Received by OSTI
SEP 18 1989

Evaluation of Allowed Outage Times (AOTs) From a Risk and Reliability Standpoint

DO NOT MICROFILM
COVER

Prepared by W. E. Vesely

Science Applications International Corporation

Brookhaven National Laboratory

Prepared for
U.S. Nuclear Regulatory
Commission

AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 2120 L Street, NW, Lower Level, Washington, DC 20555
2. The Superintendent of Documents, U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20013-7082
3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC Office of Inspection and Enforcement bulletins, circulars, information notices, inspection and investigation notices; Licensee Event Reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG series reports and technical reports prepared by other federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal and periodical articles, and transactions. *Federal Register* notices, federal and state legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Office of Information Resources Management, Distribution Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, and are available there for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

DISCLAIMER NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability of responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

NUREG/CR-5425
BNL-NUREG-52213
RG, RX

Evaluation of Allowed Outage Times (AOTs) From a Risk and Reliability Standpoint

NUREG/CR--5425

TI89 017669

Manuscript Completed: July 1989
Date Published: August 1989

Prepared by
W. E. Vesely

Science Applications International Corporation
2941 Kenny Road, Suite 245
Columbus, OH 43221

Under Contract to:
Brookhaven National Laboratory
Upton, NY 11973

Prepared for
Division of Systems Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555
NRC FIN A3230

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

MASTER

EB

ABSTRACT

This report describes the basic risks associated with allowed outage times (AOTs), defines strategies for selecting the risks to be quantified, and describes how the risks can be quantified. This report provides a basis for risk-based approaches for regulatory and plant implementation. The AOT risk evaluations can be applied to proposed one-time AOT changes, or to permanent changes. The evaluations can also be used to quantify risks associated with present AOTs, and in establishing AOTs from a risk perspective.

The report shows that the standard way of calculating AOT risks in probabilistic risk analyses (PRAs) generally is not sufficient when evaluating all the risks associated with an AOT in order to assess its acceptability. The PRA calculates an average AOT risk which includes the frequency at which the AOT is expected to occur. Other risks associated with an AOT include the single downtime risk, which is the risk incurred when (given) the AOT has occurred. The single downtime risk is generally the most applicable risk in determining the acceptability of the AOT. The single downtime risks are generally much larger than the PRA-averaged risk. For more comprehensive evaluations, both risks should be calculated. The report also describes other risks which can be considered, including personnel and economic risks. Finally, the report discusses the detailed evaluations which are involved in calculating AOT risks, including considerations of uncertainty.

EXECUTIVE SUMMARY

This report describes the basic risks associated with allowed outage times (AOTs), defines strategies for selecting the risks to be quantified, and describes how the risks can be quantified. This report provides a basis for risk-based approaches for regulatory and plant implementation. The AOT risk evaluations can be applied to proposed one-time AOT changes, or to permanent changes. The evaluations can also be used to quantify risks associated with present AOTs, and in establishing AOTs from a risk perspective.

The report shows that the standard way of calculating AOT risks in probabilistic risk analyses (PRAs) generally is not sufficient when evaluating all the risks associated with an AOT in order to assess its acceptability. The PRA calculates an average AOT risk which includes the frequency at which the AOT is expected to occur. Other risks associated with an AOT include the single downtime risk, which is the risk incurred when (given) the AOT has occurred. The single downtime risk is generally the most applicable risk in determining the acceptability of the AOT. The single downtime risks are generally much larger than the PRA-averaged risk. For more comprehensive evaluations, both risks should be calculated. The report also describes other risks which can be considered, including personnel and economic risks.

AOT risks can be calculated at various "levels", namely the component level, the system level, the safety function level, the accident sequence level, the core-melt frequency level, and the overall risk (accident frequency times consequence) level. The report discusses the various technical issues involved in calculating the AOT risks at a given level, and describes the associated resource requirements. As the report indicates, it is generally best to calculate the risks at the safety function level or higher if system interactions are to be comprehensively treated.

The report also describes the proper ways that risks from multiple AOTs should be considered, so that risks are properly accumulated from proposed multiple AOT changes, but are not counted twice. Generally, average AOT risks which include the frequency of occurrence of the AOT need to be accumulated but single downtime risks do not since they apply to individual AOTs. Criteria considerations in determining the acceptability of calculated AOT risks are described, and the merits of relative risk criteria versus absolute risk criteria are discussed. Finally, the report discusses the detailed evaluations which are involved in calculating AOT risks, including considerations of uncertainty.

CONTENTS

	<u>Page</u>
ABSTRACT	iii
EXECUTIVE SUMMARY	v
LIST OF FIGURES	viii
LIST OF TABLES	ix
FOREWORD	xi
 1. OVERVIEW OF THE GENERAL AOT PROBLEM	 1
1.1 Introduction	1
1.2 Definition of Allowed Outage Times	1
1.3 Identifying the Various Risks Associated with AOTs	2
1.4 Possible Regulatory Approaches for AOT Determinations	2
1.5 Criteria for Controlling AOT Risks	4
1.6 Generic Versus Plant Specific Evaluations	5
1.7 Types of Analyses Used in the Evaluations	5
1.8 The Role of Reliability Assurance	5
 2. STRATEGIES FOR ADDRESSING THE VARIOUS AOT RISKS	 7
2.1 Introduction	7
2.2 Single Risk Problems	7
2.3 Problems of Multiple Risk Considerations	10
 3. THE LEVELS AT WHICH AOT RISKS CAN BE CONTROLLED	 13
 4. CRITERIA CONSIDERATIONS FOR DETERMINING THE ACCEPTABILITY OF AOT RISKS	 17
 5. MEASURES FOR QUANTIFYING AOT OPERATING ACCIDENT RISK	 23
5.1 Introduction	23
5.2 Risk Measures at the System Level	25
 6. SUMMARY AND CONCLUSIONS	 33
 REFERENCES	 35
 APPENDIX A. MEASURES FOR QUANTIFYING AOT OPERATING ACCIDENT RISK AT DIFFERENT RISK LEVELS (COMPONENT, FUNCTION, ACCIDENT SEQUENCE AND OVERALL RISK LEVEL).	 A-1
 APPENDIX B. THE AVERAGE DOWNTIME FOR A GIVEN SPECIFIED AOT	 B-1
 APPENDIX C. THE DISTRIBUTION OF CUMULATIVE DOWNTIME	 C-1
 APPENDIX D. CONSIDERATION OF THE CUMULATIVE RISKS FROM MULTIPLE AOTS	 D-1
 APPENDIX E. CRITERIA CONSIDERATIONS WHEN THE COMPONENT APPEARS IN MULTIPLE SYSTEMS	 E-1

LIST OF FIGURES

<u>Figure</u>		<u>Page</u>
1.	Decision Process for Evaluating AOTs	12
2.	A Stepwise Level Process for Deciding if Accident Risk is Significant	16

LIST OF TABLES

<u>Table</u>	<u>Page</u>
1. Risks Associated With AOTS	3
2. Sources of Risk Information and Problem Areas	3
3. Possible Regulatory Approaches for AOT Determinations	4
4. Criteria and Risk Control Alternatives	5
5. Advantages and Disadvantages of Strategies	8
6. Cases in which the Operating Accident Risk is the Pivotal Risk	9
7. Levels at Which AOT Accident Operating Risk Can Be Evaluated and Controlled	13
8. The Chain of Control Connecting the Different Levels at Which Risk May Be Addressed	14
9. Criteria Considerations at the Component Level	18
10. Criteria Considerations at the System Level	18
11. Criteria Considerations at the Function Level	19
12. Criteria Considerations at the Sequence Level	19
13. Criteria Considerations at the Overall Risk Level	20
14. Implementation Considerations for Absolute Criteria	20
15. Implementation Considerations for Relative Criteria	21
16. Considerations for Direct Implementation of Criteria	22
17. Considerations for Indirect Implementation of Criteria	22
18. Controls at the System Level	32
A.1. Controls at the Component Level	A-3
A.2. Controls at the Function Level	A-6
A.3. Controls at the Sequence Level	A-9
A.4. Controls at the Overall Risk Level	A-11

FOREWORD

This report is prepared as part of a research project on Procedures for Evaluating Technical Specifications (PETS) Program. The objective has been to develop and demonstrate methods to utilize risk and reliability techniques in evaluating the scope, detailed requirements, and safety impact of plant technical specifications. This report was originally published as BNL Technical Report A-3230 6-28-85, in June 1985. This is a revised version of that report, now being published as a NUREG/CR in order to achieve wider distribution.

1. OVERVIEW OF THE GENERAL AOT PROBLEM

1.1 Introduction

Standard Technical Specifications (STSs) presently define allowed outage times (AOTs) for all the major components in safety systems. The goal of this work is to develop risk and reliability guidelines for evaluating the acceptability of:

1. existing AOTs, and
2. proposed modifications to the existing AOTs.

In evaluating acceptability, some or all the risks associated with AOTs may need to be addressed:

1. Operating Accident Risks,
2. Shutdown Accident Risks,
3. Shutdown Economic Risks, and
4. Occupational Radiation Risks

Operating accident risks are specifically examined and conditions are identified in which it is sufficient to address only these risks. Specific strategies and criteria are also described for determining acceptable AOTs.

Van Otterloo¹, White and Cross², Jacobs³, and Mankamo⁴ were among the earliest authors to address aspects of rising risk analyses to determine acceptable AOTs. This document attempts to treat all the different contributions to operating risk which are associated with an AOT (or AOTs) and to describe various approaches which can be used to control different risks.

1.2 Definition of Allowed Outage Times

The AOTs are part of the limiting conditions for operation (LCOs) for the plant. The AOT for a component is the period of time during plant operation during which the component can be inoperable. The component may be inoperable because it has failed and is under repair; the AOT then is termed the unscheduled AOT. The component may also be inoperable because the component is taken out of service for scheduled testing or maintenance; then AOT the is termed the scheduled AOT.

During the AOT, the probability of an accident occurring is generally higher because of the component being down. If the AOT is exceeded, the plant generally must be brought to a shutdown state. The plant can request an extension to an AOT; however, requests are evaluated on a case-by-case basis. In the past, the establishment of AOTs and determination of AOT extensions have not been founded on systematic reliability and risk considerations. The objective of this work is to develop approaches, strategies, and criteria which can be used in evaluating AOTs on such bases.

1.3 Identifying the Various Risks Associated with AOTs

The first step in placing AOTs and AOT extensions on a sound basis is to identify the various risks associated with AOTs. Table 1 lists these risks and defines them. All these risks are additional risks in that they occur when the component goes down and would not be incurred otherwise.

Various strategies can be used to control and minimize AOT risks. Table 2 gives the availability of models and information for evaluating each type of risk and also gives special problem areas in its evaluation. The availability of information needs to be taken into account in developing AOT strategies based on calculation and assessment of the risk.

Table 2 shows that operating accident risks can be evaluated from models available from existing PRAs. Shutdown accident risks can be evaluated by extending current PRAs; current PRAs, however, do not generally address shutdown risks. Shutdown economic risks could be obtained from available models and computer codes which evaluate shutdown costs, although such applications have been plant-specific and, hence, limited.

Finally, occupational exposures could be evaluated from plant records and plant specific studies; however, no general models exist. It is important to note that all these risks do not need to be evaluated. Which risks are evaluated will depend upon the AOT strategy used in determining acceptable AOTs; the possible strategies and their rationale will be discussed later.

1.4 Possible Regulatory Approaches for AOT Determinations

Table 3 defines the regulatory approaches which can be used in determining AOTs. In the first approach, AOT values are specified for components or categories of components; this is the approach used now, though its basis is not clear. In the second approach, procedures and criteria are specified for determining AOTs using generic or plant specific models. In the third approach, only the criteria are specified, with the procedures for the analyses selected by the applicant.

Each of these general approaches in Table 3 can be varied. For example, as a variant of Approach 1, AOT values can be specified as a function of various design and operating characteristics. For Approach 2, the criteria which determine acceptance AOT values can be quite specific and quantitative, or can be qualitative. In Approach 3, the procedures for evaluating AOTs can be quite prescriptive or can be rather general.

The regulatory approaches in Table 3 also apply for determining acceptable AOT extensions. In the first, acceptable AOT extensions would be given. In the second, procedures and criteria for determining acceptable AOT extensions would be given. In the third, only criteria for acceptable AOT extensions would be given. The advantages and disadvantages in Table 3 apply to AOT extensions.

Table 1. Risks Associated With AOTS

1. Operating Accident Risks	Additional public risks from accidents incurred while the plant is operating and the component is down
2. Shutdown Accident Risks	Additional public risks from accidents incurred when AOT is violated and the plant is shut down
3. Shutdown Economic Risks	Additional economic losses incurred because the plant has to be shut down when the AOT is violated
4. Occupational Radiation Risks	Additional radiation risks incurred by personnel having to repair the component

Table 2. Sources of Risk Information and Problem Areas

<u>Risk</u>	<u>Information Sources</u>	<u>Problem Areas</u>
1. Operating Accident	PRA, Reliability Analyses	PRA Uncertainties
2. Shutdown Accident	Potentially from PRAs	PRAs have not generally analyzed this risk
3. Shutdown Economic Risks	Nuclear plant outage modeling by ANL, EPRI, and utilities	Plant specific, no general applicable models
4. Radiation Occupational Risks	AIF study, plant records	No general applicable models

Table 3. Possible Regulatory Approaches for AOT Determinations

<u>Approach</u>	<u>Advantages</u>	<u>Disadvantages</u>
1. AOT values specified	Simplest and most efficient for regulation	Requires substantial analyses to have a foundation; can be overly prescriptive
2. AOT analysis approaches and criteria specified	Intermediate regulatory effort needed, yet allows some flexibility in evaluation	Requires justifiable analysis approaches; approaches can be constraining
3. AOT criteria specified	Most flexibility allowed in evaluation	Requires the most regulatory effort; approaches need to be checked on a case-by-case basis

1.5 Criteria for Controlling AOT Risks

Table 4 gives the various general criteria and risk control alternatives which can be used in any of the regulatory approaches identified. The level at which control is focused is the level at which risk is explicitly controlled. The ultimate goal in any strategy is to control all the various risks associated with AOTs, but the controls can be explicitly placed at different levels, from the level of the lowest component to top overall risk which incorporates considerations of both accident occurrence and consequence.

There are different risks associated with AOTs and there are two general methods which can be used to control these risks, (a) by controlling an overall risk index which aggregates or integrates the constituent risks, or (b) by controlling the individual risks themselves. The aggregated approach includes the cost-benefit approach.

Finally, the scale on which risk is controlled can either be a relative scale or absolute scale. On an absolute scale, AOT risks are controlled to some absolute criterion. On a relative scale, AOT risks are controlled with regard to some other reference risk.

Table 4. Criteria and Risk Control Alternatives

1. Method of addressing the different AOT risks:	Aggregated Risk Index	Individual Risk Measures
2. Level at which control is focused:	Component/System/Function	Sequence/Overall Risk
3. Scale for risk control:	Absolute	Relative

1.6 Generic Versus Plant Specific Evaluations

AOT risks and their regulation can be approached and evaluated from either a generic or plant specific basis. The regulatory approaches are generally simpler to implement if standard generic models can be specified which cover categories of plants. However, the generic models need to be validated that they represent or bound the individual plants covered.

Consideration must be given to the use of plant specific models and plant specific data where they exist. The plant specific evaluations can customize the AOTs to the individual plant's designs and operations; the resulting AOTs will control risks but allow more flexibility in the plant's operations.

1.7 Types of Analyses Used in the Evaluations

Various types of analyses can be used to evaluate AOT in any strategy encompassing quantitative and qualitative analyses and encompassing deterministic and probabilistic analyses. PRA and reliability analyses are particularly suited to quantifying the accident risks and reliabilities associated with AOTs; time-independent analyses, time-dependent analyses, Markov analyses, and other quantitative techniques address particular problems.

Quantitative PRA and reliability analyses must be supplemented by operations, engineering, and economy considerations. The degree to which these other various considerations enter will depend on the particular approach and strategy.

1.8 The Role of Reliability Assurance

In approaches to determine AOTs, the conclusions have to be based on assumptions and models used to evaluate the various risks. Therefore, the role of reliability assurance programs in assuring the validity of these assumptions and models must be considered.

The role of the reliability assurance programs of the licensee can be particularly important when system reliability and effectiveness of repair significantly impact acceptable values of AOTs. Where effective reliability assurance programs are in place, more flexible AOTs may be allowed because of the greater reliability or effectiveness of repair which can be assumed. The monitoring of component reliability behavior and repair performance can also be important in assuring that degradations in performance are signaled and corrected before significant increases in risk are incurred.

2. STRATEGIES FOR ADDRESSING THE VARIOUS AOT RISKS

2.1 Introduction

There are two basic methods for addressing the various AOT risks:

1. address different risks individually, and
2. address the risks as an aggregate

In the former method, the risks are separately evaluated for their acceptability, and they are then individually and simultaneously controlled. If certain risks are assessed to be dominant, then only those are evaluated in detail and focused upon for control.

In addressing the risks as an aggregate, the risks are combined in some overall index, which is controlled. Cost-benefit analysis is one example of an aggregate control strategy, where the risks are translated to equivalent dollars, and the sum or net dollars is the focus of control. As another example of an aggregate approach, individual risks can be multiplied by individual importance weightings and the weighted sum of the risks controlled.

Table 5 shows the advantages and disadvantages of the two strategies. Controlling individual risks is more direct and involves more straightforward evaluations, since the risks do not have to be translated to a common scale. For example, if all risks are translated to equivalent dollars, then decisions may need to be made on the dollar value of life. An advantage of controlling aggregate risks is that an explicit balancing and trade-off among the risks is explicitly shown. However, the aggregate risk index may have little discriminating power and be insensitive to AOT changes.

The strategy which is more effective in practice depends upon the particular AOT problem, and the availability of models and data for the evaluations. However, general guidelines can be given in determining the most effective strategy to use. All the AOT problems can be divided into two types, where one AOT risk need only be considered, and where several AOT risks are dominant. The first decision to make is which type of problem is being addressed.

2.2 Single Risk Problems

In certain problems, the assessments can focus on one pivotal AOT risks. This single risk will, in general, be the operating accident risk associated with AOTs. The problems for which the operating accident risk can be focused upon are:

1. Where the accident operating risk associated with an AOT is clearly unacceptable by itself.
2. Where an AOT allows adequate repair to be performed and results in insignificant accident operating risks.

Table 5. Advantages and Disadvantages of Strategies

Controlling Individual Risks

<u>Advantages</u>	<u>Disadvantages</u>
1. More direct explicit control of the risks is performed	1. Establishing criteria on different risks can be difficult
2. More straightforward evaluations of the risks are performed	2. Balance of risks is not explicitly done

Controlling an Aggregate Risk

<u>Advantages</u>	<u>Disadvantages</u>
1. Direct balancing of the risks is performed	1. Requires conversion constants or weights to place all risks on same scale
2. Tradeoffs among the risks are more directly shown	2. The aggregate risk index can be insensitive to AOT changes; establishing a criterion on the aggregate risk can be difficult

3. Where an increase in an AOT results in insignificant associated accident risks and there is no significant occupational exposure associated with the AOT.
4. Where an increase in several AOTs results in insignificant operating accident risk associated with all the AOTs and there is no significant occupational exposure associated with the AOTs.

In all the cases, the dominant risk is the accident operating risk. The first two cases involve evaluation of AOTs themselves; the last two cases involve evaluation of AOT extensions. Table 6 summarizes situations when the accident operating risk is the dominant risk.

The rationale for these cases is as follows. In Case 1, when the operating accident risk is unacceptable compared to some guideline or goal, then the accident risk is a dominant consideration and must be reduced. This case assumes there are absolute or relative criteria or goals on what constitutes unacceptable accident risks. If there are no such criteria or goals, Case 1 does not apply.

Table 6. Cases in which the Operating Accident Risk is the Pivotal Risk

1. When the operating accident risks associated with an AOT is unacceptable by itself.
 2. When an AOT allows adequate repair and has insignificant associated accident operating risk.
 3. When an increase in an AOT gives insignificant operating risk and insignificant occupational exposure.
 4. When increases in multiple AOTs give insignificant cumulative accident operating risks and insignificant occupational exposure.
-

For Case 2, if an AOT allows essentially all repairs to be adequately performed and the operating accident risk is insignificant, then this is sufficient justification for not changing the AOT. Extending the AOT will not allow more repairs to be completed, and will increase the operating accident risk. On the other hand, if the AOT has insignificant operating accident risk, then it does not need to be decreased. Thus, the AOT represents an acceptable specification from the standpoints of risk and operations.

The reason that the operating accident risk is dominant for Case 3 is as follows. When an AOT is increased, the various risks associated with the AOT change:

1. operating accident risk increases,
2. shutdown accident risk decreases,
3. shutdown economic risk decreases, and
4. radiation occupational exposure may either increase, decrease, or remain unchanged.

The accident operating risk increases because the AOT increases. The shutdown accident and economic risks decrease because the likelihood of going to shutdown decreases with a longer AOT. Therefore, if the increase in the accident operating risk can be shown to be insignificant, then the total risk associated with the AOT will decrease or insignificantly change: this is sufficient to justify the AOT extension.

Since there is no reason simply to change AOTs if they are long enough to allow adequate repair, there must be justification in Case 3 to show that the present AOT is unacceptably short for adequate repair to be performed. (Note that Case 3 applies to both one-time AOT extensions and permanent AOT extensions.) For one-time extensions, the operating accident risk that needs to be

considered is the risk associated with the one extension. For a permanent extension, the operating accident risk that needs to be considered is the cumulative risk from all future projected downtime occurrences.

The rationale for Case 4 is similar to Case 2, except that multiple AOT extensions are considered. The risk that needs to be considered is the total or cumulative accident risk associated with all the AOT extension.

For the above cases, since the operating accident risk can be focused upon to assess the acceptability of the AOT, it is more direct and straightforward to deal with the risk itself. This means that the strategy of controlling the individual risk itself is more straightforward than controlling an overall aggregate index (the options previously given in Table 5). While this latter strategy can give the same results and conclusions, it can be encumbered by being concerned with risks which are not pertinent, or with conversions of risks to a common scale. With consistent conversions, however, the aggregate risk strategy will give the same results as the individual risk strategy.

2.3 Problems of Multiple Risk Considerations

Multiple AOT risks must be considered in the following cases:

1. When an AOT causes significant operating accident risks and decreasing the AOT significantly impacts the capability of repair being performed during the AOT.
2. When an increase in an AOT to allow adequate repair causes a significant increase in operating accident risk.
3. When an increase in several AOTs to allow adequate repair causes a significant increase in the cumulative operating accident risk.

In Case 1, decreasing the AOT results in the following changes in the various AOT risks:

1. operating accident risk decreases,
2. shutdown accident risk increases,
3. shutdown economic risk increases, and
4. occupational radiation risk can vary.

The shutdown accident and economic risks increase because the likelihood of going to shutdown increases with some repairs cannot be completed in the decreased AOT. If the increases in shutdown risks are assessed not to be significant or relevant, then the operating accident risk can be focused upon a single pivotal risk as discussed previously. If the increases in shutdown risk are significant, then they need to be compared with the decrease in operating accident risk. Furthermore, a possible increase in operating

accident risk, instead of a decrease, may need to be considered because downtimes may become more frequent due to the inadequacy of repairs in the shortened AOT.

Case 2 is the reverse of Case 1, in that an increase in AOT results in increased operating accident risk and decreased shutdown risks. If the increased operating accident risk is small, then the shutdown risks do not need to be considered as long as occupational risk is not significant. However, if the increased operating risk is significant, then the problem becomes a multiple risk consideration in which the increased operating risk must be compared to the decreased shutdown risks. Also, any occupational exposure must be considered.

Case 3 is similar to Case 2 except that multiple AOTs are increased, which lead to significant operating risk when the cumulative effective is considered. All three cases involve multiple risk considerations; there are other cases, but these are the more likely ones. All involve significant operating accident risks. When there are no significant operating accident risks associated with the AOT (or AOTs), then the problem can be treated as a single risk problem.

When significant operating accident risk occurs, then explicit tradeoffs among the different risks do not necessarily need to be performed. Instead, alternatives can be first examined to see if the operating accident risk can be decreased by means other than AOTs, such as increasing the availabilities of other components while the particular component is down. The availabilities may be increased by carrying out reliability assurance activities, installing more reliable components, providing additional redundancy, or by performing more frequent testing. Subsequent sections discuss these activities.

When different AOT risks are to be traded off, this can be done using an aggregate risk index or they can be individually evaluated. This problem is the multi-attribute or multi-criteria problem addressed in decision theory and there is no general solution to the problem. The solution which is most effective will depend on availability of information, the decision-maker's preferences, and the particular problem.

In conclusion, Figure 1 lays out a decision process which can be followed in deciding whether the operating accident risk can be focused upon or whether multiple risks need be considered. The decision process applies to an individual AOT or to multiple AOTs being evaluated; for the multiple AOTs, the accident risk is the cumulative risk. The figure does not show the case where the AOT has significant accident risk and also needs to be extended. However, this case simply follows the first YES-branch upward where alternatives for reducing the risk need to be identified or the risks need to be traded off.

Figure 1. Decision process for evaluating AOTs

3. THE LEVELS AT WHICH AOT RISKS CAN BE CONTROLLED

When an overall aggregate risk index is controlled, such as in a value-impact or cost-benefit analysis, there is little option as to the level at which risks are examined and explicitly controlled. In general, the risks evaluated are the overall risks, including the frequency of accidents and shutdowns and their consequences. More basic attributes can be focused upon but these need to be translated to equivalent overall risks to have a common scale of comparison.

If individual risks are focused upon, then there are more options for the levels at which the risks can be examined and controlled. The goal is still to control the overall risk, such as the overall frequency of core melt and accidents. However, the control can be implemented by controlling the lower-level contributors to risk, such as the unavailabilities of safety functions or safety systems.

In many single-risk problems the risk that needs to be examined to determine AOT acceptability is the operating accident risk associated with the AOT. Table 7 gives the levels at which the operating accident risk can be focused upon and the risk characteristics to be evaluated.

Table 7. Levels at Which AOT Accident Operating Risk
Can Be Evaluated and Controlled

<u>Level at Which Risk is Evaluated</u>	<u>Risk Characteristics Evaluated</u>
1. Overall risk	Accident frequency consequence
2. Core melt or damage	Core melt or damage frequency
3. Accident sequence	Accident sequence frequency
4. Function	Function unavailability
5. System	System unavailability
6. Component	Component unavailability

At the overall risk level, the accident frequency times consequence, or some other equivalent overall measure, is evaluated for acceptability. At the core melt or damage level, core-melt frequency is evaluated. The level of evaluation progresses to more basic contributors until, finally, component unavailability would be evaluated for acceptability. Unavailability characteristics include failure to start and failure to run. The particular measures which are used to quantify the risk characteristics are described later.

At a given level of control, criteria are established for the associated risk characteristic. For example, at the system level, criteria are defined as to what constitutes acceptable system unavailability associated with the AOT. The criteria can be flexible or quite prescriptive and can be absolute or relative. In general, for relative criteria, the particular contribution associated with the AOT is compared to the accident risk associated with other contributions. If absolute criteria are used, the particular risk associated with the AOT is compared to some absolute value. Specific criteria are discussed in the next section.

In principle, the AOT operating accident risk can be controlled at any of the levels identified in Table 7. Controlling the risk at one level controls all the risk at all higher levels. This chain relationship is shown in Table 8. The control may be initiated at any level on the left hand side of the arrows (the implication symbols) and will result in control of the overall risk. Control at lower levels must include consideration of system and component interactions. The core-melt frequency is the sum of the frequencies of the pertinent accident sequences.

Table 8. The Chain of Control Connecting the Different Levels at Which Risk May Be Addressed

In practice, the level at which the accident operating risk is controlled depends upon considerations of implementation. The higher the level at which risk is addressed, the more flexible will be the acceptable AOTs for components. For example, if criteria are established at an accident sequence level, then there would be various acceptable AOTs for the components comprising the function.

Another advantage of controlling risk at a higher level is that the acceptability criteria generally have to be less stringent. Bounding-case situations need to be considered at lower levels and logical relationships which may counterbalance the situation are not considered. For example, if a particular system enters into different accident sequences with different success definitions, the most stringent definition must be used if criteria at a system level are established. However, the sequence with the most stringent requirements on the system may also contain other reliable systems which diminish the risk contribution of the system and the AOT.

There are disadvantages to controlling risks at higher levels. The higher the level at which risk is controlled, the less specific and less prescriptive will be the acceptable AOTs, which makes it more difficult to review from a regulatory standpoint. Present technical specifications define specific AOT values for components.

Also, at higher levels the models and evaluations become more complex with greater associated uncertainties. Attempting to compensate for these uncertainties may offset the advantages of going to higher-level control.

In practice, the choice of the level at which risk is addressed is a compromise among the various advantages and disadvantages. Even with the unassociated conservatism, it is sufficient to evaluate risk at a low level if an adequate AOT is provided which allows effective repair to be performed, without causing significant risk. A longer AOT beyond that needed simply causes additional accident risk. If evaluating risk at a low level is not sufficient to allow an adequate AOT, then evaluating risk at a higher level may provide a larger AOT with adequate risk protection.

If a fixed level of risk evaluation proves to be inadequate in application, an adaptive risk level may be used where risk is evaluated only at the level and complexity needed. Figure 2 shows this adaptive type of decision process, starting from a system level evaluation; a component level evaluation could also be the starting point. If criteria do not exist at a level, then that level would be skipped.

Figure 2. A stepwise level process for deciding if accident risk is significant

4. CRITERIA CONSIDERATIONS FOR DETERMINING THE ACCEPTABILITY OF AOT RISKS

The level at which risk is evaluated influences the criteria used to control the AOT risks. Tables 9-13 list the considerations which enter in defining criteria at different levels. For the component, system, function, and sequence levels, the criteria would apply in defining the acceptable AOT operating accident risk. At the overall risk level, the criteria either apply to the operating accident risk or to the overall aggregated AOT risk. The criteria considerations apply to both AOTs and AOT extensions.

For any level of control, either absolute or relative criteria can be defined. An absolute criterion would specify an acceptable value for the AOT contribution to the risk characteristics being controlled. Equivalently, an acceptable value for the risk characteristic would be specified and a percentage of the acceptable value would be allocated to the AOT contribution.

A relative criterion at a given level would specify the acceptable contribution of the AOT risk compared to other contributions or compared to the total risk. For example, the AOT risk would be defined to be acceptable if it were less than some small percentage, such as 1 percent or 10 percent of the total risk.

For all levels except the component level, absolute or relative criteria can be applied to future projected risks from AOTs and to the risk while the component is down during a given AOT. The projected risk is the predicted risk which will occur in some future period from downtime occurrences if the AOT value is used. The projected risk accounts for the cumulative downtime which will occur in some period.

The risk while the component is down during the AOT is the immediate risk associated with a downed component. The risk is evaluated assuming (or given) the component is unavailable, with unavailability equal to 1. The unavailability of systems and functions containing the component is thus increased during the component downtime, as is the accident frequency and overall risk. Criteria and controls can be placed on these elevated values to limit their impacts. However, controls, cannot be placed on the elevated component unavailability since it is always 1.

The criteria can be implemented in a direct or indirect manner. When the criteria are implemented directly the applicant must show that their AOT or AOT extension satisfies the criteria. When the criteria are implemented indirectly, then AOTs are determined by regulations which satisfy given selected criteria, and are then given to the applicant in the technical specifications.

The question of whether to implement absolute or relative criteria directly or indirectly involves various practical considerations, that are listed in Tables 14 and 15. A bad feature of relative criteria is that good plants can be penalized. A plant with a higher risk will be granted larger AOTs than a plant with lower risk if the acceptability of AOT risk is measured

Table 9. Criteria Considerations at the Component Level

1. For absolute criteria, absolute values are required for an acceptable component unavailability associated with an AOT.
 2. For relative criteria, what constitutes a small or acceptable AOT contribution compared to the total component unavailability needs to be defined.
 3. The above criteria and controls can be placed on the risk associated with the AOT from future downtime occurrences. Since the component unavailability is 1.0 when the component is down during the AOT, controls cannot then be placed its the unavailability.
 4. For a component with different failure modes contributing to risk, the above criteria need to apply to each failure mode.
-

Table 10. Criteria Considerations at the System Level

1. For absolute criteria, absolute values are required for acceptable system unavailability from AOT contributions from the components in the system.
 2. For relative criteria, what constitutes a relative small or acceptable AOT system contribution needs to be defined.
 3. The above criteria and controls can be placed on both the unavailability from future downtime occurrences and the unavailability when the component is down during the AOT. The future unavailability can be the average or the time-dependent unavailability.
 4. When the system has different failure definitions (or equivalently, different success requirements) the above criteria need to apply to each of the definitions.
 5. When a component exists in different systems, the criteria for each of the systems need to be satisfied by the component AOT.
-

Table 11. Criteria Considerations at the Function Level

1. For absolute criteria, absolute values are required for acceptable safety function unavailability from AOT contributions from the components providing the function.
 2. For relative criteria, what constitutes a relative small or acceptable AOT function contribution needs to be defined.
 3. The above criteria and controls can be placed on both the unavailability from future downtime occurrences and on the unavailability when the component is down during the AOT. The future unavailability can be the average or the time-dependent unavailability.
 4. When a component is utilized for different functions, the criteria for each of the functions need to be satisfied by the component AOT.
-

Table 12. Criteria Considerations at the Sequence Level

1. For absolute criteria, absolute values are required for the acceptable accident sequence frequency contribution from the AOTs of the components in the sequence.
 2. For relative criteria, what constitutes a relative small or acceptable AOT contribution to the accident frequency needs to be defined.
 3. The above criteria and controls can be placed on both the accident frequency from future downtime occurrences and the frequency when the component is down during the AOT. The accident frequency can be the average or the time-dependent frequency.
 4. When a component exists in different accident sequences, the criteria for each of these sequences need to be satisfied by the component AOT.
-

Table 13. Criteria Considerations at the Overall Risk Level

1. For absolute criteria, absolute values are required for the acceptable overall risk index associated with AOT contributions from all the components.
 2. For relative criteria, what constitutes a relative small or acceptable AOT contribution to the overall risk index needs to be defined.
 3. The above criteria and controls can be placed on both the risk index considering future downtime occurrences and the risk index when the component is down during the AOT. The risk index can be the average or the time-dependent index.
 4. When a component contributes to different risk indices with associated criteria, then each of these criteria need to be satisfied by the component AOT.
-

Table 14. Implementation Considerations for Absolute Criteria

1. Safety goals could be used for core-melt frequency and early and latent risk (if these risk levels are used).
 2. Criteria for sequences, functions, and systems need to be separately established. An allocation of the safety goals is not absolutely necessary. Low criterion values could be selected to ensure low overall risks, and could still yield useable AOTs or AOT extensions.
 3. The contributions to include in the risk calculations need to be specified. The criteria may apply to only specific contributions, such as hardware, or may apply to all the contributions.
 4. The criteria may apply to the AOT risk itself or to the risk increase from the AOT, where the increase is measured against some reference risk. Evaluation of risk increases can simplify aspects of the analysis.
 5. In comparing to criteria, best estimate calculations are not necessarily sufficient. Bounding analyses ensure that the criteria are satisfied, even where there are deviations and uncertainties. If best-estimate evaluations are made, the criteria should be defined to allow tolerance to deviations or uncertainties.
-

Table 15. Implementation Considerations for Relative Criteria

1. Relative criteria can be straightforwardly specified which limit the contribution of AOT risk to a small percentage, e.g., 1-10 percent, of the total risk.
 2. Relative criteria can be defined for all levels, component through overall risk. The criteria can be implemented at a single level, or at optional multiple levels. For the latter, it would be sufficient to show that the AOT risk satisfied the criteria at any of the levels.
 3. The contributions to include in evaluating the reference risk with which AOT risk is compared, need to be specified.
 4. A bad feature of relative criteria is that low-risk plants can be given smaller AOTs than high-risk plants if the individual plant risk is used as a baseline. This feature can be removed by using a standard baseline for all plants.
 5. The relative risk criteria may apply to the AOT risk itself or to the risk increase from the AOT, where the increase is measured with regard to some reference or nominal risk value. Evaluation of risk increases can simplify certain aspects of the analysis.
 6. In comparing to criteria, best estimate calculations are not necessarily sufficient. Bounding analyses can be performed to ensure that the criteria are satisfied, even where deviations and uncertainties exist. If best estimate calculations are made, the criteria should be defined to allow tolerance to deviations and uncertainties.
-

relative to plant risk. This penalization will not be significant if plant risks do not significantly vary. To remove this feature, a standard or reference baseline can be used to compare the AOT risk.

Tables 16 and 17 list considerations for direct and indirect implementations. The question of what type of criteria to use does not necessarily involve an "either/or" decision, but can be selected based on the problem. Also, different criteria and approaches can be applied to the same problem to compare the conclusions and extract consistent results. For any of these implementations to be carried out, specific operating risks need to be evaluated and compared to the appropriate criteria. The next section discusses the specific measures and acceptable AOTs thereby determined.

Table 16. Considerations for Direct Implementation of Criteria

1. As part of the guidelines, the contributions to be addressed include model considerations, data considerations, and uncertainty considerations. The more specific and prescriptive the guidelines, the easier but less flexible the regulatory review will be.
 2. The guidelines need to address the use of generic models and generic data where no plant-specific information is readily available. Accommodations for plant-specific models and data likewise need to be described.
 3. The interfaces with plant reliability assurance programs need to be addressed. If reliability assurance programs are in place, certain conservative bounding assumptions in the risk evaluations may be lifted.
 4. The role of reliability monitoring needs to be addressed. Reliability behaviors which can significantly impact AOT risk and which need to be monitored should be identified.
-

Table 17. Considerations for Indirect Implementation of Criteria

1. The most obvious approach to indirect implementation is to use models and data to determine acceptable AOT values, or AOT extensions, which are then supplied to the utility.
 2. Acceptable AOTs can be tied to the risk importance of the component. Acceptable AOTs as a function of the risk importance of the component would be first determined. The utility would then determine the risk importance of the components according to described procedures, which would thereby determine the AOTs.
 3. Instead of tying AOTs to risk importance, the AOTs can be tied to other risk determinant characteristics of the component. Also instead of, or in addition to, defining an acceptable AOT for each occurrence, a total cumulative acceptable AOT for all downtime occurrences in some period may be defined.
 4. Accommodations for plant specific models and possible relaxations where reliability assurance programs are in place need to be addressed as does the role of reliability monitoring. These needs apply to direct or indirect criteria implementation.
-

5. MEASURES FOR QUANTIFYING AOT OPERATING ACCIDENT RISK

5.1 Introduction

Three general measures can be used to quantify the operating accident risk associated with an AOT:

f - the accident frequency when the component is down (1)

r - the risk incurred during a given downtime (2)

R - the risk incurred from accumulated downtimes (3)

At the sequence level, the accident frequency f is the (increased) accident sequence frequency when the component is down. At the function, system, and component level, the accident frequency is the (increased) function, system, or component unavailability, respectively, reflecting the increased accident sequence frequency.

The risk r during a downtime is the accident frequency multiplied by the period of component downtime. If the accident frequency is time dependent, then r is the integral of the frequency over the downtime. For a constant accident frequency (the usual case):

$$r = fd \quad (4)$$

where

d - the downtime of the component controlled by the AOT (5)

The accumulated risk R is the risk incurred from the accumulated downtimes in some time period. If D denotes the accumulated downtime of the component in some reference period T such as one year, then R can be expressed as

$$R = fD \quad (6)$$

Now D can be expressed as:

$$D = wTd \quad (7)$$

where,

w - the frequency of the downtime occurrences. Therefore, R can also be expressed as

$$R = wTfd \quad (8)$$

The quantity wT is the number of downtime occurrences in the period T .

For criteria which control the increase in operating accident risk, the corresponding measures of the difference in risk due to the component downtime are:

$$\Delta f = f - f_o \quad (9)$$

$$\Delta r = r - r_o \quad (10)$$

$$\Delta R = R - R_o \quad (11)$$

The quantities f_o , r_o , R_o are the baseline accident frequency, risk baseline during a downtime, and the baseline risk during the accumulated downtime, respectively.

The previous risk measures are all absolute risk measures. If criteria on relative risk are applied then relative risk measures are required; these are obtained simply by dividing the absolute measures by the reference risk value used for normalization. If superscript bars above the symbols denote relative values, then the relative risks are:

$$\bar{f} = \frac{f}{f_o} \quad (12)$$

$$\bar{r} = \frac{r}{r_o} \quad (13)$$

$$\bar{R} = \frac{R}{R_o} \quad (14)$$

The relative risk increases are:

$$\Delta \bar{f} = \frac{f - f_o}{f_o} \quad (15)$$

$$\Delta \bar{r} = \frac{r - r_o}{r_o} \quad (16)$$

and

$$\Delta \bar{R} = \frac{R - R_o}{R_o} \quad (17)$$

Although there appears to be many risk measures, there are only three basic ones (Eqns. (1-3)). The variations occur when differences in these risks are focused upon, or when relative values of these risks are of interest.

More specific considerations of these three basic risk measures depend upon the specific level at which risk is addressed. The following section discusses the measures and their interpretations at the system level. Detailed and similar development at the component, function, accident sequence, and the overall risk level are presented in Appendix A.

5.2 Risk Measures at the System Level

When the AOT operating accident risk is controlled at the system level, then the system unavailability impacted by the AOT is controlled. The systems focused upon are those containing the component whose downtime is to be controlled by the AOT. If the downed component is in several systems, then the unavailabilities of each of the systems needs to be controlled.

At the system level the AOT risk measures specialize to:

f - the (increased) system unavailability with the component down (18)

- Q^+ (19)

r - the (increased) system unavailability times the component downtime d (20)

- Q^+d (21)

R - the (increased) system unavailability times the accumulated downtime in some time period T (22)

- $DQ^+ = wTdQ^+$ (23)

The system measures which can be controlled are thus Q^+ , Q^+d , and wTQ^+d . (The superscript "+" on " Q^+ " denotes the increased unavailability.)

If a criterion is placed on the increased system unavailability, then

$Q^+ < \alpha_1$, (24)

where α_1 is the control value. The increased system unavailability is evaluated with the downed component unavailability set to unity. The increased system unavailability does not contain the component downtime as an explicit contribution, and hence the above control cannot be used to determine an acceptable AOT. This control, however, can identify where increased reliability assurance is necessary. If the increased system unavailability, Q^+ , is too high, it can be decreased by one of the following of activities:

1. Checking that other critical components are up before repair is begun on the downed component.
2. Where feasible, reconfiguring the system before the repair is begun (applicable to logic systems).

Control on the increased system unavailability thus can identify where reliability assurance activities are needed if the above criterion is violated. If feasible, the system may also be reconfigured to have higher unavailability during the downtime.

Instead of an absolute criterion on Q^+ , a relative criterion can be used:

$$\frac{Q^+ - Q}{Q} \leq \alpha_2 \quad (25)$$

where Q is the baseline system unavailability. This form limits the relative increase in the system unavailability to within an accepted tolerance region. For AOT extensions, Q can be the baseline (average) unavailability with either the original AOTs or the extended AOTs. If Q is evaluated with the extended AOTs, then it also must be checked to see if it has not unacceptably increased over the original Q .

The criterion placed on the second risk measure, the increased system unavailability times the component downtime, is

$$Q^+d \leq \beta_1 \quad (26)$$

where β_1 is the control value. To shed more light on the above criterion, and also the previous one on Q^+ , additional considerations are needed.

Consider an accident sequence containing the system with the downed component. Let

$$\psi = \text{the initiating event frequency of the sequence} \quad (27)$$

and,

$$Q_p = \text{the product of the unavailabilities of the other systems in the accident sequence not containing the downed component.} \quad (28)$$

The probability P^+ of the accident occurring during the period in which the component is down is:

$$P^+ = \psi Q_p Q^+d \quad (29)$$

Because of Q^+ , the probability P^+ is increased over the baseline accident probability in which the component is not given to be down. The nominal or baseline accident probabilities, Q_p , are usually derived from PRAs.

The increased probability P^+ can be compared to two baseline accident probabilities; the baseline accident probability during d , and the baseline accident probability during a reference period T such as a reactor year ($T=1$ year). The baseline accident probability P during the downtime d is:

$$P = \psi Q_p Qd \quad (30)$$

The baseline probability P_o during the period T is:

$$P_o = \psi Q_p Q T \quad (31)$$

The increased accident probability P^+ compared to P is:

$$\frac{P^+}{P} = \frac{Q^+}{Q} \quad (32)$$

The increased accident probability P^+ compared to P_o is:

$$\frac{P^+}{P_o} = \frac{Q^+ d}{Q T} \quad (33)$$

These two relations provide bases for controls not only on Q^+d , but also previously given for Q^+ . By controlling the first measure Q^+ via Eqn. (24) it is seen that the relative increase in accident probability during the downtime is controlled via the relationship in Eqn. (32). Since the probability is the accident frequency times the downtime, the increased accident sequence frequency during the downtime also is controlled.

By controlling the second measure Q^+d , via Eqn. (26) the increased accident probability during the downtime compared to the baseline probability over the reference period T is controlled via Eqn. (33). If $T=1$ year for example, then the increased probability is controlled with respect to the yearly baseline accident probability.

To relate the criterion on Q^+d more directly to the accident probabilities Eqn. (26), may be rewritten in the form:

$$\frac{Q^+ d}{Q T} \leq \beta_2 \quad (34)$$

where β_2 is a control value. As another variant, controls may be placed on the relative increase $Q^+d - Qd$:

$$\frac{(Q^+ - Q)}{Q} \frac{d}{T} \leq \beta_3 \quad (35)$$

All these variations are equivalent in that one may be obtained from the other.

To use the above equations to determine an AOT, one can conservatively assume that d equals the AOT. The maximum allowed downtime is thus controlled to be less than the specified criterion. Appendix B describes an average control approach which controls the expected AOT risk and which requires knowledge of the distribution of repair time.

It should be noted that in the above criteria, the ratio of Q^+ to Q is the characteristic which is important and which determines the acceptable AOT. If A denotes this ratio,

$$A = \frac{Q^+}{Q} \quad (36)$$

then A measures the change in the system unavailability when the particular component goes down. The quantity A can, therefore, be called the system impact, or system importance, of the downed component. In other reports (NUREG/CR-3385⁵ and NUREG/CR-3541⁶) this ratio was termed the "risk achievement worth" or the "maintenance impact".

In terms of the system importance A , the previous criteria become:

$$A \leq \alpha_2 \quad (37)$$

$$A \frac{d}{T} \leq \beta_2 \quad (38)$$

and

$$(A-1) \frac{d}{T} \leq \alpha_3 \quad (39)$$

where the first criterion controls the unavailability measure (Q^+) and the second two alternatives control the unavailability-downtime measure (Q^+d).

Finally, the criterion placed on the third risk measure, the increased system unavailability times the accumulated downtime over a reference period is:

$$DQ^+ \leq \gamma_1 \quad (40)$$

To shed light on this criterion, considerations similar to that given previously may be used. The probability H^+ of an accident occurring during the accumulated downtime in a reference period T is:

$$H^+ = \psi Q_P Q^+ D \quad (41)$$

The baseline accident probability H during the downtime period, where the component is not known to be down, is:

$$H = \psi Q_P Q D \quad (42)$$

The reference accident probability H_0 over the total reference time period is:

$$H_0 = \psi Q_P Q T \quad (43)$$

The increased projected probability H^+ compared to H then is:

$$\frac{H^+}{H_0} = \frac{Q^+}{Q} \quad (44)$$

Similarly, the increased probability H^+ compared to H_0 is:

$$\frac{H^+}{H_0} = \frac{Q^+ D}{Q T} \quad (45)$$

From Eqn. (44) above, it is seen that controls on the first risk measure Q^+ (Eqn. (24)) also control the relative increase in the accident probability during the accumulated downtime in any period. Thus, controlling Q^+ controls the relative increased accident frequency, the increased accident probability in a given downtime, and the increased accident probability in accumulated downtimes.

Equation (45) gives a basis for understanding the controls on the third measure, the accumulated downtime risk, as given by the control Eqn. (40). By using this equation, the increased accident probability during the accumulated downtime in a reference period is thereby controlled compared to the baseline accident probability over the same period.

Expressing the accumulated downtime D as:

$$D = wTd \quad (46)$$

the control equation, Eqn. (40) becomes:

$$Q^+ wTd \leq \gamma_1 \quad (47)$$

Equation (45) relating the increased probability to the baseline probability similarly becomes:

$$\frac{H^+}{H_0} = \frac{wQ^+ d}{Q} \quad (48)$$

It should be noted that the reference period, T , does not directly enter into Eqn. (48) because the frequency w of downtime occurrences used. A control equation on the accumulated risk where D is expressed as wTd , and which is more directly related to the relative accident probability control is thus:

$$\frac{wQ^+ d}{Q} \leq \gamma_2, \quad (49)$$

Instead of the frequency of downtime occurrences, the projected number N of downtime occurrences in some period T can also be used. Letting

$$N = wT \quad (50)$$

the control equation on the accumulated risk is alternatively:

$$\frac{N Q^+ d}{Q_T} \leq \gamma_3 \quad (51)$$

Expressed in this form, the control is similar to the control on the risk from a given downtime. This is similar to Eqn. (34) with N as an additional factor.

The controls on the accumulated AOT risk as given by Eqn. (47) or (51) differ from the controls on the risk from a given downtime (the second risk measure) given by Eqn. (34) and its variants. They differ because the frequency of downtime occurrences w , or equivalently, the projected number of occurrences N , is also considered. Bounding values of w or N can be used in these controls to accommodate variations in the frequency or number of occurrences.

The controls on the different risk measures give different acceptable values for the AOT. The smallest acceptable AOT may be selected, such that all the criteria are satisfied. In many applications, one control equation will dominate, and the acceptable AOT for this equation will satisfy the other control equations.

For the control equation on the accumulated downtime risk, the accumulated downtime D was expressed in terms of a given downtime d to obtain a criterion on d . Alternatively, Eqn. (40) can be used to define a separate direct control on the accumulated downtime D . Appendix C discusses the modeling of the probability distribution of D to determine the likelihood of violating such a control. The above form of the control equation involving the individual downtime, d , will control the accumulated downtime risk provided that the observed downtime occurrence frequency, w , is monitored to ensure it is consistent with the value used in the equation.

The control on the accumulated risk in the form given by Eqn. (49) has an additional interpretation. The system unavailability, Q , can be written as the sum of various contributions which include the unavailability from downtime occurrences. Controlling the accumulated risk by this criterion also controls the downtime contribution to system unavailability.

Like previous criteria, the above criteria on the accumulated risk can be expressed in terms of the downed component impact or importance A on the system. In terms of importance, the control equations, Eqns. (49) and (51), can be written as:

$$w A d \leq \gamma_2 \quad (52)$$

and,

$$N A \frac{d}{T} \leq \gamma_3 \quad (53)$$

All the criteria apply equally to an AOT extension; d in the control equations is the extended downtime. The baseline unavailability, Q , can either be the average unavailability with the extended downtimes, or the original downtimes. If it is evaluated with the extended downtimes, then this new reference, Q , needs to be compared to the original Q (with the original downtimes) to ensure it has not increased unacceptably.

In calculating the system unavailability Q^+ with the component down, there are special considerations beyond those in a usual PRA evaluation. The original minimal cut sets of the system cannot necessarily be used to calculate Q^+ by simply setting the downed component unavailability equal to 1. The resulting minimal cuts may no longer be minimal (by perhaps containing replicates of the same contribution) or may not be comprehensive enough (because of truncations in obtaining the original minimal cut sets). Also, when the component is down, other components may be reconfigured which are not adequately reflected in the original minimal cut sets. The original fault-tree models therefore may need to be re-evaluated to obtain valid, comprehensive, minimal cut sets.

When quantifying Q^+ , testing schemes of other components may also need to be modified, if these surveillance test intervals are modified during the AOT. If certain components are required to be tested before repair is begun on the downed component, the unavailabilities of these other components must be modified in calculating Q^+ . Finally, since the AOT component is given to be down, other component unavailabilities may need to be increased if common-cause potentials are assessed to be significant (if they are not incorporated in the PRA).

For multiple AOTs, or multiple AOT extensions for different components, the previous criteria can be applied to the AOT of each component. There are two additional considerations:

1. the cumulative risk effect from all the AOTs, and
2. the interaction among the different AOTs and among surveillance test intervals and AOTs.

The cumulative effect can be handled in several ways. If several AOTs or extensions are to be simultaneously evaluated, then the sum of AOT risks needs to be controlled, that is, the sum of the accumulated unavailabilities (e.g., Eqns. (26) and (47) or their variants) over the different component AOTs must be less than some control value (β_1 or γ_1 say). If AOTs are evaluated singly in a stepwise manner, then the reference baseline unavailability, Q , can be consecutively updated after AOT and the control equation, Eqns. (26) or (47) applied to each new evaluated AOT. Either approach, can work in practice. Appendix D describes cumulative risk considerations in more detail.

The consideration of interactions can also be handled in several ways. When a given component is down, Q^+ should include the updated AOTs and updated test intervals of the other components. To determine the possible impact of multiple components being simultaneously down, Q^+ can be evaluated with all these components assumed to be down (their unavailabilities all set to 1). If Q^+ is too large, reliability assurance activities can be instituted to ensure this condition does not occur. If multiple AOTs and surveillance test intervals are to be simultaneously evaluated, then these new values can be used together in the calculations of Q^+ , Q^+d , and wTQ^+d . The risk measure for each AOT (d) and the sum of the measures over the AOTs then need to satisfy the criteria.

Thus, the evaluations which are required are thus detailed but fairly straightforward. The practical question of what models to use for the system unavailability will depend upon specific system and plant considerations. If a system has several different failure definitions, then the criteria need to be satisfied for each failure. Equivalently, the criteria need to be satisfied for the most stringent success definition, giving the maximum Q^+ or Q^+/Q . Appendix E outlines the detailed considerations which are involved when the component appears in multiple systems.

Table 18 summarizes the possible controls on the system unavailability giving acceptable AOTs giving one criterion for each risk measure controlled. Other variants are straightforwardly obtainable, as described in the text.

Table 18. Controls at the System Level

1. Controls on the system unavailability during the downtime

$$\frac{Q^+}{Q} \leq \alpha$$

Q = baseline system unavailability
 Q^+ = increased system unavailability

2. Controls on the risk from a given downtime

$$\frac{Q^+}{Q} \frac{d}{T} \leq \beta$$

d = component downtime
 T = reference period

3. Controls on the risk from accumulated downtimes

$$w \frac{Q^+}{Q} d \leq \gamma$$

w = projected frequency of downtimes

6. SUMMARY AND CONCLUSIONS

A framework has been established for evaluating AOTs from a standpoint of reliability and risk. The framework which was presented allows different strategies to be developed for evaluating AOT risks and for determining AOTs which provide acceptable risks. Based on the arguments made for considering only AOT operational risks, strategies based on AOT operational risk considerations are the most feasible and most straightforward to implement. Both the single downtime risks (the second risk measure), and the cumulative downtime risks (the third risk measure) must be considered.

From the discussions concerning different risk level strategies based on controlling function unavailabilities are the most feasible, in that system interactions are incorporated and that a high degree of flexibility is provided in determining the AOTs. Strategies can also be based on controlling the core-melt frequency; these strategies provide even more flexibility, however, more comprehensive models are required.

Finally, based on the criteria and risk measure considerations, either absolute criteria or relative criteria can be used to assess AOT risks and determine acceptable AOTs. However, if relative criteria are used, one must ensure that the baseline risks are acceptable and that good plants are not penalized.

REFERENCES

1. Van Otterloo, R.W., "Identification of Standards for Allowable Repair Periods for Safety Systems," SRS Quarterly Digest, January 1979.
2. White, R., and Cross, A., "Repair of Majority Vote Safety Systems," SRS Quarterly Digest, April 1979.
3. Jacobs, I.M., "Safe Test Intervals and Allowable Repair Time for Engineered Safeguards Systems," SRS Quarterly Digest, October 1979.
4. Mankamo, T., "Standards for Allowable Repair Periods in Standby Safety System", SRS Quarterly Digest, October 1981.
5. Vesely, W.E., Davis, T.C., Denning, R.S., and Saltos, N., Measures of Risk Importance and Their Application, NUREG/CR-3385, July 1983.
6. Vesely, W.E., Davis, T.C., and Saltos, N., Measures of the Risk Impacts of Testing and Maintenance Activities, NUREG/CR-3541, November 1983.

APPENDIX A. MEASURES FOR QUANTIFYING AOT OPERATING ACCIDENT RISK AT DIFFERENT RISK LEVELS (COMPONENT, FUNCTION, ACCIDENT SEQUENCE AND OVERALL RISK LEVEL)

A.1 Risk Measures at the Component Level

When the component risk associated with the AOT is focused upon, then the risk measures become:

f = the component's unavailability when it is down during the AOT (A-1)

$= 1$ (A-2)

r = the unavailability of the downed component times the period d in which it is down (A-3)

$= 1 \times d = d$ (A-4)

R = the accumulated component downtime in some time period T controlled by the AOT (A-5)

$= D = wTd$ (A-6)

where w is the frequency of downtime occurrence.

The AOT controls the component downtime in that the downtime, d , is constrained to be less than the AOT,

$d \leq \text{AOT}$ (A-7)

The bounding case is to assume the downtime equals the AOT, $d = \text{AOT}$. For this assumption, the maximum AOT risk is thus controlled not to exceed the specified criterion. (Appendix B describes a modeling approach which controls the average AOT risk not to exceed the criterion. This requires knowledge of the distribution repair time.) If the accident risk is acceptable in the bounding case where $d=\text{AOT}$, then it will be acceptable for actual d since all accident risk characteristics (at all levels) are a non-decreasing function of d .

If the AOT operating accident risk is controlled at the component level, then f , r , and R , or some variant of them are the relevant measures. The measure f is not controllable, since it is always unity. The downtime risk r , in this case the component downtime d , can be controlled to be small compared to some reference period T in which the component is to be available:

$\frac{d}{T} \leq \alpha$ (A-8)

where α is the acceptability criterion.

During plant operation, the component goes through cycles of being up and down. If T is selected as the time period for one cycle of operation, then:

$$T = 1/\lambda \quad (A-9)$$

where λ is the component failure rate. T is thus the mean time between failures. Eqn. (A-8) then becomes:

$$\lambda d \leq \alpha \quad (A-10)$$

The quantity λd is the approximate component unavailability contribution from the downtime and by Eqn. (A-10) the downtime d is thus controlled such that the unavailability contribution is less than α .

If downtimes for the component occurs at a higher frequency w than the failure rate, w should be substituted into Eqn. (A-10) to give:

$$w d \leq \alpha \quad (A-11)$$

This higher frequency will occur, for example, if the component is brought down when it appears to be degraded instead of having completely failed. A general relationship is to use:

$$w = \lambda k \quad (A-12)$$

where k is the downtime occurrence multiplication factor.

Equations (A-10) and (A-11) represent absolute control criteria. A relative criterion is obtained by comparing the contribution d to the total component unavailability q

$$\lambda \frac{d}{q} \leq \beta \quad (A-13)$$

Again, if the frequency w of downtimes is larger than λ then w should replace λ in Eqn. (A-13).

The other measure of the component risk associated with the AOT is the accumulated downtime D . The criteria on D is

$$D \leq \gamma \quad (A-14)$$

where γ is some control value. The control equation can equivalently be divided by T to give

$$\frac{D}{T} \leq \gamma' \quad (A-15)$$

where γ' is some new control value ($\gamma' = \gamma/T$). Expressing D in terms of wTd as in Eqn. (A-6) gives:

$$wd \leq \gamma' \quad (A-16)$$

which is the same as Eqn. (A-11).

Thus, if D is expressed in terms of w , T , and d , no new control equation results. Consequently, the control of the risk from a given downtime, Eqn. (8), also controls the risk from accumulated downtimes (Eqns. (A-15)-(A-16)). However, to control the cumulative downtime risk, a downtime frequency, w , needs to be assumed. If $w = \lambda$ is assumed, then the number of component downtime occurrences must be monitored to ensure this assumption is valid. Even if $w = k\lambda$ is assumed, to allow tolerances for an increased frequency of downtimes ($k > 1$), monitoring is still necessary. A later section discusses the possible optional controls on D directly, not only at the component level but at higher levels.

The practical question is whether controlling the downtime via Eqns. (A-10) or (A-13) will yield low accident risks and still yield meaningful AOTs. The absolute criterion value can always be selected to be small enough to yield small accident sequence frequencies, core-melt frequencies, and overall risk. Considering the actual values for failure rates and investigating actual applications will determine whether workable AOTs are obtainable.

For the relative criterion β in Eqn. (A-13), the practical question again is whether the reference unavailability q can be meaningfully selected to yield a small relative contribution and a workable AOT. Actual cases and applications need to be considered.

Finally, the accident frequency while the component is down during the AOT is not controlled by the above criteria. This case needs to be separately examined by failing the component and then calculating the system unavailability, function unavailability, or accident sequence frequency which will determine if controls at these higher levels are necessary.

Table A.1 summarizes the possible controls on the component unavailability associated with the AOT. To control the bounding situation, the downtime d is assumed to be the AOT. For downtime extensions, d becomes the new extended downtime. For AOTs calculated for different components, each component AOT must satisfy the controls.

Table A.1. Controls at the Component Level

1. The component unavailability during the downtime is not controllable.
 2. Controls on the downtime and also average unavailability from downtimes:

absolute criteria:	$wd \leq \alpha$	d = component downtime
		w = projected frequency of downtimes occurrences
relative criteria:	$\frac{wd}{q} \leq \beta$	q = component total unavailability
-

A.2 Risk Measures at the Function Level

The measures and criteria at the function level are analogous to those for the system level. Because of the parallel structure, the results will be presented with only a brief discussion.

The three risk measures at the function level are:

f = the (increased) function unavailability with the component down (A-17)

$$= \hat{Q}^+ \quad (A-18)$$

r = the (increased) function unavailability times the component downtime d (A-19)

$$= \hat{Q}^+ d \quad (A-20)$$

and,

R = the (increased) function unavailability times the accumulated downtime in some time period T (A-21)

$$= wT\hat{Q}^+ d \quad (A-22)$$

In the above, the superscript caret symbol "^" denotes that the unavailability is a function unavailability instead of a system unavailability (without the superscript). The safety function is the function containing the component whose AOT is to be evaluated. If the component is in several functions, then each function is separately evaluated.

The criterion on the increased function unavailability can be expressed in one of the following alternative forms:

$$\hat{Q}^+ \leq \alpha_1 \quad (A-23)$$

$$\frac{\hat{Q}^+}{\hat{Q}} \leq \alpha_2 \quad (A-24)$$

or

$$\frac{\hat{Q}^+ - \hat{Q}}{\hat{Q}} \leq \alpha_3 \quad (A-25)$$

where $\hat{Q}$ is the baseline function unavailability.

The criterion on the increased function unavailability times the component downtime can be expressed as:

$$\hat{Q}^+ d \leq \beta_1 \quad (A-26)$$

$$\frac{\hat{Q}^+d}{\hat{Q} T} \leq \beta_2 \quad (A-27)$$

or,

$$\frac{\hat{Q}^+ - \hat{Q}}{\hat{Q}} \frac{d}{T} \leq \beta_3 \quad (A-28)$$

where T is the reference period. As for the parallel criteria on the increased system unavailability times the component downtime, the above criteria control the increased accident probability during the downtime relative to the baseline probability over the time period, T.

Finally, the criterion on the increased function unavailability times the accumulated downtime in a reference period can be expressed as:

$$wT\hat{Q}^+d \leq \gamma_1 \quad (A-29)$$

$$\frac{w\hat{Q}^+d}{\hat{Q}} \leq \gamma_2 \quad (A-30)$$

or,

$$\frac{N\hat{Q}^+d}{\hat{Q}T} \leq \gamma_3 \quad (A-31)$$

The above criteria can also be expressed in other equivalent forms, for example, involving $\hat{Q}^+ - \hat{Q}$, as in the previous criteria. As for the parallel criterion at the system level, the above criteria control the increased accident probability over the accumulated downtimes in some reference period, compared to the baseline accident probability in this same period.

The arguments which show that the above criteria control the increased accident probability are the same as those given previously, except the system unavailability is replaced by function unavailability. The important risk characteristic is the function impact, or importance, A, of the downed component:

$$\hat{A} = \frac{\hat{Q}^+}{\hat{Q}} \quad (A-32)$$

As in Eqns. 37-39, all the criteria can be written solely in terms of $\hat{A}$ and the downtime, d.

The calculations are similar to those at the system level. If multiple AOTs or AOT extensions are evaluated, then they can be done either simultaneously or stepwise. For simultaneous evaluation, the sum of the accumulated

risks (the terms on the right hand sides of the control equations) needs to be controlled. To account for interactions, the relevant updated AOTs and updated test intervals must be used in evaluating the unavailabilities. These considerations are similar to those at system level. Also, a separate control can be placed on the accumulated downtime D using Eqns. (A-29)-(A-31) and defining $D = wTd$, or $D = Nd$. Appendix C describes distribution considerations if the focus is on D.

Whether system or function evaluations are simpler in practice depend upon several considerations. A particular system model may be simpler to evaluate but there may be different failure definitions of the system to be considered. The function model may be more complex but safety functions can be better isolated and be more uniquely defined. The tradeoffs between the system level and function level of control can be evaluated in actual applications.

Table A.2 summarizes the possible controls at the function level; the table is similar to Table 18 with the function unavailability now the risk characteristic.

Table A.2. Controls at the Function Level

1. Controls on the function unavailability during the downtime

$$\frac{\hat{Q}^+}{\hat{Q}} \leq \alpha$$

$\hat{Q}$ = baseline function availability
 $\hat{Q}^+$ = increased function unavailability

2. Controls on the risk from a given downtime

$$\frac{\hat{Q}^+ d}{\hat{Q} T} \leq \beta$$

d = component downtime
 T = reference period

3. Controls on the risk from accumulated downtimes

$$\frac{\hat{wQ}^+ d}{\hat{Q}} \leq \gamma$$

w = projected frequency of downtimes

A.3 Risk Measures at the Accident Sequence Level

The risk measures at the accident sequence levels are fairly straightforward and need little further clarification. At the sequence level, controls are placed on the frequencies of the accident sequences containing the downed component with the AOT.

The three risk measures are:

f - the (increased) accident sequence frequency with the component down (A-33)

- F^+ (A-34)

r - the (increased) accident frequency times the component downtime (A-35)

- F^+d (A-36)

and,

R - the (increased) accident frequency times the accumulated downtime in some reference period T (A-37)

- wTF^+d (A-38)

The increased accident frequency F^+ is defined as:

$F^+ = \psi Q^+ Q_p$ (A-39)

where from Section 5.2, ψ is the initiating event frequency (Eqn. 43), Q^+ the increased unavailability of the system containing the downed component (Eqn. 19), and Q_p the product of the unavailabilities of the systems not containing the downed component (Eqn. 28). Instead of system unavailabilities, function unavailabilities may also be used (placing a caret superscript " $\wedge$ " above the Q s, as in the previous section).

The second risk measure, F^+d , is the increased accident probability during the downtime and was denoted by P^+ in Section 5.2:

$P^+ = F^+d$ (A-40)

The third risk measure is the increased accident probability during the accumulated downtime in the reference time period T . This measure was denoted by H^+ in Section 5.2:

$H^+ = wTF^+d$ (A-41)

Criteria on the three risk measures are:

$F^+ \leq \alpha_1$ (A-42)

$F^+d \leq \beta_1$ (A-43)

and,

$wTF^+d \leq \gamma_1$ (A-44)

These criteria control the increased accident frequency, increased accident probability from a given downtime, and the increased accident probability from accumulated downtimes, respectively.

The above criteria are expressed as absolute criteria. They also can be expressed in relative form:

$$\frac{F^+}{F} \leq \alpha_2 \quad (\text{A-45})$$

$$\frac{F^+d}{FT} \leq \beta_2 \quad (\text{A-46})$$

and

$$\frac{wF^+d}{F} \leq \gamma_2 \quad (\text{A-47})$$

In the above equations, F is the baseline accident frequency in which the component is not known to be down, and T is the reference period. The quantity FT is the baseline accident probability in period T . In Section 5.2, FT was denoted as P_0 (or H_0). Another variation is to replace F^+/F with the relative difference $(F^+ - F)/F$.

The basic risk characteristic which enters into all the above criteria is the downed component's impact, or importance, B , on the sequence:

$$B = \frac{F^+}{F} \quad (\text{A-48})$$

These relative criteria can be expressed in terms of B .

The criterion in the increased accident frequency F^+ does not control AOT since the downtime does not enter into F^+ . However, the criterion can be used to identify where reliability assurance is needed; to satisfy the criterion, critical components can be tested to lower F^+ before repair is begun on the downed component. In some cases, the system may also be reconfigured to lower F^+ .

The criteria on P^+ and H^+ provide controls on the AOT. For the most comprehensive control, the AOT must satisfy both criteria. In application, however, one criterion may dominate the other, so that if the AOT satisfies one equation, the other will automatically be satisfied. The accumulated downtime D may also be directly controlled. Appendix C describes distribution considerations for determining the likelihood of violating a control on D .

The actual values selected for the criterion values α , β , and γ will depend upon considerations for implementation. The values should be selected so as to control not only the contribution from a given sequence but the cumulative contribution from all the sequences impacted by the AOTs. The

calculations are similar to those at the system level where now, for example, accident sequence minimal cut sets are involved. As discussed earlier, either simultaneous or sequential calculations may be performed.

The advantage of sequence control is that accident sequence frequencies are directly controlled. This can result in greater flexibility for acceptable AOTs. The disadvantage is that modeling and evaluations are more complex with more uncertainties entering. The tradeoffs can be evaluated in actual applications.

Table A.3 summarizes the controls at the accident sequence level.

Table A.3. Controls at the Sequence Level

1. Controls on the accident sequence frequency during the downtime

$$\frac{F^+}{F} \leq \alpha$$

F = baseline accident frequency
F⁺ = increased accident frequency

2. Controls on the risk from a given downtime

$$\frac{F^+ d}{F T} \leq \beta$$

d = component
T = reference period

3. Controls on the risk from accumulated downtimes

$$\frac{w f^+ d}{F} \leq \gamma$$

w = projected frequency of downtimes

A.4 Risk Measures at the Overall Risk Level

The risk measures and criteria at the overall risk level are similar to those at the accident sequence level, except that consequences are considered. Also, the criteria may apply to the sum of the risks from various sequences.

The three risk measures are:

$$f = \text{the (increased) accident frequency sequence times the consequence with the component down} \quad (\text{A-49})$$

$$r = \text{the (increased) accident probability times the consequence during the component downtime} \quad (\text{A-50})$$

$$= f d \quad (\text{A-51})$$

and,

R = the (increased) accident probability times the consequence during accumulated downtime in some reference time period (A-52)

$$= wTfd \quad (A-53)$$

The consequence can be of any type, such as the expected man-rem per accident sequence, the expected early fatalities per accident sequence, or the expected accident economic costs per sequence. Instead of expected values, other characteristic values of the consequence distribution may be used.

If the consequences are set equal to unity for each sequence, then the controls are put on the total accident frequency and probability. For example, if the accident is defined to be a core-melt accident then:

f = the increased core-melt frequency when the component is down (A-54)

r = the increased core-melt probability during a component downtime period (A-55)

R = the increased core-melt probability during the accumulated downtimes in some reference period (A-56)

These risk measures would also be obtained at the sequence level in the previous section by defining a sequence to be core melt.

Absolute criteria on these risk measures are:

$$f \leq \alpha_1 \quad (A-57)$$

$$fd \leq \beta_1 \quad (A-58)$$

and,

$$wTfd \leq \gamma_1 \quad (A-59)$$

Relative criteria can be obtained by dividing by a baseline accident frequency time consequence f_o :

$$\frac{f}{f_o} \leq \alpha_2 \quad (A-60)$$

$$\frac{fd}{f_o T} \leq \beta_2 \quad (A-51)$$

$$w \frac{f}{f_o} d \leq \gamma_2 \quad (A-52)$$

The increased accident frequency, f , times the consequence does not contain the component downtime, and hence a criterion on it will not provide acceptable AOTs. As before, the control can be used to determine where critical components need to be assured to be up before the repair is begun on the downed component. In some cases, system reconfiguration can also lower f to an acceptable value.

The two criteria on the accident probabilities times consequence (the second two measures) provide definitions of acceptable AOTs. Both can be applied (together) for the most comprehensive control; however, for actual implementation, only one may be sufficient because of its dominance.

The advantage of controlling at the overall risk level is that more flexibility is gained in defining acceptable AOTs. However, the models and evaluations are more complex. Actual evaluations with specific consequence measures can be carried out to determine the tradeoffs in specific cases. Table A.4 summarizes the controls at the overall risk level.

Table A.4. Controls at the Overall Risk Level

1. Controls on the accident sequence frequency times consequence during the downtime

$$\frac{f}{f_o} \leq \alpha$$

f_o - baseline risk frequency
 f - increased risk frequency

2. Controls on the accident probability times consequence from a given downtime

$$\frac{Fd}{F_o T} \leq \beta$$

d - component downtime
 T - reference period

3. Controls on the accident probability times consequence from accumulated downtimes

$$w \frac{f}{f_o} d \leq \gamma$$

w - projected frequency of downtime occurrences

APPENDIX B. THE AVERAGE DOWNTIME FOR A GIVEN SPECIFIED AOT

The component downtime d appears in the various equations for the AOT operating risk. If d is taken as the maximum downtime for an AOT, then d is simply equal to the AOT value; the maximum AOT risk is thereby controlled via the risk-control equations. If d is taken as the average downtime for an AOT, then d is smaller than the AOT value; in this case, the average AOT risk is controlled.

To determine the relationship between d and the AOT for the case where the average AOT risk is controlled let

$g(r)$ = the probability that the repair is completed in time interval r per unit time (B-1)

$G(r)$ = the probability that the repair time interval is less than or equal to r (B-2)

and,

$d_{\max}$ = the acceptable AOT (B-3)

The quantity $g(r)$ is the repair density function for the component. $G(r)$ is the cumulative repair distribution function and is related to $g(r)$ by:

$$G(r) = \int_0^r g(r') dr' \quad (B-4)$$

The repair distribution is estimated from records of the component's repair times.

If d is taken as the average downtime, then d is expressible as

$$d = \int_0^{d_{\max}} r g(r) dr + (1-G(d_{\max})) d_{\max} \quad (B-5)$$

Thus, knowing $g(r)$ and $G(r)$, d can be determined in terms of $d_{\max}$ using Eqn. (B-5). This relation can then be substituted into all the risk control equations to determine $d_{\max}$, which is the acceptable AOT controlling the average AOT risk.

APPENDIX C. THE DISTRIBUTION OF CUMULATIVE DOWNTIME

Introduction

A standby or operating component goes through a cyclic pattern of being up, or in an operable state, and then being down, or in a failed state. The component can be down because of a failure, a maintenance being performed, or a test being conducted. The successive periods in which the component is up or down can vary because of the random nature of the uptimes and downtimes.

The cumulative downtime in some period is the sum of the individual downtime durations in that time. The probability distribution of the cumulative downtime depends upon the frequency at which the component is brought down and the distribution of the durations of individual downtime. Knowledge of the cumulative downtime distribution is important for allowed downtime approaches which control the cumulative downtime in some period. The cumulative downtime distribution gives the likelihood that a given, allowed cumulative downtime will be violated in the period.

The cumulative downtime also generates a cumulative downtime risk for the component. When the component is down, then there is an associated downtime risk due to the component being out of service. Thus, when the component is down for some cumulative downtime, then there is an associated cumulative downtime risk for that time period. The probability distribution of cumulative downtime risk is determined from the distribution of cumulative downtime and the downtime risk associated with a given downtime. The distribution of cumulative downtime risk is thus intimately related to the distribution of cumulative downtime. The cumulative downtime risk distribution shows the degree to which the cumulative downtime risk is controlled for a given allowed cumulative downtime.

The following sections describe approaches for determining the distributions of cumulative downtime and cumulative downtime risk. The first two sections describe the approaches for a single component; the third and fourth sections describe approaches for a system of components.

Cumulative Downtime Distribution for a Single Component

For a single component, it is assumed that the individual uptime durations have the same probability distribution and the individual downtime durations have the same probability distribution, i.e., that there are no systematic trends in time in the uptime and downtime. In general, the probability distribution of the uptime durations and the probability distribution of the downtime durations are different and can be of any discrete or continuous form. Under these assumptions, the uptimes and downtimes form an alternating renewal process and standard renewal equations can be used to obtain the cumulative downtime distribution.

From Gnedenko, Belyayev and Solovyev¹, page 115, for an alternating renewal process, the equation for the cumulative uptime distribution can be expressed as:

$$P(h_t < s) = \sum_{n=0}^{\infty} [G_n(t-s) - G_{n+1}(t-s)] F_{n+1}(s) \quad (C-1)$$

where,

$$P(h_t < s) = \text{the probability that the cumulative uptime } h_t \text{ in period } t \text{ is less than } s. \quad (C-2)$$

$$G_n(t-s) = \text{the probability that the sum of } n \text{ downtime durations is less than or equal to } t-s. \quad (C-3)$$

$$G_{n+1}(t-s) = \text{the probability that the sum of } n+1 \text{ downtime durations is less than or equal to } t-s. \quad (C-4)$$

and,

$$F_{n+1}(s) = \text{the probability that the sum of } n+1 \text{ uptime durations is less than or equal to } s. \quad (C-5)$$

The distribution $G_n(t-s)$ is the n th convolution of the downtime distribution $G(x)$; each downtime duration is assumed to have the same distribution $G(x)$. The distribution $G_{n+1}(t-s)$ is the $(n+1)$ th convolution. The distribution $F_{n+1}(s)$ is the $(n+1)$ th convolution of the uptime distribution $F(x)$; each uptime duration is assumed to have the same distribution $F(x)$. The convolutions are started with $F_0(x) = 1$ and $G_0(x) = 1$ for all values x .

Since the cumulative downtime is simply t minus the cumulative uptime, Eqn. (C-1) also provides the cumulative downtime distribution. Let

$$D_t = \text{the cumulative downtime in period } t \quad (C-6)$$

$$= t - h_t \quad (C-7)$$

Hence, Eqn. (C-1) can be rewritten as:

$$P(t - D_t < s) = \sum_{n=0}^{\infty} [G_n(t-s) - G_{n+1}(t-s)] F_{n+1}(s) \quad (C-8)$$

or,

$$P(D_t > t-s) = \sum_{n=0}^{\infty} [G_n(t-s) - G_{n+1}(t-s)] F_{n+1}(s) \quad (C-9)$$

Substituting

$$d = t - s \quad (C-10)$$

one finally has:

$$P(D_t > d) = \sum_{n=0}^{\infty} [G_n(d) - G_{n+1}(d)] F_{n+1}(t-d) \quad (C-11)$$

Using standard renewal relations, Eqn. (C-11) can also be written in terms of the distribution of the number of downtimes and uptimes. Let

$$P[N_r(d) = n] = \text{the probability that the number of repairs or restorations } N_r(d) \text{ in period } d \text{ equals } n. \quad (C-12)$$

and

$$P[N_f(t-d) > n] = \text{the probability that the number of failures } N_f(t-d) \text{ in period } t-d \text{ is greater than } n. \quad (C-13)$$

Then

$$P(D_t > d) = \sum_{n=0}^{\infty} P[N_r(d) = n] P[N_f(t-d) > n] \quad (C-14)$$

To determine $P(D_t > d)$, Eqn. (C-11) or Eqn. (C-14) can be used. Equation (C-11) is generally more useful when the downtime and uptime distributions are the prime interest and not the numbers of failures or repairs occurring. Since the successive terms in the summations in Eqns. (C-11) and (C-14) generally decrease significantly with increasing n , only a relatively few terms need be calculated. The error in truncating the series can be bounded using standard approaches to determine the preciseness of the truncated series.

To determine $P(D_t > d)$ using either Eqns. (C-11) or (C-14), the uptime distribution $F(x)$ and the downtime distribution $G(x)$ are required as input. From these distributions, the convolutions $G_n(x)$ and $F_n(x)$ are calculated and are used in the equations.

The uptime and downtime distributions are obtained from historical data and from knowledge of the component's characteristics. Parametric distributions, such as the gamma and normal, can be used where justified. In many cases only partial information will be known or can be meaningfully obtained from the data. For example, only the approximate median and spread may be obtainable without assuming unjustifiable distribution shapes. In these cases of partial information, bounds can be obtained on $G(x)$ and $F(x)$ and hence on $P(D_t > d)$. Sensitivity studies can also be performed using various parametric families for $G(x)$ and $F(x)$ which are constrained to be consistent with the partial information.

The calculation of the convolutions $G_n(x)$ and $F_n(x)$ can be done explicitly in some cases. For example, convolutions of normal distributions and gamma distributions are other normal and gamma distributions, respectively. Convolutions of mixtures of normals and of mixtures of gammas are expressible as finite sums of normals and gammas, respectively. These mixture models can be particularly appropriate when there are distinct failure modes requiring significantly different repair times. When the convolutions are not explicitly determinable, then discrete numerical evaluations can be performed. Since the convolution integrals are one-dimensional, standard, efficient, techniques can be used.

Cumulative Downtime Risk Distribution for a Single Component

When the increase in risk is independent of the time at which the component actually goes down, then the cumulative downtime risk distribution is simply obtained from the cumulative downtime distribution. This time-independent case is the one standardly treated in PRAs.

Let

f = the (increased) accident frequency whenever the component goes down. (C-15)

When core-melt frequency is the specific risk characteristic evaluated, then f is the increased core-melt frequency. Alternatively, f can be the increased frequency of specific accident sequences which are the focus of the risk evaluation. Surrogates for the accident or core-melt frequency can also be used. If safety function unavailability is the risk characteristic of interest, then f is the increased safety function unavailability. At a system level, f can be the increased system unavailability. Economic or health consequences can also be incorporated in f . The particular risk characteristic thus depends upon the particular risk focused upon in the evaluations.

When time independence is assumed, f is a constant. For various risk characteristics, f is straightforwardly obtainable from the PRA or from the reliability evaluation. The actual value of f will depend upon the importance of the component to the risk characteristic. Instead of the value of the (increased), accident frequency, f can also be calculated as the incremental increase (difference) over the normal value.

Let

R_t = the cumulative downtime risk associated with the cumulative downtime of the component in time period t . (C-16)

Then R_t is defined to be:

$R_t = D_t f$ (C-17)

where D_t is the cumulative downtime of the component in time period t . In words, Eqn. (C-17) states that the cumulative downtime risk is the cumulative

downtime times the increased accident frequency. The cumulative downtime risk is thus the increase in the expected number of core melts in period t , which can be taken as the increase in the core-melt probability in the period (as is usually done in PRAs). If f is a surrogate for the core-melt frequency, then the cumulative downtime risk R_t is the increased surrogate value times the cumulative downtime; the cumulative downtime risk is thus the increased contribution to the overall average surrogate value in time period t . Let

$$P(R_t > r) = \text{the probability that the cumulative downtime risk } R_t \text{ is larger than some value } r. \quad (C-18)$$

Then using Eqn. (C-17):

$$P(R_t > r) = P(D_t f > r) \quad (C-19)$$

$$= P(D_t > \frac{r}{f}) \quad (C-20)$$

$$= P(D_t > d) \quad (C-21)$$

where,

$$d = \frac{r}{f} \quad (C-22)$$

Hence, the cumulative downtime risk distribution, r , is directly obtained from the corresponding cumulative downtime distribution.

Cumulative Downtime Distribution for a System of Components

Consider a system of components which can be of any logic structure and contain any number of components. The components, in general, may be different from one another. The cumulative downtime for all the system components in some period is simply the sum of the cumulative downtimes for the individual components. It is desired to obtain the probability distribution of this cumulative downtime for all the system's components.

Assume the downtimes of the individual components are the independent. Also assume that the downtimes and uptimes of an individual component form an alternating renewal process as in the previous section.

Let

$$D_t = \text{the cumulative downtime of all the system components in period } t. \quad (C-23)$$

and

$$D_t^{(k)} = \text{the cumulative downtime of the } k\text{th component in the system during period } t. \quad (C-24)$$

Then,

$$D_t = D_t^{(1)} + D_t^{(2)} + \dots + D_t^{(N)} \quad (C-25)$$

where, in general, there are N components in the system. Thus, from Eqn. (C-25), the cumulative downtime distribution of all the system components is the convolution of the distribution of individual component cumulative downtimes. This can be written symbolically as:

$$P(D_t < d) = P(D_t^{(1)} < d_1) * P(D_t^{(2)} < d_2) * \dots * P(D_t^{(N)} < d_N) \quad (C-26)$$

where "*" denotes the convolution operator and d_i are dummy variables.

Knowing the individual component's cumulative downtime distributions $P(D_t^{(k)} < d)$, standard numerical techniques for convolutions can be used to obtain the cumulative downtime distribution $P(D_t < d)$ of all the system's components. This is particularly efficient if there are relatively few components (less than 5) and the distributions are discrete with relatively few points (less than 10).

Monte Carlo simulations may also be performed to estimate the convolution. A cumulative downtime for each component is sampled from its cumulative downtime distribution $P(D_t^{(k)} < d)$. The cumulative downtimes for the system components are then summed to obtain a sample of the cumulative downtime for all the system components. This is repeated over several samples, and standard techniques are used to estimate the cumulative downtime distribution $P(D_t < d)$ and its characteristics. The Monte Carlo simulations can be effectively performed at this level if the component cumulative downtime distributions are discrete or are of a continuous family for which effective sampling techniques are available (such as the normal distribution).

More basic approaches can also be used in determining the cumulative downtime distribution of all the system components. Some of these approaches can yield straightforwardly obtainable results about the characteristics of the distribution. For these more basic approaches, the cumulative downtime D_t of all the components is expressed as:

$$D_t = \sum_{j=1}^M d_j \quad (C-27)$$

where d_j are now the individual downtime durations of the N different components. To explicitly differentiate the different components, Eqn. (C-27) can be re-expressed as:

$$D_t = \sum_{i=1}^{N_t^{(1)}} d_i^{(1)} + \sum_{i=1}^{N_t^{(2)}} d_i^{(2)} + \dots + \sum_{i=1}^{N_t^{(N)}} d_i^{(N)} \quad (C-28)$$

where $d_i^{(k)}$ are the individual downtime durations of component k and there are a total of $N_t^{(k)}$ downtimes for component k in time period t . Equations (C-27) and (C-28) are simply re-expressions of Eqn. (C-25) in terms of the individual component's downtime durations.

Equations (C-27) or (C-28) may be used as a basis for Monte Carlo simulations at a basic uptime-downtime level. For each component, consecutive uptimes and downtimes are sampled from the appropriate distributions, $F^{(k)}(x)$ and $G^{(k)}(x)$, governing the individual component's uptime and downtime durations. The number of downtime durations in time period t and the cumulative sum of these durations are used to obtain a sample of the cumulative downtime for all the components. This procedure is repeated and estimates are then made of the distribution and its characteristics. This basic Monte Carlo approach can also be used on a single component to estimate the component's cumulative downtime distribution. (Effectively, for this case, the system is the one component).

The Monte Carlo simulations at the basic component uptime-downtime level are generally not as efficient as Monte Carlo simulations of the direct, cumulative downtime distributions $D_t^{(k)}$ which were described earlier (for Eqn. (C-25)). Where Eqn. (C-27) or Eqn. (C-28) is most effective is in straightforwardly determining characteristics of the cumulative downtime distribution when additional assumptions are made.

Assume the downtimes of component k occur with a constant occurrence rate, w_k . This assumption implies the uptime distribution is exponential, $F^{(k)}(x) = 1 - \exp(-w_k x)$. The downtime duration distribution $G^{(k)}(x)$ can still be of any general form.

Also, assume that the total downtime occurrence rate, which is the sum of the individual component rates w_k , is the same regardless of whether components are down or up. This assumption implies that a component, when down, could again fail during its downtime with occurrence rate w_k . These additional downtimes have durations described by the same downtime duration distribution $G^{(k)}(x)$. This assumption of failures possibly occurring during the downtime is conservative, in that the determined cumulative downtimes will be larger than actual due to these additional downtime contributions. This conservatism will be small if the expected number of additional downtime occurrences in the downtime duration is small ($w_k d \ll 1$).

The assumption of a constant occurrence rate, w_k , is consistent with usual PRA assumptions. However, in general the downtime occurrence rate w_k is higher than the component failure rate, and is some multiple of the failure rate. The assumption of additional downtimes occurring during a downtime will generally result in negligible conservatisms because $w_k d$ is indeed generally much smaller than 1. (This assumption can also account for failures caused by the repair activities). The degree of conservatism can be checked by comparing the results subsequently determined for a single component with the exact, alternating renewal results given previously (Eqn. C-11).

Under the assumptions of constant occurrence rates, w_k , which do not change during downtimes, the cumulative downtime of all the system components are described by a compound Poisson process. The total number of downtime occurrences in time period t is given by the Poisson distribution with total occurrence rate w ,

$$w = \sum_{k=1}^N w_k \quad (C-29)$$

All the moments of D_t can be determined using standard techniques for compound Poisson processes. For example, from Cinlar², page 93, the expectation of $E[\exp(-\alpha D_t)]$, where the constant $\alpha \geq 0$, is:

$$E[\exp(-\alpha D_t)] = \exp(-wt(1-g(\alpha))) \quad (C-30)$$

where,

$$g(\alpha) = \int_0^{\infty} e^{-\alpha u} dG(u) \quad (C-31)$$

and,

$$G(u) = \sum_{k=1}^N \frac{w_k}{w} E[d^{(k)}] \quad (C-32)$$

The distributions $G^{(k)}(u)$ are the individual downtime distributions of the different components. The symbol " $E[]$ " denotes the expectation of the random variable in the brackets.

Equation (C-30) allows the moments of D_t to be obtained by standard, differentiation techniques. For example, taking the first derivative of Eqn. (C-30) with respect to α and then setting α equal to zero gives

$$E[D_t] = wt E[d] \quad (C-33)$$

and,

$$E[d] = \sum_{k=1}^N \frac{w_k}{w} E[d^{(k)}] \quad (C-34)$$

where $E[d^{(k)}]$ is the expected individual downtime duration of the k th component. Higher order moments of D_t can similarly be obtained.

With knowledge of the moments of D_t , various standard techniques can be used to select the distribution which best fits the moments of D_t . For example, the Pearson family or the Johnson family can be used, as is often done. This moment-fitting approach allows the distribution of D_t to be approximated effectively and with relatively little computation. Also, for any

finite number of moments used for fitting, complete knowledge of the individual component distributions $G^{(k)}(u)$ is not required, but only their moments are needed.

Cumulative Downtime Risk Distribution for a System of Components

The cumulative downtime risk distribution for a system of components is related to the cumulative downtime distribution, but the relationship is not as simple as for a single component. Assume again a system of arbitrary components whose downtimes are independent and form alternating renewal processes. Let

R_t = the cumulative downtime risk in time period t for all the components in the system. (C-35)

The cumulative downtime risk R_t is defined by:

$$R_t = R_t^{(1)} + R_t^{(2)} + \dots + R_t^{(N)} \quad (C-36)$$

where $R_t^{(k)}$ is the cumulative downtime risk for the k th component. The cumulative downtime risk $R_t^{(k)}$ for the k th component is again (c.f., Eqn. C-17):

$$R_t^{(k)} = D_t^{(k)} f_k \quad (C-37)$$

where f_k is the increased accident frequency when component k is down.

From Eqn. (C-36), the system downtime risk distribution $P(R_t < r)$ is again the convolution of the individual component distributions, which are now the component cumulative downtime risk distributions:

$$P(R_t < r) = P(R_t^{(1)} < r_1) * P(R_t^{(2)} < r_2) * \dots * P(R_t^{(N)} < r_N) \quad (C-38)$$

The same approaches described in the previous section for the cumulative downtime distribution can, therefore, be used for the system cumulative downtime risk distribution.

As in the previous section, the system cumulative downtime risk can be accurately approximated by the compound Poisson process now using the formula:

$$R_t = \sum_{j=1}^M d_j f_j \quad (C-39)$$

where f_j is the increased accident frequency for the individual downtime duration d_j . The downtime duration distributions $G(u)$ and $G^{(k)}(u)$ in Eqns. (C-31) and (C-32) are now replaced by the downtime risk distributions $G(u)$ and $G^{(k)}(u)$ where

$$G(u) = \sum_{k=1}^N \frac{w_k}{w} \bar{G}^{(k)}(u) \quad (C-40)$$

and,

$$\bar{G}^{(k)}(u) = G^{(k)}\left(\frac{u}{f_k}\right) \quad (C-41)$$

An important additional distribution which is desired is the conditional distribution that the cumulative system downtime risk is acceptable (below some value) when the cumulative downtime is controlled to be below some value. Let

$$P(R_t < r / D_t < d) = \text{the probability that the system cumulative downtime risk } R \text{ is less than } r \text{ when (given) the total downtime } D_t \text{ is less than } d. \quad (C-42)$$

The probability $P(R_t < r / D_t < d)$ is important for determining how well the downtime risk is controlled when the total system downtime is controlled by specifying some allowed cumulative downtime value, d . With knowledge of $P(R_t < r)$ and $P(D_t < d)$, the distribution $P(R_t < r / D_t < d)$ is directly determinable from $P(R_t < r, D_t < d)$; where

$$P(R_t < r, D_t < d) = \text{the probability that the system cumulative downtime risk } R \text{ is less than } r \text{ when (given) the total downtime } D_t \text{ is less than } d. \quad (C-43)$$

The distributions $P(R_t < r / D_t < d)$ and $P(R_t < r, D_t < d)$ are straightforwardly obtained from Monte Carlo simulations of D_t and R_t , using the basic convolution formulas (Eqns. (C-26) and (C-38)). The evaluations are the same as previously described except now a sample consists of the pair of values (R_t, D_t) . The evaluations are particularly straightforward if the distributions are discrete. Other standard, bi-variate approaches could also be used such as regression analysis, and bi-variate distribution fitting approaches, based, for example, on moments.

References for Appendix C

1. B.V. Gnedenko, Y.K. Belyayev, and A.D. Solov'yev, Mathematical Methods of Reliability Theory, Academic Press, New York, 1969.
2. E. Cinlar, Introduction to Stochastic Processes, Prentice-Hall, Englewood Cliffs, New Jersey, 1975.

APPENDIX D. CONSIDERATION OF THE CUMULATIVE RISKS FROM MULTIPLE AOTS

When AOTs are evaluated for several components, then the cumulative risk from all these AOTs collectively need to be considered. If each AOT is determined to satisfy the criteria in the previous sections, then the question is, what is the cumulative risk effect of the criteria being satisfied. Consideration of the cumulative risk impacts will allow the criteria to be set such that the risks from each AOT, as well as the collective risks, are both acceptable.

The consideration of cumulative risk impacts is particularly pertinent when several AOTs are being evaluated at the same time (simultaneous evaluations). If AOTs or AOT extensions are being evaluated one at a time, then the most updated AOTs and test intervals are used in the calculations of the risk measures. By this updating, the cumulative effect thus is taken into account in a stepwise manner. Consideration of the cumulative impact discussed here is not a particular problem for one-at-a-time AOT evaluations, although the discussions will still give insights on establishing acceptable values for the criteria.

Criteria at the sequence level will be used as the examples. The guidelines which are developed for sequence criteria will also directly apply to criteria at the system, function, and overall risk level. The guidelines will transfer over to the system and the function criteria because of the interrelationships between accident sequence frequencies and system and function unavailabilities.

The criteria on the first risk measure controls the increased frequency F^+ during the AOT. There is no cumulative effect from different AOTs since, in general, component downtimes occur at different times. The exception is when several components can be down at the same time. As discussed previously, the effects of multiple components being down can be checked by calculating F^+ with these components down. If F^+ is larger than the criterion, then reliability assurance procedures can be instituted. The criteria are thus not affected or changed, but reliability assurance procedures are instead instituted.

The second risk measure, the increased probability in a given downtime, F^+d , is also not affected by cumulative risk considerations. Like the first measure, the criteria on the second measure controls the risk, in this case the increased probability, from a given downtime. There is no cumulative consideration since a given downtime is focused upon and controlled.

The above considerations also apply to the first and second risk measures at the system, function, and overall risk level. Since the associated criteria control the risk from a given component's downtime, there is no cumulative risk to be taken into account. If the first risk measure is too high, then reliability assurance activities can be instituted to reduce the risk.

However, cumulative risk considerations are pertinent for the third risk measure. For accident sequences, the third risk measure is the increased accident probability from accumulated downtimes in some future reference period. Absolute criteria on this measure will be considered, but the conclusions will also apply to relative criteria.

A given component AOT must satisfy (similar to Eqn. A-44) the absolute criterion:

$$w_i T F_i + d_i \leq \gamma \quad (D-1)$$

where w_i is the frequency of downtime occurrences of the component, say component i , F_i the increased frequency from the component being down, and d_i the component downtime.

As discussed in the previous sections, if the component appears in multiple sequences then F_i can be taken to be the maximum impacted frequency. As also previously discussed, the AOT can be determined by assuming the d_i is the AOT.

If there are L total components where AOT risks are to be controlled, then the collective risk, P , from these components is

$$P = \sum_{i=1}^L w_i T F_i + d_i \quad (D-2)$$

The quantity, P , is the total increased accident probability from all the component downtimes occurring in the reference period T . Hence:

$$P \leq L \gamma \quad (D-3)$$

If each component AOT is determined such that its associated increased accident probability is less than γ , then the sum of the accident probabilities will be controlled to be less than $L\gamma$.

For relative criteria, each component must satisfy

$$\frac{w_i F_i + d_i}{F_i} \leq \gamma \quad (D-4)$$

Hence, summing over the components:

$$\sum_{i=1}^L w_i F_i + d_i \leq \gamma \sum_{i=1}^L F_i \quad (D-5)$$

or

$$\frac{\sum_{i=1}^L w_i F_i^+ d_i}{\sum_{i=1}^L F_i} \leq \gamma \quad (D-6)$$

When several downed components appear in the same sequence, then the summation in the denominator of (D-6) will "double count" these sequence frequencies. As an illustration, assume two components are in the same sequence. Then:

$$w_1 \frac{F^+}{F} d_1 \leq \beta \quad (D-7)$$

and

$$w_2 \frac{F^+}{F} d_2 \leq \beta \quad (D-8)$$

where there is no subscript on F and F^+ since they are the frequencies of the same sequence.

Hence:

$$w_1 F^+ d_1 + w_2 F^+ d_2 \leq \beta(F+F) = 2\beta F \quad (D-9)$$

Therefore:

$$w_1 F^+ d_1 + w_2 F^+ d_2 \leq 2\beta \quad (D-10)$$

and the sum of the relative risks is less than 2β .

Equation (D-6) can consequently be modified to:

$$\frac{\sum w_i F_i^+ d_i}{\sum_{\text{unique}} F_i} \leq K\beta \quad (D-11)$$

where K is some number less than the total number of components being simultaneously evaluated.

In practical applications, K is the number of times the different downed components appear in the same dominant sequences. Thus, if each component AOT is determined such that the relative risk is less than γ , then the sum of the risks will be less than $K\gamma$. The multiple K is the number of times the different downed components appear in the same dominant sequences.

APPENDIX E. CRITERIA CONSIDERATIONS WHEN THE COMPONENT APPEARS IN MULTIPLE SYSTEMS

Introduction

The following sections describe considerations in establishing acceptable risk criteria when the component appears in multiple system, functions, or sequences.

System Criteria Considerations when the Component Appears in Multiple Systems

When AOT operating accident risk is addressed at the system level, then the first question that must be asked in evaluating a component AOT is, what systems contain the downed component. If more than one system contains the component, then consideration must be given to satisfying the criteria for each of the different systems.

Assume there are n different systems containing the same component whose AOT is evaluated. If the component AOT is to be determined such that the risk criteria are to be satisfied for each system, then each system needs to be separately evaluated to determine its Q^+ and Q to substitute into the criteria equations. The minimum AOT which is determined from these separate system evaluations is then the acceptable AOT for which the criteria are simultaneously satisfied for all the systems.

Alternatively, the maximum Q^+ , if absolute criteria are used on the maximum Q^+/Q if relative criteria are used, over all the pertinent systems, can be used in the criteria equations to give the acceptable AOT. Using the maximum impacted system will give the same acceptable AOT as evaluating the systems individually. The system giving the maximum Q^+ or the maximum Q^+/Q can often be selected without evaluating all the systems. This maximum system is the system most impacted by the component being down.

If the risks from the individual systems are controlled, then the sum of the accident risks are controlled. For absolute criteria, this means the increased accident sequence frequencies and probabilities are controlled to some absolute level. The particular absolute level will be determined by the system contained in the accident sequences, the number of dominant sequences considered, and the absolute criteria placed on each system risk measure.

If the system risks are controlled with relative criteria then the following considerations apply. For the first risk measure, by Eqn. (32) if:

$$\frac{Q_1^+}{Q_1} \leq \alpha \quad (E-1)$$

then

$$\frac{F_i^+}{F_i} \leq \alpha \quad (\text{E-2})$$

for each sequence i containing the system. Hence from E-2:

$$F_i^+ \leq \alpha F_i \quad (\text{E-3})$$

and summing over the sequences

$$\frac{\sum F_i^+}{\sum F_i} \leq \alpha \quad (\text{E-4})$$

Consequently, if the relative increased system unavailability is controlled to some level α for all n systems containing the component, then the relative increased accident frequency, summed over all the sequences containing the systems, will be controlled to this same level α .

Consider the relative criterion on the second risk measure. By Eqn. (33) if:

$$\frac{Q_i^+}{Q_i^T} \leq \beta \quad (\text{E-5})$$

$$\frac{P_i^+}{P_{oi}} \leq \beta \quad (\text{E-6})$$

Summing over the sequences containing the function (component) gives

$$\sum P_i^+ \leq \beta \sum P_{oi} \quad , \quad (\text{E-7})$$

or

$$\frac{\sum P_i^+}{\sum P_{oi}} \leq \beta \quad (\text{E-8})$$

From the above it is seen that if the second system risk measure is controlled to β , then the sum of the increased accident probabilities is controlled to β .

Consideration of the criterion on the third risk measure is completely analogous to that for the second measure. The result will thus simply be stated. Control of the third risk measure to β will control the sum of relative increased accident probabilities to be less than β .

Function Criteria Considerations When the Component Appears in Multiple Functions

If AOT risk is controlled at the function level and if the component appears in multiple functions, then each of these functions must be considered. Specifically, each different function needs to be considered when determining an AOT which satisfies the risk criteria. Since the considerations parallel those for system level control described in the previous section, only the important points will be highlighted.

To determine an AOT such that the risk criteria are satisfied for each function, each function unavailability may be evaluated and the acceptable AOT determined for that function. The minimum of the AOTs then gives the required AOT. Alternatively, and equivalently, the maximum $\hat{Q}^+$ for absolute criteria and the maximum $\hat{Q}^+/\hat{Q}$ for relative criteria, over the functions, may be determined and the acceptable AOT determined for this maximum impacted function.

If each function is controlled to some absolute criteria, then the increased frequency and probability of the accident sequences containing the functions will be controlled to some absolute criteria value. The particular absolute criteria value will depend upon the number of functions in each sequence, the number of (dominant) sequences considered, and the absolute criteria placed on each function.

If the relative increased function unavailability, $\hat{Q}^+/\hat{Q}$, is controlled to be less than α for all the functions, then the relative increased accident sequence frequency for all sequences containing the functions will be controlled to be less than α . The relative sum of the increased frequencies will also be less than α , compared to the baseline sum.

If the second (or third) risk measure for the function is controlled to be less than β then each increased accident probability containing the functions will be controlled to be less than β . The sum of the increased accident sequence probabilities will also be controlled to be less than β .

Sequence Criteria Considerations when the Component Appears in Multiple Sequences

If risk is controlled at the sequence level and the component is in multiple sequences, then the different sequences need to be considered in determining an acceptable AOT. The acceptable AOT for each sequence may be determined, and the minimum AOT then selected. Alternatively, the sequence with maximum F^+ for absolute criteria or with maximum F^+/F for relative criteria can be determined, and the acceptable AOT determined for this maximum impacted sequence.

If the increased frequency F^+ of each sequence is controlled to be less than α_1 , then the sum of the dominant increased sequence frequencies will be less than $M\alpha_1$, where M is the number of dominant sequences containing the component. If the increased relative frequency F^+/F is controlled to be less than α_2 , then the sum of the increased relative frequencies will be less than α_2 compared to the baseline sum.

With regard to the increased accident probabilities of the second and third measures, if each accident sequence is controlled to some absolute criterion β_1 , then the sum will be controlled to the absolute criterion $M\beta_1$. If the relative increased probabilities are controlled to be less than β_2 for each sequence, then the sum of the relative increased probabilities will be controlled to be less than β_2 with regard to the baseline sum.