SKI Report 95:67

Analysis Tools for Reliability Databases

Joan Dorrepaal

January 1996

ISSN 1104-1374
ISRN SKI-R--95/67--SE

SKI
STATENS KÄRNKRAFTINSPEKTION
Swedish Nuclear Power Inspectorate

SKI Report 95:67

Analysis Tools for Reliability Databases

Joan Dorrepaal

RISÖ National Laboratory,
DK-4000 Roskilde, DENMARK

January 1996

gotab Stockholm 1996

Foreword:

Ir. Joan Dorrepaal's post-graduate work at RISÖ National Laboratories mainly during 1995, was evaluated by a supervisory committee at the TU Delft on 1995-12-15.

Two evaluations were given, one relating to the quality of written and verbal presentations, and the other relating to Ir. Dorrepaal's overall helpfullness, initiative and originality during his project work. Both evaluations were very high (= 9 on a scale of 10).

The analytic tool which Ir. Dorrepaal made during his post-graduate work, will be used and furter tested in March-April 1996, by Prof. R.M. Cooke from TU Delft and Prof. Hokstadt from SINTEF, in studies concerning various models about degraded failure modes, competing risks and other active theoretical issues. The outcome of this work will be better analytical tools and new possibilities to use information in reliability databases.

SKI, Stockholm, 1996-02-08

The work presented in this report is performed against the contractor SKI, under the contract; SKI 94441, Dnr 14.2 - 941451.

The work is also performed for SKI, within the SKI program "Plant Safety Assessment".

Preface

This report outlines the work done in subproject 3 of NKS-RAK-1 (Scandinavian research program on reactor safety) on *maintenance strategies and ageing* under contract with SKI (Swedish Nuclear Power Inspectorate). In this work we have developed analysis tools that will be installed at the TUD[1] reliability database. The TUD database is built to support the maintenance staff at the nuclear power plants (NPPs) and the risk/reliability staff both at the NPPs and at SKI. The analysis tools developed in this work are meant to make the data analysis easier for these users by guiding them through the steps of a general reliability analysis of a group of components of their choice.

The work is performed at the risk analysis groups in the Technical University Delft and Risø, national laboratory and financed by SKI. The work is supervised by Prof. R.M. Cooke from the Technical University Delft, J.L. Paulsen from Risø, national laboratory and R. Nyman from SKI. They gave me the important feeling that I belonged to their "team" and I'm glad that I can continue working with them in 1996. In this context I would also like to thank Dr. K.E. Petersen, head of the risk analysis department at Risø for his corrections and suggestions for improvement of early draft versions of this report.

I'm grateful to M. Clementz of the maintenance department of Barsebäck and J. Jönsson and P. Jacobson of the risk/reliability department at Sydkraft Consultancy. They could answer many of my questions concerning the background of the operating experience data that is stored at the TUD database. I acknowledge the assistance of S. Skagerman and L. Pettersson from the TUD office in supplying me with all the data I asked for.

Further, I would like to stress that I have greatly profited from the work of Prof. J. Møltoft from Denmarks Technical University and Prof. D.R. Cox. Most of the analysis tools developed in this work are based on insights I got through reading their clearly written work.

J.W. Dorrepaal

Technical University Delft
Risø national laboratory
january, 1996

[1] An acronym, for Tilforliglighed-Underhal-Drift or Reliability-Maintenance-Operation

Contents

Summary

This report outlines the work performed at Risø national laboratory, under contract with SKI (Swedish Nuclear Power Inspectorate). The main goal of the work is to develop *analysis tools for reliability databases* that can suit the information needs of the users of the so called TUD [2] database, which is a reliability database (RDB) for 12 nuclear power plants (NPPs) in Sweden and 2 NPPs in Finland. The TUD database stores operating experience data in the form of the failure reports, filled in by the maintenance engineer, that describe the failures and the resulting repair jobs on a large part of the equipment at the NPPs. Furthermore, the TUD contains background data on operating conditions, design, maintenance and test programs on the equipment at the NPPs and registers the changes in operating modes of each NPP (cold shutdown, hot shutdown etc).

As NPPs get older, the equipment in the safety and process systems reach an age where the failure data may be observed to deviate from those predicted by the manufacturer. The equipment may experience a "mid-life crisis" and maintenance performance should be reviewed with the purpose of re-optimizing safety and productivity. It turns out that with the proper analysis tools installed, the TUD database is especially powerful in identifying this deviating equipment.

The users of the TUD database are mainly the maintenance staff and the risk/reliability staff both at the power stations and at SKI. Since 1993 the TUD is structured as a multi-user relational database. The users have direct access to the TUD database through a personal computer that is connected to the server on which the TUD database runs. This so called "client server" application makes it possible for the users to, on line, retrieve and analyse the information at the TUD database as well as supplying data to it.

In this work it is shown that the current multi-user relational database structure of the TUD system can give its users a *broader perspective* on maintenance performance and safety. Naturally, one can expect that a maintenance engineer has a good understanding of the current state of the equipment (s)he is responsible for. Yet, one can ask oneself the question whether this current state is better than, say five years ago or what the current state is of the whole process/safety system in which the equipment functions. These are examples of questions that require a broader perspective on reliabilty and costs. This broader perspective can be acquired with the analysis of proper (historic) operating experience data. The TUD database supplies this opererating experience data.

[2] An acronym for Tilforliglighed-Underhal-Drift or Reliability-Maintenance-Operation

The structure of the TUD database makes it possible for the users to have an enormous flexibility in building a pool of component sockets for analysis. For example, the TUD user can decide to look at the behaviour of a population of component sockets of the same type or (s)he can choose to investigate a system as a whole and compare the performance with similar systems or component sockets in other NPPs. The analysis tools developed in this work are the result of going through the following analysis steps:

step 1. Investigate and select the data;

step 2. Make simple plots of the data;

step 3. Analyse the data with statistical methods, including analysis of trend and dependency;

step 4. Combine and implement these three steps in a prototype RDB with an easy user-interface.

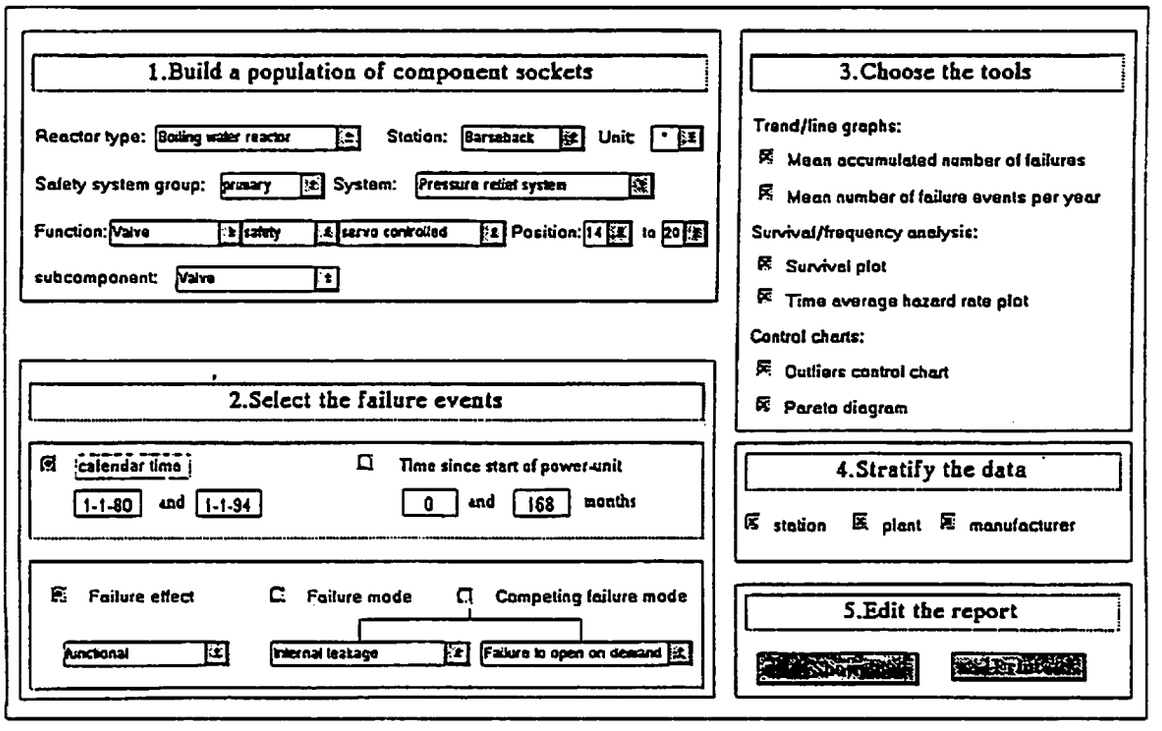


Figure 0.1: Analysis user-interface for a reliability database

The resulting user-interface of the prototype RDB developed in this work, guides the user through the following steps:

4a Build a population of sockets (subcomponent or component level);

4b Select the time-window and the failure events;

4c Select the analysis tools to be incorporated in the report;

4d Adjust the default report and print the report.

Examples of "simple" analysis tools for a reliability database are given in figure 0.2.

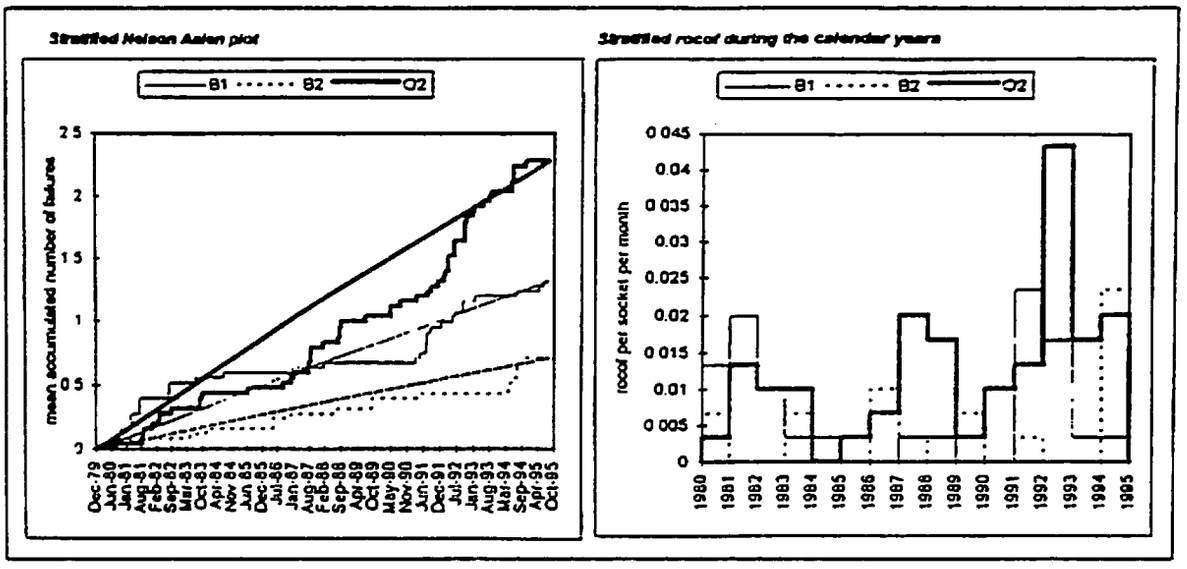


Figure 0.2: Examples of analysis tools for a reliability database

The prototype RDB developed in this work, shows that when the proper analysis tools are installed, the TUD database can help its users in identifying possible common cause failures and trends in reliability and costs of a population of component sockets. Furthermore, the influence of test/maintenance programs, operating conditions and design can be checked by stratifying the population of component sockets on these criterea.

Chapter 1

Background

1.1 Introduction

This report outlines the work performed in 1995 at Risø national laboratory, under contract with SKI [1]. The main goal of the work is to develop *analysis tools for a reliability database* that can suit the information needs of the users of the TUD [2] database, which is a reliability database (RDB) for 12 nuclear power plants (NPPs) in Sweden and 2 NPPs in Finland.

The work is part of the NKS-RAK-1 [3] project concerning maintenance strategies and ageing. As NPPs get older, the equipment reach an age where the failure data may be observed to deviate from those predicted by the manufacturer. The equipment may experience a "mid-life crisis" and maintenance performance should be reviewed with the purpose of re-optimizing safety and productivity. One of the results of this work is that a RDB like the TUD database is especially powerful in identifying this deviating equipment. Furthermore, it is shown that the database strucure of the TUD system is especially suitable for giving its users a broader perspective on maintenance performance and reliability of large groups of equipment like a process/safety system as a whole or a group of component sockets of the same type. This broader perspective can lead to new insights and possible improvements.

For a RDB like the TUD database, at least three types of users can be distinguished:

1. *The risk/reliability staff*, wishing to predict reliability of complex systems and equipment at the nuclear power station;

2. *The maintenance staff at the power station*, interested in measuring and optimizing maintenance performance;

3. *The component designer*, interested in optimizing component performance.

[1] Swedish abbreviation for Swedish Nuclear Power Inspectorate
[2] An acronym for Tilforliglighed-Underhal-Drift or Reliability-Maintenance-Operation
[3] Swedish abbreviation for Scandinavian Nuclear Safety Program-Reactor Safety-project 1

Discussions with the TUD office led us to conclude that only the first two groups of users are considered as users of the TUD database. In this work we have therefore concerned ourselves with the development of tools that can suit the information needs of the maintenance staff and the risk/reliability staff both at the power stations and at SKI. From now on we will call these two groups of users the *TUD users.*

The TUD database contains failure reports and engineering reports on a large part of the equipment in the process and safety systems at the NPPs. Further, the TUD registers the changes in operating modes of each NPP. Since 1993 the TUD users have direct access through a personal computer to the server on which the TUD database runs. This so called "client server" application makes it possible for the users to retrieve and analyse the information at the TUD database as well as supplying data to it. The resulting information feedback loop is illustrated in figure 1.1.

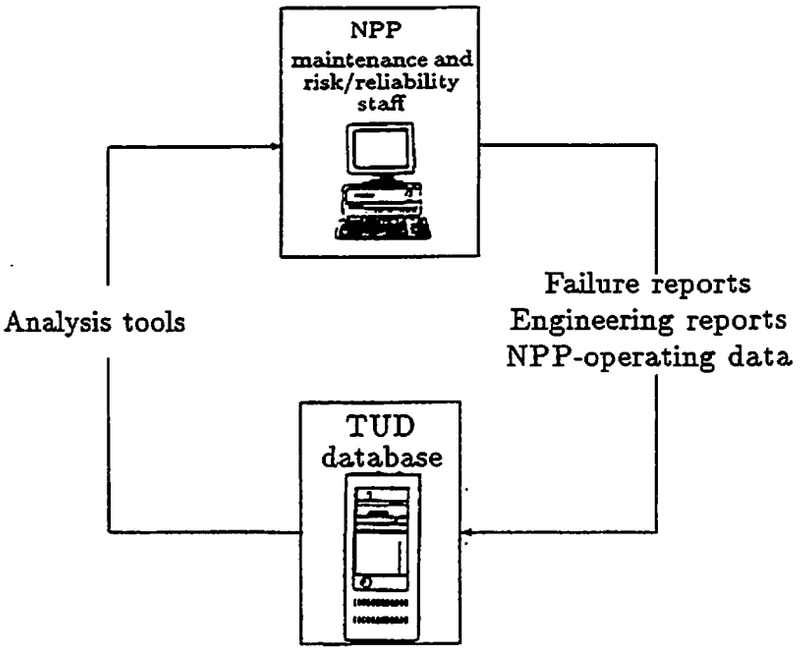


Figure 1.1: Operating experience feedback loop

Currently, the information at TUD database is mainly used for the Swedish T[4]-book [T-book, 1995] of which an updated version comes out every second year. The T-book provides reliability parameters for the unavailability computations that are done for the safety-critical equipment at the NPPs as part of the probabilistic safety assessments (PSA). Hence, the T-book only considers safety critical failure events. The other main source of information for the T-book are therefore the Licensee Event Reports (LER) assembled at SKI. The data processing methodology used for the T-book, is described in [Pörn, 1990] and reviewed in [Cooke et al.,1995].

[4]An acronym for Tilforliglighed or Reliability

The (feedback) analysis tools developed in this work are supposed to be installed at the TUD database. The idea is that the TUD database provides a simple user interface that enables the user to easily select the equipment (s)he wants to analyse together with the analysis tools. Next, the tools convert the "raw" TUD data on the selected equipment into a number of simple plots with numerical support. These plots show different aspects of the data and together form a report on the selected equipment. By installing the tools at the TUD database, the TUD users can make updates of that report anytime.

The main problem of the TUD database has been the lack of motivation of the personnel in the maintenance departments to report failures to the TUD database. At many stations the maintenance personnel does not make use of the TUD database, and will consequently not be very happy with the extra effort this reporting demands of them. Improving the operating experience feedback can improve the motivation of the station personnel responsible for the failure reporting and consequently improve the quality of the failure reporting.

1.2 Goals of the work

The main goal of this work is to supplement SKI's interest in the development of new methods, which can use the information in the TUD database and LERs for maintenance and safety purposes. These new methods are planned to be installed at the TUD office and used by the NPP staff. The users are mainly staff members working with maintenance and safety problems. Moreover, the methods have to support the investigators and inspectors at SKI in their analysis work concerning nuclear safety. The following subtasks are defined by SKI order 94441:

- Discuss maintenance problems in the Nordic NPPs;
- Develop measures for maintenance performance;
- Investigate the type of data available to elicit the problems;
- Develop methods for indicating maintenance performance based on the merged data;
- Describe and discuss the problems for the users of the maintenance data;
- Describe the use for the regulatory body SKI of the methods developed.

This work is part of the NKS-RAK-1 project, the projectmembers of NKS-RAK-1 have chosen several common accident sequences to illustrate their methods. These accident sequences concern, along others, two safety systems at the boiling water reactors (BWR) in Sweden and Finland; the pressure relief system (314) and the core vessel spray system (323) respectively. In connection with our work, we are asked to look at:

- Ageing aspects for the 314 system especially the control and pilot valves;

- Maintenance and ageing aspects for 323 low pressure part, control, valves and pumps.

In the remaining part of the report we will refer to all these systems as the *benchmark systems.* Descriptions of these systems are given in appendix B.

1.3 Outline of the report

This report describes the steps that are followed in this work. We started our work with the investigation of the type of data available at the TUD database, STAGBAS [5] and the local maintenance database for the equipment in the benchmark systems. Chapter 2 starts with an overview of these different databases and their relation to the TUD system. Next, the contents of the TUD failure reports, engineering reports and unit operating time readings are described. A big part of the work concentrated on investigating which aspects of the data are useful for processing with analysis tools. The conclusions of this work are described in the last section of chapter 2.

The objective of the data analysis should guide the development of the analysis tools. The main objective of the analysis is already stated in the projects workorder: measuring maintenance performance. Yet, we have made a further investigation into the objectives or information needs of the TUD users, which is described in Chapter 3. Chapter 3 describes the information needs of the maintenance staff and risk/reliability staff at the station and at SKI.

The goal of the work is the development of analysis tools that suit the information needs of the TUD users. During the development of (in our opinion) useful tools we went through the following steps:

step 1. Investigate and select the data;

step 2. Plot the data;

step 3. Statistical analysis of the data including analysis of trend and dependency;

step 4. Combine these steps in a prototype RDB.

Most of this work is based on methods developed within the field of reliability analysis (repairable systems analysis see [Ascher and Feingold, 1984]). In addition, ideas from the theory of quality control are used to easily present the data and the results of the analysis.

For the statistical analysis in step 3, probabilistic models are developed for which the mathematical background is given in appendix A. In this appendix the appropriate models for the failure/repair process of a repairable component socket are discussed. These models differ in the assumptions they make on the failure/repair process, and their plausibility is therefore evaluated.

[5] Database for Licensee Event Reports

In order to check the usefulness of the developed analysis tools, once they function on the TUD system, we have chosen to build a prototype RDB in Microsoft Office's relational database package ACCESS. We have loaded this prototype RDB with the TUD data we received for the benchmark systems. The prototype RDB gives us many new insights in the functioning of the TUD system and shows that the flexibility of this system is the key for the successful use of many of the tools.

The extra benefit of creating our own database is that it is now easy to incorporate the LERs and even the local maintenance data in this database system. This way we can judge the accuracy of our tools based only on the TUD information compared to the situation where all experience data is available. This work will be carried out in 1996.

As described in the previous section, part of this work is to run the developed analysis tools on the TUD data on the equipment in the benchmark systems. The results of this data processing is described in Chapter 5. During the work we have discussed our ideas with members of the maintenance staff at the power station, and the risk staff at the power station and SKI. The discussion of the prototype RDB is done together with:

- Mats Clementz (maintenance engineer at Barsebäck)
- Peter Jacobsson (risk analyst at Barsebäck)
- Jerry Jönsson (consultant at Sydkraft)
- Stig Olsson and Patrick Lindell (SKI inspectors)

and will be briefly described in chapter 5. The work planning of 1995 is given in the table below.

Table 1.1 : *Project planning 1995*

	feb	mar	apr	may	jun	jul	aug	sep	oct	nov
Investigate and classify the data	•	•	•	•						
Analyse data and develop tools			•	•	•	•				
Model the failure/repair process					•	•				
Identify the information needs								•		
Discuss the tools wit the users									•	
Make a prototype program							•		•	•

Chapter 2

Investigation of the data collected at the TUD database

2.1 Introduction

In this chapter we investigate the TUD data available on equipment at each of the 12 NPPs in Sweden and for 2 NPPs in Finland. For the equipment at these NPPs there exist four main information systems that contain operating experience data:

1. TUD database

   The TUD database contains engineering reports and failure reports on subcomponent socket level for 12 NPPs in Sweden and 2 NPPs Finland. Further, one can find the NPP operating time readings at TUD. The type of data at the TUD will be further explained in the next section of this chapter.

2. STAGBAS

   STAGBAS contains ROs [1] that give information on safety related failure events, including an analysis of failure causes, consequences and corrective actions taken. Since the ROs concern critical events, only the critical failure events that lead to a repair on that same component socket correspond to a failure report in the TUD system. Consequently, STAGBAS only contains a fraction of the failures reported to the TUD system. STAGBAS is currently being modified and will function as a modern relational database much like the TUD system. This means that the analysis tools developed for the TUD system can be easily installed at STAGBAS as well.

3. Local maintenance information systems

   The local maintenance information systems are computerised systems for the processing of work orders. These workorders are based on predefined

[1] Swedish equivalent of Licensee Event Reports (LERs)

planned tests and maintenance actions, as well as on reporting of failures discovered during plant operation and outages.

After a detection of a failure at Barsebäck the maintenance engineer fills in a failure report which results in a workorder for a corrective maintenance job. Yet, a workorder can also be generated based on a preventive (not result of a failure) maintenance job. Next, the maintenance engineer receives a work permit and can start with the maintenance work. After the maintenance is performed the maintenance history will be incorporated in the failure report which will eventually be included in the TUD database. It is possible that during the preventive maintenance job a failure is detected, this failure will be reported to the TUD as well. The maintenance engineer follows the sequence:

failure report $\Rightarrow$ work order $\Rightarrow$ work permit $\Rightarrow$ maintenance history in failure report

4. KSU's database on plant disturbances and scram reporting

   KSU runs a computerized information system covering data on plant disturbances and safety-related occurrences. The TUD incorporates the NPP operating history part of this database.

Operating experience databases such as described above are part of a good functioning reliability/safety program. Such a reliability/safety program should be integrated in all the phases of the life cycle of the equipment at the NPPs, from design to operation. The next figure reflects the result of a good functioning reliability program on the reliability of the equipment throughout the different phases of the equipments lifecycle and the role of an operating experience database.

Nuclear equipment, e.g. safety systems, are complex, high technology systems that must operate for long periods of time without serious failure and with a very long total life. A great amount of redundancy and diversity is used in nuclear facilities to ensure the safety of the plant. A large portion of the safety systems operate remotely while depending on human operators for control functions. Repairs, inspections and overhaul of equipment are usually done at specific time intervals, when the plant is down for nuclear refueling. This process generally follows a pattern of increasing complexity, depending on the operating times accumulated by the systems.

The physical environment in which the equipment operates is very severe and can have a serious detrimental effect on the complex mechanical and electronic components of the equipment. High temperatures, high vibration, high humidity and the presence of corrosive fluids and gases take their toll. This means that throughout its operating phase, the reliability characteristics may start deviating from those predicted by the supplier. A reliability database (RDB) like the TUD database can help establishing these deviations. As discussed in Chapter 1, we can distinguish three types of users for the TUD database; the component designer, the maintenance staff at the power station, and the risk/reliability staff.

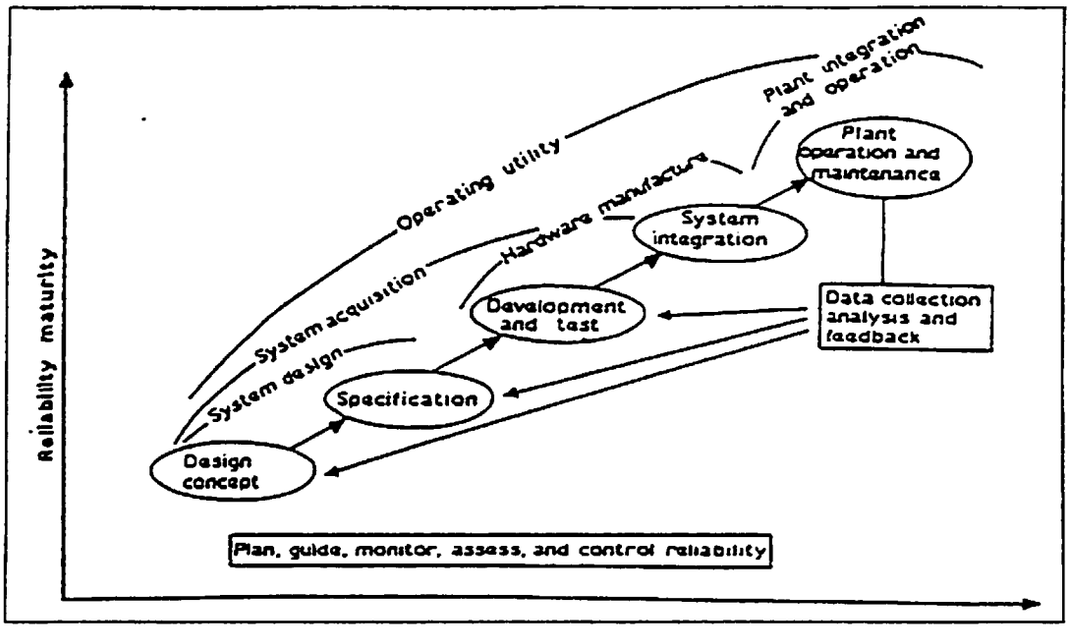


Figure 2.1: Equipment life cycle

The role the TUD database plays in the reliability/safety programs at the NPPs and in the Nordic research programs, is to give its users *a broader perspective* on issues concerning safety, reliability, maintenance and costs of the equipment at the NPPs. This way, the different types of users can isolate areas of their concern and establish priorities for further investigation.

In the next chapter we try to define the objectives of the maintenance staff and risk/reliability staff and explore their information needs. In this chapter we take a look at the "raw" data which lies in the TUD-database.

2.2 Type of data collected

The TUD database contains failure reports, engineering reports (background data describing the observed equipment) and unit operating data from certain equipment in twelve Swedish and two Finnish nuclear units.

In the TUD database, the repaired equipment is classified up till the level of the subcomponent sockets. A socket is a functional position in a system, occupied by one component during one service sojourn. The component socket i.d. consists of the system number and the functional position within the system. The subcomponent i.d. consists of the component socket i.d. and the subcomponent type. Now for each combination of NPP i.d. and socket i.d. the TUD database can supply

- Engineering reports;

- Failure reports;

- NPP operating data.

Engineering reports

Table 2.1 : *Contents of the engineering reports on component socket level and on subcomponent socket level*

Content summary on component socket level

Plant	Socket	Operating modes	Maintenance	Subcomponents
• Station • Unit	• System • Position	• Percentage of total operating time • Dates of activation of changes of operating modes	• Interval/frequency	• List

In this work, we have used these reports to create a table that contains the subcomponent sockets per component socket i.d. The use of this table will become clear in chapter 4, where we describe the developed prototype RDB.

Clearly, the fields *Operating modes* and *Maintenance* can be used for a detailed analysis of the component sockets behavior and maintenance performance. Nevertheless, we have not yet incorporated these fields in our analysis tools and consider that work for future projects. Ideas for using the *Maintenance* field are given in [Laakso et al., 1995].

Table 2.2 : *Contents of the engineering reports on subcomponent socket level*

Content summary on subcomponent socket level

Plant	Socket	Manufacturer/design	Operating data
• Station • Unit	• System • Position • Subcomponent	• Code for manufacturer • Type designation • Codes for design	• First start time • End of follow up • Operating environment -internal -external • Descriptive codes for operating mode and circumstances

From these reports we have formed a table that contains the subcomponent i.d. together with the information that lies in the *manufacturer/design* field. An extract of this table is given below.

Table 2.3 : *Example of an extract of the engineering reports*

NPP		Socket			Type	Manufac	Start
STN	BLK	SYS	Position	subcomponent		turer	operate
B	1	323	P001	Electrical motor		ASE	1-oct-76
B	1	323	P001	Other electronics			1-oct-76
B	1	323	P001	Sensor			1-oct-76
B	1	323	P001	Pump	CE	KSB	1-oct-76
B	1	323	P002	Electrical motor		ASE	1-oct-76
B	1	323	P002	Other electronics			1-oct-76
B	1	323	P002	Sensor			1-oct-76
B	1	323	P002	Pump	CE	KSB	1-oct-76

This table is included in the prototype RDB so that it is possible for the user to pool subcomponent sockets of the same design and compare performance of subcomponents from different manufacturers. The other fields in these engineering reports on subcomponent level are not incorporated in the development of the analysis analysis tools. We have made this restriction due to a limitation in time for this work and future work should include these fields.

Failure reports

Table 2.4 : *Contents of the failure reports*

Content summary on (sub)component socket level

Plant	Socket	Failure fields	Repair fields	Text
• Station	• System	• Detection date	• Code for repair action	• Failure
• Unit	• Position	• Codes for:	• Date start repair	- observation
	• Subcomponent	-Detection mode	• Date replenished	- type
		-Effect of failure		- cause
		-Type of failure		• Repair
				- action

The part of the TUD database that contains the failure reports gives information on the socket time histories. A service sojourn of a socket begins when a new or repaired (sub)component goes on line, and terminates when the (sub)component is removed for any reason whatsoever. In this work we have formed a table based on all fields of the failure reports, except the explanatory text. This table forms naturally the basis of the failure data analysis and an extract is shown below.

Table 2.5 : *Example of the failure reports for the 323P001 and 323P002 pumps from 1980 onwards*

NPP		Socket			Failure fields				Repair fields				
STN	BLK	System	Position	Subcomponent	Failure detection	Detection date	Failure effect	Type failure	Repair action taken	Start repair	Start available	Man	Manhours
B	1	323	P001	Pump	C	08/7/83	L	J	C	08/7/83	21/7/83	3	312
B	1	323	P001	Pump	B	04/9/91	K	E	B	08/1/92	08/1/92	2	14
B	1	323	P002	Pump	D	18/3/81	L	E	C	18/3/81	18/3/81	3	16
B	1	323	P002	Pump	D	03/5/91	K	E	C	04/5/91	04/5/91	3	33
B	1	323	P002	Pump	D	08/1/92	K	E	B	09/1/92	10/1/92	2	32

The failure fields of the TUD failure reports give respectively the code for the method of detection, the part that failed, the codes for failure effect and the failure type. The repair fields give respectively the code for type of repair, the data-time that the (sub)component was taken out of service for repair, the date-time that the (sub)component was replenished, the number of men used and the manhours spend on the repair job.

Table 2.6 : *Failure and repair field coding*

Failure detection		Type of failure		Action taken	
A	Alarm	A	Fracture/Crack	H	Replacement of component with new item
B	Operation supervision and service observation in controlroom	D	Internal tube leakage		
		E	External sealing leakage		
H	Operation supervision and service observation otherwise	F	Internal sealing leakage	B	Replacement of component with same item
		G	Deformation, displacement		
C	Preventive maintenance	H	Vibration noise		
D	Test	I	Deposit,blockage	C	Repair no replacement
E	Inspection	J	Biting, seizure		
G	Real demand	L	bad contact	D	Replacement of part of component
		M	Open circuit		
Effect of failure		N	Ground/Insulation fault	Z	other (cleaning, lubrication
A	Won't clode/stop/disconnect	O	Short circuit		
B	Won't open/start/connect	P	Out of adjustment		
C	Spurious close/stop/disconnect	R	base program fault		
D	Spurious open/start/connect	S	Application program fault		
E	Signal (measuring value) fails	T	database fault		
F	Spurious signal	U	Corrosion, erosion, wear		
G	faulty measuring value (signal)	W	Operating error		
H	faulty regulation (governing)	X	Unidentified fault		
K	Other functional failure	Y	Control equipment fault		
L	Non-functional obstruction	Z	Other		

NPP operating data

The TUD database contains information on the operating history of the NPPs. This operating history is given by the time instances at which the operating conditions are changed. The identified operating conditions are:

- cold shut down;
- hot shutdown/hot standby;
- start/stop process;
- power operation.

Together with these conditions, the turbine trips and reactor scrams are also given.

2.3 Aspects of the data of importance for the analysis

In this section we discuss those aspects of the data that have influenced the development of the analysis tools. Naturally, there are information needs that cannot be fulfilled with the part of the sockets operating history that lies at the TUD database. This section is meant to describe the boundaries that we encountered during this work. Furthermore, the quality of the data will be briefly discussed. A report that concerns this issue is to be expected soon in the SKI reporting series.

The following boundaries of the information at the TUD database were encountered during this work:

(i) *The TUD database records only the repair actions and not the preventive maintenance actions although these actions have a big influence on the reliability of the component*

In the introduction of this chapter, the sequence that results in a failure report for the TUD office is described. It showed that the workorders that are part of the preventive maintenance program, will not be included in the TUD database unless a failure was detected during this preventive maintenance job.

To illustrate the problems we run into when we want to judge the quality of the maintenance service, we give the full maintenance history on B2-311V005, taken from the local maintenance information system at Barsebäck (BVT) and compare that with the data at the TUD database on this socket.

Table 2.7 : *Example of local maintenance data and TUD failure reports on a component socket*

B2-311V005 in period april-87 to feb-1990			
	Date	Description	Class
BVT reports:	28-sep-87	*Functional test*	
	18-jan-88	Replace of split pen	CM
	10-feb-88	*Tightness test*	
	27-jul-88	*Functional test*	
	6-sep-88	*Tightness test*	
	15-sep-89	Repair of drainagepipe	CM
	10-oct-89	*Functional test*	
TUD reports:	11-sep-89	Repair of packing	CM

source: Barsebäcks local maintenance databae (BVT) and TUD database
PM = preventive maintenance; CM = corrective maintenance

(ii) *The failure cause cannot be read from the failure fields*

A consequence of the fact that the failure report is filled in before the actual maintenance job starts, is that the failure cause is usually not known at that stage. Due to the fact that this field was not always filled in after the repair job was finished, the TUD failure reports no longer contain this field.

In [Cooke et al.,1995] the design of a modern reliability database is discussed. Here the failure fields in the failure reports differ slightly from those in the the TUD-database. The failure fields contain the method of detection, the failure mode, the failure cause, the failure mechanism and the functional consequence of the failure respectively. Information on the failure mechanism and failure mode can be read from the failure field codes. The table below shows how to classify the failure mode of a valve socket from the codes.

Table 2.8 : *Failure mode classification of a valve component socket*

TUD failure field code		Failure mode
Effect of failure on item	Type of failure	
A		Failure to open on demand (FTO)
B		Failure to close on demand (FTC)
C		Spurious closing (SPC)
D		Spurious opening (SPO)
	F	Internal leakage (INL)
	A, E	External leakage (EXL)
E,F,G		Abnormal instrument reading(AIR)

(iii) *The repair fields do not contain the maintainable parts that are repaired*

When we want to process the operating experience data to support the maintenance staff, we would like to be able to distinguish which maintainable part of the component socket was repaired. In the table below we give an example of how the subcomponents can be further subdivided in maintainable parts.

Table 2.9 : *Maintainable parts of a valve*

Equipment unit:	Valve		
Subcomponents	Valve	Actuator	Control and monitoring
Maintainable parts:			
	Valve body	Diaphragm	Control unit
	Bonnet	Spring	Monitoring
	Seat rings	Case	Actuating device
	Packing	Piston	Power supply
	Seals	Stem	
	Other valve	Indicator	
	components	Seats/gaskets	
		Pilot valve	
		Positioner	
		Gear	
		Other actuator	
		components	

(iv) *There are not always suitable codes for describing the failure event and/or repair action*

The failure/repair codes given in table 2.6 are often not suitable for classifying the failure event and/or repair action. In that case the maintenance engineer, responsible for the failure report, has to take the general code (other failure type, other failure effect or other repair). With this general code the data analysis with the help of a computer is less powerful. Still, the explanatory text in the failure report explains the failure event and repair action taken, when the user wants to read the reports.

(v) *The operating experience data of a component is related to the socket at which it failed and not to the component itself*

This is a subtle difference, it can be the case in a system with built in redundancy (for example the 314 system) that different components are entering and leaving the sockets. This can result in the problem that we can spot the weak sockets (positions in the system) but we cannot trace weak components.

(vi) *Failures of a socket are only reported to the TUD when the failure results in a repair action*

In the introduction we explained that a failure report is written when a maintenance engineer wants a work permit to repair the failure. A functional failure of a socket can, however, be the consequence of a failure of equipment that is not considered to be part of that socket. This failure event is reported as a failure report of the equipment that is repaired.

On the other hand, STAGBAS does link the critical failure events to the socket that critically failed. It is thus only possible to give accurate estimates of critical failure rates on the basis of the operating history stored in the TUD database and STAGBAS together.

There are two aspects of the quality of the data that should be considered when we want to draw conclusions from the analysis.

(vii) *Not a 100 % coverage of the recording*

There does not exist a 100 % coverage of the failure reports on the actual repairs that occur at the component sockets. An investigation is made at the TUD office concerning this problem and will result in a SKI-report.

(viii) *No homogeneity of the reporting among different stations*

When we see differences in the number of failure events in similar groups of equipment at different stations, this can be due to better maintenance performance or to heterogeneity in reporting among the different stations. Inter-station comparisons or pooling of similar equipment at different stations should therefore be handled carefully.

Chapter 3

Description of TUD users and their information needs

3.1 Introduction

The goal of this work is to develop reliability data analysis tools that can can be installed at the TUD database and support the work of the TUD users; the maintenance staff and the risk/reliability staff both at the nuclear power station and at the regulatory body, SKI. The (feedback) functioning of these tools is illustrated in figure 1.1. In this chapter the work and objectives of the TUD users are roughly described, resulting in a list of applications of the TUD databse.

The regulatory body, SKI is installed by the Swedish government to secure the safety of the public. SKI supports the Nordic research efforts (NKS) in the area of nuclear safety of which this work is a part. SKI's demand on the equipment at the NPPs is that of safe/reliable functioning. The utilities demand the equipment to be *operational cost-effective.* However, cost-effectiveness and reliability/safety are closely connected at a nuclear power station. SKI has the authority to shut down the NPP in the case of risk situations. The large cost of NPP down time provides an economic incentive towards maintaining the reliability at the equipment at the accepted level.

For the purpose of preserving both operational cost-effectiveness and safety at the power stations, the utilities have employed a maintenance staff and a risk/reliability staff at the power station. Broadly speaking, the maintenance staff has to keep the equipment operational cost-effective within the reliability restrictions set by the risk/reliability staff in the safety technical specifications (TS). In addition, the risk/reliability staff searches constantly for scenarios that can effect the safety of the power station and tries to find means to lower their rate of occurrence.

In the following sections we describe the work and information needs of the TUD users.

3.2 Maintenance staff at the nuclear power station

The task of the maintenance staff is to make an overall cost-effective maintenance program for the equipment at the NPP that meets the safety/reliability requirements set by the risk/reliability staff in the safety technical specifications.

The systems and equipment used in the NPPs are sophisticated, complex, difficult to maintain and expensive. They are expected to operate for long periods of time without serious failure and must have a very long total life. Typically, the physical environment in nuclear plants is severe and can have serious degraded effects on the equipment. A large portion of the safety systems (which are of main concern for SKI) operate remotely while depending on human operators for control functions. From these considerations we recognise the importance of a good maintenance program when the reliability of the equipment at the plant has to be preserved. A good maintenance program takes care of:

- Cost-effective maintenance scheduling that keeps the equipment sufficiently reliable throughout its life cycle;
- Providing the maintenance personnel with the necessary skills, knowledge, resources and support to perform their maintenance actions properly.

The different aspects of a good functioning maintenance program are described in the work of [Sandén and Chockie, 1994]. The TUD database with the proper tools installed, is able to support especially the first aspect of a good maintenance program which is on a management level. In building a cost-effective maintenance schedule there are two major classes of maintenance actions that can be distinguished:

1. *Preventive maintenance* aims to reduce the probability of failure, and can be divided into two subclasses:

   a. systematic or scheduled maintenance; replacement or revision of parts of components at predetermined moments in time

   b. condition based maintenance; the decision to replace or revise is made according to the outcome of a diagnostic study under for example test, inspection or continuous monitoring

   The implementation of preventive maintenance can result in the detection of potential faults and shifts in performance specifications for correction prior to an actual equipment failure. In addition, periodic preventive maintenance also increases the familiarity of the technician with the functional and service aspect of the equipment.

2. *Corrective maintenance* is the repair after failure. The repair activity can be subdivided into:

a. Planned repair; repair action can be postponed and suitably planned

b. Emergency repair; repair or rectification as soon as possible

Failures of equipment in safety systems are demanded to be repaired within a limited amount of time. This emergency maintenance cannot be planned in advance and in some cases requires a costly NPP shutdown. ($ 1.000.000 per day)

Figure 3.1 illustrates the relationship between preventive maintenance, corrective maintenance, equipment reliability and costs.

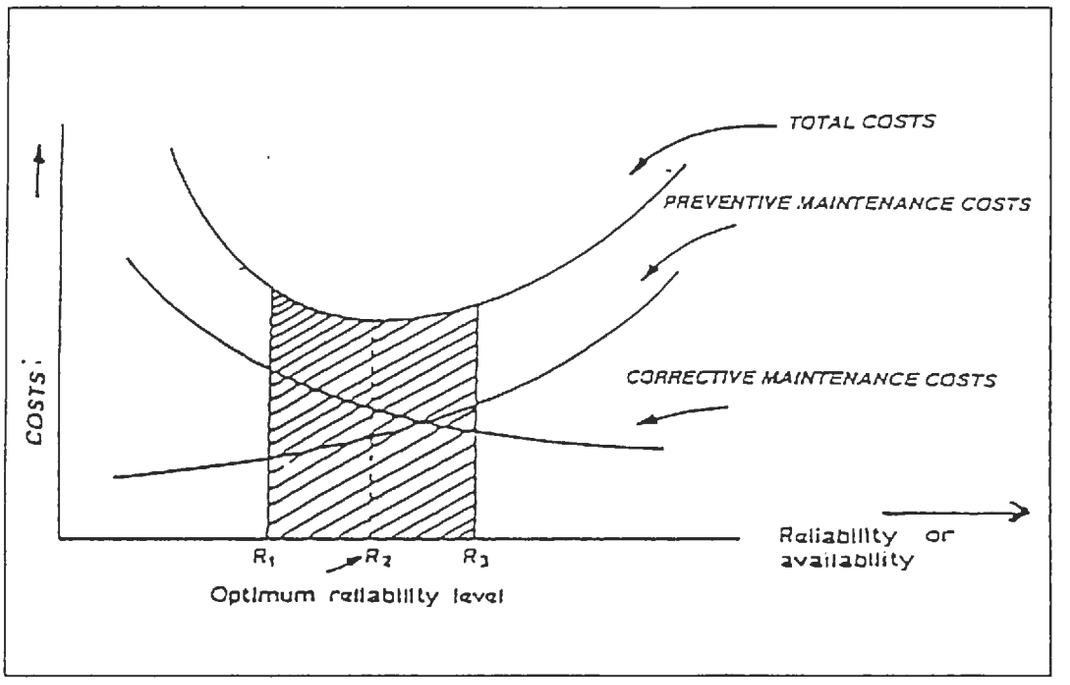


Figure 3.1: Reliability and costs
R_1 = minimal demanded reliability; R_2 = optimum reliability level; R_3 = Current reliability level

The classification of the different maintenance actions on the equipment at a NPP into corrective and preventive maintenance is shown in table 3.1.

Table 3.1 : *Maintenance actions*

Notation	Definition	Class
modify	replacement of the item with new engineering characteristics	CM/PM
replace	replacement of the item with same engineering characteristics	CM/PM
repair	repair/adjustment of the item no replacement	CM
service	periodic service tasks no disassembling of the item	PM
overhaul	major overhaul of the item	PM
inspection	periodic inspection, scrutiny with/without disassembling	PM
other	other maintenance activity	

CM = corrective maintenance; PM = preventive maintenance

Apart from replacement and modification, all the maintenance actions as stated in the above table are necessarily performed on *maintainable parts* of equipment at the NPP. The maintainable parts of a valve are given in table 2.7.

As mentioned previously , the maintenance program on equipment situated in the safety systems at the NPP are strongly guided by their TS. The TS request *periodic tests* and *direct maintenance follow ups in case of failure on demand.* Since a portion of the safety systems operate within the containment, the maintenance is usually done at specific time intervals, when the NPP is down for refueling.

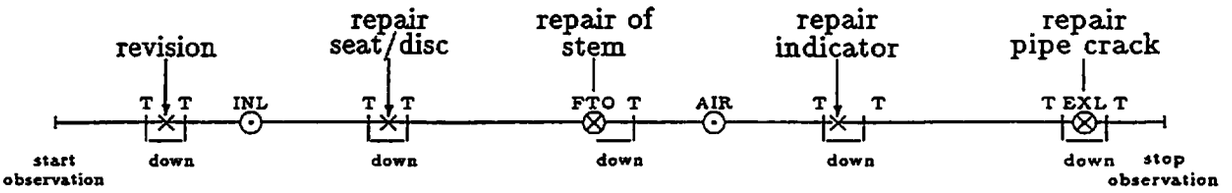
The 314 pressure relief system (described in appendix B) is a standby system situated in the reactor containment. Due to the fact that the radiation and steam pressure are too high during the operating period of the NPP, tests and maintenance can only be performed when the plant is shut down. Thus resulting in the following test schedule:

- One test while shutting down the plant to annual overhaul

- One test while starting up from the annual overhaul

Emergency maintenance of the pressure relief system leads to an expensive shut down of the plant. In figure 3.2 an idea is given of the types of maintenance actions taken on such a main valve socket throughout the operating years.

From the investigation of the information at the TUD database such as described in the previous chapter, we learned that the TUD database does *not* register all the maintenance actions on the equipment at the NPP. This limitation makes it difficult to judge the maintenance program as a whole. However, the maintenance staff is responsible for the local maintenance information system at the nuclear station. Hence, they have both the TUD database and the local maintenance information systems at their disposal to identify:



⊙ = failure detection time ; × = maintenance action; T = test

Figure 3.2: Example of the operating history of a main relief valve (314V001-V020)

(i) Common cause failures;

(ii) Weak sockets in a system (outliers);

(iii) Whether and how

- test/maintenance programs
- operating conditions
- design

influence the reliability of the sockets;

(iv) Trends in

- reliability of the sockets during the operating years of the NPP
- costs of maintenance during the operating years of the NPP

(v) Repair induced failures.

3.3 Risk/reliability staff at the nuclear power station and at SKI

The objective of the risk/reliability staff at the power station is to keep the risk of release of radioactive materials under the accepted level. Furthermore, the regulatory body in Sweden, SKI has a risk/reliability staff as well which supports the SKI inspectors appointed to the different NPPs in Sweden. The main task of the SKI inspector is to investigate whether the safety at the NPPs they are appointed to, is at an acceptable level. The main source of information the SKI risk/reliability staff and inspectors at SKI work with are the LERs assembled at SKI and stored in STAGBAS. The LERs contain descriptions of safety critical events at the NPPs in Sweden.

When the risk/reliability staff at the station and at SKI is confronted with a safety critical event, a further investigation has to be made into its root causes.

The information at the TUD database can then be of help for the inspector to prepare the right questions for the maintenance staff responsible for the equipment that critically failed.

The staff and inspectors at SKI broadly want to identify similar issues from the operating experience data as the risk/reliability staff at the power station. There is though an extra aspect to the work of the staff at SKI: The staff at the SKI office are both on-line connected to the TUD database AND STAGBAS. A combination of these two operating experience databases can give extra insights and should be considered in this work.

The maintenance and test programs for safety critical sockets are strictly guided by the safety technical specifications (TS). The revision of these technical specifications is part of the work done by the risk/reliability staff. One method used is probabilistic risk analysis (PRA). The Nordic research project NKA-RAS-450 (1987-1990) concerned this topic; optimizing of technical specifications by use probabilistic methods see [Laakso et al.,1990]. The following stages can be pointed out in a PRA:

- Initial information collection

  Piping, electrical and instrumentation drawings are collected, as well as test, maintenance, operating and administration procedures. Discussions with design engineers and plant personnel contribute as well. Both generic and (if available) plant specific occurrence rates of undesired events, including "initial events", component failures and human errors, must also be collected.

  The Swedish T-book [T-book, 1995] which is based on the failure reports and LERs of critical failure events, gives generic and NPP specific estimates of the rate of occurrence of undesired component failures for the 14 NPPs in Sweden and Finland.

- Event tree development and system modeling

  In this phase the possible accident sequences (branches of the event tree) are identified. System modeling involves the study of safety systems which must fail in order for accident sequences to be realized. A useful classification of failures is in *failure modes, effects and mechanisms.* This classification allows the risk/reliability analyst to determine the way in which components and subcomponents interact with each other.

- Analysis of human reliability and procedures

  The testing, maintenance and operating procedures are reviewed to identify the potential human errors to be included in the system analysis.

- Data-base development

  Identifying data sources, compiling data, selecting appropriate mathematical reliability models and estimate their parameters, and assessing the frequencies of initiating events are activities in this phase.

- Accident sequence quantification

  Computer codes are initialized, run and the results interpreted.

  * External event analysis
  * Uncertainty analysis
  * Development and interpretation of results

The risk/reliability staff at the nuclear power station should work close together with the maintenance staff. This means that the information needs of the maintenance staff stated in the previous section, should interest the risk/reliability staff as well. In addition to these information needs, the safety/reliability staff wants to identify:

(i) Estimates of rates of occurrence of undesired events;

(ii) Measures of human reliability.

Chapter 4

Tools developed for the TUD users

4.1 Introduction

In the previous chapter we have investigated the information needs of the users of the TUD database which resulted in a list of applications of the TUD database. In this chapter we describe the tools that are developed in this work. The statistical methods which support most of these tools, are described in appendix A.

The analysis tools developed in this work are the result of going through the following analysis steps

step 1. Investigate and select the data;

step 2. Make simple plots of the data;

step 3. Analyse the data with statistical methods, including analysis of trend and dependency;

step 4. Combine and implement these three steps in a prototype RDB.

The "environment" in which the tools are to function is the TUD database. The TUD database is a relational database system in ORACLE which runs under a UNIX operating system. In this work we have developed a prototype RDB in Microsoft Access based on the failure reports and engineering reports of the benchmark systems.

This prototype RDB enables us to design the analysis tools according to the possibilities of a relational database. Second, it facilitated the analysis of the benchmarksystems which was one of the goals of the work and will be presented in the next chapter. The main user-interface of the prototype RDB is shown in figure 4.1.

The analysis steps the TUD user has to go through in this prototype RDB are:

4a. Build a population of sockets (subcomponent or component level);

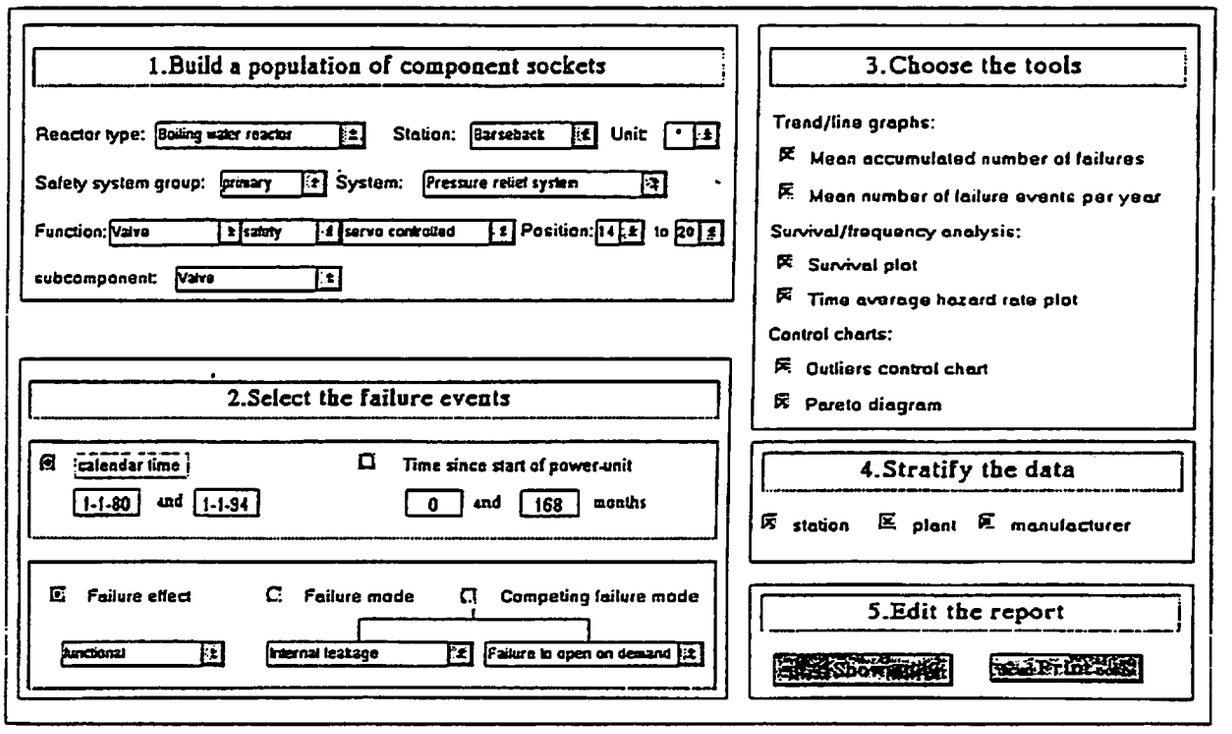


Figure 4.1: Analysis user-interface for a reliability database

4b. Select the failure events;

4c. Select the analysis tools to be incorporated in the report;

4d. Adjust the default report and print the report.

In this chapter we explain the possibilities for the user in each of these four steps of data analysis. We start with exploiting the possibilities of the TUD database for pooling equipment and selecting data on different types of failure events which are step 1 and 2 of the user-interface.

Once the data is selected on the pool (population) of sockets, there is a first need for simple charts that give the complete picture of the selected failure events. In these charts a distinction is still made between the sockets. This enables the user to judge whether there are outliers in the group of equipment which should be treated seperately.

When no distinction is made between the individual sockets in the population, several graphical presentation tools are developed that can compress the data in one understandable graph. The advantages of using graphs (plots) are that it makes information easier to remember, helps the user pick out trends and patterns and can reveal hidden facts and relationships not previously recognised. However, when the data is sparse, the user has to be careful not to jump to conclusions based only on the graphs. This can be avoided by supporting the graphs with statistical confidence bounds and significance levels. The statistical methods that underlie this support are discussed in appendix A.

Next, stratification of the selected pool of equipment in different strata (subgroups) is an effective method to isolate the cause of a problem and compare the performance of different plants, manufacturers etc. When the graphs show differences between the strata, the so called homogeneity of the entire population can be questioned. The stratified data will be accompanied with a significance level for homogeneity in the population.

4.2 Pooling of equipment and selection of failure events

In this section we will first give the motivation for building a population of sockets for analysis. Next, we discuss the general features of the operating experience data at the TUD database for a pool of sockets and give the different approaches towards the selection of failure events the users can have.

Pooling equipment

When the user wants to investigate a single socket, the data is often too sparse to apply statistical methods. However, it has to be emphasized that this is still the preferable situation; to treat the data from each socket separately when possible.

In most of the safety systems of a NPP, there exists built in redundancy which means that multiple copies of the same component socket are available in that system (see appendix B). Moreover, the same safety systems exist in different NPP's which provides the possibility of large pool of similar sockets. Hence, there exist possibilities for the user to pool different sockets and regard them as a population of *similar* sockets. Naturally, this provides the analysis tools with more failure/repair events so that stronger statistical results can be obtained. Yet, by regarding the sockets as similar, the assumption of homogeneity is made. There exists statistical tests for homogeneity within a population of sockets, which are described in the appendix A. In section 4.4 we give stratification methods for a population of sockets which together with the statistical tests, enable the user to check the plausibility of homogeneity within the population.

Note that the user can have other intentions for pooling equipment than only making inference on one socket type. It is well possible that the user wants to investigate equipment situated in a certain part of the plant or the behavior of a system as a whole, the resulting pool of sockets is then *not* regarded homogeneous.

Component socket operating mode and time related versus demand related failures

There are three classes of operating modes for a component socket:

1. continuous operation

2. standby

3. intermittent

Components operating in the standby mode are normally passive, but can be intermittently called upon to perform some function. In the intermittent mode a component is sometimes in continuous operation and sometimes in standby. This can arise when two or more components are available to perform a single function and are placed in service intermittently.

The failure cause gives reasons why a (sub)component fails. These reasons may lie outside the (sub)component itself, as when a (sub)component fails due to over-stress caused by other failures upstream. Failure causes are grouped into two broad categories, *time-related failures* and *demand related failures*. Most commonly, a failure occurring when the component is called ito service from standby mode is classified as demand related. Failures occurring while te component is in continuous operation are classified as time-related.

The operating mode of the component socket should be taken into account when analysing the failure data. For example; when analysing the failure data of a pool of similar sockets, it is well possible that one socket has the operating mode continuous operation while the other sockets are redundant and are in standby. Naturally the socket in continuous operation is much more subject to time related failures associated with the failure mechanism wear.

Moreover it should be noticed that a component socket that has the operating mode continuous operation, does *not* operate steady and continuously throughout the whole calendar year. For each NPP there exists periods of cold shutdown, hot shutdown and start/stop processes and differences in power operation. This means that there exist time related failures, notably those related to failure mechanism wear, for which calendar time might not be the most useful metric. For this reason the user can choose between NPP operating time and calendar time for the analysis of the data.

A component socket that is in standby operating mode is subject to demand related failures. When we assume that this component socket does not degrade during standby, the statistical analysis of the failure data is quite simple. The metric we use for the analysis is then preferably *number of demands*.

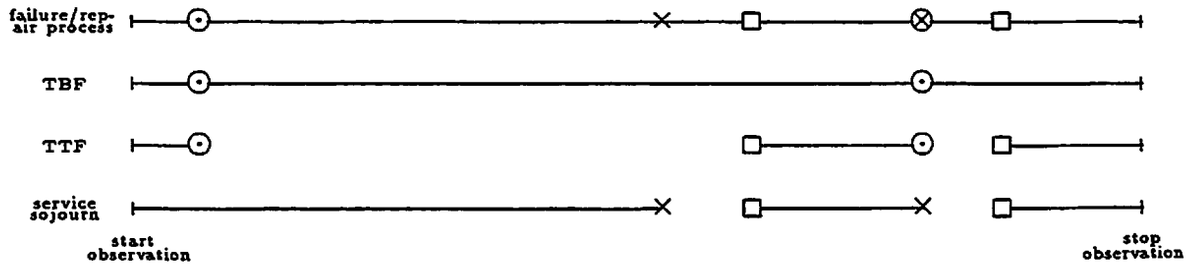
Service sojourns, time to failure and time between failure

From the description of the contents of a failure report, we know that for each socket there exists information on three different events occurring in time: the failure detection date, the start of repair date and the replenished at socket date respectively.

From the events start of repair event and replenished at socket, we get the so called socket *service sojourns*. A service sojourn begins when a new or repaired subcomponent goes on line, and terminates when a subcomponent is removed for any reason whatever.

From the failure detection events, we get information on times between failure (TBF). Note that the failure detection date need not be the date that the subcomponent socket failed. When the failure is not discovered during continuous monitoring (detection mode A or B) we can not be sure about the exact date of the failure event.

The failure detection events together with the replenished at socket events give us information on the times to failure (TTF).



⊙ = failure detection time ; × = start repair ; □ = replenish at socket

Figure 4.2: Different possibilities of inter-event times

Selecting a series of more than one type of failure events

When the user has chosen a population of sockets to analyse, (s)he can choose to make distinctions between the failure events that occur at a socket. There are now two possibilities:

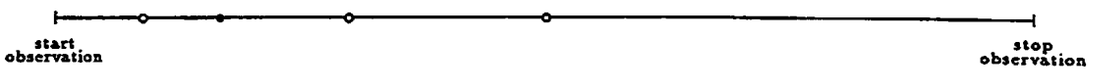
1. The user wants to investigate the interdependence between the different types of failure events;
2. The user wants to select only one of the types of failure events and continue the analysis with only these failure types.

Note that in the second case the user disregards some of the failure events of the socket. When the user wants to check whether there is a trend in the number of functional failures of the subcomponent socket, (s)he selects only the functional failures for the analysis.

For each failure report the user can choose to further label the failure/repair event from the codings in the failure and repair fields such as given in table 2.6. We give now two examples of "labeling" the failure events:

1. Looking at functional/ nonfunctional failure events;

   In the case that the user is interested in the reliability of the subcomponent socket. The failure event of a subcomponent socket can be classified as functional or nonfunctional. Note that this is on subcomponent socket level and a functional failure of a subcomponent does not necessarily imply a functional failure of the socket.



o = non-functional failure ; • = functional failure

Figure 4.3: Failure events classified as functional and non-functional failure

2. Looking at the failure modes.

   As discussed in section 3.3, one of the objectives of the risk/reliability analyst is to estimate the rate of occurrence of undesired events. In the case that these undesired events are critical failures of a component socket, a helpful classification of this failure is in failure cause, mechanism, modes and effects. The failure fields do, however, not classify the failure directly into failure modes. Nevertheless we can use the codes to classify into the failure mode such as showed in table 2.8.

   There exist broadly three classes of failure modes; *critical, degraded and incipient failures.* The work on competing risk analysis discussed in the report by [Cooke et al., 1993] is based on this classification of the failure events.

4.3 Analysis tools for a reliability database

We consider the situation where the user has chosen the following set-up for the start of the analysis:

1. a population of sockets;
2. a time-window in which to analyse the failure events;
3. one or more types of failure events;
4. stratification of the population in subgroups (strata).

In this section we present the analysis tools developed in this work. The statistical support for the tools is given in appendix A. The following tools are discussed:

- Quality control tools;
- Trend/line graphs;
- Survival/frequency graphs;
- Competing risk graphs;
- Stratified graphs.

In the following table an idea is given of which tools can suit which information needs of the TUD users.

Table 4.1 : *Tools for the TUD users*

Information needs	Tools				
	Quality control tools	Trend/ line graphs	Survival/ frequency tools	Competing risk graphs	Stratified graphs
1. Common cause failures	•				
2. Weak sockets in a system	•				
3. Investigating dependencies on design/operating conditions/ maintenance/test			•	•	•
4. Trends in reliability and maintenance costs		•			
5. Repair induced failures	•		•	•	
6. Estimating rates of occurrence			•	•	

4.3.1 Quality control tools

The (quality) control tools are based on methods developed in quality control (QC). Quality control is defined as a set of techniques for economically producing goods and services that meet the customers requirements. Typically, QC techniques are applied in manufacturing processes. Naturally, these techniques can usually not be directly applied for analysing a failure/repair process. Nevertheless, some of the techniques showed to be helpful in the preliminary analysis of the data.

Failure/repair events sheet

A failure/repair event sheet visualises the failure/repair processes of the sockets in a population.

How to make a failure/repair event sheet? The idea is simple; we assign to each socket a column in a spread sheet and each row in the spreadsheet represents a calendar month in the chosen time window. Now, for each month, i at which a failure is detected at a socket, j the corresponding the spreadsheet cell(i,j) is colored. Similarly, for each month, j that a repair is performed at socket i, the cell(i,j) contains horizontal lines and the cells corresponding to the months in which the socket has been waiting for repair, contain vertical lines. In the case that the user wants to distinguish more than one failure type the failure types can be assigned different colors.

How to use a failure/repair event sheet? The failure/repair event sheet is a powerful tool in the preliminary analysis of the data. Especially the interdependencies between the sockets are revealed as clusters of colored cells. Clusters can be the result of common cause failures (CCF) which is a topic of major interest for the risk analyst (see section 3.3). Further, by giving different types of

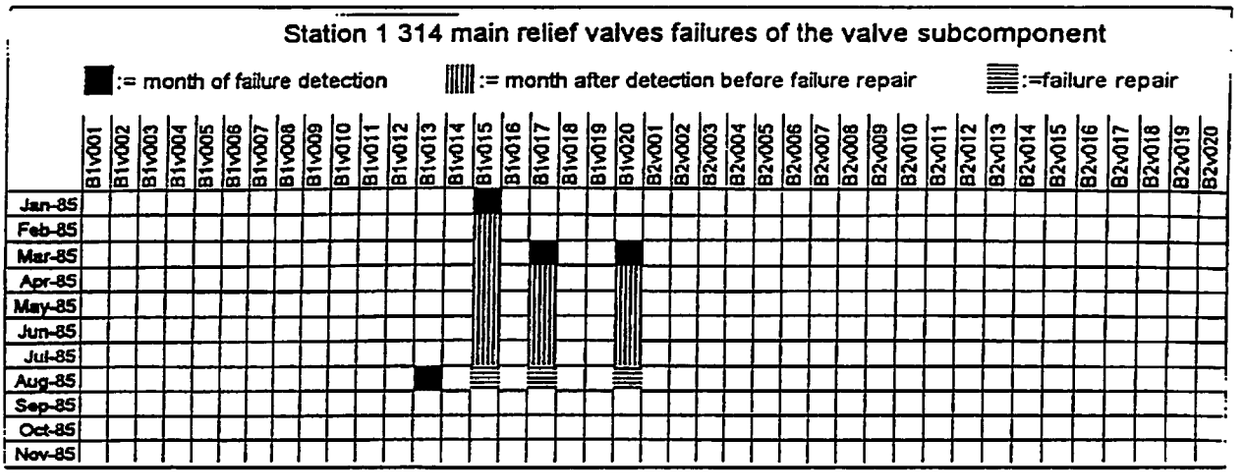


Figure 4.4: Failure/repair sheet

failures/repairs different colors, the interdependency of these two types of failures can be studied. In addition, when the user chooses to study functional or critical failure events, unavailability times due to long down times of the socket are spotted immediately.

Outliers control chart

A control chart is a type of line graph that is used to assess the stability of a process, which is in this case the number of failures per socket in a population of sockets. Instead of the number of failures the maintenance engineer can decide to take the mean time to repair (MTTR) repairhours spend on the socket.

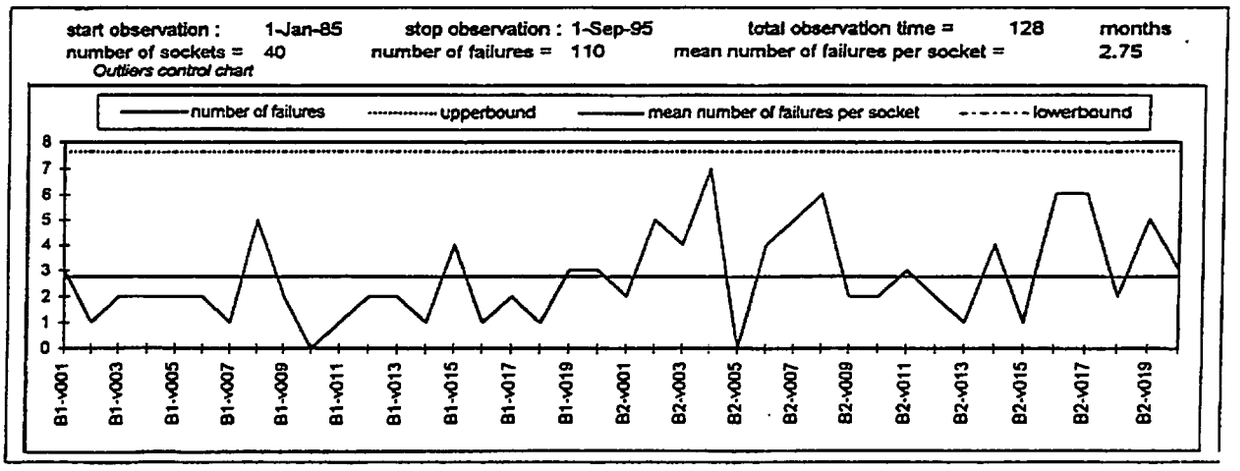


Figure 4.5: Outliers control chart

How to make an outliers control chart? The chart shows the number of failure events or MTTR of a certain type (such as chosen by the user) per socket in the population. A center line representing the mean number of failures or MTTR per socket is drawn on the graph, together with upper and lower control

limits. The control limits are the values at the two sided 5% significance levels for a statistical test called the *log-rank test* (described in section A.6).

How to use an outliers control chart? The control limits serve as a guides to distinguish random causes of variation from specific causes that should be investigated. If the number of failure events of a socket falls within the control limits, then variation is considered to be from random causes and the population is considered homogeneous. The plotted points that fall outside the control limits point at a possible non-homogeneous population and the sockets connected to these points are outliers.

The level of siginificance for homogeneity in the population is generated with a homogeneity test. It should be noted that this test fits the purpose of a rough indication for outliers in the population since we only look at the number of failures per socket. There exist stronger tests when we take more information from the failure/repair processes than only the number of failure events. These tests are briefly described in section A.6.

Pareto diagrams

A Pareto diagram is a specialized bar graph that can be used to show the relative frequency of failure events.

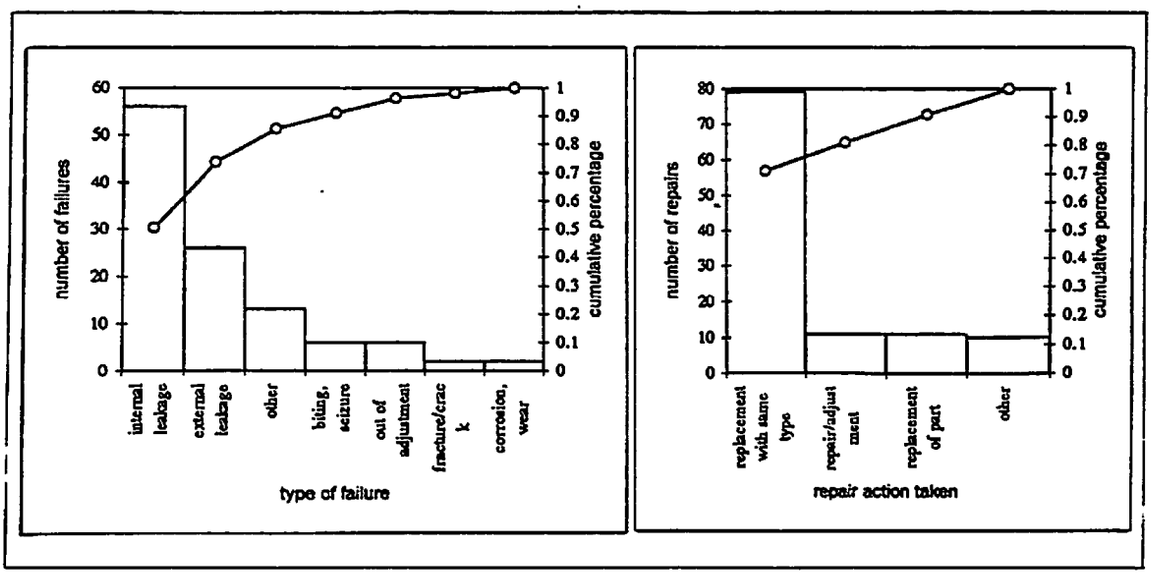


Figure 4.6: Pareto diagram

How to make a Pareto diagram? The user has chosen a population of sockets and a time window for the analysis. There are many possibilities for the item category of the Pareto diagram. A natural choice is to take one of the fields in the failure report that contain the failure/repair data codes. Next, we count the number of failures per item and the Pareto diagram presents this information in descending order, from the largest category to the smallest (again instead of the number of failures the maintenance engineer can decide to take the repairhours

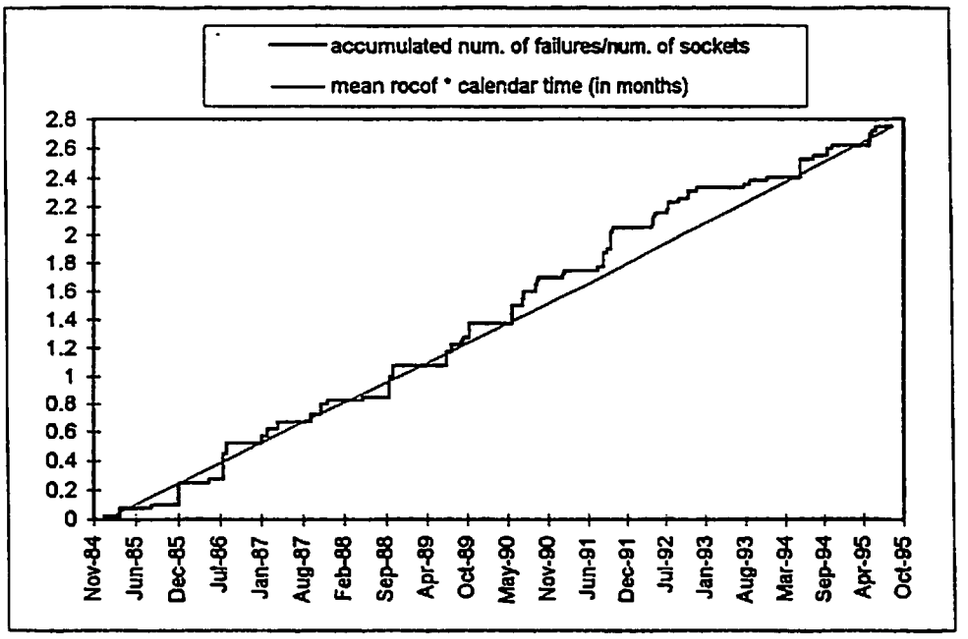


Figure 4.7: Nelson Aalen graph

in the population, the mean rocof should be approximately constant in all time windows and the Nelson Aalen graph should approximate a straight line.

The control limits serve as a guide to distinguish random causes of variation in the rocof from specific causes that should be investigated. If the Nelson Aalen graph fall within the control limits, then variation is considered to be from random causes and the failure process is considered to have no trend. Yet, if the Nelson Aalen graph fall outside the control limits, this signifies a trend in the mean rocof of a socket in th population.

Rate of occurrence of failures (rocof) per socket per month during a calendar year

The estimator of the rocof in any time window can be read from the rocof for a calendar year. This is due to the fact that maintenance schedules are yearly based with main focus on the refueling periods.

How to make the rocof during a calendar year graph? The rocof per year is defined as:

$$\hat{\alpha}(t) := \frac{\text{number of failure events in } [a_{i-1}, a_i) \text{ where } t \in [a_{i-1}, a_i)}{\text{number of sockets in the population x 12 (months)}}$$

where a_i is the i-th year. This is anestimator of

$$\alpha(t) := \text{rate of occurence of failure events per months for a socket at time } t$$

Since the rocof for the different calendar years is a statistical estimator, there is a probability that the graph shows a slight trend when the underlying failure

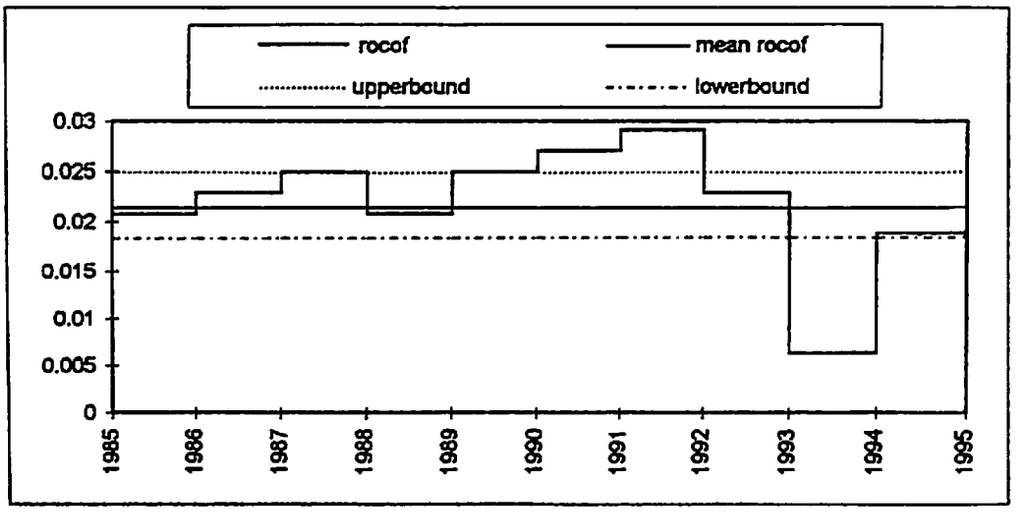


Figure 4.8: Rate of occurrence of failures (rocof) during a calendar year

process is homogeneous Poisson (a mathematical concept of no trend in the rocof described in section A.2). The control limits represent this probability, α. This means that when the mean accumulated number of failures crosses one of the control limits, the user can decide that the failure/repair process is not Poisson with a probability of being wrong less than α.

How to use the rocof during a calendar year graph? By looking at the rocof *per clendar year*, the local fluctuations due to detection of failure events in refueling periods is avoided. An advantage of the cumulative plot (mean number of failures) is that it enables small systematic changes in the rocof to be noticed readily. Advantages of the rocof for the different calendar years (non-cumulative plot) is that local (yearly) fluctuations in the rocof are directly identified.

The control limits serve as a guide to distinguish random causes of variation in the rocof from specific causes that should be investigated. If the rocof falls within the control limits, then variation is considered to be from random causes and the failure process is considered to have no trend. Yet, if the rocof falls outside the control limits, this signifies a trend in the rocof of a socket in th population.

Accumulated repairhours graph

How to make the accumulated repairhours graph? When the number of sockets at risk in the population is constant throughout the whole time window, $(0, T]$ the accumulated number of repairhours at time t, $N_{repairhours}(i)$ is defined as:

$$N_{repairhours}(i) := \text{total repair hours up till the } i\text{-th repair}$$

How to use the accumulated repairhours graph? Now, the slope of the accumulated repairhours graph in between any two points on the disctrete axis, is an estimator of the mean time to repair (MTTR) in between these two repair jobs. In the case that there is no trend in the performance of the maintenance

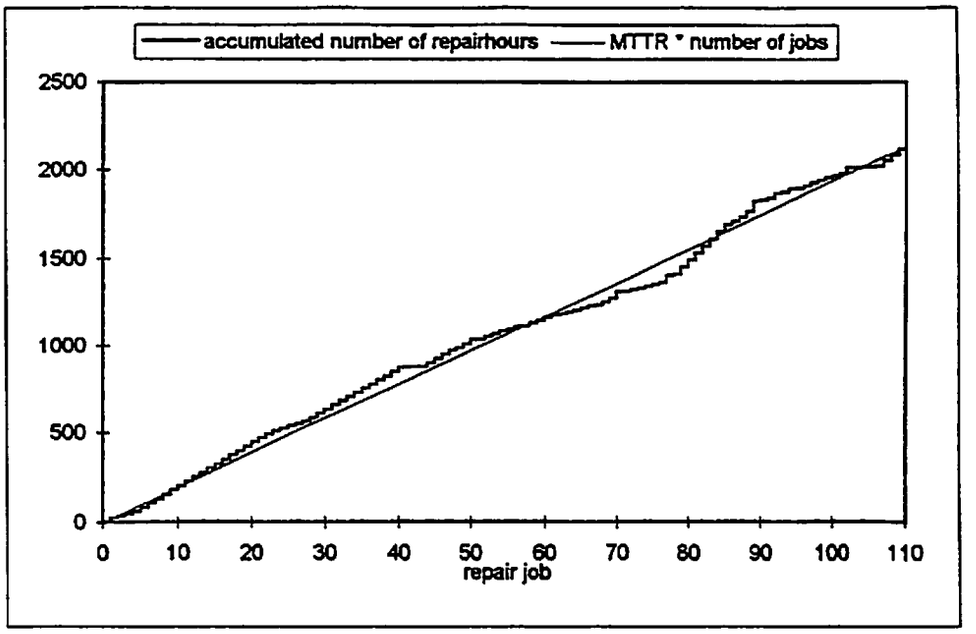


Figure 4.9: Accumulated repairhours

crew, the MTTR should be approximately constant in between both repair jobs and the accumulated repairhours should approximate a straight line.

MTTR during a calendar year graph

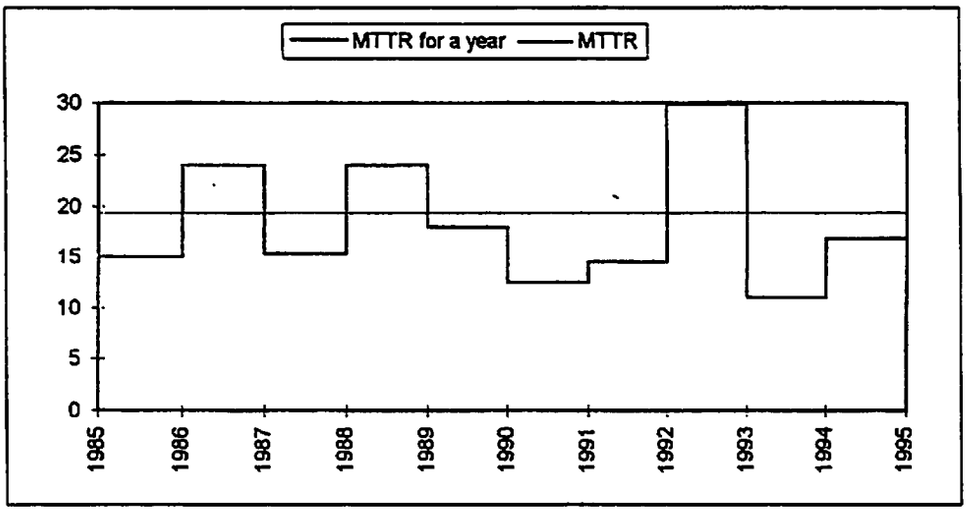


Figure 4.10: MTTR during a calendar year

How to make the MTTR during the calendar year graph? The MTTR during a calendar year is defined as:

$$\hat{\alpha}_{repairhours}(t) := \frac{\text{number of repair hours in } [a_{i-1}, a_i) \text{ where } t \in [a_{i-1}, a_i)}{\text{number of repairs in } [a_{i-1}, a_i)}$$

where a_i is the i-th year. Which is an estimator of

$$\alpha_{repairhours}(t) := \text{MTTR for a socket at time } t$$

How to use the MTTR during a calendar year graph? By looking at the MTTR during a year, the local fluctuations due to emphasis on maintenance in refueling periods is avoided. An advantage of the cumulative plot (total number of repairhours up till the i-th socket) is that it enables small systematic changes in the MTTR to be noticed readily. Advantages of MTTR during a calendar year (non-cumulative plot) is that local (yearly) fluctuations in the mean number of repair hours are directly identified.

4.3.3 Survival/frequency graphs

The survival/frequency graphs result from the description of the failure/repair process of a socket as a sequence of inter-event times. For the inter-event time the user can decide to take, the time between failure (TBF), time to failure (TTF) or the service sojourn (as described in the previous section). The mathematical background of this description is given in section A.4.

Particularly, we can only use the survival graphs when the failure/repair process is assumed to be *a renewal process.* That is, each time the socket is repaired it is returned to as good as after the last repair before the start of the observation. Therefore, it should be verified whether the failure/repair process can be regarded as a renewal process. The *Laplace test* and *exponential scoring test* are two statistical test that generate a significance level for no trend in the rocof and are described in subsection A.6.1. Hence, these significance levels should at least be checked before using the survival/frequency graphs.

Survival function

When the user is interested in the overall frequency distribution of the inter-event times, the so called empirical survival function is helpful representations of the series of events.

How to make the empirical survival function? The empirical survival function is *an estimator* of the survival function. In the case of *no* censors the empirical survival function is simply defined as:

$$\hat{S}(x) := \frac{\text{number of inter-event times larger than } x \text{ months}}{\text{total number of inter-event times}}$$

and is an estimator of

$$S(x) := \text{probability of survival beyond } x \text{ months after repair}$$

How to use the empirical survival function? In the case of no censors in the data, the empirical survival graph shows the frequency of failures events that occurred later than x months after the repair of the socket. In the case of censors

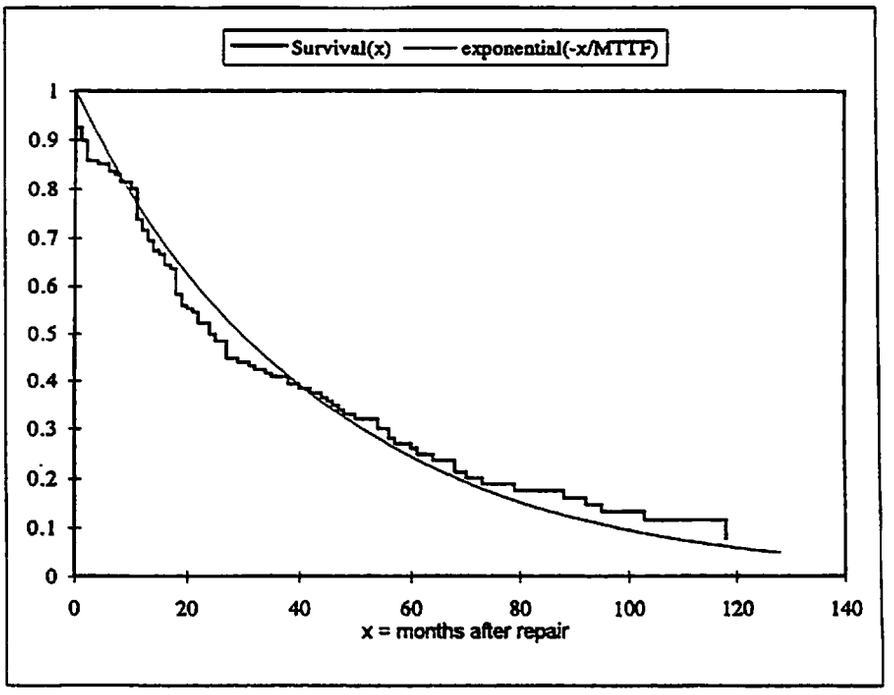


Figure 4.11: Empirical survival function

in the data, the empirical survival function is an estimator of the probability of surviving beyond time x after repair.

When the failure data would have been obtained from a maintenance policy where only corrective maintenance (repair) would be performed, the survival function could give an indication where preventive maintenance should be performed to lower the cost of maintenance (see figure 3.1).

By plotting the exponential distribution for the case that the failure/repair process is considered Poisson, the deviation between these graphs is an indication whether the Poisson process is an appropriate description.

Time average hazard rate

The estimator of the time average hazard rate tells us whether there is a trend in the hazard rate, $\lambda(x)$. For grasping the concept of hazard rate of a socket, consider a component known not to have failed since time x after it is replenished at the socket, then the hazard rate is roughly speaking the probability of almost immediate failure of a socket known to have reached time x.

How to make the estimator of the time average hazard rate? The estimator of the hazard rate can be defined as follows:

$$\hat{\lambda}(x) := \frac{\text{number of inter-event times in } [b_{i-1}, b_i) \text{ where } x \in [b_{i-1}, b_i)}{\text{number of inter-event times} \geq b_{i-1}}$$

Consider a socket known not to have failed at time x then $\hat{\lambda}(x)$ is an estimator be the limit of the ratio to Δx of the probability of failure in $(x, x + \Delta x)$ such

spent). Points are plotted for the cumulative total in each bar and connected with a line to create a graph that shows the relative incremental addition of each category to the total.

How to use a Pareto diagram? By making a Pareto diagram of the number of failures against the failure types in a population of sockets, the user can determine the principal failure types in the population. In other words, a Pareto diagram shows the maintenance engineer where to focus for improvement.

4.3.2 Trend/line graphs

The trend/line graphs result from the description of the failure/repair process of a socket as a counting process. The mathematical background of this description is given in section A.3.

When the user is interested in changes in the average rate of occurrence of failure events (rocof) or hours spend on repair, there are broadly two methods of graphical presentation, one based on cumulative numbers and the other on individual numbers of occurrences. Both these graphs make *no* distinction between the different sockets in the population. Hence, the user should verify whether this underlying assumption of homogeneity is justified. Means to verify the assumptions are stratified plots (discussed in subsection 4.3.5) and the outliers control chart presented previously under quality control charts.

Nelson Aalen graph

When the user is interested in trends in the rate of occurrence of failure events (rocof) in a population of sockets, the Nelson Aalen estimator, $\hat{A}(t)$ of the expected number of failures of a socket in the time-window can be of assistance.

How to make the Nelson Aalen graph? When the number of sockets at risk in the population is constant throughout the whole time window, $(0, T]$ the Nelson Aalen graph is defined as:

$$\hat{A}(t) := \frac{\text{total number of failure events in } [0, t)}{\text{number of sockets in the population}} \qquad t \in (0, T]$$

which is an estimator of

$$A(t) := \text{expected number of failure events for a socket in } [0, t)$$

Since the Nelson Aalen is a statistical estimator, there is a probability that the graph shows a slight trend when the underlying failure process is homogeneous Poisson (a mathematical concept of no trend in the rocof described in section A.2). This probability is given by the significance level of no trend generated by the *Laplace test* which is explained in section A.6.2.

How to use the Nelson Aalen graph? Now, the slope of the Nelson Aalen graph in between any two points in time is an estimator of the mean rocof in this time window. In the case that there is no trend in the performance of the sockets

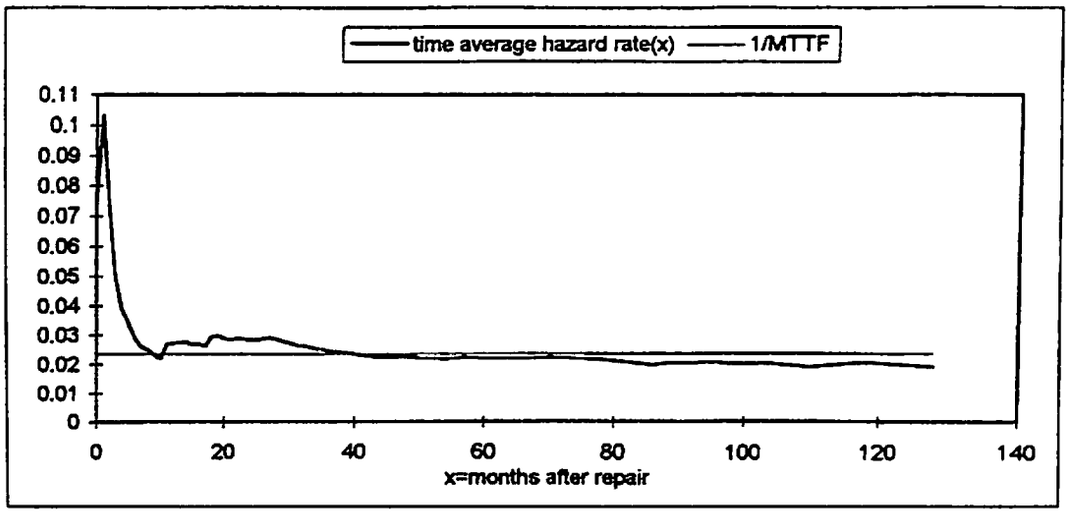


Figure 4.12: Time average hazard rate

as defined in the previous section. The estimator of the time average hazard rate can then be defined as follows:

$$\hat{\bar{\lambda}}(x) := \text{average of the estimated hazard rates up til time } x$$

How to use the estimator of the time average hazard rate? In the case that the failure/repair process is reasonably consistent with a Poisson process, the time average hazard rate should be approximately constant. A constant hazard rate means that when the maintenance crew inspects the socket and finds no failure, the sockets behaviour after the inspection will be the same as just after the repair which is as good as new.

The time average hazard rate follows trends in the hazard rate but has the advantage over the estimator of the hazard rate that local (random) fluctuations are smothered.

Repair time distribution function

When the user is interested in the overall frequency distribution of the repairhours spend on a repair job, the so called empirical repair time distribution function (d.f.) is a helpful representation of the repair jobs performed.

How to make the repair time distribution function? The empirical repair time distribution function is *an estimator* of the repair time d.f. The empirical repair time d.f. is simply defined as:

$$\hat{F}_{repair}(x) := \frac{\text{number of repair times smaller than } x \text{ hours}}{\text{total number of repair times}}$$

which is an estimator of

$$F_{repair}(x) := \text{probability that the repairtime is less than } x \text{ hours}$$

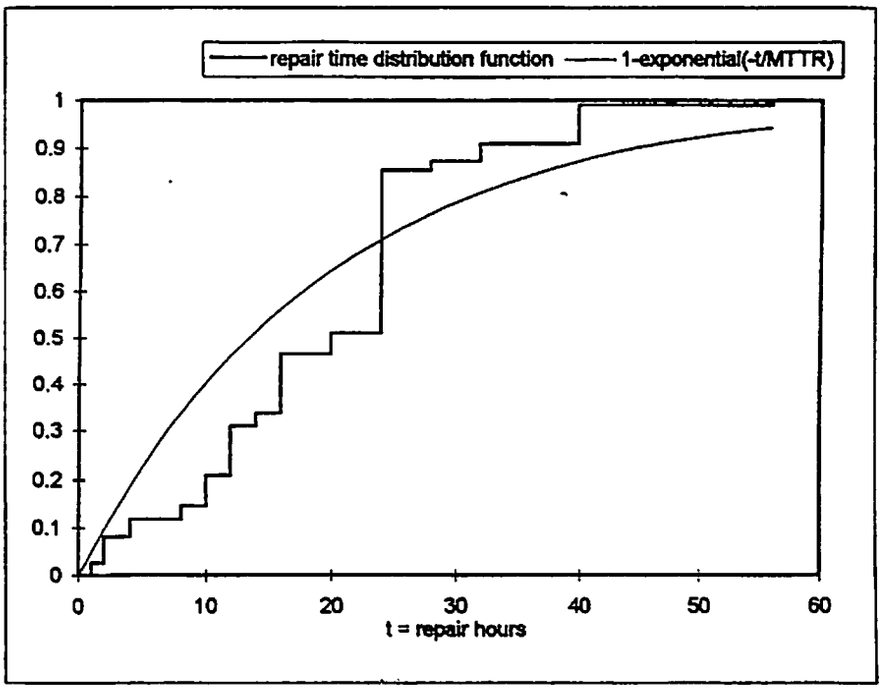


Figure 4.13: Empirical repair time distribution function

How to use the empirical repair time distribution function? The empirical repair d.f., shows the frequency of repair jobs that took less than x hours. This can give the maintenance planner an idea of the costs of a corrective maintenance job which can support the decision of the total maintenance planning which includes preventive maintenance (see figure 3.1).

4.3.4 Competing risks graphs

The subsurvival/frequency graphs result from the description of the failure/repair process of a socket as a competing risk process. In the competing risk situation the user distinguishes more than one type of failure events in which a socket inter-event time can end.

For the inter-event time the user can decide to take, the time between failure (TBF), time to failure (TTF) or the service sojourn (as showed in figure 4.2). The mathematical background of this description is discussed in section A.5. Particularly, we can only use the subsurvival graphs when the failure/repair process is assumed to be *a renewal process.* That is, each time the socket is repaired it is returned to as good as new. Therefore , it should be verified whether the failure/repair process can be regarded as a renewal process. The *Laplace test* and *exponential scoring test* are two statistical test that generate a significance level for no trend in the rocof and are discussed in subsection A.6.1. Hence, these significance levels should at least be checked before using the subsurvival graphs.

Subsurvival functions

A graphical tool to analyse the interdependencies of more than one type of failure is a plot of the so called empirical subsurvival functions.

How to make the empirical subsurvival function? These are estimator of the subsurvival functions defined as:

$$\hat{S}_i^*(x) := \frac{\text{number of inter-event times ending in a type i event and larger than } x}{\text{total number of inter-event times}}$$

which is an estimator of

$S_i^*(x) :=$ probability that the service sojourn ends in a type i failure and is longer than x months

Empirical subsurvival functions contain all the observable information from the competing failure processes.

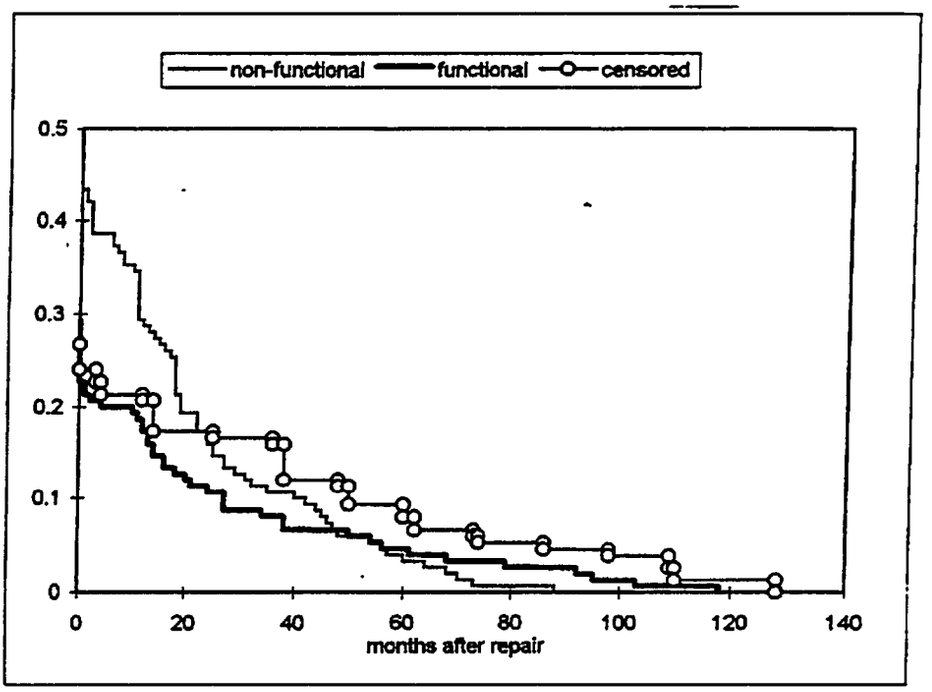


Figure 4.14: Empirical subsurvival functions

How to use the empirical subsurvival function? A typical example of the use of the empirical survival functions is when the user prefers the ending of a lifetime in one of the two types of failure chosen. These types can be critical against degraded or functional against non-functional. Typical, the user prefers a subcomponent socket to end its lifetime in a non-functional failure and a component socket in a degraded failure. One, indicator that this situation is met in practice, is simply that the number of failures of type 1 is smaller than the number of failures of type 2. This can be read from the empirical subsurvival functions by $S_1^*(0) < S_2^*(0)$. More generally the user desires that for all times t

(in months), (sub)component sockets in service at time t are more likely terminate their current sojourn in a failure of type 2 than of type 1. This leads to the following translation:

$$\text{for all } t \quad S_1^*(x) < S_2^*(x)$$

Conditional subsurvival function

The empirical conditional subsurvival functions are an estimator of the conditional subsurvival functions defined as:

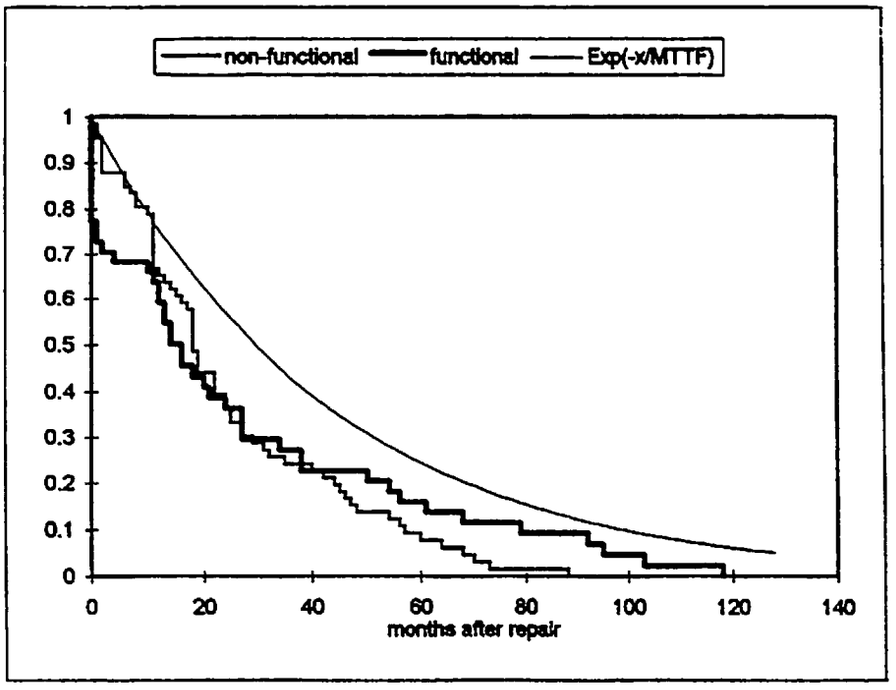


Figure 4.15: Empirical conditional subsurvival functions

How to make the empirical conditional subsurvival function?

$$\hat{S}_{i|X_i<X_j}(x) := \frac{\text{number of inter-event times ending in a type i event and larger than } x}{\text{total number of inter-event times ending in a type } i \text{ event}}$$

and is an estimator of

$S_{i|X_i<X_j}(x)$:= probability that the service sojourn is larger than x given that it ends in a type i failure

How to use the empirical conditional subsurvival function? can be used for verifying whether the failure processes leading to the different types of failure are independent under the assumption of exponentiallity. Further, the conditional subsurvival functions indicate whether the lifetime ending in a type 1 failure is close to the lifetime that would have ended in a type to failure when a type 1

would not have occurred. The idea of using this information is as follows: when the maintenance engineer wants to repair a non-functional failure just before a functional failure would have occurred at the subcomponent socket we would get:

$$S^{*}_{1|X_1<X_2}(x) \approx S^{*}_{2|X_2<X_1}(x)$$

4.3.5 Stratified data plots

The users main interest may lie in the result of grouping data by type of failure, manufacturer, plant, system etc. The method of grouping data by common points of characteristics to better understand similarities and characteristics of data is called **stratification.**

Table 4.2 : *Stratification methods*

Stratification	**Use**
By manufacturer	The performance of different manufactures can be investigated
By station	The performance of similar groups of equipment at different stations can be checked
By NPP	The performance of similar groups of equipment in different NPPs can be checked
By system	The performance of similar groups of equipment in different systems can be checked
By socket	The differences in performance within a population of component sockets can be checked

Stratification and comparison is an effective method for isolating the cause of a problem and comparing performance of different groups of equipment.

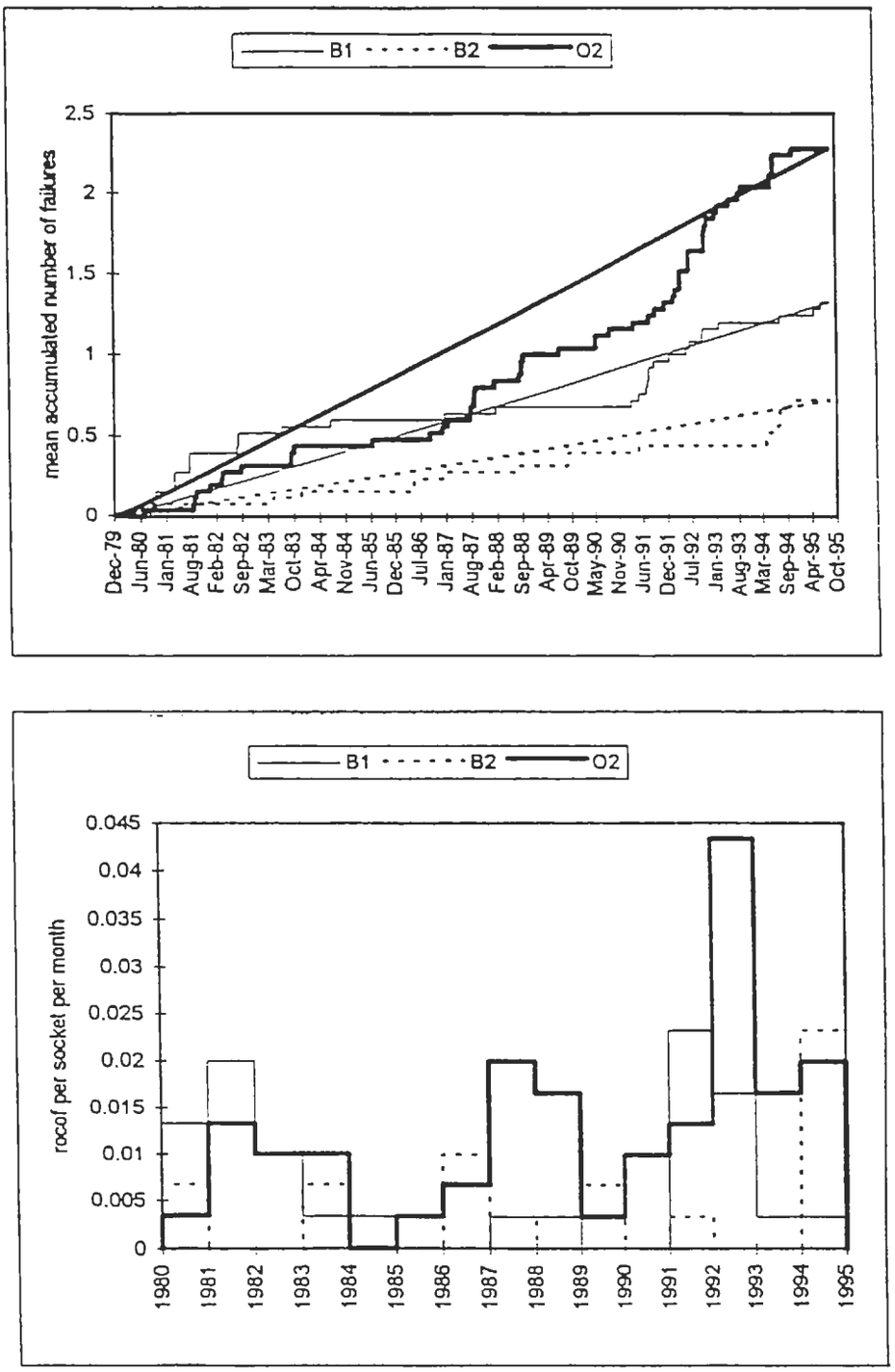


Figure 4.16: Stratified trend/line graphs

Chapter 5

Results and conclusions

5.1 Introduction

In this chapter the analysis tools, as described in the previous chapter, are presented for a number of populations of sockets situated in the benchmarksystems (described in appendix B). The user-interface given in figure 4.1 guided the user through a number of steps, resulting in a "reliability" report on the chosen population. In this chapter we first analyse the general reliability behaviour of the benchmark systems. Next, we will present the report such as generated by the prototype RDB developed in this work for a homogeneous population of sockets and give our interpretation of the results. In the last section of this chapter we will give the conclusions of the work outlined in this report.

5.2 Results for the benchmark systems

In this section we analyse the TUD data from two stations, the data form station 1 come from two identical NPPs (B1 and B2) and the data from station 2 come from one NPP (O2) of a similar type as the two NPPs of station 1. Due to the fact that all three NPPs are of a similar type, we could expect that the reliability function, when no preventive maintenance is performed, of the equipment at these NPPs is similar and that the difference in failure/repair behaviour is due to differences in the maintenance performance. Here it is necessary to stress again point (viii) of section 2.3, where the homogeneity in recording of different stations is questioned. This means that differences in failure/repair behaviour of similar sockets in different stations can be due to different maintenance strategies or different reporting behaviour.

5.2.1 Pressure relief system, 314

The pressure relief system (314) is described in section B.2. In this section we first analyse the TUD data from the population of all main sockets of the 314 system such as given in table B.1. We look at the failure/repair processes of

these component sockets from 1 january 1980 to the 1 september 1995. Next, within this population we look closer at the behaviour of the main pressure relief valves (V001-V020). Yet, these component sockets will be analysed in another time-window, [1-jan-85, 1-sep-95]. Within this time window we have a stronger support for using the tools coming from the survival analysis. The results of the this analysis will be given in a report format such printed with the user-interface given in figure 4.1.

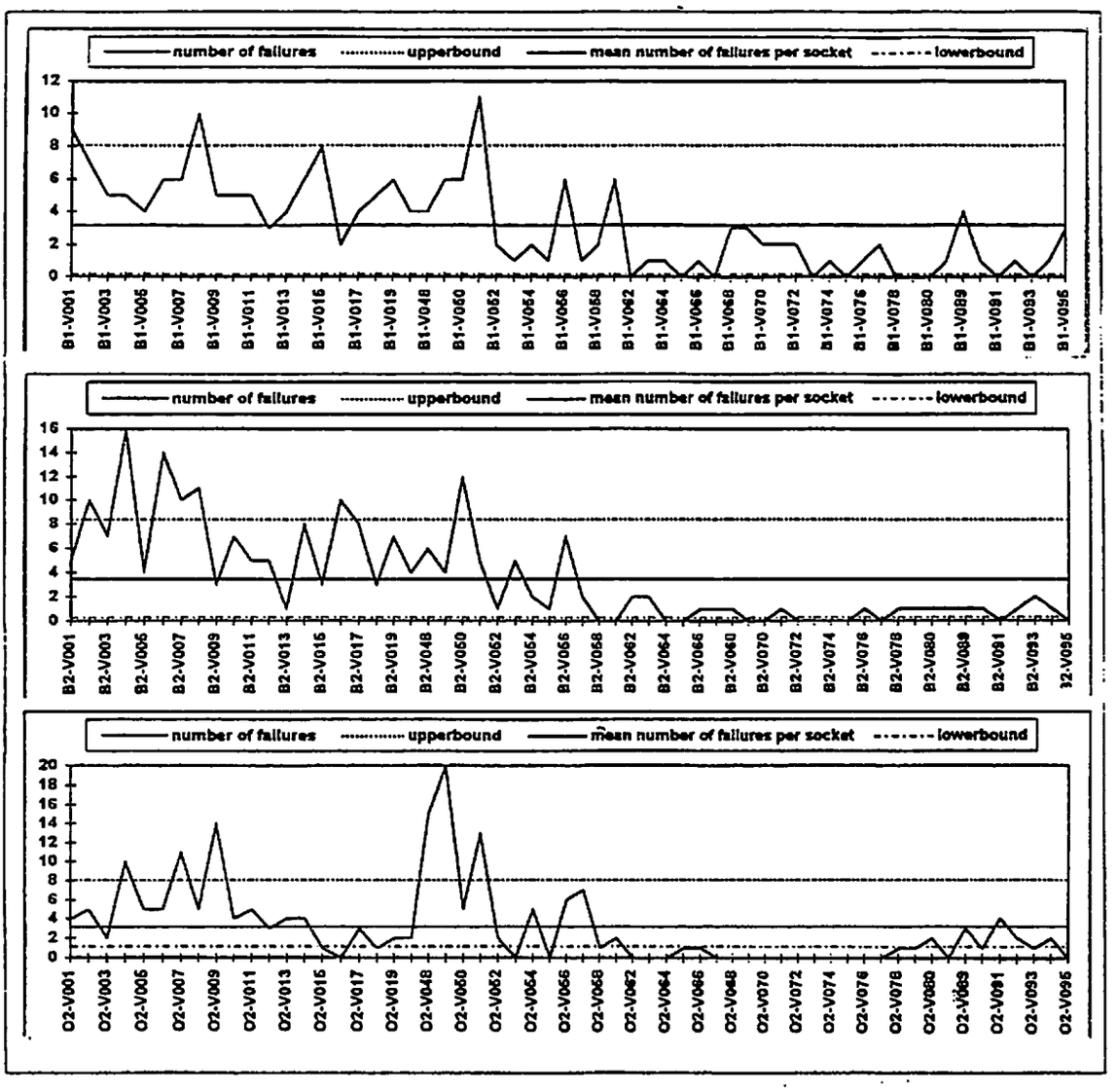


Figure 5.1: Outlier control chart for the main sockets of the 314 system at the three NPPs

In figure 5.1 the behaviour of the main sockets of the 314 system such as given in table B.1 for the three NPPs can be roughly evealuated. The main sockets of the 314 system exist of different types of valves and do *not* form a homogeneous population. The outliers control charts show that the number of failures for the

different sockets of the 314 system at the three NPPs is fluctuating heavily. Especially O2 shows a strong peak for the control valves motor operated (V048, V049). The impulse operated pilot valves (V062-V081) and electromagnetic operated pilot valves (V089-V095) have siginificantly less failures than the safety, closing and control valves for all three NPPs.

It is apparant that the three NPPs do not differ very much in the mean number of failures per component socket in the population. For the two NPPs from station B this is to be expected since a similar maintenance strategy is followed in these two NPPs. It is, however, interesting to see that the third NPP (O2) that is situated in a different station, has a roughly similar behaviour when we judge purely from the outliers control charts. Still, with the outliers control charts, we do *not* look at the time behaviour of the failures. In the extreme case, it could be that the sockets of the different NPPs fail roughly the same number of times in the whole time window but that the failures in one NPP occur almost only in the first years of observation and the failures in the other NPPs in the last years of observation which is naturally worse behaviour.

The stratified trend/line graphs in figure 5.2 show that the reliability of the 314 system, at the NPPs behaves indeed differently in time.

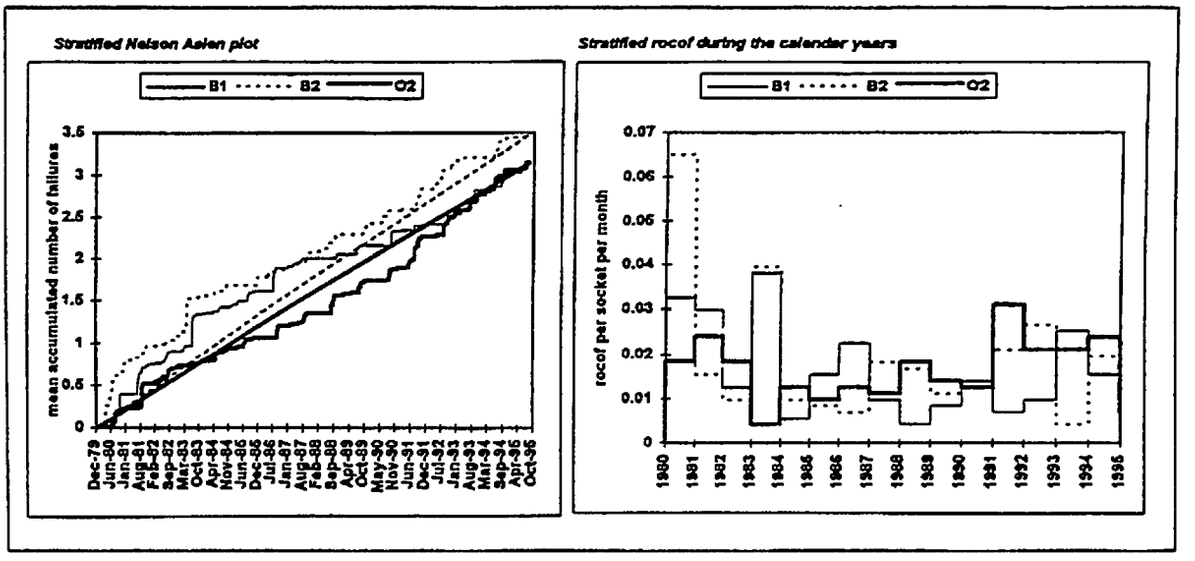


Figure 5.2: Stratified trend/line graphs for the main sockets of the 314 system

The two NPPs at station 1 show a decreasing rocof in time while the NPP at station 2 shows an increasing rocof in time. This would not have been observed when we would only have looked at the outliers control charts. Further, we see that B2 has a peak in the rocof in 1980 and that both B1 and B2 have a peak in 1983. The rocof of O2 gradually increases from 1983 onwards which is a sign of decreasing reliability for the 314 system at this NPP.

We will know look at the population of the main pressure relief valves (V001-V020) and only at the failures of the valve subcomponent. When we want to do a proper survival analysis, it is necessary that there is no trend in the data. For

this reason and for the fact that the maintenance engineer is mostly interested in the recent performance, we chose a time window of the last 10 years, [1-jan-85, 1-sep-95]. On the following pages the report format is given such as generated by the prototype RDB developed in this work (see figure 4.1)

On the first two pages of the reliability report for the main valves at the two NPPs at station 1, the failure/repair sheet is given. We know that the non-emergency maintenance activities for the 314 system are performed during the overhaul periods. This means that when a non-emergency failure is detected in the control room, the maintenance engineer wiats with the repair to the next annual overhaul. This is the reason for the long periods in between failure detection and failure repair on the failure/repair sheet. When we want to look for clusters, we should look whether there are rows (observation months) with several black cells (failure detection at a socket). There are indeed many clusters in the failure processes of the main relief valves at station 1 which could indicate common cause failures (CCF). Furthermore, we spot many early failures after repair for which the failure/repair processes of B2-V002 and B2V003 in the period sep-88 to aug-90 are a good example.

On page 3 of the reliability report for station 1, the outliers control chart of the population of main valves at the two NPPs shows heavy fluctuations. These fluctuations are, however, not yet significant enough ($> 15\%$) to disregard homogeneity and we can continue the analsysis with the assumption of homogeneity in the population.

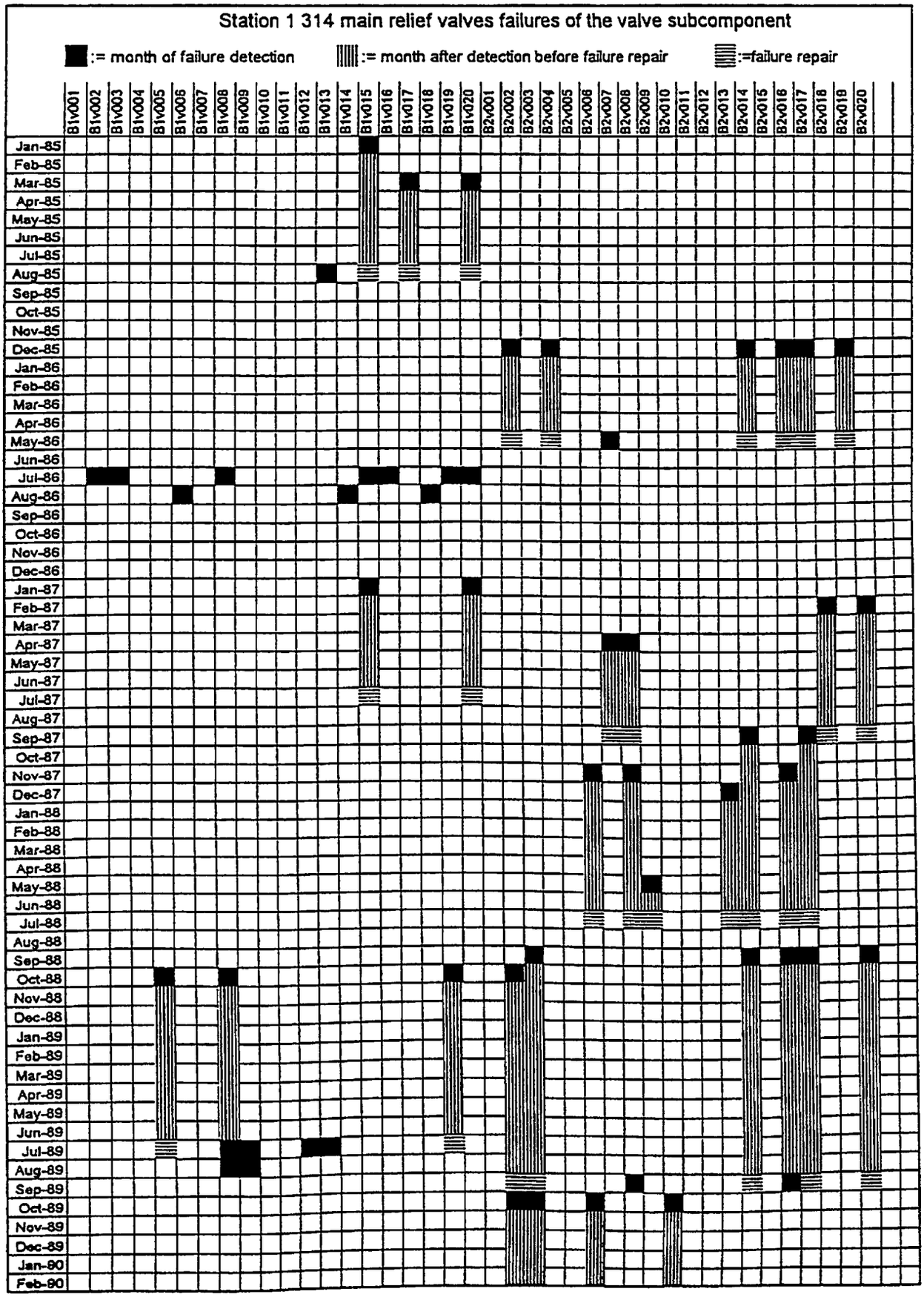
Before we embark on the trend/line graphs, it should be noticed that we do assume that there is *no* significance for clusters in the failure/repair processes of the sockets in the population. We have not yet developed a test that can support this assumption and it might be uncalled for to continue the analysis with this assumption. The Nelson Aalen graph and the rocof graph show a reasonably constant rocof with a dip in 1993. Both the Laplace test and the linear rank test give a significance level of no trend higher than 10% so that survival analysis can be performed. The empirical survival function and time average hazard rate show that there are relatively many early failures after repair. Due to these early failures after repair, the failure process can *not* be regared as Poisson. The significance level for exponentiality is less than 2%.

From page 4 of the reliability report we learn that the repair time for the failures of the valve subcomponent of the main relief valves is very stable. The outliers control chart shows a stable mean time to repair (MTTR) for the sockets in the population. This is again supported by the accumulated number of repairhours and the MTTR during the calendar years. The repair time distribution function shows a big step around 25 hours.

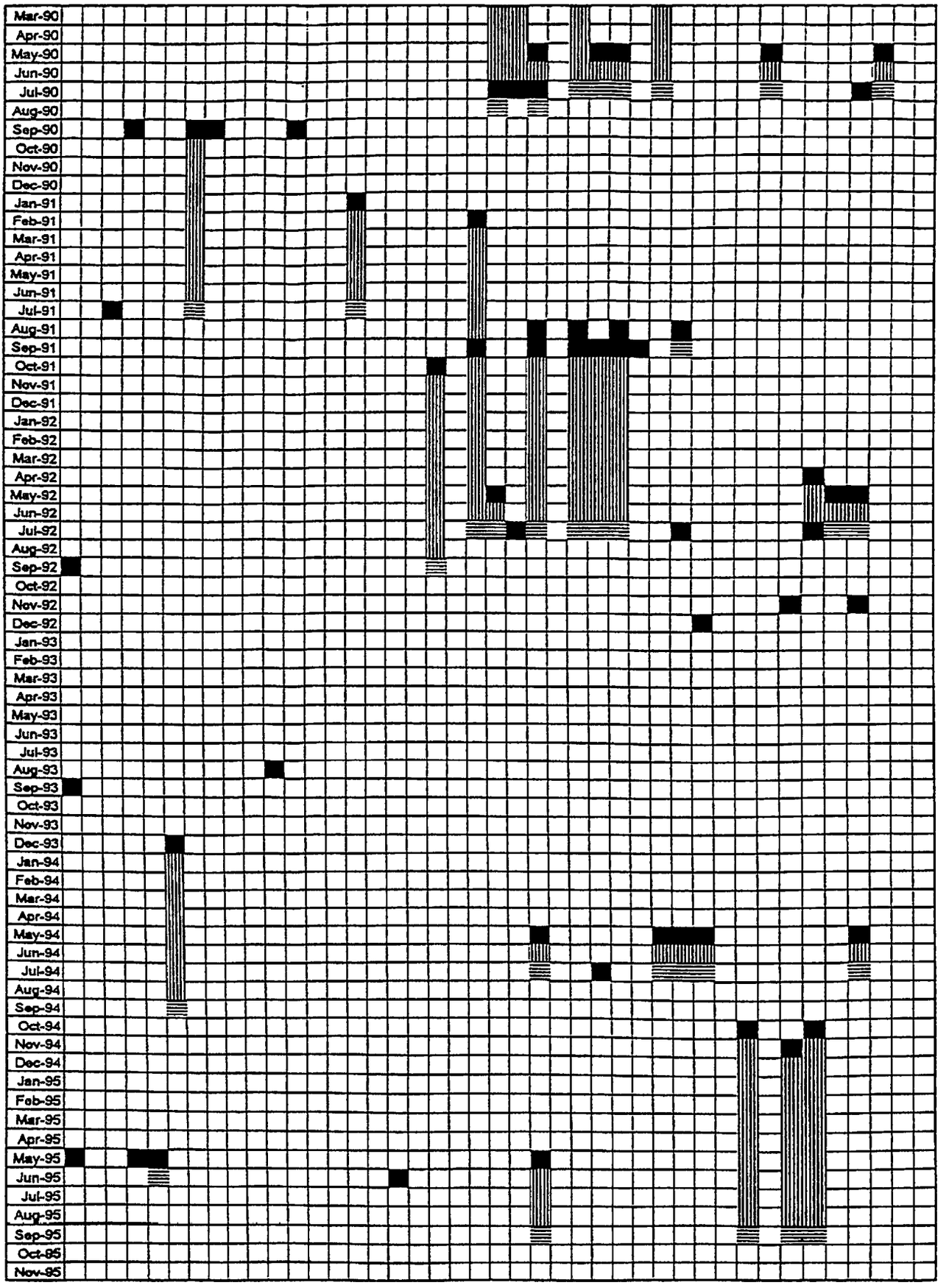
The Pareto diagrams on page 5 of the reliability report show that the main part of the failures (around 70%) is detected in the control room. This is due to the fact that the most part of the failures are leakages which can be detected by sensors. A large part (around 70%) of the repair actions taken, is replacement with the same type of subcomponent so that the renewal process model is justified.

The subsurvival functions for functional and non-functional failures show that up til around 60 months after repair the probability that the sockets service sojourn will end in a non-functional failure is larger than the probablity that the service sojourn will end in functional failure. This is also what the reliability staff prefers as a situation. The conditional subsurvival functions show no definite pattern of relation although we learn that there are many early functional failures after repair. the prefered situation would be when the conditional subsurvival function for the non-functional failures lies just underneath the conditional subsurvival function of the functional failures. This would have meant that the probability of a non-functional failure repair is higher than the probability of a functional failure *and* the repair of the non-functional failure is just before the subcomponent fails functionally. Again we stress that this last aspect is *not* yet the case at station 1.

Station 1 reliability report page 1



Station 1 reliability report page 2



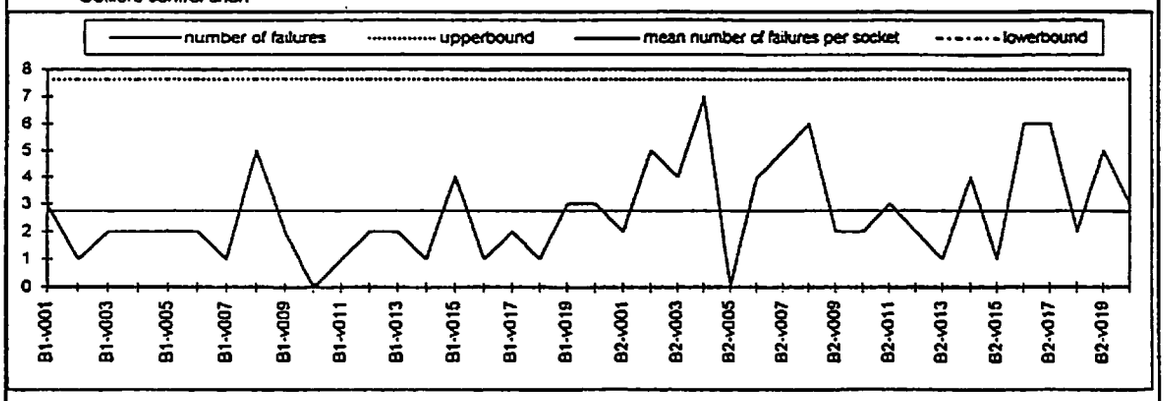
Station 1 reliability report page 3

Station 1 314 main relief valves failures of the valve subcomponent

start observation : 1-Jan-85 stop observation : 1-Sep-95 total observation time = 128 months

number of sockets = 40 number of failures = 110 mean number of failures per socket = 2.75

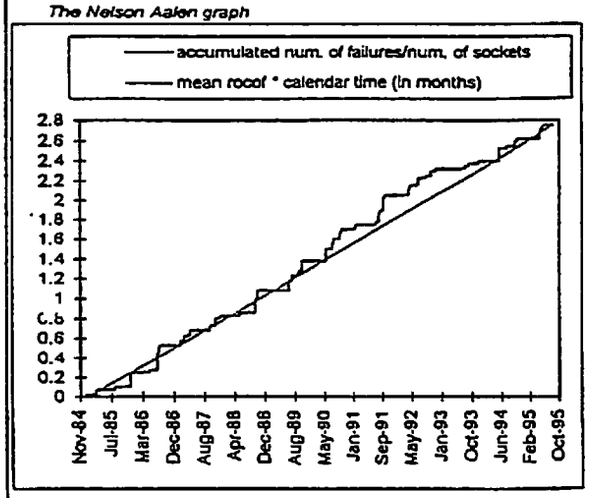
Outliers control chart



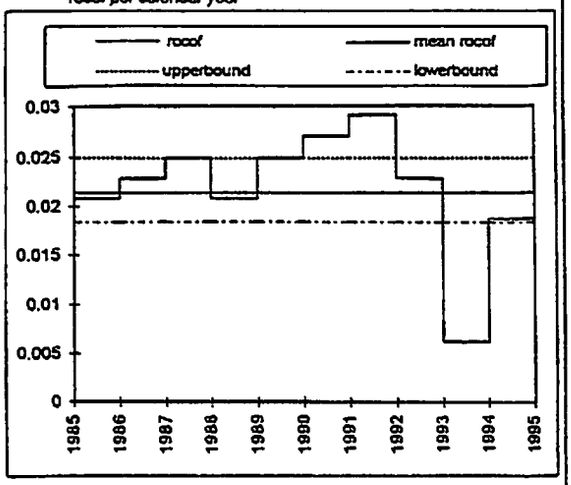
Significance level of homogeneity in the population: 0.18

mean rate of occurrence of failures (rocof) = 0.021 failures per socket per month

The Nelson Aalen graph



rocof per calendar year

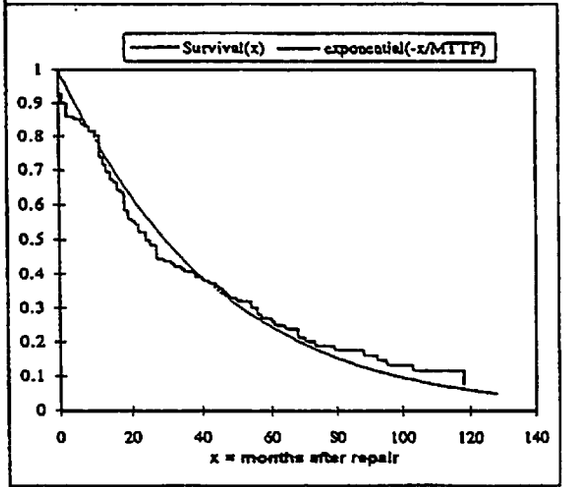


Laplace significance level of no trend: 0.31 Linear rank significance level of no trend: 0.12

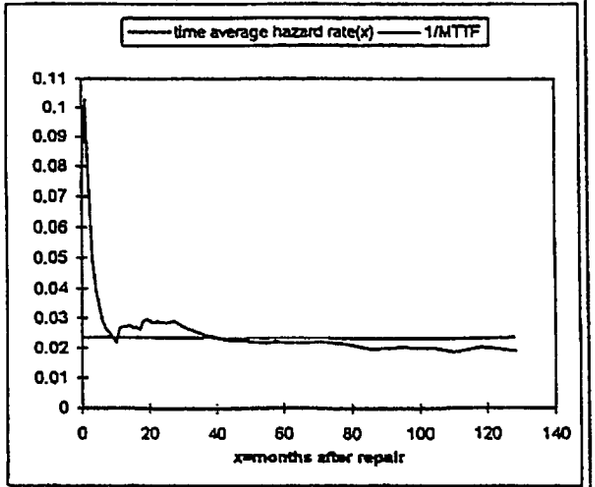
mean time between failure = 46.55 months = 1/ mean rocof

mean time to failure (MTTF)= 42.59 months

Empirical survival function



Time average hazard rate



Significance level of exponentiality: 0.01

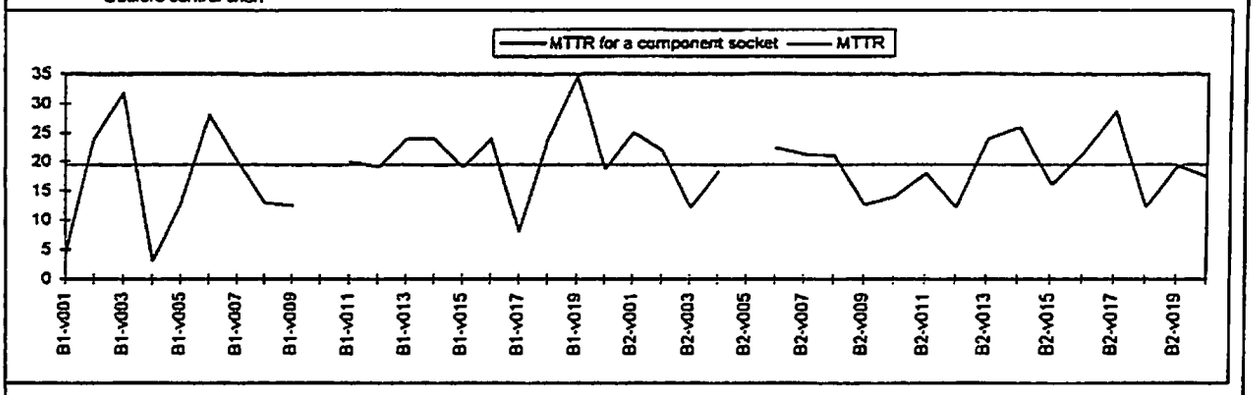
Station 1 reliability report page 4

Station 1 314 main relief valves failure of the valve subcomponent

start observation : 1-Jan-85 stop observation : 1-Sep-95 total observation time = 128

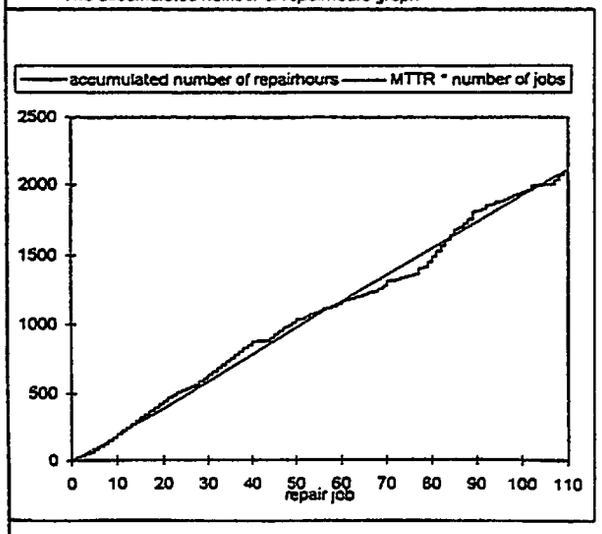
number of sockets = 40 number of repairs = 110 mean number of repairjobs per socket = 2.75

Outliers control chart

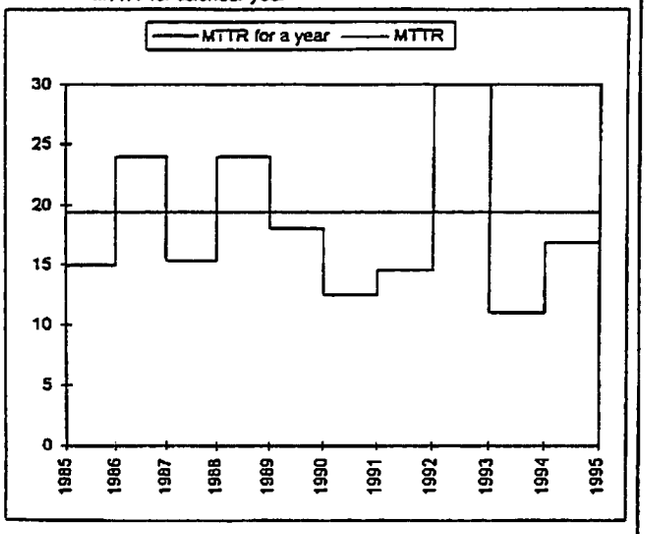


mean time to repair (MTTR) = 19.41 hours

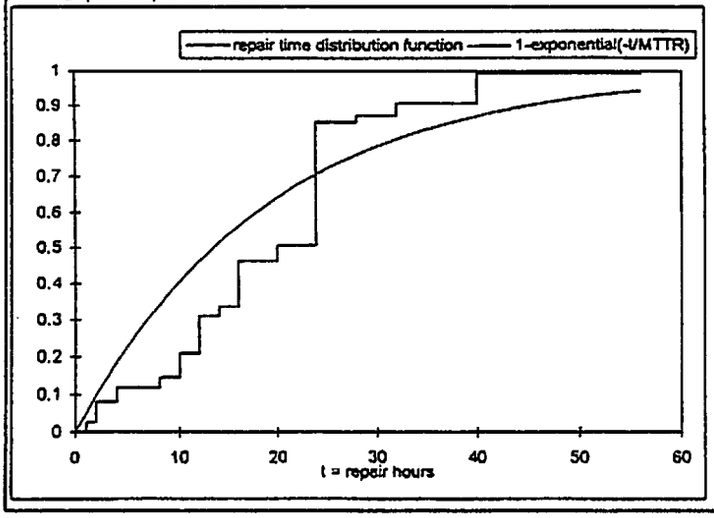
The accumulated number of repairhours graph



MTTR for calendar year



Empirical repairtime distribution function

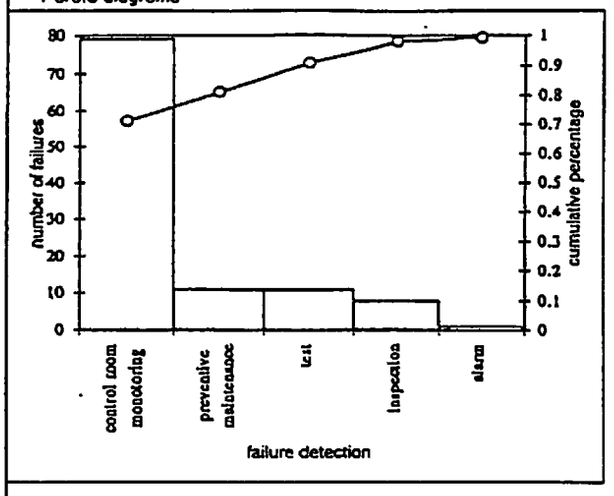


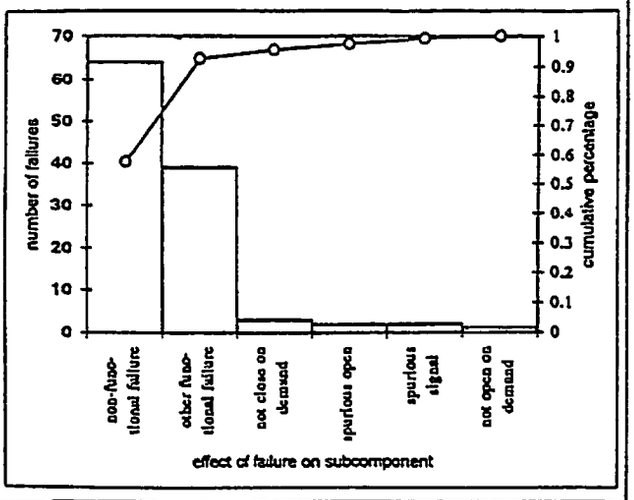
Station 1 reliability report page 5

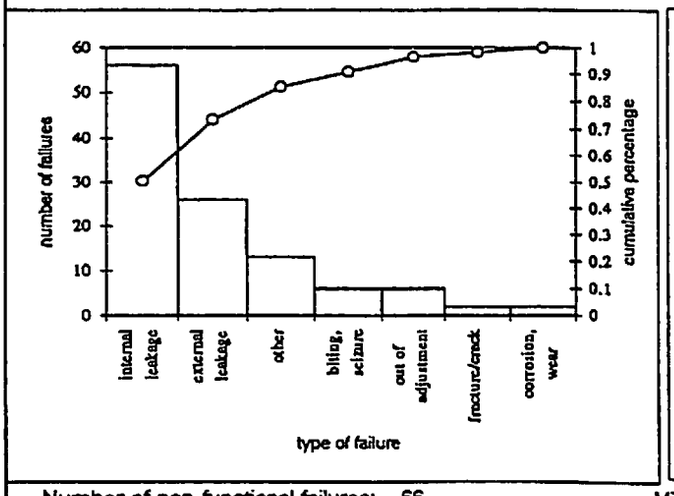
Station 1 314 main relief valves failures of the valve subcomponent

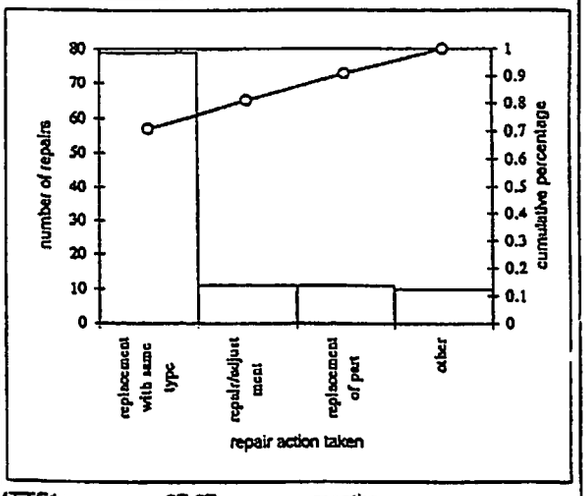
start observation : 1-Jan-85 stop observation : 1-Sep-95 total observation time = 128 months
number of sockets = 40 number of failures= 110

Pareto diagrams



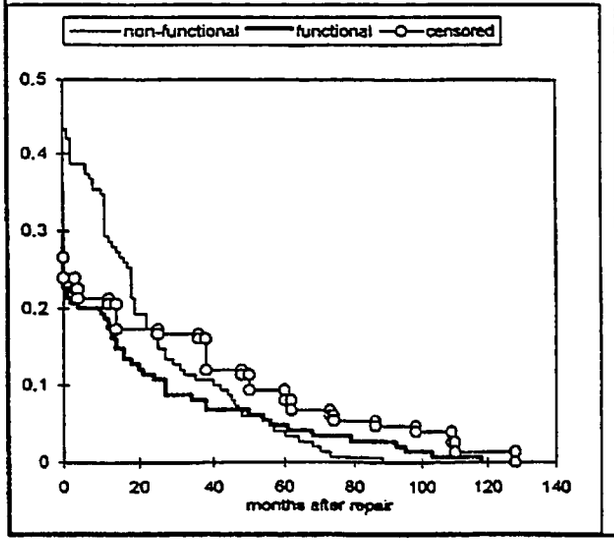




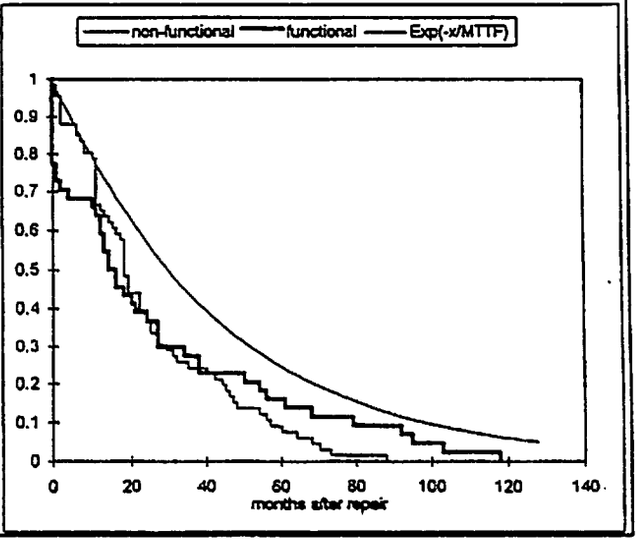


Number of non-functional failures: 66 MTTF1: 37.67 months
Number of functional failures: 44 MTTF2: 33.57 months

Subsurvival functions



Conditional subsurvival functions



On the first two pages of the reliability report for the main valves at the NPP at station 2, the failure/repair sheet is given. We know that the non emergency maintenance activities for the 314 system are performed during the overhaul periods. Yet, the periods from failure detection to failure repair are much smaller than for station 1. When we want to look for clusters, we should look whether there are rows (observation months) with several black cells (failure detection at a socket). There are many clusters in the failure processes of the main relief valves at station 2 which could indicate common cause failures (CCF). We spot not as many early failures after repair as for the main valves of station 1.

On page 3 of the reliability report for station 2, the outliers control chart of the population of main valves at the NPP shows heavy fluctuations. These fluctuations are, however, not yet significant enough ($> 5\%$) to disregard homogeneity and we can continue the analsysis with the assumption of homogeneity in the population.

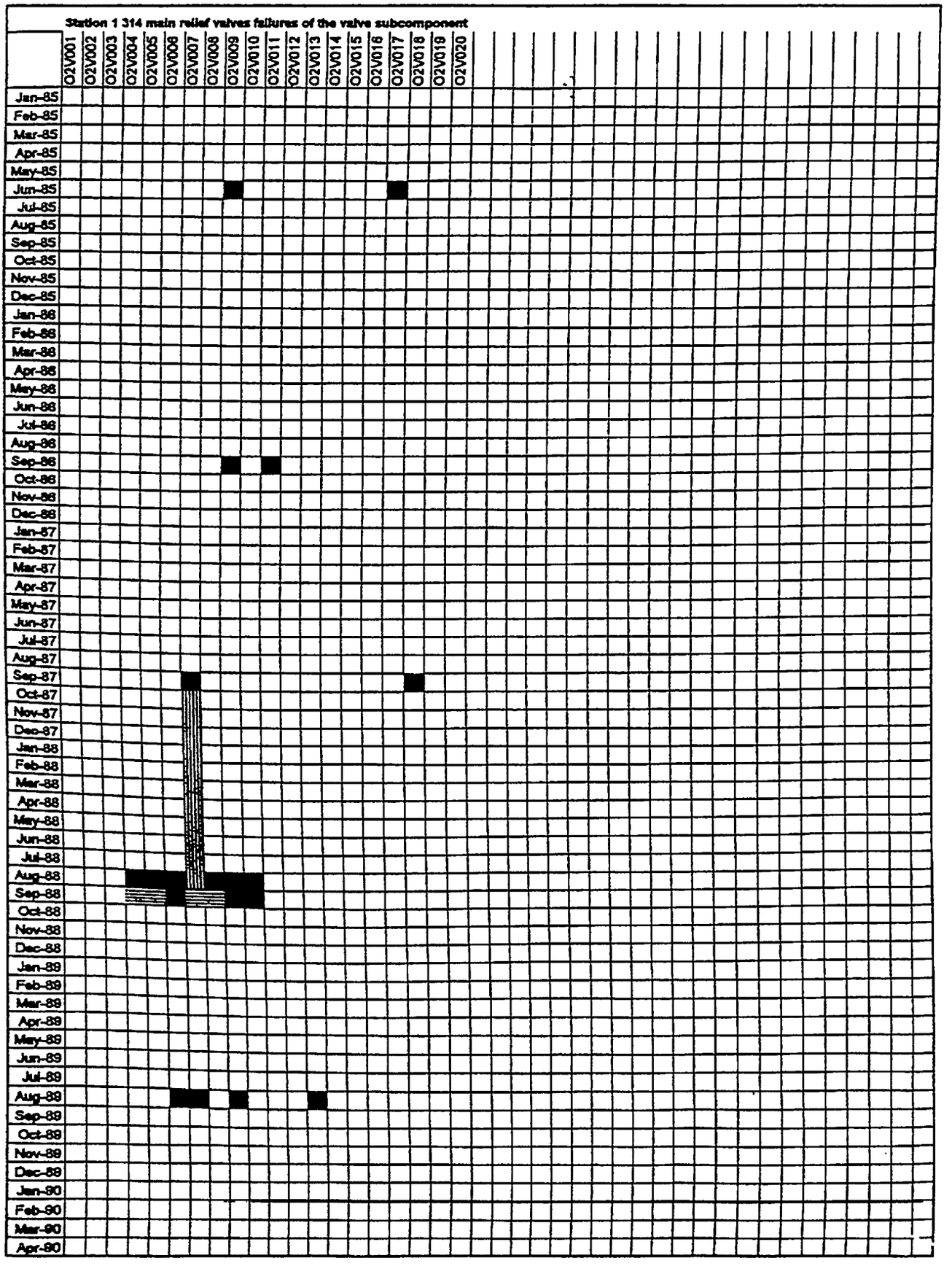
Before we embark on the trend/line graphs, it should be noticed that we do assume that there is *no* significance for clusters in the failure/repair processes of the sockets in the population. We have not yet developed a test that can support this assumption and it might be uncalled for to continue the analysis with this assumption. The data is rather sparse which accounts for the step like behaviour in the Nelson Aalen graph and survival function. The Nelson Aalen graph and the rocof graph show a reasonably constant rocof with a peak in 1991 and a dip in 1993 (as for station 1). Both the Laplace test and the linear rank test give a significance level of no trend higher than 25% so that survival analysis can be performed. The empirical survival function and time average hazard rate show a reasonable fit with the exponential distribution. This is due to the fact that there are less early failures after repair than at station 1. The significance level for exponentiality is larger than 15%.

From page 4 of the reliability report we learn that the repair time for the failures of the valve subcomponent of the main relief valves is fluctuating much. The accumulated number of repairhours graph shows that the MTTR is getting smaller with the number of repair jobs performed. This can be largely accounted for by the year 1985 which is a strong peaking outlier for the MTTR used for the repair jobs. during the calendar years. The repair time distribution function shows a big step around 18 hours. The MTTR at station 2 is a little smaller than at station 1.

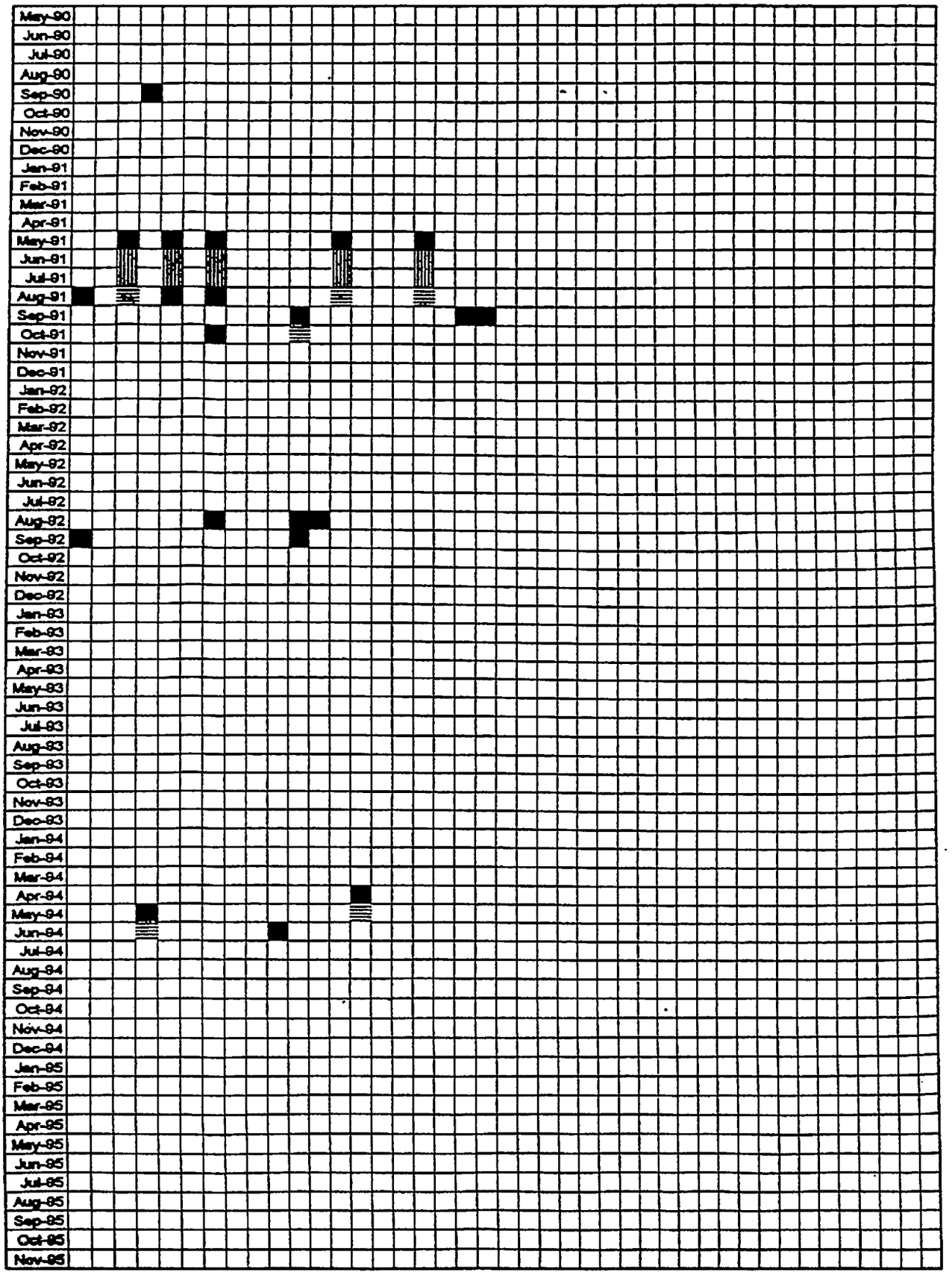
The Pareto diagrams on page 5 show roughly a similar picture as for station 1 except for the effect of the failure. The main part of the failures (around 60%) is detected in the control room. This is due to the fact that the most part of the failures are leakages which can be detected by sensors. A large part (around 70%) of the repair actions taken is replacement with the same type of subcomponent so that the renewal process model is justified. The subsurvival functions for functional and non-functional failures show a reverse picure compared to station 1. Up til around 60 months after repair the probability that the sockets service sojourn will end in a non-functional failure is larger than the probablity that the service sojourn will end in functional failure. This is also what the reliabil-

ity staff prefers as a situation. The conditional subsurvival functions show no definite pattern of relation although the conditional subsurvival function for the functional failure lies roughly close under the conditional subsurvival function of the non-functional failures. This is in fact what the maintenance engineer wants to achieve but in combination with a subsurvival function of non functional that lies *above* that of functional failures.

Reliability Report station 2 page 1



Reliability Report station 2 page 2



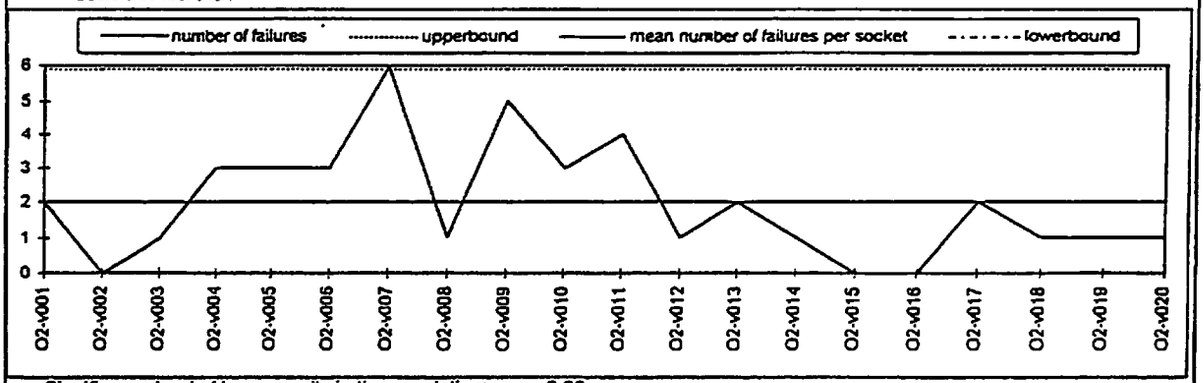
Reliability Report station 2 page 3

Station 2 314 main relief valves failures of the valve subcomponent

start observation : 1-Jan-85 stop observation : 1-Sep-95 total observation time = 128 months

number of sockets = 20 number of failures = 40 mean number of failures per socket = 2.00

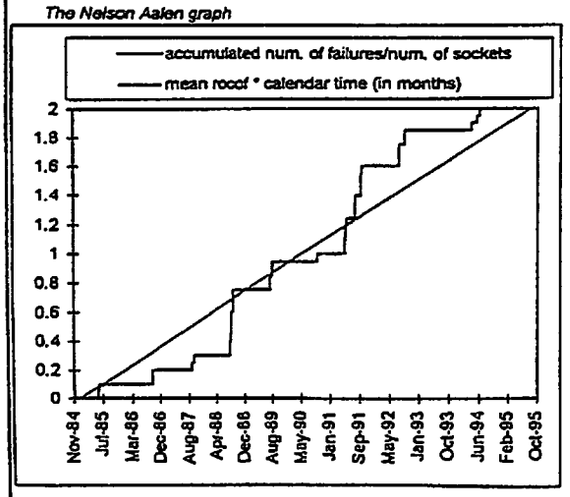
Outliers control chart



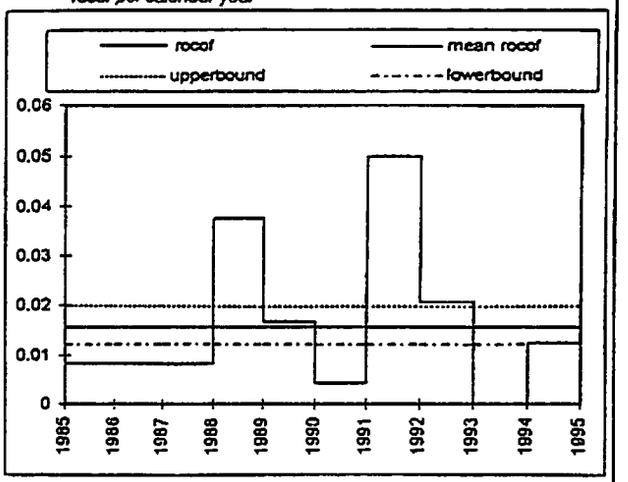
Significance level of homogeneity in the population: 0.09

mean rate of occurrence of failures (rocof) = 0.016 failures per socket per month

The Nelson Aalen graph



rocof per calendar year

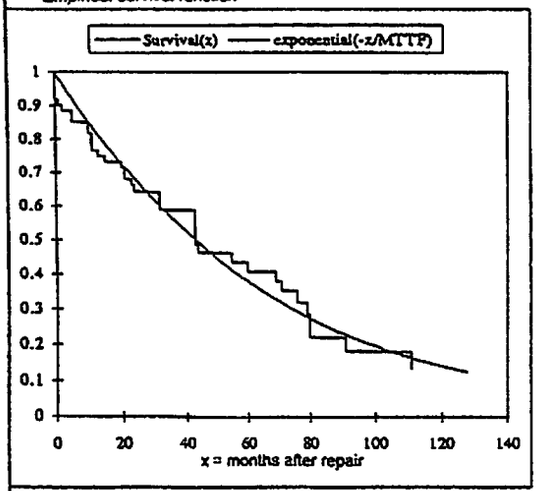


Laplace significance level of no trend: 0.87 Linear rank significance level of no trend: 0.28

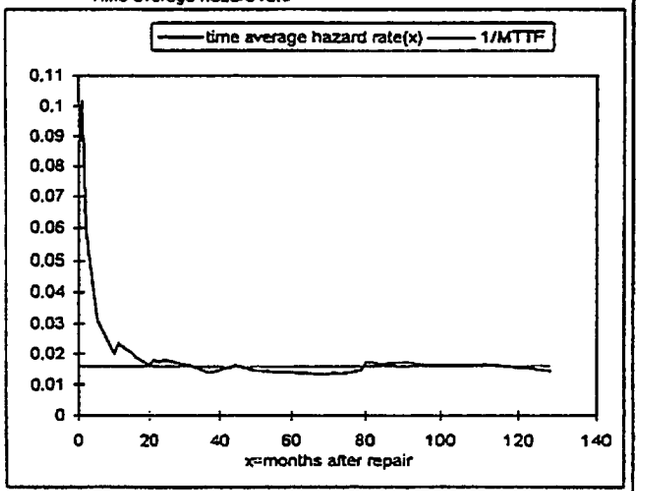
mean time between failure = 64.00 months = 1/ mean rocof

mean time to failure (MTTF)= 63.10 months

Empirical survival function



Time average hazard rate



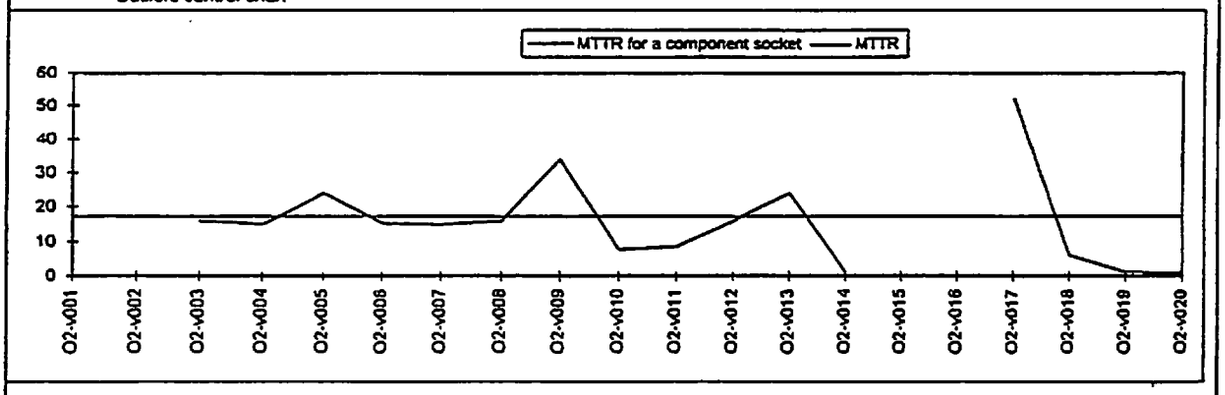
Significance level of exponentiality: 0.15

Reliability Report station 2 page 4

Station 2 314 main relief valves failure of the valve subcomponent

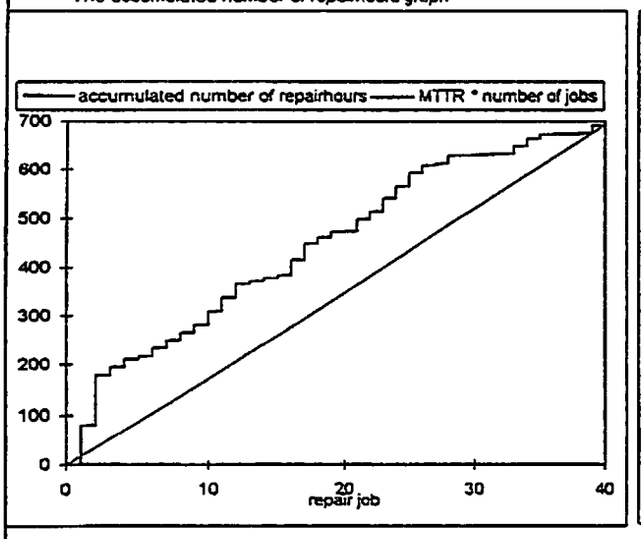
start observation :	1-Jan-85	stop observation :	1-Sep-95	total observation time =	128
number of sockets =	20	number of repairs =	40	mean number of repairjobs per socket =	2.00

Outliers control chart

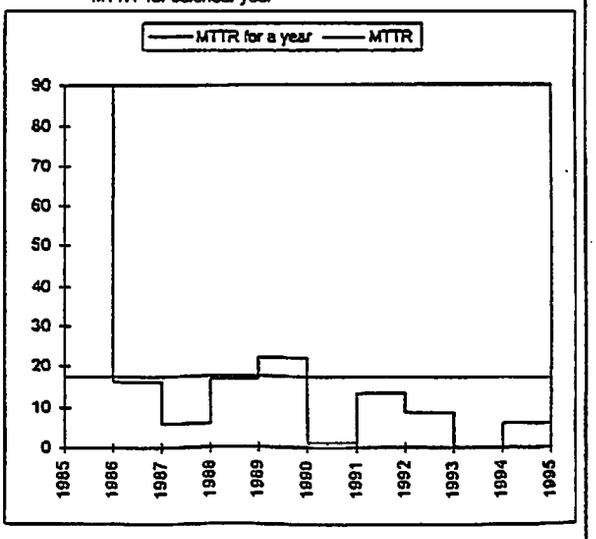


mean time to repair (MTTR) = 17.33 hours

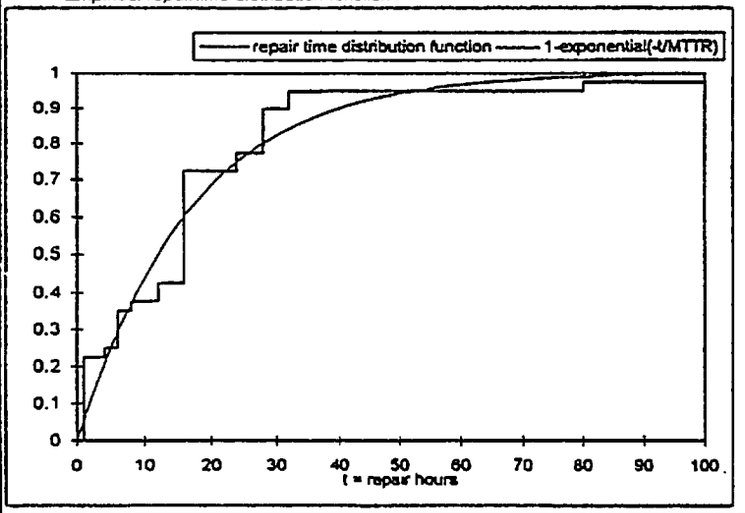
The accumulated number of repairhours graph



MTTR for calendar year



Empirical repairtime distribution function



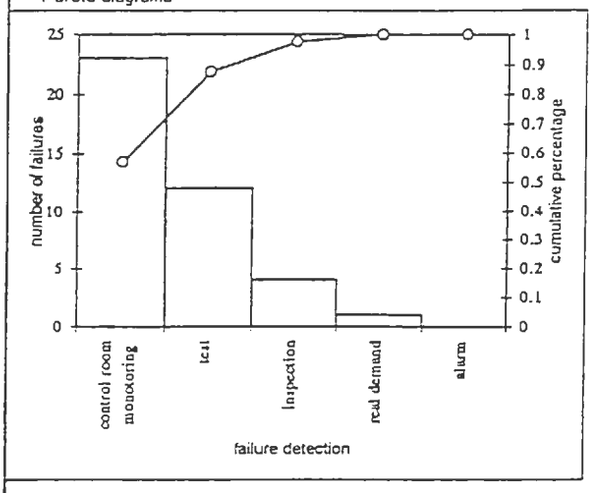
Reliability Report station 2 page 5

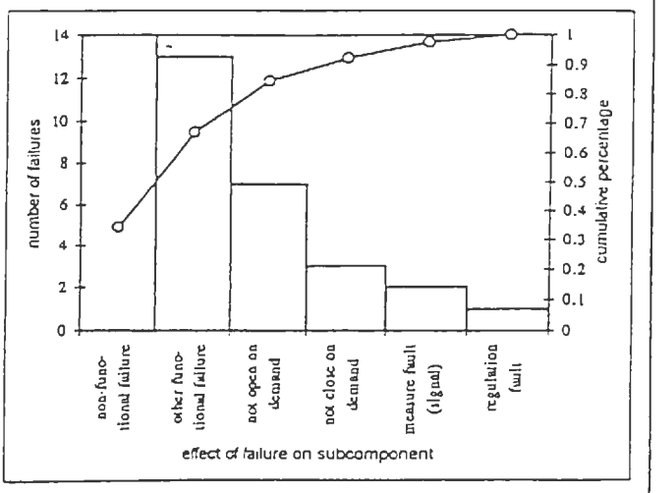
Station 2 314 main relief valves failures of the valve subcomponent

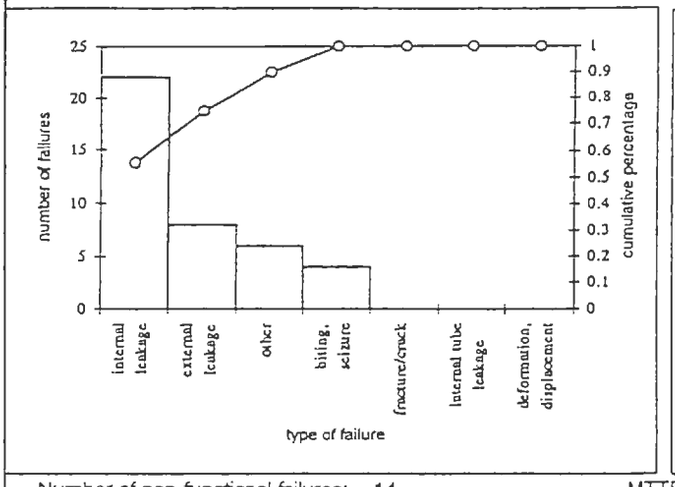
start observation : 1-Jan-85 stop observation : 1-Sep-95 total observation time = 128 months

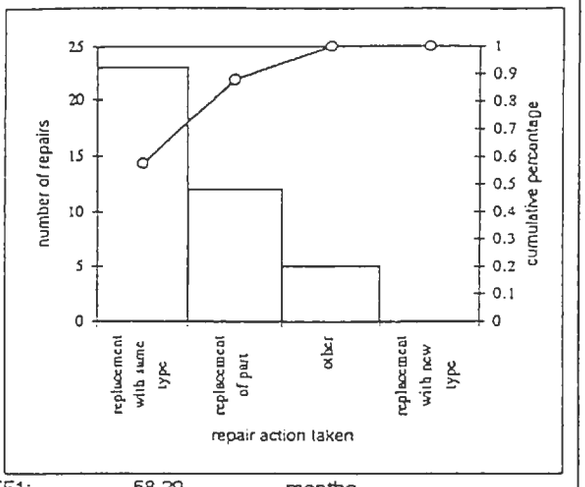
number of sockets = 20 number of failures= 40

Pareto diagrams



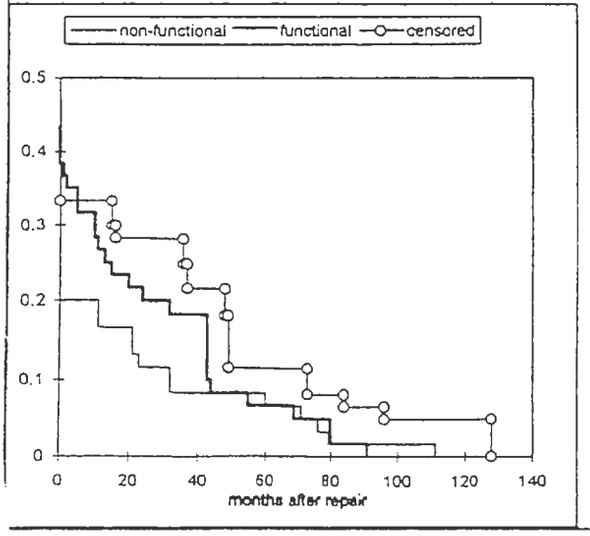




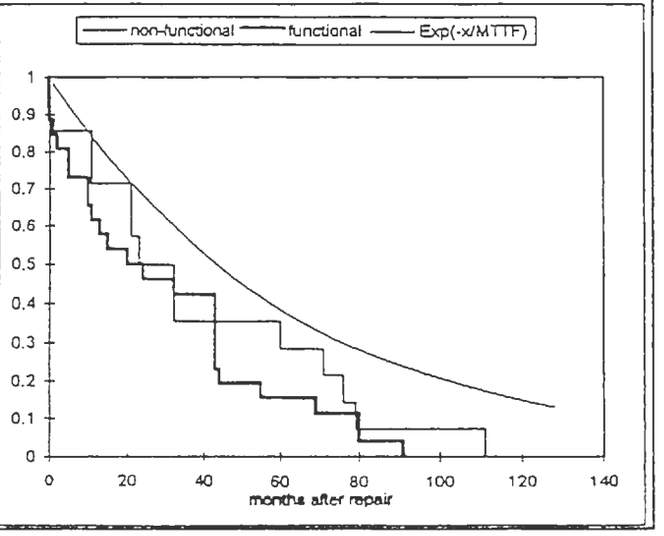


Number of non-functional failures:	14	MTTF1:	58.29	months
Number of functional failures:	26	MTTF2:	59.81	months

Subsurvival functions



Conditional subsurvival functions



5.2.2 Core vessel spray system, 323

The core vessel spray system is described in section B.3. In this section we analyse the TUD data from the population of all main sockets of the 323 system such as given in table B.2. We look at the failure/repair processes of these component sockets in the time window, [1-jan-80, 1-sep-95].

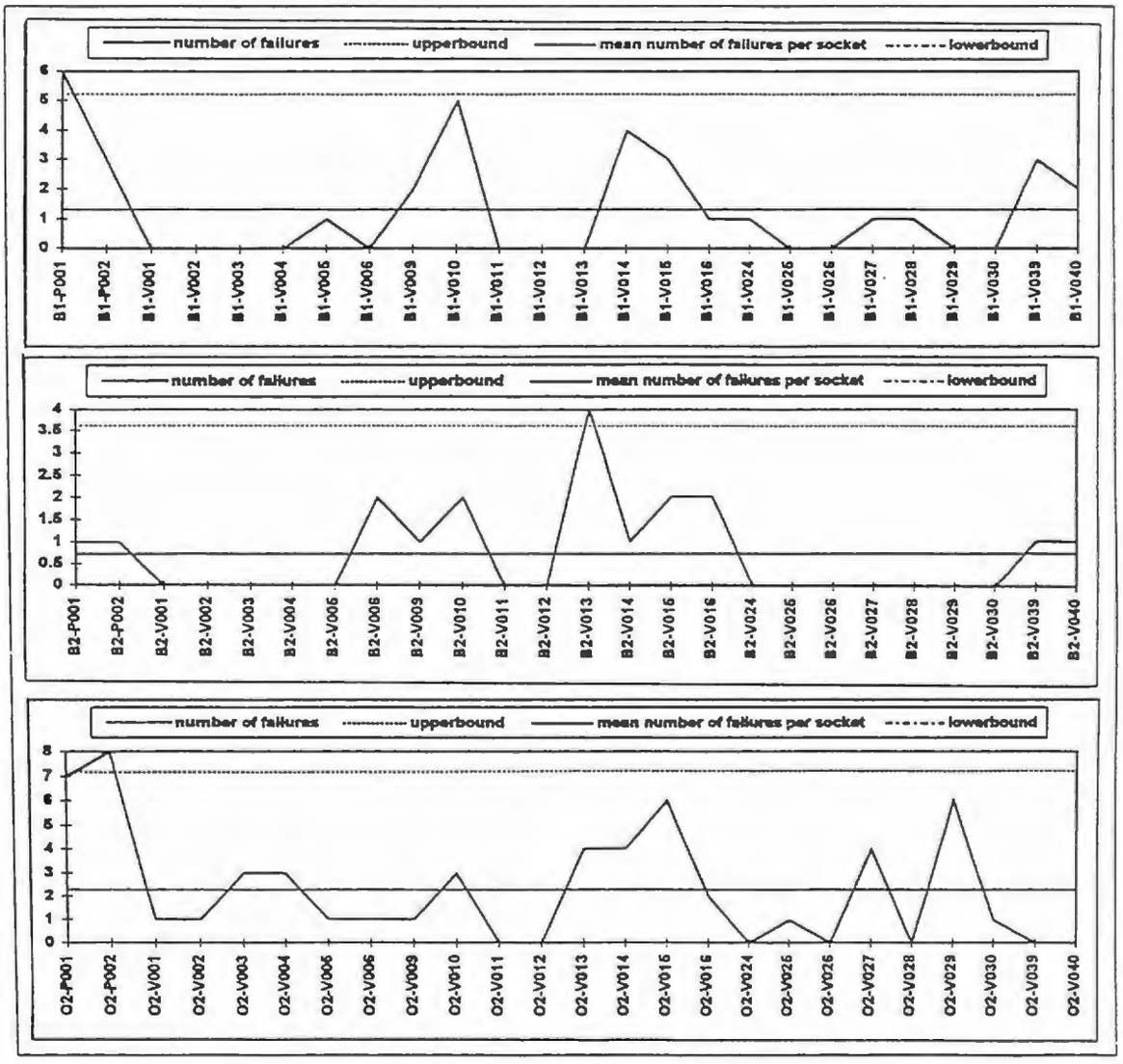


Figure 5.3: Outlier control chart for the main sockets of the 323 system at the three NPPs

In figure 5.3 the behaviour of the main sockets of the 323 system such as given in table B.2 for the three NPPs can be checked. The main sockets of the 323 system exist of different types of valves and pumps and do *not* form a homogeneous population. The outliers control charts show that the number of failures for the different sockets of the 323 system at the three NPPs is fluctuating heavily. Although the mean number of failures per socket of B1 is much higher

than at B2, the pattern of failures is rather similar for these two NPPs. It should be noticed that the check valves (V001,V002,V011,V012,V025,V026) at both B1 and B2 do not fail at all which is not the case for O2. The centrifugal pumps at B1 fail very seldom compared to the other NPPs. The mean number of failures for the sockets of the 323 system at O2 is much higher than at the other NPPs and compared with station 1 it is apparant that the safety valves (V039,V040) do not fail.

It is now interesting to see the time behaviour of the failures at the different NPPs. We should then look more at trends than at magnitude when we want to compare the three NPPs. The stratified trend/line graphs in figure 5.4 show that the reliability of the 323 system, at the NPPs behaves indeed differently in time.

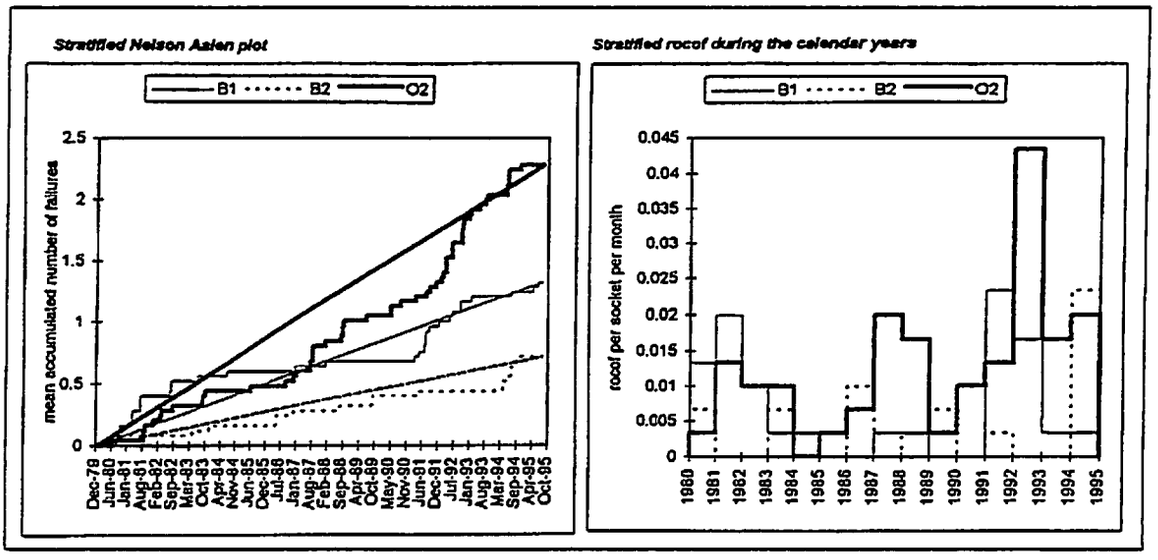


Figure 5.4: Stratified trend/line graphs for the main sockets of the 323 system

From the Nelson Aalen graph we learn that the rocof of B1 first decreases and then increases. B2 shows a slowly increasing rocof in time and O2 shows a strong increase in the rocof in time. All three NPPs show roughly an increasing rocof which means that the reliability of the 323 system decreases. When we look at the rocof during the calendar years we see a strong fluctuation for all three NPPs. There are even calendar years where the whole system does not fail at all. There are peaks in the rocof In 1992 for O2 and in 1994 for B2.

5.3 Conclusions

The main goal of the work was the development of methods/tools that can be installed at the TUD database and help the users with analysing the TUD-data. More specifically, these tools should be able to measure maintenance performance.

During this work we soon found out that the TUD database does *not* record all the maintenance actions on the components sockets at the NPPs. This aspect of the data is described in section 2.3 and boils down to the fact that only *corrective* maintenance actions (repairs) are reported to the TUD database and not the preventive maintenance actions. This makes an accurate measure of the maintenance performance based on this data alone, difficult. To illustrate the problem, lets take two components whose failure/repair history is practically the same but whose preventive maintenance history very much differs. The maintenance perfrrmance of the component with the most preventive maintenance actions is then obviously worse than the one who "achieves" the same reliability with less preventive maintenance actions (less costs such as illustrated in figure 3.1). In other words, we can judge the reliability of the components with the TUD data but *not* the underlying maintenace program.

Due to this aspect of the data we took a broader "reliability" approach to the analysis of the data than specific maintenance performance measures. This resulted in a prototype reliability database (RDB) based on the information and structure of the TUD database but with a set of tools installed that can suit the different information needs of the TUD-users such as described in table 4.1. The prototype RDB guides the user through the analysis steps and generates a so called reliability report on the population of component sockets chosen by the user. An example of such a reliability report is given in the previous section together with an interpretation of the results.

Discussions with the maintenance engineers and risk/reliability staff let us to believe that the tools so far developed, can support both the mainteance staff and the risk/reliablity staff in their daily work. When the maintenance engineer wants to alter the maintenance program on component sockets of importance to the safety of the NPP, this must be discussed with risk/reliability staff. The motivation for altering the maintenance program, needs to be motivated and supported with properly analysed operating experience data. Further, the maintenance staff at a NPP is submitted to changes in personnel and newcomers can be better prepared to their job by learning from the operating experience data.

The other user group, the risk/reliability staff uses, so far, mostly the data processing methods (see [Pörn, 1990] and [Cooke et al.,1995]) that result in the figures published in the T-book [T-book, 1995] every two years. Nevertheless, this user group needs to judge the maintenance performance and reliability of the safety critical components and is helped with an updated "on line" possibility of analysis, such as made possible with the "client server" relational database structure of the TUD database (see figure 1.1).

The tools developed in this work are in fact the first steps of reliability data analysis and can be followed by more sophisticated methods in the future. Yet,

the results in practice of these methods should be judged from the quality of the data that are avaliable at that moment. The results of the tools developed in this work should therefore be handled carefully when there exists uncertainty about the coverage and homogeneity of the recording such as decribed in section 2.3. Nevertheless, the coverage and homogeneity of the data can improve when the maintenance personnel knows that their recoding work leads to improvement in their daily work.

In 1996 this work will continue and the data recorded in the local maintenance databases will be incorporated to judge maintenance performance. Further, there is a need for the analysis of data from condition monitoring of components so that preventive maintenance actions can be optimally planned.

Bibliography

[Ascher and Feingold, 1984] H.E. Ascher and H. Feingold (1984) *Repairable systems reliability*, Marcel Dekker, New York.

[Cooke et al., 1993] R.M. Cooke, T.Bedford, I. Meilijson and L. Meester (1993) *Design of reliability databases for aerospace applications*,Report of Faculty of Technical Mathematics and Informatics at the Technical University Delft 93-110.

[Cooke et al.,1995] R.M. Cooke, J.W. Dorrepaal and T. Bedford (1995) *Review of SKI Data Processing Methodology*, SKI Report 95:2, Swedish Nuclear Power Inspectorate 1995.

[Cox,1962] D.R. Cox (1962) *Renewal Theory*, Methuen & Co LTD, London.

[Cox and Lewis, 1966] D.R. Cox and P.A.W. Lewis (1966) *The Statistical Analysis of Series of Events*, Methuen & Co LTD, London.

[Cox and Oakes, 1984] D.R. Cox and D. Oakes (1984) *Analysis of Survival Data*, Chapman and Hall, London/New-York.

[Hokstad, 1993] P. Hokstad (1993) *Reliability Modelling and the Martingale Intensity Process*, SRE-93 symposium i Malmö.

[Kalbfleish and Prentice, 1980] J.D.Kalbfleisch and R.L.Prentice (1980) *The statistical analysis of failure time data*, John Wiley and Sons, Inc New York.

[Laakso et al.,1990] K.Laakso, M.Knochenhauer, T.Mankamo and K.Pörn (1990) *Optimization of technical specifications by use of probabilistic methods*, final report of Nordic research project in reactor safety, NKA-RAS-450.

[Laakso and Simola, 1992] K. Laakso and K. Simola (1992) *Analysis of failure and maintenance of motor operated valves in a Finish muclear power plant*, VTT Research Notes 1322.

[Laakso et al., 1995] K. Laakso, S. Hänninen and L. Hallin (1995) *How to evaluate the effectiveness of a maintenance program*, paper presented at BALTICA III, International Conference on Plant Condition and Life Management. Helsinki-Stockholm, june 6-9,1995.

[Mankomo, 1991] T. Mankamo (1991) *CCF Analysis of High Redundancy Systems Safety/relief valve data analysis and reference BWR application*, SKI Technical Report NR 91:6, Swedish Nuclear Power inspectorate 1991.

[Møltoft, 1994] J. Møltoft (1994) *Reliability engineering based on field information -the way ahead*, Quality and reliability engineering international Vol 10 399-409, 1994.

[Peterson, 1976] A.V. Peterson (1976) *Bounds for a joint distribution function with fixed subdistribution functions: Application to competing risks*, *Oroc. Nat. Acad. Sci. USA*, 73 (1),11-13.

[Pörn, 1990] K. Pörn (1990) *On Empirical Bayesian Inference Applied to Poisson Probability Models*, Linköping Studies in science and Technology, Dissertation No. 234, Linköping.

[Sandén and Chockie, 1994] P. Sandén and A.Chockie (1994) *SKI Reference Book, Maintenance* Prepared for the Swedish Nuclear power Inspectorate (SKI).

[T-book, 1995] T-book, reliability data of components in Nordic Nuclear Power Plants, 4rd edition (1995).

[Tsiatis, 1975] A. Tsiatis (1975) *A nonidentifiability aspect in the problem of competing risks*, *Proc. Nat. Acad. Sci. USA*, 72 20-22.

Appendix A

Statistical support

A.1 Introduction

We consider the situation where the user has chosen the following set-up for the start of the analysis:

(i) a population of sockets (component or subcomponent level);

(ii) stratification of this population into strata;

(iii) a time-window in which to analyse the failure events;

(iv) one or more types of failure events.

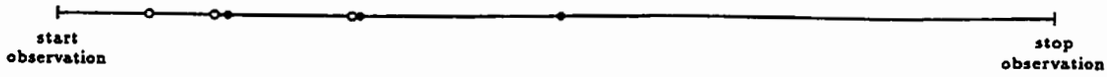
The failure history of a (sub)component socket can be considered as a series of events distributed haphazardly along the time axis. It is a realization of a so called *stochatic point process* (SPP). Typical, the user can choose to make distinctions between the failure events that occur at a socket. There are now two possibilities:

1. The user wants to investigate the interdependence between the different types of failure events;
2. The user wants to make no distinctions between the different types of failure events.

These situations are pictured in figure A.1 and A.2.

Guided by the information needs of the users, we have developed a set of analysis tools, which are presented in chapter 4. Generally, all these tools consist of the following three ingredients

1. a graph or chart possibly with confidence bounds;
2. control limits drawn on the graph;
3. numerical support (significant level, estimate of mean,..)



o = type 1 failure ; • = type 2 failure

Figure A.1: Series of two types of failure events

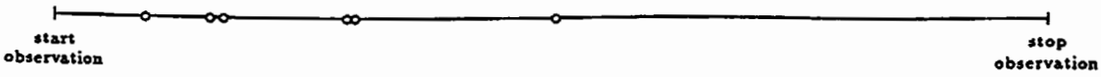


Figure A.2: Series of both types of failure events

The working of the tools is simple. The graphs are in fact, *statistical estimators* of probabilistic descriptions or models of the series of events. Along with these statistical estimators, confidence bounds can be generated. Next, a statistical test can be developed that generates the control limits for the data when a set of model assumptions is valid. When a graph or chart breaks through its control limits, this is an indication for the user to reconsider whether the set of model assumptions is plausible.

The purpose of this chapter is to give the statistical background for the possible "ingredients" of a tool; estimators, confidence bounds, control limits and significance levels. First we give the set of model assumptions which the user can make when applying a tool and discuss their plausibility. Second the graphical representations of the series of failure events are discussed. The *trend/line graphs* presented in subsection 4.3.2 are captured in the counting process description of the series of events. The counting process description will be discussed in section A.3. The *survival/frequency graphs* discussed in subsection 4.3.3 are based on the sequence of inter-event times description. This description will be discussed in section A.4. Next, the *subsurvival/frequency graphs* of subsection 4.3.4 are based on the competing risk analysis which will be described in section A.5. Third, the significance tests are discussed which generate the control limits and significance levels to the graphs.

A.2 Model assumptions

In this section, the set of model assumptions is given and their plausibility is discussed. In figure A.3 an overview is given of the model assumptions that need to be made for the different models of the series of events which is also called in literature a *stochastic point process (SPP)*.

Model assumption 1 : *The stratum (subgroup) of n sockets is homogeneous*

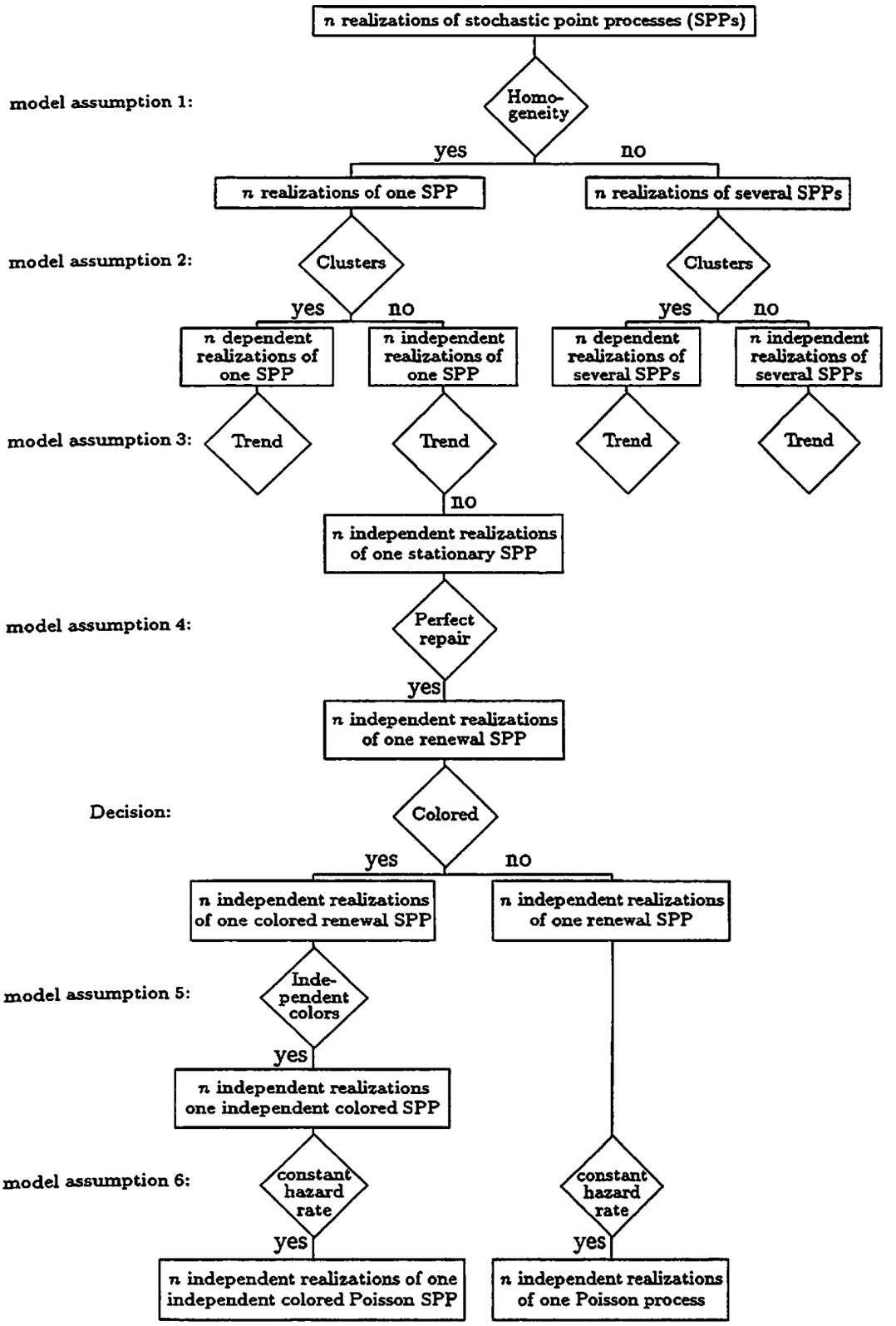


Figure A.3: Model assumptions for a population of (colored) stochastic point processes

Homogeneity within a group of (sub)component sockets can be assumed in the case that the (sub)components are similar in design, operating circumstances

and maintenance/test regime. Nevertheless, this assumption should always be checked with the failure data on these (sub)component sockets. In the case of outliers, the user can decide to treat these separately. A significance test for heterogeneity is given in the section A.6.

Model assumption 2 : *The failure/repair processes of the n different sockets in a stratum are independent*

What we in fact assume is that there are no *clusters* of failures in the stratum of sockets. In the extreme case all the sockets in the stratum could fail together in a small interval on the (calendar) time axis. This would indicate a strong dependency between the sockets and a possible common external cause of the failures in the sockets. This assumption should therefore always be checked.

Model assumption 3 : *The failure/repair process of a socket in a stratum is stationary*

In mathematical terms a *stationary series of events* is defined by the following requirements:

(a) the distribution of the number of events in a fixed interval $(t_1', t_1'']$ is invariant under translation, i.e. is the same for $(t_1' + h, t_1'' + h]$ for all h;

(b) the joint distribution of the numbers of events in fixed intervals $(t_1', t_1'']$, $(t_2', t_2'']$, is invariant under translation, i.e. is the same for the pair of intervals $(t_1' + h, t_1'' + h], (t_2' + h, t_2'' + h]$ for all h;

(c) generally the same invariance property must hold for the joint distribution of the number of events in a set of k fixed intervals, for all $k = 1, 2, \ldots$.

Characteristics of a stationary series of events of importance to this work are:

* the distribution of the number of events in an interval of the time window depends only on the length of the interval;

* the *expected number of failure events in an interval of the time window* is proportional to the length of the interval;

* there exists no trend in the *mean rate of occurrence of failure events* throughout the length of the time window.

The assumption of stationarity might not hold when for example the time window is large and the socket is subject to ageing/degradation or improvement due to modifications. Stationarity should therefore always be tested. Significance tests for trend in the rate of occurrence are discussed in section A.6.

Model assumption 4 : *Each time a socket fails, it is repaired to as good as new*

This model assumption implies that a socket is completely or perfectly repaired, similar to replacement with a new one. The plausibility of this model assumption can be easily questioned. Yet, we have a major modeling benefit of this assumption by the fact that the series of events is now *a renewal process.*

A renewal process is a process in which the intervals between events are independently and identically distributed. Let's consider the situation that the user chooses to regard the time to failure, X_j for the length of the interval between the $j-1$-th and the j-th failure event. Now, *only* when the user decides to start and stop the observation with a failure event can the sequence $\{X_j\}$ be regarded as *a stationary sequence of intervals between events.*

A stationary sequence of intervals between events is defined by the requirement that the joint distribution of any k of the intervals between events, for all $k = 1, 2, \ldots$, is invariant under the translation along the discrete "time " axis j. Consequently, by assuming that the X_j are independent and identically distributed, and starting and stopping the observation with a failure event the *common distribution function* of the $\{X_j\}$ can be used for the probabilistic description of the series of events. Yet, in this case the definition for stationary series of events as given above does *not* hold.

Table A.1 : *Consequences of the choice of start and stop of observation*

Failure/repair process	**start and stop observation arbitrary**	**start and stop observation at instants of failure events**
Renewal	Stationary sequence of events and non stationary sequence of intervals between events	Stationary sequence of intervals between events and non-stationary series of events

We should now bear in mind that the user has chosen an *arbitrary time window.* Hence, the start of observation time is not the instant of the first failure event and the stop observation time is not the instant of the last event. With this "observation" we get the following logical relation between the model assumptions:

Arbitrary time window and Model assumption 4 $\Rightarrow$ Model assumption 3

Looking again at the sequence of intervals between events as illustrated in figure A.4, it becomes immediately clear that we run into problems with both X_1 and X_{r_i+1} (where r_i is the number of failures in the i-th stratum). Both these intervals are so called *censored data.* One speaks of censored data when the observations give some information about the value of a random variable, but when the value itself cannot be observed. We denote the random variable censored time to failure as Z_i. The situation we run into with a random time window is shown in figure A.4. One speaks of *right censoring* in lifetime data when a component is observed to live to a given time, but is then withdrawn

from observation. *Left censoring* refers to a situation in which we see a component expire, but do not know when the component started. The left censoring problem will be avoided by taking for X_1 the time between the last event before the start of observation and the first failure event after the start of observation. When NO failure events are registered before the start of the observation, we take the start of operation of the socket as the last event.

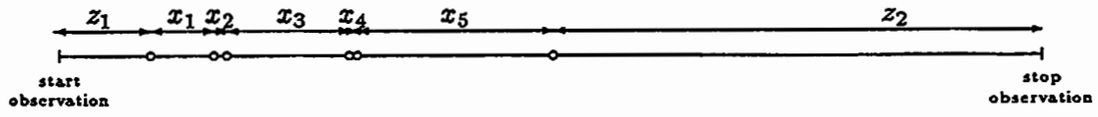


Figure A.4: Censored intervals between failure events

This censoring problem speaks in favor of using the counting process description of the series of events. However, the intervals between events will give us extra insight in the behavior of the series of failure events especially when the user distinguishes between different types of failures. Hence, the observed $\{X_j\}$ and Z are pooled and we can concentrate on the so called *survival analysis* of the data. In the case of no trend in the data, pooling the data and performing survival analysis is justified. What we then in fact do is predicting the lifetime behavior of the socket by processing all the former life times. In the case that the user does not want to include early lifetimes, the time-window can be adjusted.

When the user distinguishes between different types of failure events, the following model assumption can be made:

Model assumption 5 : *The failure processes leading to different types of failure events are independent*

When the different failure types are related to separate subcomponents, the assumption of independence may be reasonable. In other instances, for example when we look at degraded and critical failure modes of the same subcomponent, the independence assumption is suspect or even implausible.

Model assumption 6 : *The failure events for the socket occur randomly in time at a constant rate*

A mathematical model of a completely random series of events is the *Poisson process.* Consider events occurring along the time axis. Let λ be a constant with the dimensions of reciprocal of time. It will measure the mean rate of occurrence of failure events over the period of time covered in the timewindow chosen by the user and will be called the *probability rate of occurrence.* Denoted by $N_{t,t+h}$, the random variable defined as the number of events occurring in $(t, t+h]$, where $h > 0$. The conditions for a Poisson process of rate λ are that as $h \to 0$

$$\text{prob}(N_{t,t+h} = 0) = 1 - \lambda h + o(h)$$

$$\text{prob}(N_{t,t+h} = 1) = \lambda h + o(h)$$

and that the random variable $N_{t,t+h}$ is statistically independent of the number and positions of events in $(0, t]$.

A very important consequence of the Poisson process description is that the occurrences of events in any section of the time-axis are independent of the preceding sections of the process. Thus the origin from which the first time to failure X_1 is measured maybe defined from a variety of ways. Particularly

(a) the time point from the previous failure event;

(b) an arbitrary chosen time origin.

Similar, the end of the interval that starts with the last failure event, X_{r_i+1} can be chosen as

(c) the time point of the next event;

(d) an arbitrarily chosen end of observation time.

Further the sequence of intervals $\{X_j\}$, where X_1 is the time from the time origin to first failure and X_{r_i+1} is the time from the last failure to the end of observation time, are mutually independent and identically distributed with d.f. $e^{-\lambda t}$.

These consequences are captured in the following table:

Table A.2 : *Consequences of choice of start and stop of observation*

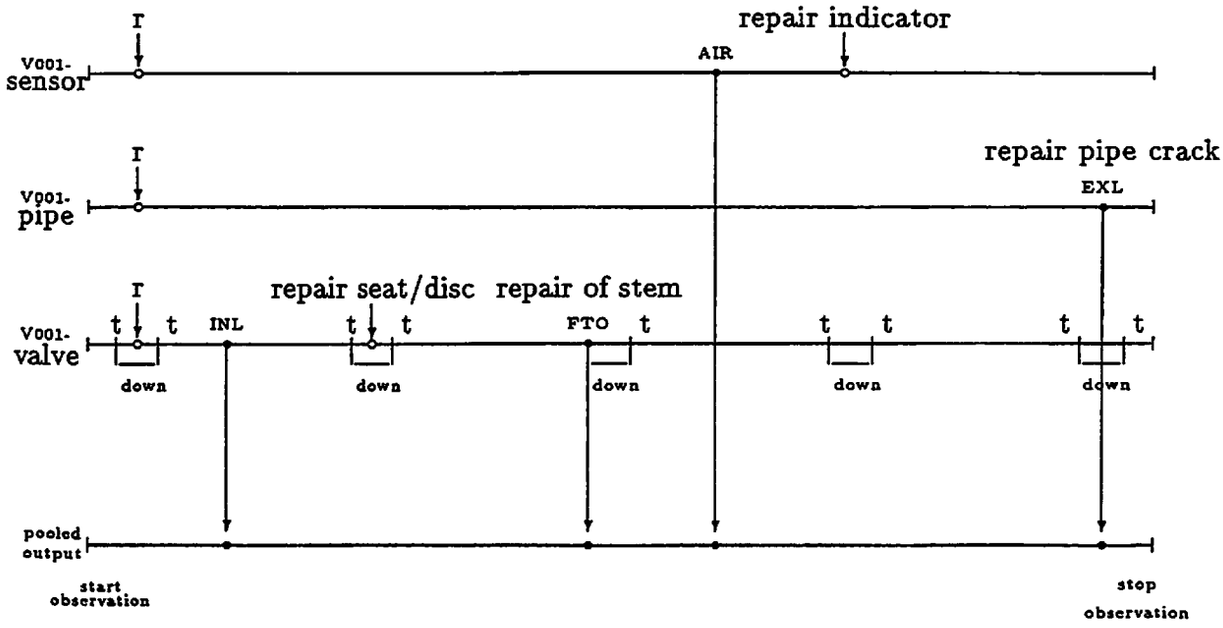
Failure/repair process	**start and stop observation arbitrary**	**start and stop observation at instants of failure events**
Poisson	Stationary sequence of events and stationary sequence of intervals between events	Stationary sequence of intervals between events and stationary series of events

This results in the following relation between the model assumptions

$$\text{Model assumption 6} \quad \Rightarrow \text{Model assumption 3 and 4}$$

This Poisson process model is justified in two cases. First in the case that the failure event sequence is the result of a superposition of a large number, p of independent stationary series of failure events. Specifically when the chosen timewindow is short compared to the mean times between events in the pooled output times p. This result is discussed in [Cox and Lewis, 1966]. This is in fact close to what we encounter with our series of event of a socket. Since each socket consists

of a number of maintainable parts, each time one of these maintainable parts fails this is registered as a failure event for the entire subcomponent socket. Hence, when we assume that the separate series of events of the maintainable parts are stationary and independent, the series of events of the subcomponent socket is *a superposition of series of events.* In figure A.5 the result of superimposing several series of events is shown.



o = repair ; • = failure detection
t = test; r= revision; INL = internal leakage; EXL = external leakage; AIR = abnormal instrument reading; FTO = failure to open on demand

Figure A.5: Pooled output of 314V001 subcomponent sockets

Second in the case that the failure events occur due to random external causes or design flaws. This model assumption leads to the Poisson process description of the failure event series. This description is the easiest to handle mathematically and will be assumed plausible for our data when there is no trend in the data.

A.3 Counting processes

The user has chosen to investigate the pattern of certain failure events for a population of sockets in a certain time-window. Further, the user has stratified the population. We consider the case that there are made no distinctions between the failure events. In section 4.3.2, we introduced two types of trend/line graphs; the Nelson Aalen graph and the mean rocof per year graph. These graphs should give the user:

1. an indication of differences in performances between the subgroups (strata);

2. an indication of trend in the performance of the component sockets in a subgroup (stratum) or entire population. in the subgroups.

The trend/line graphs follow directly from the the counting process description of the series of failure events. The counting process description catches the behaviour of a stratum of the population by registering its total number of failure events from the start of observation onwards, let

$$N_i(t) = \text{number of failure events in the } i\text{-th stratum } (0, t]$$

Remark that $N_i(t)$ is just a mathematical notation and that *no* model assumptions are made on the series of events, yet. Further, it is important to realise that $N(t)$ is a random variable, and the count of failure events we observe, forms in statistical terms, a so called *sample path* of this random variable.

In the case that the user has stratified the population into k homogeneous strata, we can denote these series of events as k separate counting processes, $N_i(t), i = 1, \ldots, k \; t \geq 0$. The entire population can then be denoted by the vector, $\mathbf{N}(t)$ which is called the k-variate counting process

$$\mathbf{N}(t) = (N_1(t), \ldots, N_k(t)) \tag{A.1}$$

Note that with this $\mathbf{N}(t)$ description of the stratified population, we do *not* take into account the number of sockets at risk at time t in each stratum, $r_i(t), i = 1, \ldots, k$. It is well possible that the user has stratified the population of sockets into strata of different sizes. This means that we cannot compare the $\{N_i(t), i = 1 \ldots, k\}$ when we look for differences in performances of the strata. Further, we have *not* yet used the assumption of homogeneity within each stratum.

Let's now first introduce the intensity process of the i-th stratum, $I_i(t)$

$$I_i(t) := \lim_{dt \to 0} prob(\text{failure occurs within the } i\text{th stratum in } (t, dt])/dt \tag{A.2}$$

When the failure/repair processes of the sockets in a stratum are consistent with that of a homogeneous stratum, the user can make

Model assumption 1

When the failure/repair processes of the sockets in a stratum shows no strong clusters, the failure processes can be regareded independent and we make

Model assumption 2

When both model assumptions 1 and 2 are made, the following relation holds

$$I_i(t) = \alpha_i(t) r_i(t) \tag{A.3}$$

where $\alpha_i(t)$ is the rate of occurrence of failure (rocof) of a socket in the i-th stratum. The k-homogeneous strata can now be mathematically described by

the counting process $\mathbf{N}(t) = (N_i(t), \ldots, N_k(t))$ having intensity process $\mathbf{I}(t) = (I_i(t), \ldots, I_k(t))$ of the multiplicative form $I_i(t) = \alpha_i(t) r_i(t)$. So, we should actually look at the $\alpha_i(t)$ in each stratum for getting an indication of the differences in performance of the strata. Particularly, when the user assumes that the entire population is homogeneous, no distinctions are made between the sockets in the different strata which implies that the rates of occurrences are similar:

$$\alpha_1(t) = \ldots = \alpha_k(t)$$

In order to (hopefully) clarify the counting process description of a stratified population, we introduce the counting process description of a single socket in a stratum. Let

$N_{ij}(t)$ = number of failure events of the j-th member of the i-th stratum in $(0, t]$

Let

$$A_i(t) = E(N_{ij}(t)) \tag{A.4}$$

The Nelson Aalen graph, $\hat{A}_i(t)$ is an estimator of the expected number of failures in the interval $[0, t)$,

$$\hat{A}_i(t) = \Sigma_{j|t_j \leq t} r_i \;\; (t_j)^{-1} \tag{A.5}$$

where t_j is the time at which the j failure event occurred. In the case that the number of sockets at risk in $(0, t]$ is constant, r_i the estimator $\hat{A}_i(t)$ is nothing else than the accumulated number of failure events over all r_i sockets divided by the number of sockets, r_i.

The variance of the counting process of a socket in the i-th stratum is can then be given by

$$V_i(t) = E(N_{ij}(t)^2) - \{E(N_{ij}(t)\}^2$$

The Nelson Aalen estimator, given in equation (A.5), can thus be regarded as an estimator of the expected number of failures of a socket in the i-the stratum in the timewindow $(0, t]$.

The analysis tool, rocof during a calendar year, is an estimator of the rate of occurrence of failure events, $\alpha_i(t)$. If we subdivide the observation period $(0, t_0]$ into intervals of equal lengths Δt and count the number of failures at the beginning of the i-th interval, d_i and the number at risk at the beginning of the i-th interval, r_i then the rocof, $\alpha_i(t)$ for that interval can be estimated by

$$\hat{\alpha}_i(t) = \frac{d_i}{r_i \Delta t} \text{ with } t \text{ in the } i\text{-th interval}$$

By taking the calender years as the interval lengths, we estimate the mean number of failures in that year. So far, we only assumed that each stratum is a homogeneous group of sockets and that the realizations of the stochastic point

process (SPP) are independent. The next step in the analysis of the series of events is to verify whether there a significant trend in the rocof (see figure A.3). In the next section, statistical tests will be introduced that generate a significance level for no trend in the rocof. When there is no apparent trend in the rocof, it is *possible* to make

Model assumptions 3

Note that model assumption 3 is made possible by the fact that the user chooses the time-window arbitrarily (without looking at the series of events). There exists now a direct relation between the expected number of failure events in a time-window of length t and the expected inter-event time of a socket in the i-the stratum, $E(X_i)$:

$$A_i(t) = \frac{t}{E(X_i)} \tag{A.6}$$

and

$$\alpha_i(t) = \frac{1}{E(X_i)} \tag{A.7}$$

This means that when stationarity is assumed, the Nelson Aalen estimator can be used for the estimation of both $E(X_i)$ and the rocof of a socket in the homogeneous stratum. When it can be established that the observations are consistent with a renewal process, the analysis of the series of events can be made more specific. When we make

Model assumptions 4

In order to get a better understanding of the result of making model assumption 4, we define the *conditional* rate of occurrence, $\alpha_{ic}(t)$ as discussed in [Hokstad, 1993] defined as:

$$\alpha_{ic}(t) = \lim_{dt \to 0} prob(\text{failure occurs for a socket in the } i\text{-th stratum in } (t, dt] \mid \mathcal{F}_t)/dt$$

where $\mathcal{F}_t$ is the history or state of the socket at time t. Now, in the case that we have a renewal process the socket history is recorded by *local time* x which is the time elapsed since the last repair before t and when X is defined as the interval between two failure events we get that the conditional rate of occurrence is equal to the so called hazard rate, $\lambda(x)$.

$$\alpha_c(t) = \lambda(x)$$

Let the hazard rate be

$$\lambda(x) = \lim_{\Delta x \to 0^+} \frac{\text{prob}(x < X \leq x + \Delta x \mid x < X)}{\Delta x} \tag{A.8}$$

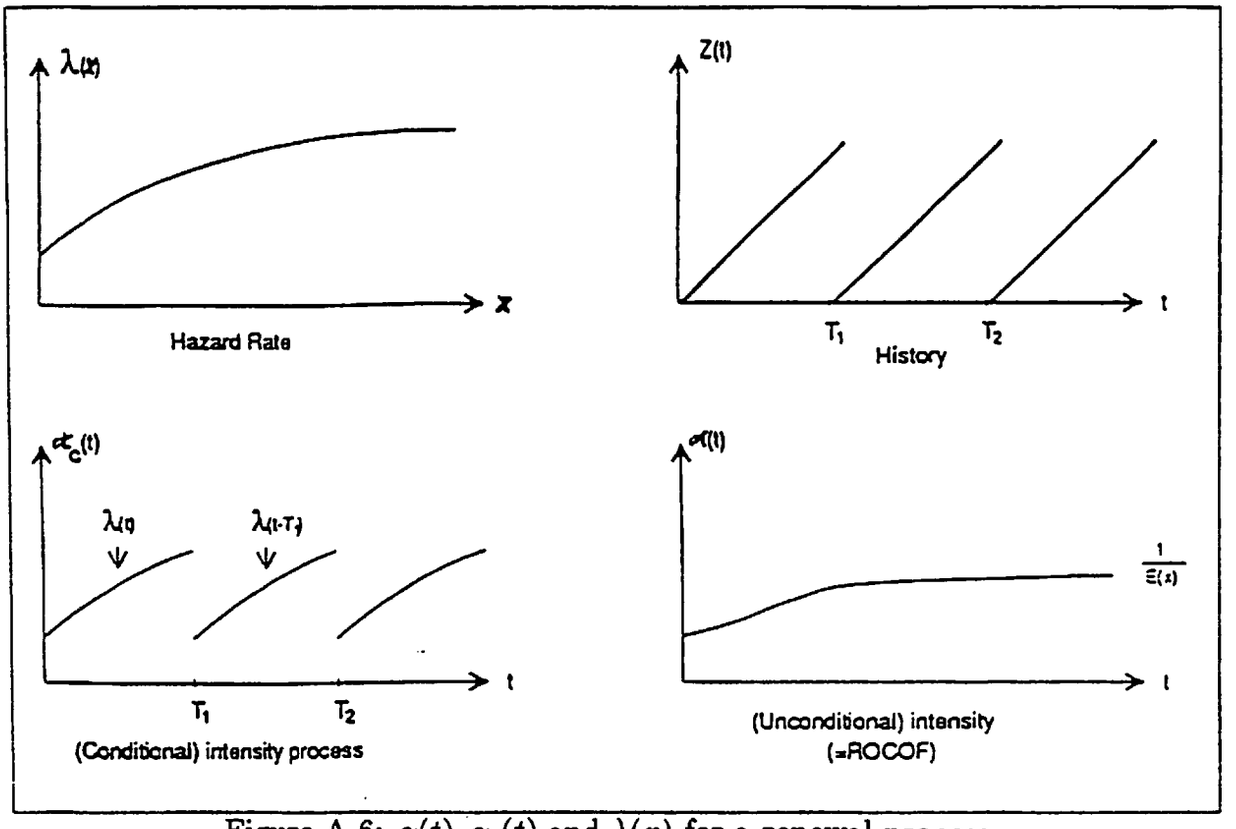


Figure A.6: $\alpha(t), \alpha_c(t)$ and $\lambda(x)$ for a renewal process

The hazard rate will be further discussed when the survival/frequency analysis tools are described. For the time being, figure A.6 is illustrative for the renewal process.

Further, the following relation exists for a stationary renewal process:

$$\lim_{t\to\infty} \frac{V(t)}{A(t)} = C^2(X) \tag{A.9}$$

where $C(X)$ is the coefficient of variation of the *inter-event time* X

$$C^2(X) = \frac{\text{var}X}{\{E(X)\}^2}$$

For a Poisson process, $C(X) = 1$, so that when the estimator of the variance approximates the Nelson Aalen estimator this indicates that the observations are consistent with a (homogeneous) Poisson process. Now, Barlow and Prochan showed that for a stationary renewal process, if $\lambda(x)$ is monotone non-decreasing, then $V(t)$ is less than $A(t)$ for all t and the inequality is reversed when $\lambda(x)$ is monotone non-increasing. In particular when the $\lambda(x)$ is constant, the the index of dispersion, $V(t)/A(t)$ of the process equals one.

Thus, by estimating the variance $V(t)$ of the counting process $N_{ij}(t)$, we can get an indication of the behaviour of the hazard rate of the renewal process. In the case that the failure/repair process is consistent with a Poisson process the user can make

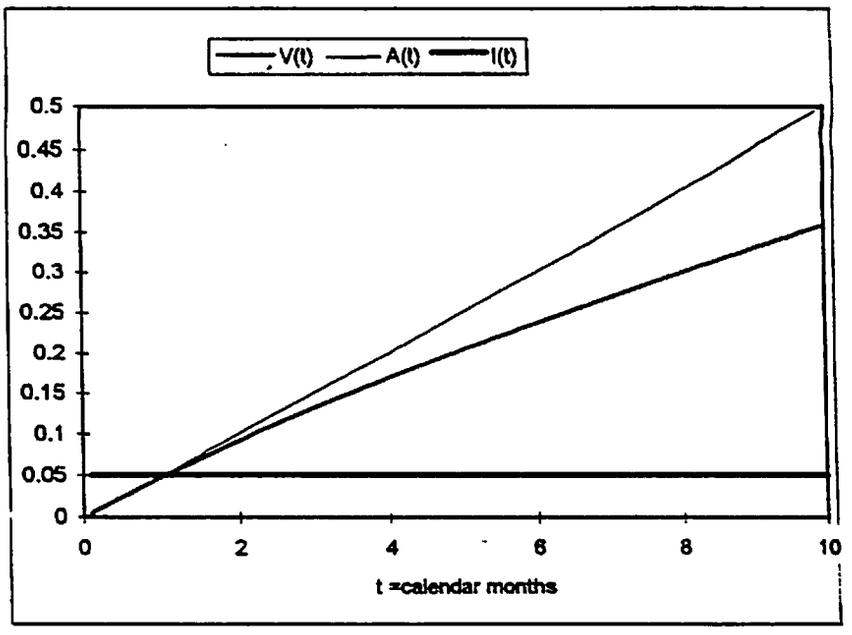


Figure A.7: $A(t), I(t)$ and $V(t)$ for a stationary counting process with monotone non-increasing $\lambda(x)$

Model assumption 6

With this assumption, we can calculate the confidence interval of the mean rate of occurrence, α_i to a confidence level of $1-\gamma$ as follows (see [Cox and Lewis, 1966]):

$$\frac{\chi^2_{\frac{\gamma}{2}}(2r_i)}{2t_0} < \alpha_i < \frac{\chi^2_{1-\frac{\gamma}{2}}(2r_i+2)}{2t_0}$$

In the rocof during calendar years graph, we have drawn the control limits equal to the confidence bounds of α_i. When the Nelson Aalen estimator crosses these control limits, this is an indication for the counting process to be not Poisson. This can either be due to too strong fluctuations or a monotonic trend in the rocof.

A.4 Survival analysis

The user has chosen to investigate the pattern of the failure events for a population of sockets in a certain time-window. Further, the user has stratified this population and no distinctions are made between the failure events.

The survival/frequency representations of the series of events are related to the description of the series of events as a sequence of successive inter-events times such as discussed in the previous section. In this description, the interval between the $j-1$-th and the j-th failure event is denoted by the random variables X_j. From the discussion in section 4.1, we know that this definition of the interarrival times implies that we look at time between failure detection dates. Yet, the user

can chose to regard service sojourns or time to failures as well without further complications.

From the discussion in the previous section we know that when the user chooses an arbitrary timewindow, we run into problems with both X_1 and X_{r_i+1}. Both these intervals are *censored data.* The left censoring problem will be avoided by taking for X_1 the time between the last event before the start of observation and the first failure event after the start of observation. When *no* failure events are registered before the start of the observation, we take the start of operation of the socket as the last event.

Still we have to cope with the last interval that is censored with the end of observation time. The sequence of intervals between events, can*not* be regarded stationary when we take this last interval into our analysis. By the fact that the failure data of a socket is sparse, it is not advisable to disregard the last interval. In the next table the intervals between events including the censored interval are given for main relief valves to the wet well.

Table A.3 : *Time to failures (TTF) of a population of component sockets*

Main valves to the wet well of the pressure relief system (314)

	Measured intervals								
Socket	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	$\bar{x}$
B1-314V014	30	13	18	37	104*				46
B1-314V015	33	2	18	18	11	6	42	45*	26
B1-314V016	66	36	105*						92
B1-314V017	41	2	38	116*					61
B1-314V018	41	13	48	104*					61
B1-314V019	33	33	36	27	27	31*			37
B1-314V020	62	20	11	6	93 *				46

* = rightcensored lifetime.

If we want to pool the inter-event times from the sockets in a stratum, we have to make

Model assumption 1 and 2

The further analysis of the intervals between events depends on making the extra assumption that the data on failure/repair process are consistent with a renewal process (see figure A.3). It is, however, a difficult problem to test the consistency of the data with a renewal process, especially in our case where only few failure events occur for each socket. In the case that there is an apparent trend in the rocof the assumption should clearly *not* be made. We make now

Model assumption 4

on the series of events. For a renewal process the intervals between events are independent and identically distributed. Each socket series of failure events can now be characterized by a non-negative random variable, X, called its *time to failure* which has a p.d.f. $f_X(x)$, zero for negative x, that is

$$f_X(x) = \lim_{\Delta x \to 0+} \frac{\text{prob}(x < X \leq x + \Delta x)}{\Delta x}$$

with

$$\int_0^\infty f_X(x)dx = 1$$

$$\text{MTTF} = E(X) = \int_0^\infty x f_X(x)dx$$

The variance of the inter-event times is defined as:

$$\text{var}(X) = \int_0^\infty x^2 f_X(x)dx - \{E/X)\}^2$$

The distribution of X is determined by $f(x)$, but it is for most purposes convenient to work with other functions equivalent to $f(x)$. One such function is the *survival function*, $S(x)$, which gives the probability that a socket has not failed up to time x.

$$\begin{aligned} S(x) &= \text{prob}(X > x) \\ &= 1 - \textstyle\int_0^x f(x)dx \end{aligned}$$

Clearly, $S(0) = 1, S(\infty) = 0$ and $S(x)$ is a non-increasing function of x. Another function equivalent to $f(x)$ is the *hazard rate*, $\lambda(x)$ defined as follows. Consider a socket known not to have failed at time x and let $\lambda(x)$ be the limit of the ratio to Δx of the probability of failure in $(x, x + \Delta x)$ such as defined in the previous section.

$$\lambda(x) = \frac{f(x)}{S(x)} \tag{A.10}$$

The essential concept in connecting the counting process descriptions with the interval between events is the *conditional* rate of occurrence, $\alpha_c(t)$ as defined in the former section.

$$\lambda(x) = \alpha_c(t)$$

When we define the cumulative hazard function, $\Lambda(x)$ as follows

$$\Lambda(x) = \int_0^x \lambda(s)ds$$

then we get the following extra relationship

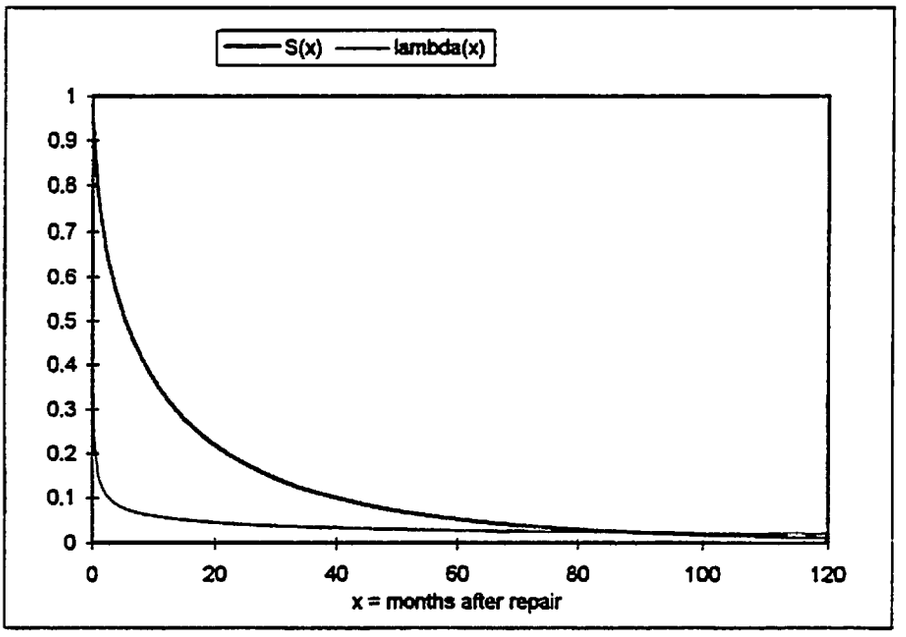


Figure A.8: $S(x)$ and $\lambda(x)$ for a renewal process

$$S(x) = e^{-\Lambda(x)} \tag{A.11}$$

There are many parametric families of distribution functions which can be used as models for the distribution of times between failure events. For the most part, their attraction is analytical simplicity, although some arise from practical considerations and in particular from the theory of life testing of physical equipment. We will discuss here only the *Gamma distribution* which is one of the most useful distributions; the density function is defined by

$$f(x) = \frac{\rho(\rho t)^{\kappa-1}}{\Gamma(\kappa)} e^{-\rho x}$$

and

$$E(X) = \frac{\kappa}{\rho}, \quad \text{and} \quad C^2(X) = \frac{1}{\kappa} \tag{A.12}$$

The parameters of the Gamma distribution can be estimated from the relations for the mean and the coefficient of variation. When $\kappa = 1$, the Gamma distribution is the exponential distribution. From section A.1 we know that a renewal process with exponential distribution of times between events is similar to a Poisson process.

The analysis tool (empirical) survival graph is a non-parametric statistical estimator of the survival function. When there are enough observations to form a histogram from the grouped data and we have *no* censored data, the calculation of the empirical survival function for selected x is straightforward.

$$\hat{S}(x) = \text{ proportion of intervals longer than } x$$

Yet, with censored data we take a more general approach for estimating the survival function. Let's say that we have n time instants $x_1 < \ldots < x_n$ at which $d_i i = 1, \ldots, n$ failures occur and r_i sockets are at risk just before a_i. Then the product-limit estimator has the following form

$$\hat{S}(x) = \prod_{l=1}^{i-1}(1 - \hat{\lambda}_l)$$

where $\hat{\lambda}_l = \frac{d_l}{r_l}$ which is the maximum likelihood estimator of the failure rate at x_l. The Greenwood estimator if the variance is

$$\text{var}[\hat{S}(x)] = \frac{[\hat{S}(x)]^2[1 - \hat{S}(x)]}{r(x)} \tag{A.13}$$

Table A.4 : *Estimation of the survival function with the Kaplan-Meier estimator*

Barsebäck 1 314V014-314V020

a_j	d_j	r_j	λ_j	S_j	var(S_j)
2	1	34	0,029	0,97	0,000815
6	2	33	0,061	0,91	0,002223
11	2	31	0,065	0,85	0,003451
13	2	29	0,069	0,79	0,004477
18	3	27	0,111	0,71	0,005428
20	1	24	0,042	0,67	0,006169
27	2	23	0,087	0,62	0,006342
33	1	20	0,05	0,59	0,007114
36	2	19	0,105	0,53	0,006891
37	1	17	0,059	0,49	0,007265
38	1	16	0,063	0,46	0,007199
42	2	15	0,133	0,40	0,006431
45	2	13	0,154	0,34	0,005861
48	1	10	0,1	0,31	0,00649
53	2	9	0,222	0,24	0,004789
74	1	7	0,143	0,20	0,004725
78	1	6	0,167	0,17	0,003992

The hazard rate can be estimated by first choosing an interval width, Δx and then taking the estimator

$$\hat{\lambda}_j := \frac{d_j}{\Delta x(r_j - \frac{1}{2}(d_j - m_j)}$$

where m_j is the number of lifetimes that are censored during the j-th interval,(a_{j-1}, a_j). The logarithm of the Kaplan-Meier estimator could be used to estimate the cumulative hazard function, in [Kalbfleish and Prentice, 1980] it is though suggested to take

$$\hat{\Lambda}(x) := \Sigma^{(x)} \frac{d_j}{r_j}$$

where $\Sigma^{(x)}$ denote the sum over j where $a_j < x$. The variance for this estimator can be estimated by

$$\text{var}\bar{\Lambda}(x) = \Sigma^{(x)} \frac{d_j}{r_j(r_j - d_j)} \tag{A.14}$$

When the data on the series of events is consistent with that of a Poisson process the analysis of the intervals between events is further simplified. We make

Model assumption 6

which results in the following simple relation

$$S(x) = e^{-\lambda x} \tag{A.15}$$

where λ is the constant rate of occurrence of the Poisson process and can be estimated with the Nelson Aalen estimator, $\bar{A}(t)$ as follows:

$$\hat{\lambda} = \hat{A}(t)/t \tag{A.16}$$

A.5 Competing Risks

The user has chosen to investigate the pattern of a number of failure events for a population of sockets in a certain timewindow. Further, the population is stratified and the user is interested in studying the interdependence of two or more types of failure events. Possible objectives could be to study

(a) the distribution of failure time for, say, type 1 failures, other types of failures having been eliminated;

(b) the comparison of, say ,type 1 failures in two or more groups of individuals having different properties for the other types of failure;

(c) the effect on the marginal distribution of failure time of eliminating or reducing type 1 failures.

We start with assuming that the sockets in a stratum form a homogeneous group and that the failure/repair processes of the sockets are independent, we make

Model assumption 1 and 2

In the case that our interest is focused on one type of failure and we would like to study that type of failure on its own, we are in a situation of competing risks, different failure events are competing to "kill" the component. Hence, we never observe the different failure types together. We make now

Model assumption 4

that is, after a failure event the component socket is repaired to as good as new and replenished at its socket. The series of events with k types of failure events can in this case be described by, the random variable (Y, V) where Y denotes the life time and V indicates the type of failure, and takes values in $(1, \ldots, k)$.

Let, Y_i be the notional failure time that would then be observed if all types of failure events except the i-th were suppressed. The actual next failure time, denoted by Y when there are k types of failure, is then $\min(Y_1, \ldots, Y_k)$. and is a sample of (Y, V).

To determine the distribution of, say Y_i, we may as well assume that $i = 1$, $X = Y_1$ and put $Z = \min\{Y_2, \ldots Y_k\}$. Then the observed variable is a sample of (Y, V) where $V = 1_{\{X<Z\}}$ or

$$(Y, V) = (\min\{X, Z\}, 1_{\{X<Z\}})$$

In other words, we observe the least of X and Z, and observe which it is. Let us now first look at the *joint distribution* of (X, Z),

$$S_{XZ}(x, z) = prob(X > x\ , Z > z) \tag{A.17}$$

where Z is thus a right censored life variable. Let the *subsurvival functions* be

$$S^*_X(x) = \text{prob}(X > x \text{ and } Z > X) \tag{A.18}$$

with hazard rate

$$\lambda^*_X(x) = \lim_{\Delta \to 0} \frac{\text{prob}(x \leq X \leq x + \Delta \text{ and } Z > X)}{\Delta} \tag{A.19}$$

and

$$S^*_Z(x) = \text{prob}(Z > x \text{ and } X > Z)$$

with hazard rate

$$\lambda^*_Z(x) = \lim_{\Delta \to 0} \frac{\text{prob}(x \leq Z \leq x + \Delta \text{ and } Z > X)}{\Delta}$$

Now the following relationships hold

$$S^*_X(x) + S^*_Z(x) = S_{XZ}(x, x) \tag{A.20}$$

$$\lambda^*_X(x) = S_{XZ}(x, x) \left[\frac{\delta \ln(S_{XZ}(x, z))}{\delta x} \right]_{z=x} \tag{A.21}$$

and

$$S_X^*(x) = \int_t^\infty \lambda_X^*(s)ds \tag{A.22}$$

This means that when we choose a simple parametric form for the joint distribution of X and Z, we can estimate the parameters with the observed data.

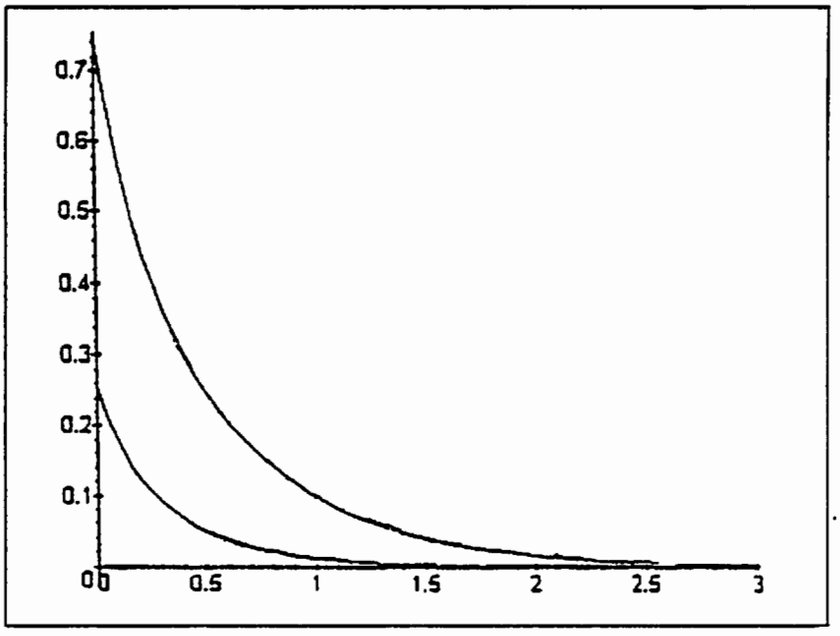


Figure A.9: $S_X^*(x), S_Z^*(x)$ for a competing risk process

When we want to determine the distribution of $S_X(x)$ without assuming independence, or any other special condition.The best we can hope for are bounds and these can be achieved from the extreme cases:

(a) for every observed failure of type 2, the unobserved value of X is only slightly greater than the observed failure time.

(b) for every observed failure of type 2, the unobserved failure time X is effectively infinite.

This gives two bounds on the survival function of X, the survival function of all failures and the survival function of failures of type 1, treating other failures as corresponding to infinite type 1 failure time.

$$S_{XZ}(x) \leq S_X(x) \leq S_X^*(x) + S_Z^*(0) \tag{A.23}$$

which equals

$$S_X^*(x) + S_Z^*(x) \leq S_X(x) \leq S_X^*(x) + S_Z^*(0) \tag{A.24}$$

The empirical subsurvival function $\bar{S}_X^*(x)$ is defined as:

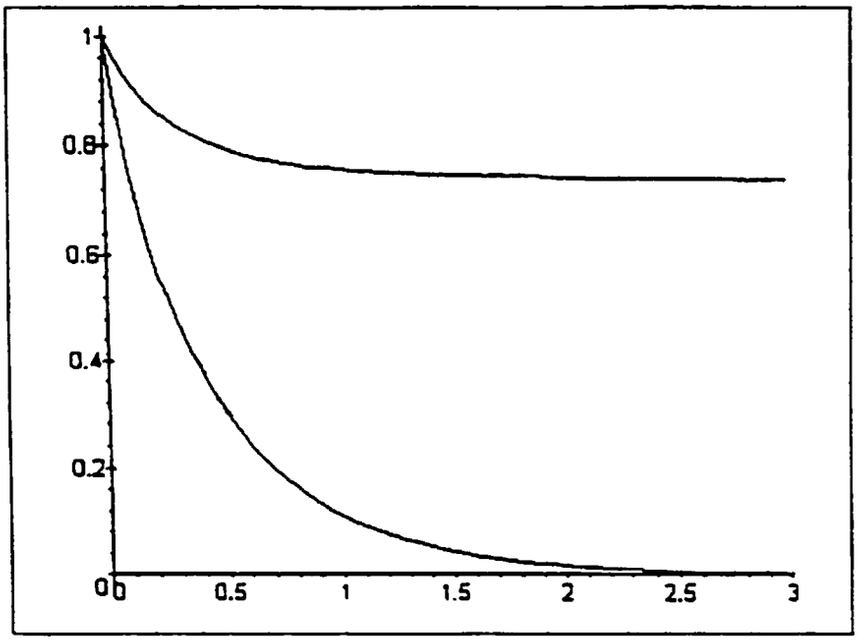


Figure A.10: Bounds on $S_X(x)$ for a competing risk process

$$\bar{S}_X^{\infty}(x) = \frac{\text{number of intervals ending in a type 1 failure } > x}{\text{total number of intervals}}$$

In [Cox and Oakes, 1984] the following relation between the two hazards is postulated:

$$\lambda_X(x \mid Z = z) = (1 + \phi)\lambda_Z(x \mid Z \geq z)$$

Now by giving weight to ϕ we give in fact weight to the dependency between X and Z, $\phi = 0$ implies independency and $\phi = \infty$ implies the strongest possible dependency.

After some calculation this relationship results in the following joint distribution

$$S_{XZ}(x, z) = ([S_X(x)]^{-\phi} + [S_Z(z)]^{-\phi} - 1)^{-1/\phi} \tag{A.25}$$

To simplify further analysis we make

Model assumptions 6

The hazard rates for both processes are now assumed constant, λ_X and λ_Z respectively. From the joint distribution we get that

$$S_{XZ}(x, z) = (e^{(\lambda_X \phi)x} + e^{(\lambda_Z \phi)z} - 1)^{-1/\phi}$$

with

$$\lambda_Z^{\infty}(z) = e^{(\lambda_Z \phi)z} \lambda_Z \left(e^{(\lambda_X \phi)z} + e^{(\lambda_Z \phi)z} - 1\right)^{-\frac{\phi+1}{\phi}} \tag{A.26}$$

and

$$\lambda_X^*(x) = e^{(\lambda_X \phi)x} \lambda_X \left(e^{(\lambda_X \phi)x} + e^{(\lambda_Z \phi)x} - 1 \right)^{-\frac{\phi+1}{\phi}} \tag{A.27}$$

When we take for example $\phi = 1$ we get

$$\lambda_Z^*(z) = \frac{e^{\lambda_Z z} \lambda_z}{\left(e^{\lambda_X z} + e^{\lambda_Z z} - 1\right)^2}$$

and

$$\lambda_X^*(x) = \frac{e^{\lambda_X x} \lambda_X}{\left(e^{\lambda_X x} + e^{\lambda_Z x} - 1\right)^2}$$

we can find now the subsurvival function, $S_X^*(x)$. The idea is now that we can estimate $\lambda_X^*(x)$ and $\lambda_Z^*(z)$ from the data. Hence, when we assign a value to the dependence parameter ϕ. We can in fact estimate λ_X and λ_Z from A.26 and A.27.

Model assumptions 5

When the different failure types refer to separate subcomponent sockets the assumption of independence may be reasonable. In other instances, for example degraded and critical failure modes on the same subcomponent socket, the independence is implausible. Unfortunately there is no direct statistical test for independence. In fact there is a unique independent competing risk model corresponding to any given distribution of (Y, V).

Theorem A.1 *If X and Z are independent exponential lifevariables with, then*

$$\frac{S_X^*(x)}{S_X^*(0)} = \frac{S_Z^*(x)}{S_Z^*(0)} = e^{-(\lambda_X + \lambda_Z)x} \tag{A.28}$$

Further, the maximum likelihood estimator of λ_X can be easily found and is given by

$$\hat{\lambda}_X = \frac{\text{number of intervals ending in type 1 failure}}{\text{total observation time}}$$

A.6 Significance tests

Significance tests can support the user in making the right assumptions on the series of failure events. A significance test consists of a null hypothesis (related to the assumption taken by the user), an alternative hypothesis , a test statistic and an approximate distributional form of the test statistic with critical regions.

The output of the significance test for the user is a significance level for the consistency of the observed series of events with the null hypothesis. When the user decides to reject the null hypothesis, the significance level is the probability

that this decision was incorrect. Note that the significance level does NOT give an indication whether the alternative hypothesis holds.

This means that when there is for example a clear monotonic trend in the estimated rate of occurrence of failure events, the user should design a test with the null hypothesis stationary series and the alternative hypothesis monotonic trend which generates a low significance level for the null hypothesis that the series of events is stationary.

The following table gives the set-up of the tests we will discuss later on in this section.

Table A.5 : *Statistical tests discussed in this section*

Name	H_0	H_1	test statistic	approximate d.f.
Laplace	HPP	Monotonic trend	u	$N(0,1)$
Linear rank	RP/HPP	Covariates of choice	u	$N(0,1)$
Log-rank	Equal rocof's	Proportional rocof's	$v^t V^{-1} v$	χ^2_{k-1}
Goodness of fit	Equal rocof's	Crossing rocof's	z	
Comparing HPP's	Equal λ_i's	Different λ_i's	H	χ^2_{k-1}
Exponentiallity	Exponential d.f.	Weibull d.f.	u	$N(0,1)$

A.6.1 Homogeneity tests

We assume that the failure processes is a renewal. Thus we we take:

Model assumption 3

We want to design a test that gives a significance level for homogeneity in a stratum. We can simplify the notation by assuming that the number of sockets in the stratum is constant throughout the observation period. We introduce the random variable $v_i(t)$

$$v_i(t) = \bar{r}(t) - r_i(t), \quad i = 1, \ldots, k$$

where $r_i(t)$ equals the number of failures in the i-th socket in $(0,t]$,$\bar{r}(t)$ is the mean number of failures per socket in $(0,t]$ and k is the number of sockets in the stratum. We can now define

$$\mathbf{v}(t) = (v_1(t), \ldots, v_k(t))$$

The vector contains vector of the expected number of failures in the i-th socket minus the corresponding observed number of failures in each socket in $(0,t]$. The variance matrix can be calculated by

$$V_{ij}(t) = \frac{r_i(t)}{r(t)}(\delta_{ij} - \frac{r_j(t)}{r(t)}) \tag{A.29}$$

where δ_{ij} is the kronecker delta function. When the ratio of the rate of occurrence of failure events in the k sockets is approximately constant it is to be preferred to consider

$$\mathbf{v} = (v_1(T), \ldots, v_k(T))$$

where T is the end of the observation time This is the so called *log-rank test* and $\mathbf{v}$ is nothing else than the vector of the observed number of failures on a socket minus the corresponding vector of the expected number of failures. A reasonable test statistic is

$$\mathbf{v}^T \bar{V}^{-1} \mathbf{v}$$

which is asymptotic χ^2_{k-1} distributed. Otherwise, we can consider

$$\mathbf{v} = \sup_{(0,T]} \|v_1(t), \ldots, v_k(t)\|$$

Which is a so called *goodness of fit* test. When we make

Model assumption 4

In Cox en Lewis [Cox and Lewis, 1966] the following test statistic is suggested when the user wants a rough check whether a group of sockets can be regarded homogeneous:

$$H = 2\left(\Sigma_{i=1}^{k} r_i \log r_i - r \log \bar{r}\right)$$

where r_i is the number of failures in socket i, r is the total number of failures and $\bar{r}$ equals the mean number of failures per socket. H is approximately χ^2 distributed with $k-1$ degrees of freedom. We can generalise this test to a group of strata instead of sockets by taking for r_i the mean number of failure per socket in the stratum.

A.6.2 Trend tests

Laplace test

In most of the significant tests for trend, the Homogeneous Poisson process (HPP) is taken as the null hypothesis. The so called *Laplace test* is optimal in the case that the alternative Nonhomogeneous Poisson Process (NHHP). The test statistic for the Laplace test is

$$u = \frac{\frac{\Sigma t_i}{n} - \frac{1}{2}t_0}{t_0\sqrt{\frac{1}{12n}}}$$

which is approximately normally distributed with zero mean and unit variance.

Linear rank test

When we take the inter-event sequence description of the series of failure events, we get for each socket, a sequence of n intervals between failure events, where we, for the moment, disregard that the last interval is censored, $x_1, \ldots, x_n$. Along with the corresponding covariates $c_1, \ldots, c_n$ (in the general approach the covariates are vectors). Let $x_{(1)} < \ldots < x_{(n)}$ be the order statistic and the corresponding covariates $c_{(1)}, \ldots, c_{(n)}$. A linear rank statistic is one of the form

$$\mathbf{v} = \Sigma_1^n c_{(i)}^T s_i$$

where s_i is a score attached to the i-th ordered interval value and the covariates are chosen so that $\Sigma c_i = 0$. We choose the null hypothesis that the intervals between failure events are unrelated to the covariate and independent and identically distributed (coming for a renewal process). Under the null hypothesis that the intervals are independently and identically distributed random variables, all $n!$ permutations are equally likely. Under this hypothesis, the mean and variance of $\mathbf{v}$ can be obtained by consideration of the permutation distribution of the rank labels $(1), \ldots, (n)$. Then

$$\begin{aligned} E_p(\mathbf{v}) &= \Sigma_1^n s_i E_p(c_{(i)}) \\ &= \Sigma_1^n s_i E_p(\bar{c}) = 0 \end{aligned}$$

where $\bar{c} = \Sigma c_i / n$. The covariance matrix is defined by

$$\begin{aligned} V &= E_p(\mathbf{v}\mathbf{v}^T) = \Sigma\Sigma s_i s_j E_p(c_{(i)} c_{(j)}^T) \\ &= \Sigma_{i=1} n s_i^2 E_p(c_{(i)}^2) + \Sigma_{i \neq j} s_i s_j E_p(c_{(i)} c_{(j)}) \end{aligned}$$

Now $\Sigma_{i \neq j} s_i s_j = -\Sigma_{i=1} n(c_{(i)}^2)$ and $E_p(c_{(i)} c_{(j)}) = [n(n-1)]^{-1}(n^2 \bar{c}^2 - \Sigma c_i^2)$ so that

$$V = K_{2,n}(\Sigma(c_i - \bar{(c)})^2$$

where

$$K_{2,n} = (n-1)^{-1} \Sigma s_i^2$$

Which is the corrected sum over the squares of the scores. Now, we are free to choose the covariant we suspect of influencing the intervals between failure events. When we suspect a trend, we suspect in fact that the chronological number of the interval is influencing the distribution of the interval. Hence we let the covariant depend on the chronological number of the interval between events.

With the Laplace test we take as the null-hypothesis that the series of events follows a Poisson process. However, it is possible that the null-hypothesis is that the series has some other trend-free form. For example the null-hypothesis could be that the intervals between the events, $X_1, \ldots, X_n$ are independent and

identically distributed random variables not necessarily exponentially distributed, i.e. that the series is what we call a renewal process.

We can now design a linear rank test that is reasonably efficient when the data is coming from a Poisson process, and which are still valid when the data are generated by renewal process with a non-exponential distribution of intervals. The key idea is to take so called exponentially ordered scores. We take as the score the expected value of the rth largest of n independent random variables following the exponential distribution with unit mean is

$$s_{r,n} = \frac{1}{n} + \ldots + \frac{1}{n-r+1} \quad (r = 1, \ldots, n).$$

This scoring of the intervals can be seen as a normalisation of the failure process to a HPP with failure intensity 1. Yet, the question that arises is what to do with the rank of the censored datapoints. We know that the censored interval, x_n exceeds z which means that its rank can be can be correct or should be higher (in the case that z hasn't got already the highest rank). We have chosen to give equal weights to all the rank configurations that arise from ranking z from its original rank to the maximal rank.

It turns out that this produces the same result as the more general approach in the work of [Kalbfleish and Prentice, 1980]. Here, we restart with the order statistic of the *non-censored intervals*, $x_{(1)} < \ldots < x_{(n-1)}$ and assume that z lies in one of $[x_{(k)}, x_{(k+1)})$. for $k = 0, \ldots, n-1$, with $x_{(0)} = -\infty$ and $x_{(n)} = \infty$.

We can attach now the following exponential scores:

$$s_i = \Sigma_{j=1}^{i} r_j^{-1}, \qquad S_i = \Sigma_{j=1}^{i} r_j^{-1} + 1 \tag{A.30}$$

where S_i is the score for the censored interval that lies in $[x_{(i)}, x_{(i+1)}]$ and r_j is the number of intervals left to score, which starts with n and jumps two down after the censored interval is scored. When the user wants to get a level of significance for no trend in the data coming from a homogeneous stratum, we can make the stratified test statistic is:

$$u = (\Sigma v_j)\,(\Sigma V_j)^{-1}\,(\Sigma v_j)$$

where v_j and V_j are the test statistic and variance of the j-th socket in the stratum. The test statistic u is approximately standard normal distributed, $N(0,1)$.

Appendix B

Description of the benchmark systems

B.1 Introduction

A NPP consists of safety and process systems. In this work we analyse two safety systems; the pressure relief system (314) and the core vessel spray system (323), at three NPPs of the so called boiling water reactor (BWR) type. In this appendix we describe roughly the function of these systems and we give the main component sockets of these systems.

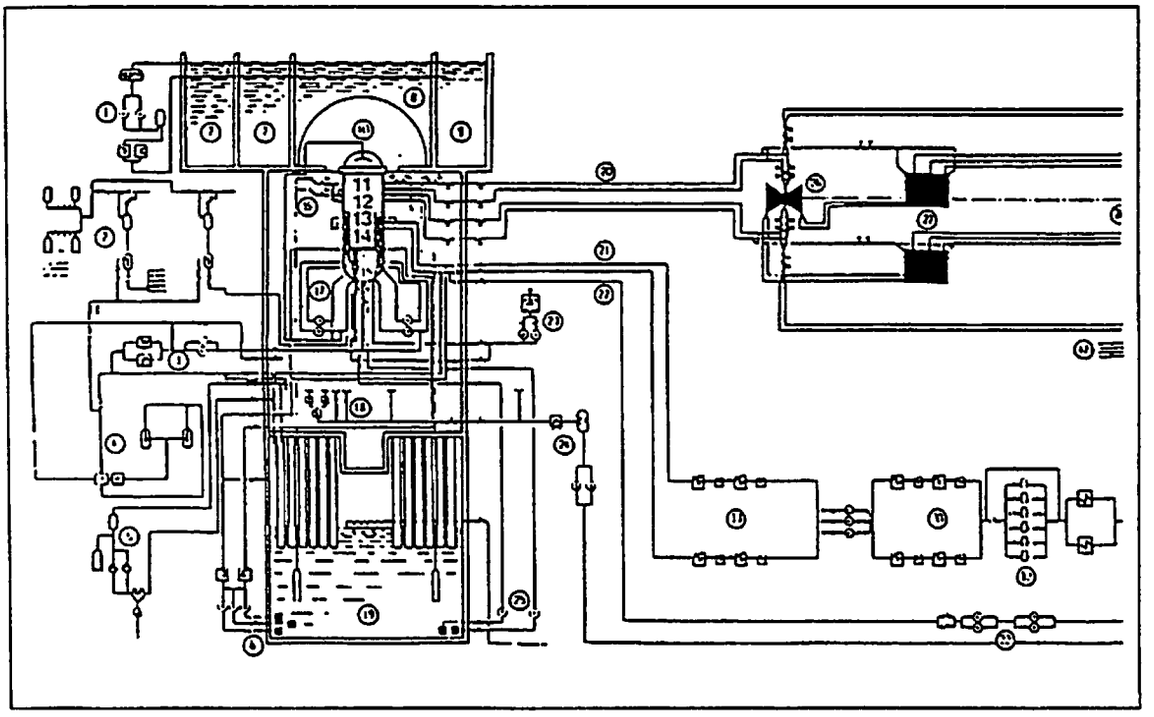


Figure B.1: Boiling water reactor
16 := pressure relief system; 25:= core vessel spray system

B.2 Pressure relief system, 314

System functions

According to the standard boiling water reactor (BWR) design, the relief system has the following safety functions:

* Depressurization whenever low pressure coolant injection is required from the 323 system;
* Overpressure protection of the reactor pressure vessel and connected systems which cannot be isolated;
* Reclosure of valves after operation.

At normal operation of the NPP the system is in standby.

System design and component sockets

Roughly, the system can be described to be composed of *steam relief valve lines* where one line consists of a pilot controlled main valve with one or two pilot valves; one electromagnetic pilot valve and/or one self-actuated impulse pilot valve which will open on high pressure in the steam line. Depending on the reactor generation, all or some of the valves units/lines blow to the condensation pool and some to the drywell. There are also other types of relief valves for regulation purposes.

In general terms the actuation of the 314 safety/relief valves at different operation situations, is initiated by an electrical opening signal supplied by the Reactor Protection System (RPS). For overpressure protection in pressure buildup transients, actuation/opening is initiated also by means of self actuated impulse pilot valves.

Table B.1 : *Valve components at the 314 system*

Socket	Type
314V001-314V013	Safety valve servo controlled
314V014-314V020	Safety valve servo controlled
314V048-314V049	Control valve motor operated
314V050-314V051	Closing valve magnetic operated (seat)
314V052-314V057	Closing valve pneumatic operated (bellow)
314V058-314V059	Closing valve pneumatic operated
314V062-314V081	Pilot valve impulse controlled
314V089-314V095	Electro magnetic pilot valve

Test and maintenance arrangements

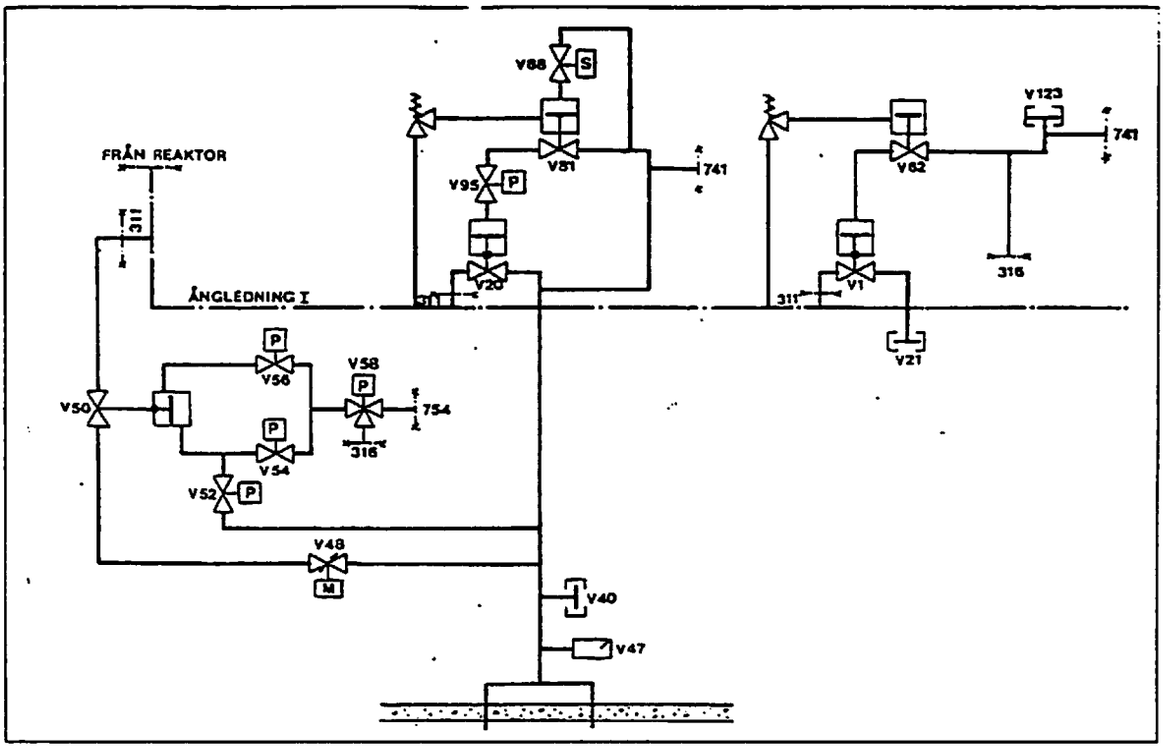


Figure B.2: Pressure relief system, 314

The general scheme of tests for safety/relief valve modules in system 314 include:

- One test while shutting down the NPP for annual overhaul;
- One test while starting up from annual overhaul and
- One or two tests during the operation period

The main valves to the dry well (V001-V013) are tested at reduced pressure (approximately 15 bar) in order to preserve rupture discs and avoid steam relief in the drywell. The main valves blowing to the wet well are tested by actuation of the electro magnetic pilot valve (V082-V095).

The self actuated pilot valves (V062-V081) are tested once a year in laboratory during annual overhaul. The inspection and preventive maintenance actions are carried out during the overhaul since the 314 system is situated in the reactor vessel.

B.3 Core vessel spray system, 323

System functions

* Cooling of the core with water from the condensation pool (316) in case of an accident that results in the decrease of the waterlevel in the core under a certain critical value.

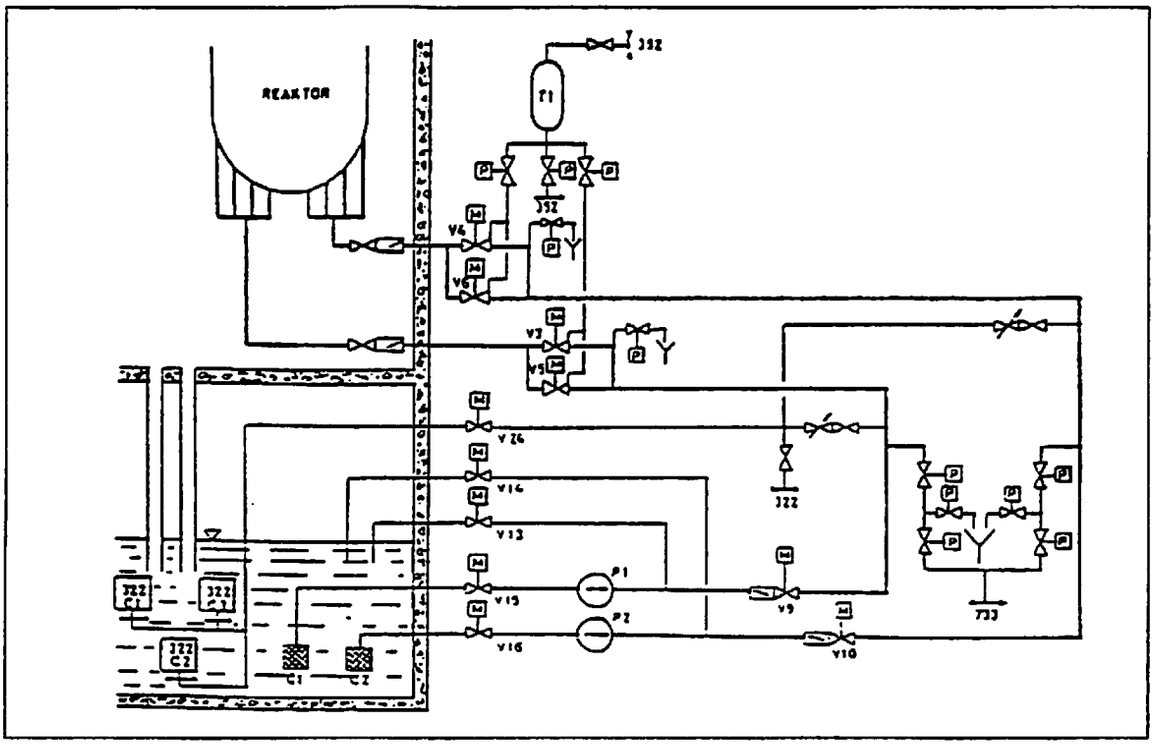


Figure B.3: Core vessel spray system, 323

At normal operation of the NPP the system is standby.

System design and component sockets

The system exists of two identical and separate circuits. Each circuit has 100 % capacity. Each circuit contains a pump (P001 and P002) that takes water from the condensation pool. In each circuit the pumped water is regulated by a control valve (V009 and V010) and two parallel coupled closing valves (V003,V005 and V004,V006). The main pipeline in each circuit split up in four lines that are connected to the core.

Each main pipeline contains feedback pipelines leading back to the condensation pool this same feedback loop can also be made by the pipelines behind the control valves, that come together and then lead back to the condensation pool. These lines are used when the system is tested.

The system starts automatically in the case of I-isolation. The pumps start working at low force and the closing valves (V003-V006) remain closed. The other valves remain closed as well. When the waterlevel in the reactor drops beneath the critical level, the closing valves are opened and the water can be pumped in the reactor when the pressure is less than 20 bar. When the pressure is down to 10 bar the flow is 170 kg/s and to avoid bigger flows the control valves (V009-V010) can be applied when the pressure is less than 10 bar.

Table B.2 *; (Main) Valve and pump component sockets at the 323 system*

Socket	Type
323P001-323P002	Centrifugal pump horizontal/vertical
323V001-323V002	Check valve
323V003-323V006	Isolation valve motor operated (gate valve)
323V009-323V010	Control valves motor operated
323V011-323V012	Check valve
323V013-323V014	Isolation valve motor operated (seat valve)
323V015-323V016	Isolation valve motor operated (gate valve)
323V024	Isolation valve motor operated (gate valve)
323V025-323V026	Check valve
323V027-323V030	Isolation valve pneumatic
323V039-323V040	safety valve

The remaining valve sockets are manual operated.

Appendix C

Glossary

Availability
Availability = real operating hours / planned operating hours
Real operating hours are calculated by substracting the down time caused by maintenance works from the planned operating hours.

Censored data
Sample items withdrawn or lost from study. With censored data you know only that the sample item survived until they left the study.

Censoring time
The time at which you cut off a study before every item fail or at which you withdraw the item before the study ends.

Colored stochastic point process
A stochastic point process for which the point events are colored according to the type of event that occurres.

Corrective maintenance
The maintenance carried out after failure detection, intended to put a system into a state in which it can perform a required function.

Competing risk
"Competing risk models" are statistical models which describe the life distribution of a system that may fail due to different causes. Each cause competes to end the component socket's life. If each cause is associated with a life variable, the component sockets's life is modelled as the minimum of these life variables.

Cumulative distribution function
Function that expresses the probability that a random variable falls at or below a given value. Also called the cumulative density function.

Down time
The time during which a component/system is in a down state.

Frequency function
A set of all the various values that individual observations may have and the frequency of their occurrence in the sample or population. A way of grouping data so that the important aspects of the raw data become more readily apparent. This is a synonym of probability density function.

Generic distribution
A probability distribution that describes an uncertainty that is relevant for a broader population than the one to which the current unit belongs.

Homogeneous group
Sets of data that have similar characteristics.

Imperfect repair
From a maintenance engineer's point of view most repair actions should be classified imperfect repair while the component will not be "as good as new" (perfect repair) nor will the component continue as if nothing has happened (minimal repair).

Maintenance
The combination of all technical and administrative actions, including supervision actions, intended to retain a system in,or restore it to, a state in which it can perform a required function.

Minimal repair
Minimal repair means that the component upon failure is restored just back to the functioning state, by no means improving or impairing the component in other ways.

Normal distribution
Common bell-shaped curve; Gaussian distribution.

Perfect repair
Perfect or complete repair resources the component to the "as good as new" conditions. It is most easily thought of as the replacement of a failed item with a new one.

Poisson process
A stochastic process in which events occur in continuous time. The probability of k events in any interval of lengthe I is independent of events in disjunctive intervals, depends only on the lenght I, and is equal to

$$\frac{(\lambda I)^k e^{-k\lambda I}}{k!}; \quad \lambda > 0$$

λ is called the intensity of the Poisson process.

Pooled data
Two or more sets of data that you collect under different conditions or from different populations and combine.

Preventive maintenance
The maintenance carried out at predetermined intervals or according to prescribed criteria, intended to reduce the probability of failure or the degradation of the functioning of a component.

Series of events
Point events occurring in a haphazard way in space or time.

Service sojourn
The time length in between the time that a component socket is replenished at its socket after repair to the time that the component is removed from its socket for any reason whatever.

Socket
Functional position in a system, occupied by one component during a service sojourn.

Stochastic point process
Point events occurring in a haphazard way in space or time.

Postadress/Postal address
SKI
S-106 58 STOCKHOLM

Telefon/Telephone
Nat 08-698 84 00
Int +46 8 698 84 00

Telefax
Nat 08-661 90 86
Int +46 8 661 90 86

Telex
11961 SWEATOM S