# Investigation of Repairability of Failures in PRA (Project DIOR)

**Erik Sparre[a], Mattias Håkansson[b], Carl Eriksson[b] and Gunnar Johanson[c]**
[a] Risk Pilot, Malmo, Sweden, erik.sparre@riskpilot.se
[b]Risk Pilot, Stockholm, Sweden, mattias.hakansson@riskpilot.se, carl.eriksson@riskpilot.se
[c] AFRY, Stockholm, Sweden, gunnar.johanson@afry.com

**Abstract:** The overall purpose of the NPSAG (Nordic PSA Group) project DIOR (Deeper Investigation of Repairability of Failures) is to better understand failure data used in PRA models. A deeper knowledge about failure causes, coupling mechanisms, repairability, timing of failures, which failures occur early/late etcetera gives the analyst valuable insights when developing state-of-the-art PSA models. Such knowledge can be relevant when introducing repair into PRA models, how to assign failure data for longer time windows, definition of CCF (concerning for example failure modes and repair possibilities).

Information about single failures in Nordic Nuclear Power Plants is gathered in the so-called TUD-database. This database has primarily been used to calculate failure probabilities and failure rates for components, but since the database also contains information about repair times, and other timing information, it is possible to calculate measures such as mean time to repair (MTTR). Information about CCFs is collected within the ICDE-project and compiled in databases.

Events from the TUD and ICDE databases have been analyzed for a selected number of components (centrifugal pumps, diesel generators and batteries). Data has been evaluated regarding severity of failures, repair times, waiting times etcetera.

In this paper, selected results and conclusions from the DIOR project will be presented.

**Keywords:** PRA, repair, CCF, MTTR

## 1. INTRODUCTION

### 1.1. Background

Repair of components failing after an initiating event is generally not modeled in PSAs. In [1] it is for example stated that:

- The time available to repair most components is generally too limited (i.e., core damage would occur before the repair is completed),
- Repair is an action that is not always governed by procedures and thus difficult to justify where alternate equipment is used as a first priority upon failure.
- The availability of spare parts cannot always be depended upon, and
- Procedures generally direct operators to use alternative equipment as a first priority upon failure.

Recent development of the PSA models involves modeling of long-term scenarios, for example up to 72 hours or more in case of fuel pool cooling. Therefore, recovery by repair or restoration may need to be included in the models for more realistic modeling. It is however not an easy task to perform a data analysis since there is limited experience of accident conditions and real demand failures. In [1], the following is noted regarding recovery data identification:

- In general, only data from actual component and system demands should be included in the recovery/repair data evaluation.
- When failures occur during actual demands, operators should be strongly motivated to try to recover the component or system.
- However, the available data mainly includes failures during surveillance tests.
- Experience data from actual demands are very limited.
- If a component or system fails to start during a surveillance test, the need for repair is not as pressing and thus not reflective of accident conditions.

Determining a repair time for a component is thus a complex task and it is important that the analyst ensure that the chosen data is suitable for the situation. The NPSAG (Nordic PSA Group) project "Deeper Investigation of Repairability of failures" (DIOR) was initiated with the purpose of investigating available repair data. This paper is a condensed version of the project report, [2].

## 1.2. Objectives

The experience of critical failures at accident conditions and real demands is very limited. The available data mainly includes failures occurring during surveillance tests and normal operation. In the DIOR data analysis, the experience data will be interpreted to determine the applicability of this data to be credited during accident conditions and actual demands.

The objectives are:

- To analyze the reported single and common cause failures regarding their recoverability in terms of ”restorability” and "repairability" (these terms are further described below).
- To analyze the single failures restoration and repair times to be credited for accident conditions.
- To determine if there are differences between single failures and CCFs when considering recovery via restore or repair of the components.
- To present conclusions on recoverability and how to apply recovery in plant PSA models.

## 1.3. Data Scope

Based on the importance in PSA, diesel generators, centrifugal pumps and batteries were included in the analysis. In this paper, focus will be on the analysis of centrifugal pumps.

Two different data sources have been used in this project:

- TUD (T-book, [3]) – the primary data source in Sweden and Finland for single failures.
- ICDE (International Common Cause Failure Data Exchange) – data collection for understanding CCF, [4].

## 2. TERMS AND DEFINITIONS

**Table 1: General Terms**

| Term | Description |
|---|---|
| **Component impairment** | **Critical failure (Complete failure)**<br>A critical fault is one that prevents the component from performing its mission as defined in the PRA. Critical faults require repair or replacement action on the component to restore the component to operability. For example, a valve that fails to open due to a mechanical failure is a critical fault.<br><br>**Degraded failure**<br>A degraded failure is such that a component can perform its mission, but at less than the optimum performance level.<br><br>**Incipient failure**<br>An incipient failure is such that there is no significant degradation in performance but there are indications of a developing fault. The difference between degraded and incipient is generally a matter of severity. |
| **Failure detection** | **Demand**: The event is a demand event, i.e., failure occurring when the function of the component(s) is required.<br>**Monitored**: The component is monitored in the control room.<br>**Other**: Includes all other detection methods, such as testing and maintenance. |
| **Mean Downtime (MDT)** | The average time that a system/component is non-operational. See further discussion below. |
| **Available time** | The time available until an undesired consequence occurs, for example, core damage. |
| **Recoverability** | For a component, the recoverability is the ability to perform restoration or repair within the available time until an undesired consequence occurs.<br><br>It is also an HRA term that covers the use of alternate trains or systems to recover a safety system-function (performed by control room operators) and the ability to correct a failed human action. The HRA aspects are not studied in this project. |

**Table 2: Repair Terms**

| Term | Description |
|---|---|
| **Repair** | Corrective action performed on the failed component by plant maintenance staff from maintenance department. For example, more severe failures where the component or its parts need to be replaced. |
| **Repairability** | A measure of the degree to which a component can be recovered after failure by actions that are performed by maintenance staff. This concept should be distinguished from simpler actions that fall under restorability. |
| **Repair waiting time** | As defined in T-book for critical faults and include all possible causes for waiting before physical action is taken. |
| **Active repair time** | The time during which actions are performed actively on a component. Excludes the waiting time where no physical action is taken. Also called net repair time. |

**Table 3: Restore Terms**

| Term | Description |
|---|---|
| **Restore** | Corrective action on the failed component by plant shift technician from operations department. For example, replacing a fuse or a similarly simple action which resolves the problem. |
| **Restorability** | A measure of the degree to which a component can be recovered after failure by actions that are performed by plant shift technician(s). This is distinct from more complex actions that fall under repairability. |
| **Restore waiting time** | Defined analogously with "Repair waiting time" above and can be assumed small for accident conditions, if accessible. |
| **Active restore time** | The active restoration time of a component. Excludes the waiting time where no physical action is taken. |

## 3. METHOD

### 3.1. General

The DIOR data analysis included the following steps:

- Classify the reported failures regarding "restorability" and "repairability"
- For single failures:
    - Note both the active repair time and the downtime
    - Perform statistical analysis using repair time data
- Questions of specific interest for CCFs are:
    - Are there recoverability differences between single failures and CCFs?
    - What type of event are the CCFs categorized as, shock or non-shock, and how common are the two types respectively?

The results of the data analysis were also tested in a pilot application.

### 3.2. Repairability/Restorability

In the DIOR data analysis, failures have been categorized into different recoverability levels according to "repairability" or "restorability" which is a measure of the degree to which a component can be repaired or restored. It is assumed that the necessary actions differ between restoration, repair, and replacement.

Three classes 1-3 are defined where "1" is the least severe:

1. Minor electrical failures that can easily be resolved by e.g., replacing a fuse or a relay. Other minor failures, such as very small leakages, fastening of hose, issues with starting or lubrication. A simple corrective action resolves the problem.
2. Diffuse failures or symptoms, such as rattle, and vibrations. Other failures such as leakages that can be temporarily fixed, loose connections. The corrective action needed requires more knowledge compared to "1".
3. Failure that leads to replacement (or repair) of the whole unit, or large essential components, due to complete failure.

Failures of class 1 are assumed to be possible to be handled by plant shift technicians and for these failures the term "**restore**" is used.

Failures of class 2 and 3 are assumed to need efforts from the plant maintenance staff and for these failures the term "**repair**" is used.

The reason for distinguishing between "restore" and "repair" is that the waiting time is different for the two, because of the differences in availability of the shift technicians and the maintenance staff on site. The classification of failures is also interesting when analysing the availability of spare parts since failures of class 1 and 2 most likely can be restored or repaired using on-site spare parts. For failures of class 3, this is not necessarily the case.

### 3.3. Downtime, Waiting Time and Active Repair Time

When evaluating repairs (and restores), the downtime is the most interesting parameter. Downtime is best described by the definition of Mean Downtime, which is "the average time per incident/failure that a system is non-operational". This includes all time associated with repair, corrective and preventive maintenance, self-imposed downtime, and any logistics or administrative delays." [5]. Equation 1 describes the relationship between Downtime ($T_r$), Waiting time ($T_W$) and the Active repair time ($T_{ar}$).

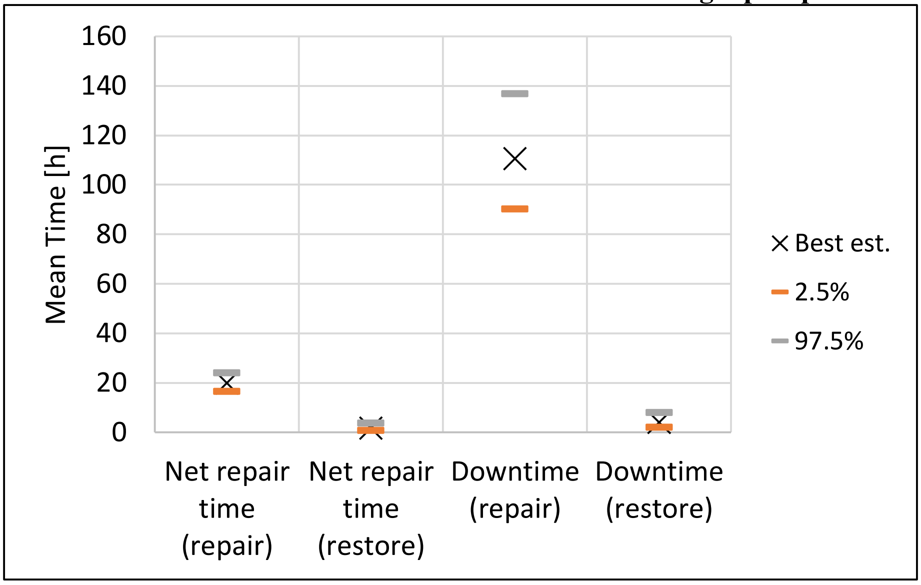
$$\boldsymbol{T_r = T_W + T_{ar}} \qquad \textbf{Equation 1}$$

In the failure reports, the downtime can be calculated as the difference between the "Start Time Not Available", which is the time point when the component became unavailable, and the "End time", which is the time point when the component is reported back into operation.

According to NUREG/CR-6823, "Handbook of Parameter Estimation for Probabilistic Risk Assessment", [1], these time points are required for a failure to be evaluated and analyzed. Failures that lack any of these time points should be excluded from the data. NUREG/CR-6823 also states that only accident conditions, i.e., failures during actual demands and monitored events should be included in the data. This means that data analysts need to assess whether the failure occurred under similar stress as a during an accident condition. This however can be difficult to assess and the reported time points in the failure reports may include uncertainties.

Active Repair Time (using T-book terminology) or Net Repair Time is the time where actual work is done. It excludes the waiting time where no physical action is taken, time for administrative work etcetera. The TUD-data contains both the net repair time and timestamps that enable the downtime to be calculated. If the calculated downtime, using timestamps, is compared to net repair time, the uncertainties in the parameter estimations are different. Centrifugal pumps have the largest data set and is used to visualize this, see Figure 1. The downtime (repair) calculated from time stamps are very high considering the severity level of the events. The downtime (restore) shows lower values. The downtime for repair is affected by occasional events that stand out by having significantly higher values, with no apparent explanation.

**Figure 1: Estimate of mean net repair time, mean downtime and uncertainties for net repair time and downtime for failure to run for centrifugal pumps.**



The example comparison between the net repair time and the downtime for the 216 centrifugal pump events show that the downtime estimates result in unreasonable large estimates with large uncertainties. Therefore, for accident conditions, the result from the net repair time is deemed the most relevant. Thus, further on in the report, the NUREG/CR-6823 definition of downtime will not be applied. Instead, downtime is defined as the net repair time from the failure report complemented with an estimated waiting time.

A waiting time of 4 hours for restore (since the plant shift technicians are onsite) and 8 hours for repair (plant maintenance staff might be offsite) is assumed. The reasoning behind 8 hours is that the plant maintenance staff is assumed to be on site only one third of the day. 8 hours is a reasonable amount of time for the staff to prepare and administer a repair, regardless of their location at the time of failure. A less severe failure, that can be restored rather than repaired, is deemed simple enough to be handled by the staff currently on site and not requiring certain expertise. Therefore, a waiting time of 4 hours is assumed.

### 3.4. Modelling Repair Failure Rate Based on Repair Data

The success or failure of repair is dependent on the downtime and the available time. The available time is the time from initiating event until the unrecoverable consequence occurs. In the statistical approach used in for example the Prosafe project [5], the probability distribution of repair times is fitted to the downtime data. Using the distribution of repair times and the available time in a specific accident scenario for specific components and failure modes, a repair failure probability can be modelled. This is most often done by assuming that if the downtime is less than the available time the repair succeeds and otherwise it fails. Since data often is presented in the form of active repair time, to calculate the downtime from the waiting time and the active repair time, Equation 1 must be used. The waiting time could be considered by either the joint distributions for waiting time and the active repair time or by simplification by using a constant screening value that must be subtracted from the available time. In this project the latter is used, see section 3.3. The Prosafe project further discusses which probability distributions that ought to be used and fitted to active repair time data, for example the exponential, normal, Weibull, gamma, and lognormal distribution. In the DIOR project, the exponential and lognormal distribution are studied further.

More information about the distribution fitting can be found in [2].

### 3.5. Common Cause Failures

The CCF analysis differs from the single failure analysis since no statistical analysis of restore and repair times is carried out. The CCF analysis addresses specific questions as stated in section 3.1. The following aspects are considered in the analysis of the CCF events.

- **Event screening**. Based on the component types included.
- **Determination of repairability**. This is performed according to the repair severity classes, see section 3.2.
- **Method of detection**. In the ICDE database, the detection method is noted. Here, this information is used to classify events into the following categories:
    - **Demand**: The event is a demand event, i.e., failure occurring when the function of the component(s) is required. In these events, the repair conditions are as close as possible to accident conditions.
    - **Monitored**: The component is monitored in the control room, i.e., the latency of the event is very short and such type of event is in CCF parameter quantifications generally excluded due to their very short unavailability time. However, these events can still give insights about the repairability and are therefore included in the analysis.
    - **Other**: Includes all other detection methods, such as testing and maintenance. The repair situation corresponds to normal operating conditions, i.e., the urgency of repair is not as imminent as during an accident scenario and the pre-assumption is that the repair times will be longer. However, in a shock event of safety critical systems, the urgency for repair is high and if these systems are affected, the situation is more like an accident scenario.
- **Determination of failure timing**. The failure timing aspect is only relevant to consider for the failure mode “failure to run”. It describes the timing between the failures, and this “timing” is categorised as “shock” or “non-shock” event. A shock event expresses that all components in the group fail simultaneously.
- **Evaluation of correlation to single failure data**. This is interesting to study since this could give the repair times for the events. Thus, the correlation to the single failure data is investigated. However, different time spans are selected between the single failure data and the CCF data, so repair times will not be possible to determine if not explicitly given in the CCF event descriptions.
- **In-depth analysis**. The selected events from the event screening are analysed in detail to determine the repairability/restorability, the detection, and the failure timing.
- **Analyse event distributions and share of events in the repairability severity classes**. The analysis is presented in section 5.2.

### 3.6. Pilot Application

The DIOR project also included a pilot application where repair probabilities for selected components were determined and the effect on the total results was studied. The details are not further described in this paper but some general conclusions are given in chapter 6

## 4. SELECTION OF DATA

Based on the importance in PRA; diesel generators, centrifugal pumps and batteries were included in the analysis. In this paper, only the analysis of centrifugal pumps is presented.

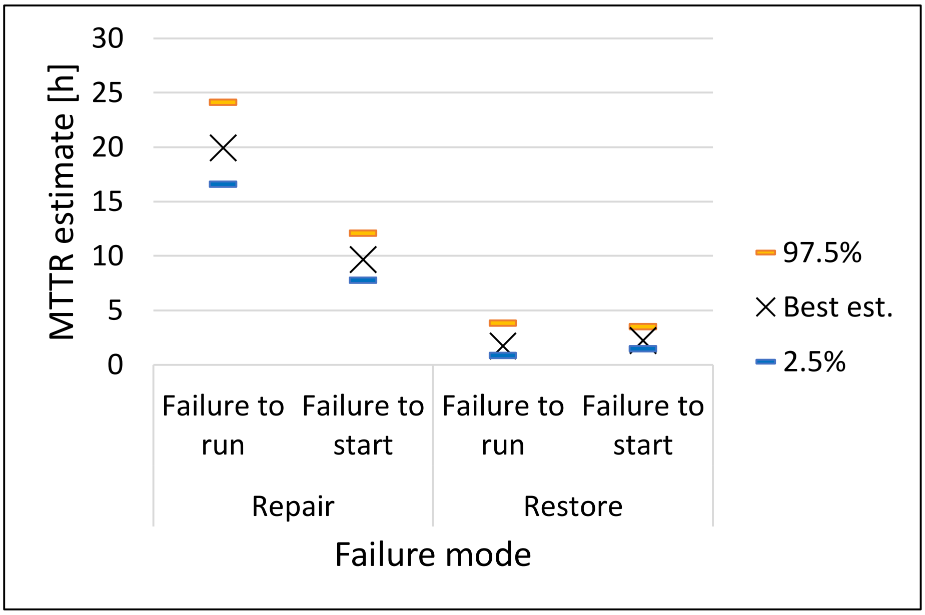
## 5. RESULTS OF DATA ANALYSIS

In this section, only selected results for the centrifugal pumps are presented for reasons of space. The complete results for diesel generators, centrifugal pumps and batteries are found in [2].

### 5.1. Single Failures – Centrifugal Pumps

Estimation of the MTTR in Figure 2 yields uncertainties that are manageable. Although there is more failure to start cases that are classified as restore compared to failure to run, it is not possible to distinguish any difference in restore time when uncertainties are considered. The low resolution of data (restore/repair time is reported in full hours and thus the data is always an integer) could be a factor contributing strongly here. In Figure 2 it is also clear that the repair time for failure to start is lower compared to failure to run. This result indicates that failures that occur earlier in the accident sequence have a lower severity and repair time.

**Figure 2: Estimate of MTTR and uncertainties for centrifugal pumps.**



Repair failure probabilities of centrifugal pumps with failure mode failure to run is shown in Figure 3 (for data, exponential and lognormal distribution plotted against available time). The lognormal distribution performs better compared to the exponential distribution.

**Figure 3: Repair failure probability for centrifugal pumps with failure mode failure to run. Repair waiting time of 8 hours is assumed.**

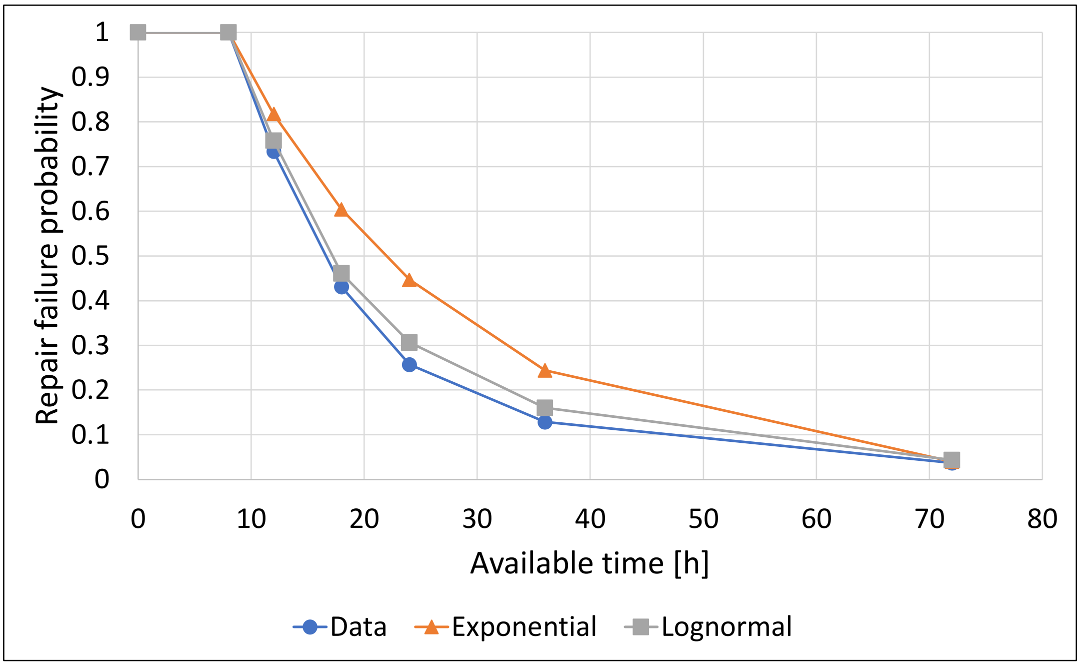
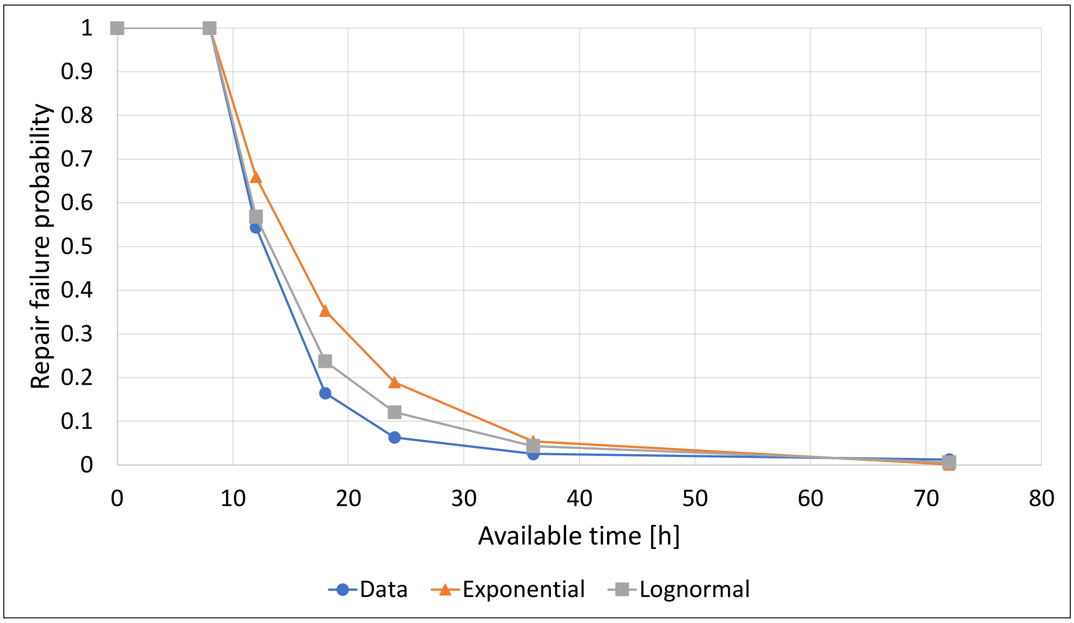


**Figure 4: Repair failure probability for centrifugal pumps with failure mode failure to start. Repair waiting time of 8 hours is assumed.**



Corresponding figures have been produced for all studied components, and for both “restore” and “repair”. All figures cannot be presented in this paper.

### 5.2. Common Cause Failures – Centrifugal Pumps

For a large portion of the centrifugal pump events (21/47, about 45% or [31%, 59%] Bayesian Credible Interval), repair was not needed, and the pumps could be restored (class 1), mainly due to faulty alignment in the system, as can be seen in Table 6 This emphasizes the importance of operability readiness verification after test and maintenance activities.

Repair of severity class 2 was possible in only 5 out of 47 events, i.e., about 11% (or [4%, 22%] Bayesian Credible Interval). Among the five events in repair severity class 2, the repairs involved a faulty switch which prevented activation. This incident had a downtime of about 6 hours. Another repair concerned air in suction paths which led to failure of the pumps. This condition was however quickly re-established. Three out of five events concerned this problem. The last event involved a failure of the air drain valve, but the valve was repaired after 40 minutes.

In severity class 3, most of the demand events (9 out of 11) had the failure mode failure to run and these events involved severe component failures. For example, problems with inappropriate oil, and problems with the suction lines to the pumps. Failure mechanisms for the remaining events in this severity class involved different types of failures, such as electrical problems, design faults and problems in the suction lines.

Only one single event was assessed as a non-shock event, so this substantiates the fact that that the timing of failures is not relevant to consider, especially for centrifugal pumps. The statistics are summarized in Table 4.

**Table 4: Failure events of centrifugal pumps.**

| Repairability | Detection | Failure mode[*] | Failure timing | Events |
|---|---|---|---|---|
| 1. Restore | Demand | FS | Shock | 4 |
| 1. Restore | Monitored | FR | Shock | 3 |
| 1. Restore | Monitored | FS | Shock | 7 |
| 1. Restore | Other | FC | Shock | 1 |
| 1. Restore | Other | FC | Non-shock | 1 |
| 1. Restore | Other | FR | Shock | 2 |
| 1. Restore | Other | FS | Shock | 3 |
| **Sum of 1. Restore** | | | | **21** |
| 2. Repair | Demand | FR | Shock | 2 |
| 2. Repair | Demand | FS | Shock | 1 |
| 2. Repair | Monitored | FR | Shock | 1 |
| 2. Repair | Other | FS | Shock | 1 |
| **Sum of 2. Repair** | | | | **5** |
| 3. Repair | Demand | EL | Shock | 1 |
| 3. Repair | Demand | FR | Shock | 9 |
| 3. Repair | Demand | FS | Shock | 1 |
| 3. Repair | Other | FR | Shock | 5 |
| 3. Repair | Other | FS | Shock | 5 |
| **Sum of 3. Repair** | | | | **21** |
| **Total** | | | | **47** |

[*] Failure to Start, “FS”. Failure to Run, “FR”, Failure to Stop, “FC”

## 6. DISCUSSION AND CONCLUSION

Since the DIOR project spanned over many topics related to single failure and common cause data, the work resulted in several conclusions and suggestions for further work. All of these cannot be fitted into this paper and therefore a selection of conclusions is given below.

Distribution fitting

- Modeling repair times could be performed with both the exponential distribution and the lognormal distribution.
- For the centrifugal pumps, that has the most data, the lognormal distribution can be seen to perform better with its relatively good curve fitting.
- The exponential distribution still performs well, and in combination with its simplicity will probably be preferred in future modelling.

Waiting Time/Accident Condition

It is likely that the repair waiting time is highly dependent on the accident conditions and the fault that has occurred. For example, HRA factors such as the stress level or the complexity of the situation impacts the situation. Also, it is not evident that repair would be initiated immediately after the failure is discovered since EOPs might direct operators toward other options, thereby affecting the available time for repair.

Many of the reported failures, especially for diesel generators, are discovered during periodic testing. Data for such events are included in the data analysis although the overall conditions probably are not like “accident conditions”. The level of stress, and other negative factors, are lower during tests, on the other hand the incentive to quickly repair/restore the component is also lower.

This is the reason why NUREG/CR-6823, “Handbook of Parameter Estimation for Probabilistic Risk Assessment”, [0], suggests that only failures occurring at situations similar to accident conditions should be included in the data analysis and for these events, the downtime should be calculated using information about when the failure occurred and when the component was operational again. Such events are however uncommon and there is no categorization of events similar to accident conditions in the TUD data. Using this method for existing TUD-data results in long downtimes which raises questions about the credibility of the method on actual data.

Instead, an alternate method is used in this report where the active repair time is complemented by an estimated wating time assumed to be 4 hours for restore and 8 hours for repair. The waiting time is an aspect that must be studied in more detail in future work.

Restorability and Repairability

For centrifugal pumps, the share of restorable CCF events is much higher compared to the single failure analysis. A high share of the pre-initiator human failure events (HFEs) is possible to restore, i.e., root cause “Human action” or “Procedure”. These events have a significant impact on the CCF reliability parameters, but they can be restored by simple operator actions to working conditions if the available time is sufficient. For repair, the single failures of centrifugal pumps tend to be more likely to be “easily repaired” (severity class 2) compared to the CCF events.

Pilot Application

A pilot application was carried out were a PRA-model for a fictious boiling water reactor was used and a scenario involving the spent fuel pool was chosen to demonstrate how repair data can be assigned. The results from the pilot application indicate that the results might be quite conservative if repair is not credited. If, for instance, sequences where the failure mode “failure to run” for centrifugal pumps are studied, the results above indicate that the result is lowered by a factor of 4 if repair is credited (the repair failure probability is 0,25).

### Acknowledgements

The authors would like to thank the Nordic PSA Group (NPSAG) for the funding and support of the project.

### References

[1] US. NRC. 2003. *Handbook of Parameter Estimation for Probabilistic Risk Assessment*. Report NUREG/CR-6823

[2] E. Sparre, C. Eriksson, M. Hakansson, J. Larsson and G. Johanson, ”*Deeper Investigation of Repairability of failures (DIOR)”,* NPSAG Report 63-001:01, April 2022.

[3] TUD Office. *T-Book. Reliability Data of Components in Nordic Nuclear Power Plants*, 8th edition, The TUD Office, 2015, Stockholm.

[4] ICDE project. https://www.oecd-nea.org/jcms/pl_25090/international-common-cause-failure-data-exchange-icde-project

[5] T. Tyrväinen, et.al., *“Prolonged available time and safe states - State of the art review”,* 2019