Reliability Analyses of EDG Systems including Multi-Diesel Configurations

Mariana Jockenhövel-Barttfeld[a], Yousef Abusharkh[b], and Manuel Güldner[c]
[a] Framatome GmbH, Erlangen, Germany, mariana.jockenhoevel-barttfeld@framatome.com
[b] Framatome GmbH, Erlangen, Germany, yousef.abusharkh@framatome.com
[c] Framatome GmbH, Erlangen, Germany, manuel.gueldner1@framatome.com

Abstract: This paper focuses on the reliability assessment of Emergency Diesel Generator (EDG) systems in nuclear power plants. Reliability analyses are performed as part of the safety demonstration process during the design phase of EDG systems in modernization and in new build projects.
The analysis aims at assessing the reliability impact of replacing one large EDG set by smaller EDG sets operating in parallel, building a so-called multi-diesel configuration. Different arrangements of small EDG sets (with and without backup equipment) are analyzed using fault trees. The best configurations from the reliability perspective are identified. The possibility of repairing backup equipment after failing in operation is considered in the reliability calculations.
The reliability analysis performed for single EDG trains and for a 2oo4 EDG system concluded that a multi-diesel configuration for the replacement of one large EDG set should involve: (a) the minimum possible amount of EDG sets in each train needed to provide the required output load and (b) at least one backup set in each train, otherwise the system availability is downgraded by the replacement. From a reliability perspective two backup sets in each train are recommended.

1. INTRODUCTION

Emergency Diesel Generator (EDG) systems at nuclear power plants (NPPs) usually involve large redundant emergency diesel generator sets. The EDG set consists of the emergency diesel engine delivering the mechanical power and the emergency diesel generator converting the mechanical power into an electrical supply together with the support systems (e.g. the start air and cooling systems, fuel oil system).

The design capacity of one large EDG set corresponds to the emergency power load required in one NPP train, which is in the range above 2000 kW up to 10000 kW per diesel aggregate set, depending on the plant design. The design capacity of the EDG system is such that the NPP can be safely shutdown by supplying the essential loads in case of an event of loss of the offsite power (LOOP), requiring at most 2 out of 4 (2oo4) trains, such as in the German NPPs with a Konvoi design.

Large diesel generator sets are highly complex and require high efforts for integration engineering and erection, very difficult replacement with other brands due to different footprints and time-consuming repair activities, requiring extended outages if one large diesel generator set is damaged.

On the contrary, small EDG sets typically supply a power below 2000 kW. EDG configurations involving multiple EDG sets operating in parallel, the so-called muti-diesel, are considered to offer several installation and operational advantages over a single large EDG set, such as the improvement in the maintainability, reliability, availability and in the flexibility for possible power expansions. In addition, small EDG sets have the advantages to require smaller and simpler buildings with the possibility to install complete functional container packages.

This paper focusses on the assessment of the reliability impact analysis of replacing one large EDG set by smaller EDG sets operating in parallel. Different arrangements of smaller EDG sets (with and without backup equipment) are analyzed using fault trees with the aim of gaining insights about the best configurations from the reliability perspective to be used in NPP modernizations projects and in new plant designs.

2. CONSIDERATION OF DYNAMIC EFFECTS

The reliability impact of replacing a large EDG set by smaller paralleled sets is estimated using fault trees. Fault tree analyses allow for a “static” (time-independent) approach to calculate the system reliability for different operation durations (mission time). In this paper, a “quasi-static” approach for modelling dynamic effects is considered in the fault trees by modelling the repair of failed backup EDG sets after they fail in operation.

Figure 1 shows a comparison of the “quasi-static” fault tree approach considered in this paper with the approach presented in [1], which considers dynamic effects in a probabilistic analysis frame for a 3oo3 EDG system using Markov chains.

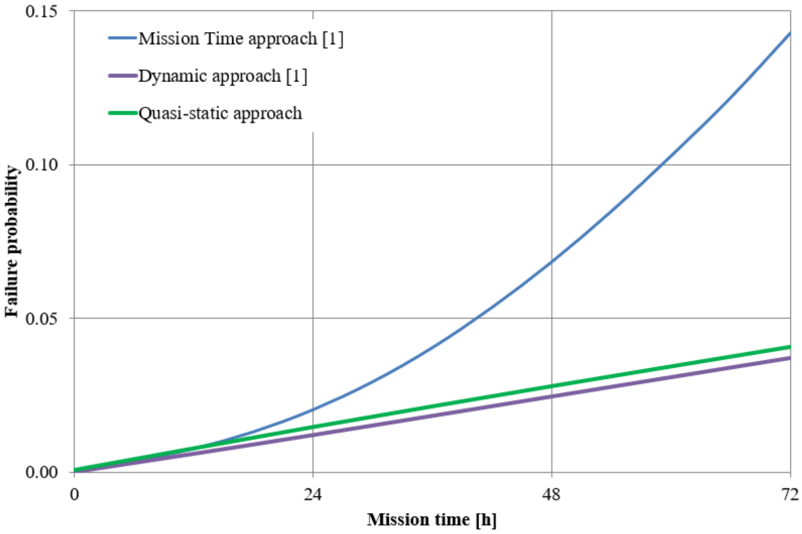

Figure 1: Comparison of a “quasi-static” approach with results from [1] for the failure of 3oo3 EDG trains

As shown in Figure 1, the approach suggested in this paper leads to slightly higher failure probabilities than the probabilities calculated in [1]. Note that a fault tree approach using a mission time model (no component repair considered) leads to very conservative probability calculations, specially for long mission times.

3. RELIABILITY ANALYSIS OF MULTI-DIESEL CONFIGURATIONS

The unavailability (failure probability on demand) of one EDG set is generally given if:

- The EDG set fails to start or
- The EDG set fails to operate within a certain mission time.

The failure to start of the EDG can be caused by undetected failures that occurred before the demand and remained latent during the standby period. The probability of failure to operate is a conditional probability given that the EDG set started successfully.

The possibility of repairing an EDG set after it fails to operate within the mission time is considered in the fault tree model. The failed components are unavailable during the repair time (mean time to repair, MTTR) and can only affect the system reliability if additional sets fail to operate during the mission time.

The following assumptions are considered for the analysis:

- The configuration of small EDG sets connected in parallel provides at least the same power load supplied by the large EDG set.
- Configurations involving safety concepts with N sets, N+1 and N+2 parallel sets are considered for the replacement of a single large EDG set.
- A large EDG set supplying approx. 6000 kW is considered for the analysis (based on the German Konvoi design).
- If the configuration involves a backup small EDG set, then it is assumed that the backup set can replace any EDG connected in parallel (i.e. it can supply the load to the consumers connected to the failed EDG). The failed backup EDG set can be repaired immediately after it fails to operate without any influence on the system reliability.
- A MTTR of 12 h is assumed for the analysis.
- A periodical test interval of one month is assumed for each EDG train with a staggered testing scheme. For configurations involving multiple EDG sets it is assumed that all sets within one train are tested simultaneously once a month (non-staggered scheme).

The following mission time (TM) scenarios are interesting for the analysis of the EDG system in nuclear applications [2]:

- Short-term LOOP with a duration of 2 hours
- Medium-term LOOP with a duration of 24 hours
- Long-term LOOP with a duration of 7 days (168 hours).

Longer mission times are also considered in this to account for the analysis of beyond-design scenarios.

The analysis conducted in this paper does not consider failures of the control and instrumentation equipment and possible dependencies between sets, which may be introduced by their controlling and synchronization. The control and synchronization of the small sets is still a challenge, which is currently being investigated in the frame of EDG research and development projects.

Contributions to the failure to start caused by the EDG unavailability due to preventive maintenance or testing activities are not considered in this analysis. This is because maintenance / testing activities are relevant after the system has been installed and commissioned. These depend on the specific plant strategies, which are not relevant in the system design phase, where the failure contributions from the equipment are of main interest.

3. COMPONENT RELIABILITY DATA

Component failure data used for reliability analyses are typically estimated with the Bayes method based on the operating experience with such equipment in the nuclear field. Component failure data are followed up and reported in component reliability databases, such as NUREG CR-6928 for US, the T-Book for northern Europe or the centralized reliability database ZEDB for German NPPs (ZEDB, 2014).

The failure rates for the failure to start/operate of the EDG sets are taken from the Centralized Reliability Database ZEDB [3], based on operating experience of German nuclear power plants collected from 1976 to 2013. These failure rates consider failures of the main components (engine and generator) and failures of the supporting systems required to guaranty the EDG set start and operation (avoiding excessive wearing), as well as failures of the electrical and control components (see Figure 2).

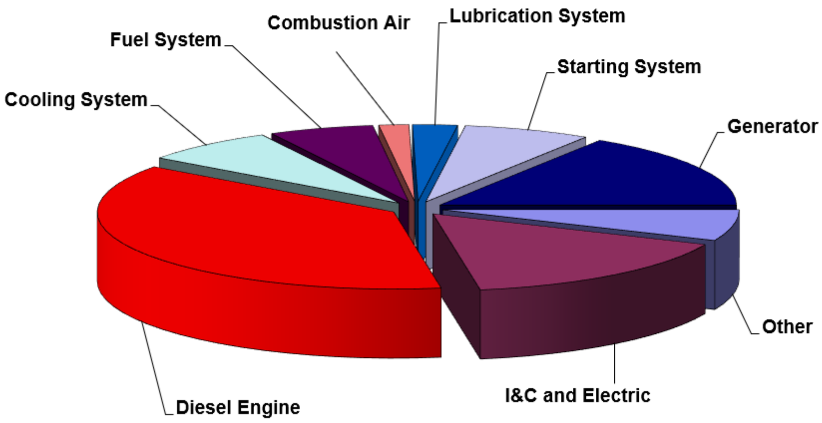

Figure 2: Contribution of EDG auxiliary systems failures to the EDG failure

The ZEDB provides failure rates for EDGs distinguishing between two power-rated groups (the so called "collectives"):

- Group 1: EDG sets with a rated power from 320 kW to 1740 kW and
- Group 2: EDG sets with a rated power from 2682 kW to 7300 kW.

Table 1 lists the failure rates estimated in the ZEDB database for these two EDG groups.

Table 1: Generic failure rates of EDG sets [3]

EDG collective groups (rated power, kW)	Failure to start [1/h]	Failure to run [1/h]
320 - 1740	4.04E-06	8.41E-04
2682 - 7300	8.60E-06	2.49E-03

The reliability data of the EDG group involving the largest electrical rated power (above 2682 kW) is considered for the large single EDG sets. The small EDG sets are assigned the reliability data of the collective group involving a rated power below 1740 kW.

Common cause failures (CCF) are modelled in the fault trees for configurations involving redundant EDG sets using the Alpha Factor Model. The CCF Alpha parameters for the failure to start and to operate are taken from NUREG/CR-5497.

4. RELIABILITY OF MULTI-DIESEL IN ONE EDG TRAIN

This section analyses the impact of replacing one large single EDG set within one train by a set of smaller sets operating in parallel with and without backup equipment.

Figure 3 compares the unavailability of the N=1, N+1 and N+2 configurations. The higher the number of paralleled sets to provide the load, the lower the availability of the configuration.

For configurations with the same number of sets, the one including two backup sets (e.g. N=3+2) has a higher availability as the one including one backup set (e.g. N=3+1). For example, for a required load of approx. 6000 kW the configuration involving 3+1 small sets (each one providing approx. 2000 kW) should be favored over a configuration with N=4+1 sets (each one providing approx. 1500 kW).

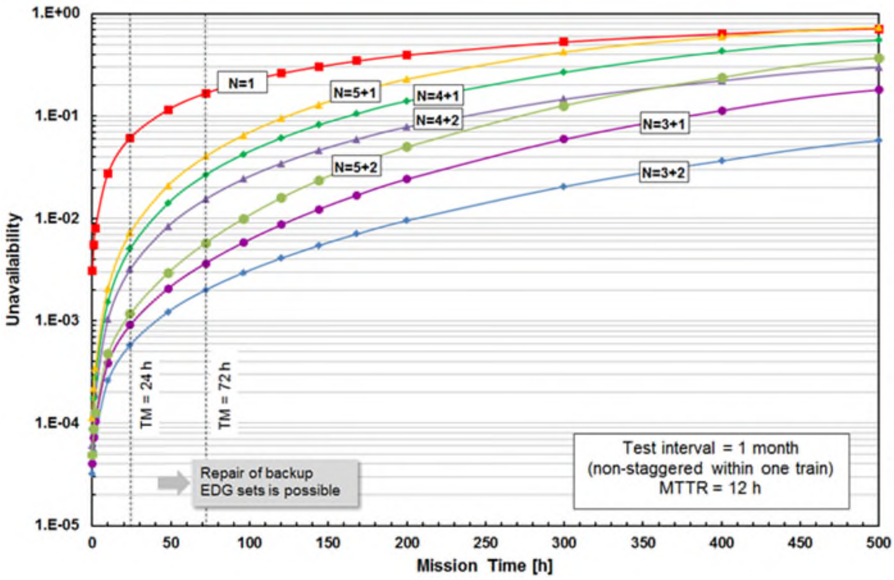

Figure 3: Unavailability of N, N+1 and N+2 configurations as a function of the mission time (one EDG train)

Figure 4 shows the availability improvement comparison for replacing one large set by N+1 and N+2 smaller sets operating in paralleled.

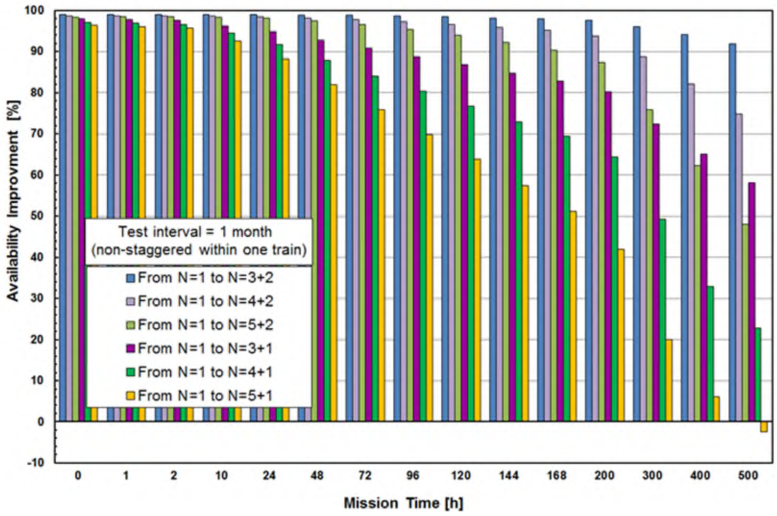

Figure 4: Availability improvement from the single large EDG to the N+1 and N+2 configurations as a function of the mission time (one EDG train)

Figure 5 shows the sensitivity analysis results for one EDG train for different values of the MTTR considered to repair the failed backup sets in the N=3+1 and N=3+2 configurations.

Note that the reliability results of the N=3+1 configuration are rather insensible to an increase of the MTTR value for the EDG sets. For the N=3+2 configuration the availability slightly increases with the increasing MTTR values.

The small influence of the increased MTTR values can be justified by the fact that failures of the backup sets are not the most important contributors to the unavailability of the different configurations. The reliability results are dominated by combination of failures of EDG sets failing within the mission time.

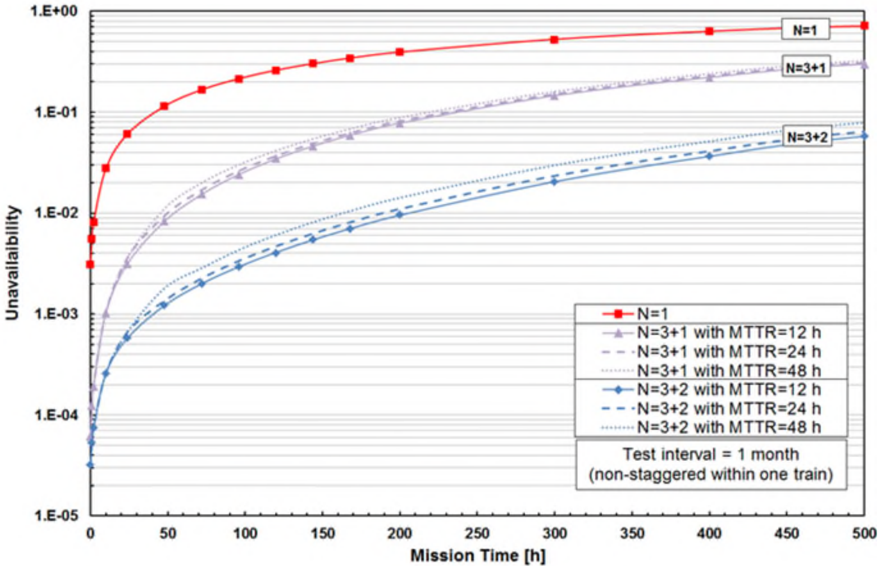

Figure 5: Sensitivity analyses for different MTTR values for the N+1 and N+2 configurations as a function of the mission time (one EDG train)

5. RELIABILITY OF MULTI-DIESEL IN THE EDG SYSTEM

This section analyses the reliability impact when one large set in each of four trains of the EDG system is replaced by N+1 or N+2 multi-group configurations. The success criterion for the emergency power supply out of the four trains is assumed to be 2oo4, i.e. two trains are required to operate during the mission time.

For the configuration involving the small paralleled EDG sets common cause failures are modelled for EDG sets within one train (all sets are tested simultaneously once a month) and also between the trains, assuming a staggered periodic testing strategy. For mission times longer than 24 h repair activities of backup sets are considered.

Figure 6 shows the unavailability of at least three (>3oo4) trains for the configurations involving one single EDG set (N=1), N+1 and N+2 configurations for N=3, N=4 and N=5 in each train as a function of the mission time.

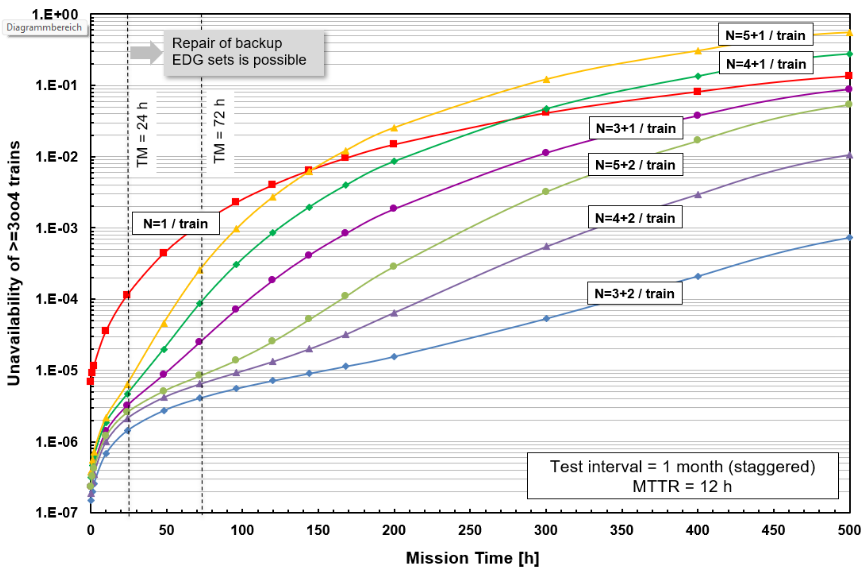

Figure 6: Unavailability of >=3oo4 trains for the configurations with N=1, N+1 and N+2 EDG sets

The system with the N=3+2 configuration in each train is the one involving the highest availability. The unavailability of the configurations involving two backup sets (N+2) in each train increases smoothly with the increasing mission time (see Figure 6). On the other hand, the unavailability of the configurations with only one backup set (N+1) in each train is much more sensible to the increasing mission time. This can be justified mathematically by analyzing the failure combinations (minimal cut sets, MCS) for each configuration.

The system with N+2 sets in each train are unavailable if three trains fail. Each train fails if three EDG sets fail, i.e. combinations of nine failed EDG sets lead to the failure of > 3oo4 trains. The system with N+1 EDG sets/train are also unavailable if three trains fail, but each train fails if two EDG sets fail. This means, combinations of six failed EDG sets lead to the failure of > 3oo4 trains.

According to this, the system with N+2 sets/train requires a larger number of failures (9) than the N+1 configuration/train (6) to be unavailable.

The results of the N+2 configuration are dominated by CCF failures, which have a higher probability than the combination of nine failed sets (three in each train), even for long mission times. The results of the N+1 configuration are dominated by combinations of six failed sets (two in each train), which have a higher probability than the CCF failures, especially for long mission times.

Finally, the availability improvement obtained by replacing one single large EDG by the multi-diesel configurations is shown in Figure 7.

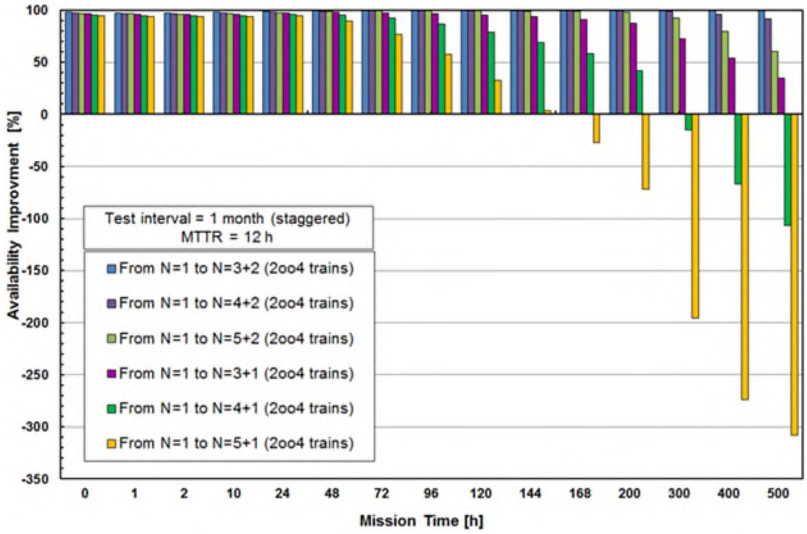

Figure 7: Availability improvement by replacing one single EDG set by N+1 and N+2 multi-group configurations in each of the 2oo4 trains

Note that for the N=3+1 and N=3+2 configurations in each train the availability of the 2oo4 system is improved more than 80% for relevant mission times in nuclear applications (approx. below 200 h).

For the N=4+1 configuration an improvement of approx. 80% is obtained for mission times up to 120 h. For longer mission times the improvement decreases rapidly given the dominance of the combination of sets which fail to operate. For a mission time of 200 h an availability improvement of approx. 40% with respect to the single large EDG set can be achieved. For mission times longer than 200 h, the system with single sets in each has a larger availability than the multi-diesel configuration. If one backup set is additionally added in each train, i.e. N=4+2, the availability is greatly improved (see Figure 7).

Concluding, the system with four trains and a success criterion of 2oo4 with multi-diesel configurations N+1 and N+2 with N=3 and N=4 in each train has higher availabilities than with single large EDG set in each train for mission time relevant in nuclear applications (approx. up to 200 h).

6. CONCLUSIONS

This paper analyzed the impact of replacing one large single EDG by smaller EDG sets operating in parallel with and without backup equipment.

The reliability analysis performed for single trains and for a 2oo4 system concluded that a multi-diesel configuration for the replacement of one large EDG set should involve:

- The minimum possible amount of EDG sets in each train needed to provide the required output load and
- At least one backup set in each train, otherwise the system availability is downgraded by the replacement. Two backup sets are recommended from the reliability point of view.

If at least one backup set is involved in the configuration the availability of the system is greatly upgraded after the replacement of the single EDG set. The more backup sets involved in the multi-diesel configuration, the higher the availability of the configuration. Backup sets add redundancy into the system and allow for repairing activities, especially for the long missions without affecting the system availability.

As analyzed for single EDG trains an increase of the MTTR values considered to repair backup sets does not influence the reliability results considerably.

The selection of a multi-diesel configuration also depends on the cost trade-offs (e.g. investment, maintenance, periodic testing), which have to be considered in the configuration selection together with reliability considerations.

Future work on reliability of multi-diesel configurations includes the consideration of the reliability of electronic controls, which may add dependencies between the EDG sets.

References

[1] Dirksen G. and Kollasko H. (2020), Quasi-static Approach for Modelling Dynamic Effects in large PSA Models, Probabilistic Safety Assessment and Management PSAM 15
[2] Jockenhövel-Barttfeld M., Abusharkh Y., Kollasko H. and Schwemmlein M. (2019), Reliability Analyses for the Safety Demonstration of EDG Systems. TÜV Symposium, Munich
[3] Centralized Reliability Database (Zentrale Zuverlässigkeits- und Ereignisdatenbank, ZEDB, 2014); TW 805-15; Band 1; ISSN 1439-7498.