targets for safety measures, should be derived on a sound basis, taking into account the target safety measure pfd and an overall fault sequence frequency target based on the potential accumulation of numerous fault sequences.**
10. **The DBA regions and guidance, when used to provide quantitative targets for safety measures, should always be treated as guidance to inform ALARP, rather than mandatory design requirements for the number of safety measures and associated pfd targets.**

# Glossary

|  |  |
| --- | --- |
| **Term** | **Definition** |
| ALARP | As Low As Reasonably Practicable |
| BEIS | Business, Energy and Industrial Strategy (Department of) |
| BSL | Basic Safety Level |
| BSO | Basic Safety Objective |
| DB | Design Basis |
| DBA | Design Basis Assessment |
| EHSQS&S  | Environment, Health, Safety, Quality Safeguards and Security  |
| FST | Fault Sequence Terminated |
| HEART | Human Error Assessment and Reduction Technique |
| HEP | Human Error Probability |
| IEF | Initiating Event Frequency |
| LCM | Low Consequence Methodology |
| mSv | Milli Sievert |
| NORMS | National Objectives, Requirements and Model Standards  |
| ONR | Office of Nuclear Regulation |
| PbD | Precluded by Design |
| Pfd | Probability of failure on demand |
| PSA | Probabilistic Safety Assessment |
| SAPs | Safety Assessment Principles |
| SDF | Safety Directors Forum |
| SILs | Safety Integrity Levels |
| SQEP | Suitably Qualified and Experienced Person |
| SSC | Structures, Systems and Components |
| THERP | Technique for Human Error Rate Prediction |

# References

|  |  |
| --- | --- |
|  | **Title** |
| 1.
 | UK Nuclear Industry Safety Case Forum Guide: Appropriate Conservatism in Safety Cases, Issue 2, March 2020.Available on the Nuclear Institutes Website. |

# Appendix A: ONR SAPs Target 4 Guidance

The ONR SAPs 2014 Edition (Rev 0) (<http://www.onr.org.uk/saps/index.htm>) provide a definition of where DBA should be carried out as a guide to their assessors. This is derived against Target 4 (Para 726 to 727) and the derivation explained within Annex 2 of the SAPs (A27 to A34) which is reproduced in this Appendix (edited only for reading standalone).

The numerical targets for DBA represent criteria for assessing the safety of the facility’s design and operations for faults that could have significant consequences. They are based on initiating fault frequencies and so take no account of the reliability of the claimed safety measures. Instead, they place the focus on the effectiveness of the safety measures in addressing the fault’s consequences (effective dose). The BSOs are set at levels where the consequences will be broadly acceptable, given the likelihood of the initiating fault. Consequences at these low levels will normally only be achievable through installation of appropriately engineered safety measures rather than mitigating systems. The DBA should demonstrate that adequate robust safety measures are in place, including the presence of at least one intact barrier at sequence termination.

For ‘frequent’ faults (i.e. those with an initiating fault frequency exceeding 1 x 10-3 pa) the BSLs are set at the legal limits for normal operational exposures, though they are not legal limits in this case. For less frequent faults, higher fault consequences are likely to be consistent with the requirement to reduce risks to ALARP (other numerical targets notwithstanding) leading to the stepped relationship shown schematically in Figure 2.



Figure 2: ONR SAPs Target 4 DBA Scheme

Annex 2 (A27 to A34) guidance on Target 4:

DBA is a rigorous and demanding method of fault analysis aimed at providing a robust demonstration of the fault tolerance of a facility. Consequently, Target 4 has been set to ensure that DBA is applied in all cases where significant consequences could arise with reasonable likelihood. The target was included in the 2006 SAPs to quantify the qualitative criteria set by Principle P25 in the 1992 SAPs. The target is intended to engender a targeted and proportionate approach in which this type of fault analysis is focussed on fault sequences making a significant contribution to overall risks.

In this approach, faults selected for DBA are chosen on the basis of their initiating fault frequency (IFF) and potential unmitigated radiological consequences as shown in Figure 2. This figure has been derived as follows: following the approach adopted in the 1992 SAPs, only faults with IFF greater than 1 x 10-5 pa should be considered for DBA. This defines the lowermost section of the boundary of the DBA Region. Furthermore, 1992 SAP P25(b) indicates that doses off the site of up to 100 mSv may be allowable in “severe” design basis fault sequences. Hence, faults with the lowest IFFs whose potential consequences are less than 100 mSv are excluded. This defines the lowest portion of the left-hand boundary of the DBA Region. The 100 mSv dose level was chosen so that the analysis would address any initiating fault that might be expected to lead to an evacuation away from the immediate vicinity of the site, taking into account the conservatism of the analysis. Appendix 2 paragraph 1 of the 1992 SAPs and the textbox following paragraph 751 provide further details of the likely consequences of off-site radiological releases.

For doses on the site, 1992 SAP P25(c) states that there should be no "excessive dose" following any design basis fault sequence. This was interpreted in the 2006 SAPs to equate to a dose of 500 mSv, since observable deterministic symptoms from accidental exposures to radiation are considered unacceptable following a design basis fault. This defines the lowest portion of the left-hand boundary of the DBA Region for doses on the site.

For more frequent faults (i.e. those with a reasonable probability of occurrence during the lifetime of the facility), it is considered unacceptable for design basis protective safety measures not to be provided for faults capable of exceeding the corresponding BSLs of 1mSv pa (off the site) or 20mSv pa (on the site) in Targets 1 and 3. The IFF for such faults has been set at 1 x 10-3 pa based on long-standing DBA practices established for UK power reactors. This defines the upper portion of the left-hand boundary of the DBA Region in Figure 2.

The remaining portion of the DBA Region boundary has been derived based on a broadly logarithmic interpolation between the limiting cases described above, in order to engender a proportionate approach. Target 4 is intended to provide a broad indication of where DBA might be expected to be applied and is not intended to be a rigid rule: duty holders are expected to develop their own methods for defining the scope of DBA tailored to their specific circumstances. Target 4 is however provided as a generic starting point for ONR inspectors, particularly where there is no well-established licensee guidance.

This definition of where DBA should be applied is not intended to imply that safety measures are not needed elsewhere. Initiating faults with consequences below the BSL still require consideration of possible safety measures and the application of relevant good practice to ensure risks are reduced to ALARP. The identification and design of these safety measures should be informed through application of PSA and Severe Accident Analysis (SAA) and the risks compared with Targets 5 to 9.

The second purpose of Target 4 is to define success criteria (i.e. performance requirements) for the design basis safety measures. These are set in terms of the residual dose consequences from the faults assuming successful operation of the safety measures. In keeping with the preference for safety measures that fully protect against, or terminate fault sequences in their early stages, the BSOs have been set at a level comparable with the BSOs for operational doses in Targets 1 and 3. In cases where it is not reasonably practicable to provide safety measures protecting to these levels, the DBA should demonstrate suitable safety measures are nevertheless in place to reduce (i.e. mitigate) potential doses to levels below the relevant Target 4 BSLs. The logic for this is as follows: any fault in the DBA Region whose mitigated consequences cannot be reduced below the BSLs would then constitute a further DBA initiating fault in its own right. However, this fault would be unprotected. Hence Target 4 defines where ONR expects to see DBA applied; the success criteria for DBA safety measures; and a region where inspectors should explore the reasonable practicability of providing protective safety measures rather than mitigating ones.

# Appendix B: Example DBA Schemes



Figure 3: DBA Scheme A

DBA Scheme A is based on Target 4. The only difference being that a factor of 10 has been applied to the public risk, to account for off-site consequences which are usually only calculated once using best estimate assessment.



Figure 4: DBA Scheme B

DBA Scheme B introduces the concept of two DBA regions. This provides full coverage of Target 4 in terms of the overall DBA region. However, it introduces more specific guidance on the number of safety measures, including for regions below Target 4:

1. Region II: Full DBA requirements should be satisfied. That is, there should be sufficient independent safety measures to ensure that, even with equipment outages for maintenance/inspection/testing and with a single unrevealed failure in the safety measures, there will still be at least one safety measure to prevent excessive consequences.
2. Region I: DBA requirements should be satisfied except that compliance with the single failure criterion is not necessary. That is, there should be sufficient independent safety measures to ensure that, even with equipment outages for maintenance/inspection /testing, there will still be at least one safety measure to prevent excessive consequences. Where the initiating event frequency, and the associated consequences, are both within an order of magnitude of the boundary between Regions I and II, particular consideration should be given as to whether it is reasonably practicable to increase the level of provisions from that specified by Region I to that specified by Region II.
3. Region 0: There are no DBA-specific requirements for safety measures.

1

1

10

-1

**DB2**

10

-1

10

-2

**LC**

10

-2

**LC**

**DB2**

10

-3

10

-3

10

-4

**DB1**

10

-4

10

-5

10

-5

**DB1**

-6

10

**DB0**

10

-6

0.001

0.01

0.1

1

10

100

0.02

0.2

2

20

200

1000

**Public/Offsite**

**Unmitigated Fault Sequence Frequency (/yr)**

**Unmitigated Consequence (mSv)**

**Worker/Onsite**

**Unmitigated Fault Sequence Frequency (/yr)**

**Unmitigated Consequence (mSv)**

Figure 5: DBA Scheme C

DBA Scheme C is intended for decommissioning activities, not for operational power stations.

Design Basis Scheme C has two DBA regions, but also introduces the concept of formally having a Low Consequence Methodology (LCM) region. The LCM region recognises that attention is still required for low consequence but high frequency events.

The Scheme specifically uses the ‘unmitigated fault sequence frequency’ rather than ‘IEF’. The dose used is defined as ‘unmitigated and conservative’ with the degree of conservatism identified as ‘not bounding’

This is accompanied by the guidance on the protection required in each region specifically identified in functionality:

1. Region II: Combined protection equivalent to two DB1 safety measures comprised from electrical, mechanical, administrative or containment protection. A single mechanical device or containment device can be acceptable if meets substantial robust functional requirements or two independent electrical channels, both independent of the control system.
2. Region I: A mechanical or containment device that meets robust functional requirements, one electrical channel, independent of the control system; or Written operating instruction meeting the specific requirements.
3. LCM: A mechanical or containment device that meets nominal functional requirements, One independent line of logic in the control system; or operator response to alarms/warnings.
4. Region 0: There are no DBA-specific requirements for safety measures.



Figure 6: DBA Scheme D

DBA Scheme D has two regions, the formal DBA region as Target 4 and DB2 regions on other schemes, termed the Safety Function A area. The second region is similar in intention to the DB1 region and LCM regions, but covers a wider range of consequences and frequency. The following guidelines apply:

1. **DBA2 Regions -** At least two independent Required Safety Measures shall deliver the overall pfd (unless an argument is being made that the hazard is Precluded by Design (PbD)/Fault Sequence Terminated (FST) by a passive feature), where:
	1. An individual Required Safety Measure is independent if its ability to perform its required function is unaffected by:
		1. the operation or failure of other equipment, and by
		2. the presence of the effects resulting from the relevant Initiating Event.

This essentially means that no single-point failure could lead to failure of more than one independent Safety Measure for the Initiating Event to which the Safety Measures apply.

* 1. Each Required Safety Measure must be capable, on its own, of either:
		1. preventing a dose from the Initiating Event. or,
		2. reducing the potential dose to a level below the DBA BSO (or, if this is not reasonably practicable, as far below the relevant DBA BSL for the Initiating Event as is reasonably practicable).
1. **Region B** - When appropriate for an exposed group, a Safety System is required which has an overall pfd that ensures fault sequence frequencies are acceptably low, when judged against the Fault Sequence Frequency Criteria. When appropriate, a single Required Safety Measure – satisfying the above independence and consequence reduction criteria and delivering the required overall pfd – shall be provided to ensure fault sequence frequencies are acceptably low, when judged against the Fault Sequence Frequency Criteria.



Figure 7: DBA Scheme E

DBA Scheme E introduces the concept of three DBA regions. This provides full coverage of Target 4 in terms of the overall DBA region. However, it introduces more specific guidance on the number of safety measures, including for regions below Target 4. This includes for the public scheme a DB1+ region. The following guidelines apply:

1. DB2 requires at least two independent Safety Measures to be available during any normally permissible state of plant operation;
2. DB1 requires at least one Safety Measure;
3. DB1+ (public only) requires one Safety Measure as a minimum, with specific consideration of the practicability of satisfying DB2.



Figure 8: DBA Scheme F

DBA Scheme F introduces the concept of four DBA regions. This provides full coverage of Target 4 in terms of the overall DBA region. However, it introduces more specific guidance on the number of safety measures, including for regions below Target 4. This includes for the public scheme a DB1+ region and a DB2+ region. The following guidelines apply:

1. DB2 requires at least two independent Safety Measures to be available during any normally permissible state of plant operation;
2. DB1 requires at least one Safety Measure;
3. DB2+ requires two Safety Measures of higher reliability (10-4/yr rather than 10-3/yr, with specific consideration of the practicability of providing three safety measures;
4. DB1+ requires one Safety Measure of higher reliability, with specific consideration of the practicability of satisfying DB2;
5. For the public, the boundary is shown beyond 10-5 per year, however below this frequency a protective safety measure may be expected, but it does not have to be justified conservatively.