ISSN: 3107-6513

A Details Study on Evaluating Emergency Diesel Generator Reliability in Nuclear Power Plants

Shiraji Md Ismail Hossen[1], Ahmar Imran[2], Nabeel Hassan[3], Borhan Uddin[4]
[1,3] School of Electrical and computer Engineering South China university of Technology, China
[2] School of Computer Sciences and Technology The University of Faisalabad, Pakistan
[4] School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou, China

Abstract:

This study presents a reliability analysis of the emergency diesel generator (EDG) system in nuclear power plants (NPPs) using fault tree analysis (FTA) in combination with survival signature method. Analysis assesses the robustness of the EDG system, which plays a critical role in sustaining essential functions during power outages. Given this importance, the system must meet high standards in design, operation, and maintenance to ensure quick start-up and reliable operation. The analysis begins by decomposing the EDG system into subsystems and components, followed by the construction of a fault tree that maps potential failure scenarios and their causal relationships. The study is based on specific assumptions, including non-repairable components, independent failure events, and defined failure time distributions.

The core technical content of the chapter centers on the calculation of the survival signature. It systematically outlines the process, including the formation of component state vectors, the use of Boolean algebra to determine system functionality, and the integration of these elements to derive the survival signature. To demonstrate the practical implementation of this method, the chapter concludes with the development of a MATLAB function that calculates system reliability. This function embodies the theoretical framework of the survival signature approach and validates its effectiveness through numerical results.

Keywords: emergency diesel generator; nuclear power plant; reliability analysis; fault tree analysis; survival signature; system reliability; failure time distributions; MATLAB; component state vectors; Boolean algebra.

1. Introduction to the Reliability Analysis of Emergency Diesel Generators in Nuclear Power Plants

Ensuring a continuous and reliable power supply to essential safety systems is a paramount concern in the operation of nuclear power plants (NPPs). The Emergency Diesel Generator (EDG) serves as the last line of defense, designed to automatically start and supply backup electrical power in the event of a complete loss of off-site power. The criticality of this function demands an exceptionally high standard of reliability. A failure of the EDG system during such a contingency can have severe safety implications, potentially leading to a core damage scenario. Therefore, a rigorous and quantitative assessment of EDG reliability is not just an engineering exercise but a fundamental requirement of nuclear safety and regulatory compliance.

Traditional reliability analysis often relies on methods like Fault Tree Analysis (FTA), which provides a logical, top-down model of system failure. While FTA effectively maps the relationships between component faults and system failure, performing dynamic, time-dependent reliability calculations for complex systems with multiple components can be computationally challenging. This necessitates the application of more advanced probabilistic methods to achieve a robust and efficient analysis. This study presents a sophisticated reliability analysis framework for the EDG system by integrating the logical modeling power of Fault Tree Analysis (FTA) with the computational efficiency of the Survival Signature method. The analysis begins with a systematic decomposition of the EDG into its critical components and subsystems, followed by the construction of a detailed fault tree that maps all credible failure pathways leading to a loss of EDG function. The core of the methodology then employs the survival signature, a powerful mathematical tool

ISSN: 3107-6513

that separates the system's structural logic from the probabilistic failure behavior of its components. This approach allows for the elegant calculation of time-dependent system reliability, efficiently handling systems with multiple components of the same type and specified failure time distributions.

The analysis is conducted under standard assumptions for such assessments, including non-repairability of components during the mission time, statistical independence of failure events, and defined failure time distributions for components. To demonstrate practical utility, the theoretical framework is implemented in a computational model. The study culminates in the development and application of a MATLAB-based computational function that embodies the integrated FTA and survival signature approach. This tool enables the calculation of key reliability metrics, providing validated numerical results that quantify the EDG's probability of successful operation over a defined mission time. The outcomes of this analysis offer critical insights for optimizing maintenance strategies, informing design improvements, and strengthening the overall safety case for nuclear power plants.

A Detailed Introduction to the Reliability Analysis of Emergency Diesel Generators in Nuclear Power Plants

I. Critical Role and Context of the Emergency Diesel Generator in Nuclear Safety

Nuclear power plants (NPPs) are complex sociotechnical systems where the primary safety objective is the continuous removal of decay heat from the reactor core under all conditions. This function relies on a suite of support systems, most of which require electrical power. The electrical distribution network is typically the primary source, but its failure—a condition known as a "loss of off-site power" (LOOP)—is a recognized design-basis accident. In such a scenario, the plant's safety is entirely dependent on its on-site, backup power systems. Among them, the Emergency Diesel Generator (EDG) stands as the principal and most robust source of backup AC power, tasked with energizing the essential electrical buses that power critical safety equipment: reactor coolant pumps, safety injection pumps, containment cooling fans, and control room instrumentation.

The EDG's performance is not merely important; it is a cornerstone of "defense in depth." Historical events underscore its criticality. During the 2011 Fukushima Daiichi accident, while the initiating cause was a tsunami, the subsequent core meltdowns were precipitated by the prolonged, station-wide loss of all AC power, a condition known as a "station blackout," which rendered the EDGs and all other backup power sources inoperable. Consequently, the reliability, availability, and start-up success of EDGs are subject to intense regulatory scrutiny worldwide. Regulatory bodies mandate stringent design standards (e.g., seismic qualifications, environmental protection), rigorous testing (monthly "no-load" runs and periodic full-load tests), and maintenance programs. The quantitative assessment of EDG reliability is a central element of Probabilistic Safety Assessment (PSA), a core methodology used to quantify risk and inform regulatory decisions. Therefore, moving beyond qualitative checks to a precise, quantitative, and analytically robust evaluation of EDG reliability is imperative for demonstrating safety, optimizing maintenance resources, and ensuring operational readiness.

II. Limitations of Traditional Reliability Methods and the Need for Advanced Approaches

The reliability of complex systems like an EDG is traditionally analyzed using techniques such as Fault Tree Analysis (FTA) and Reliability Block Diagrams (RBDs). FTA, in particular, is a powerful, deductive tool. It begins with a defined "top event" (e.g., "Failure to supply required power for a 24-hour mission") and works backward, using Boolean logic gates (AND, OR) to identify all plausible combinations of basic component failures that could cause the top event. This process creates a logical map of system vulnerability, highlighting single points of failure and critical component dependencies.

However, for dynamic, time-dependent reliability calculations, especially for systems with complex configurations and multiple identical components, traditional FTA can face combinatorial challenges. Calculating the system's reliability function, R(t)—the

ISSN: 3107-6513

probability that the system functions correctly at time t—becomes computationally intensive as the number of components grows. This is particularly true when components have different, non-exponential failure time distributions (e.g., Weibull distributions that model wear-out), and when the system structure is not a simple series or parallel configuration. Many real-world systems, including the EDG, exhibit complex voting logic (e.g., "2-out-of-3" cooling pumps required) and have multiple redundancies of the same component type (e.g., multiple fuel injection pumps, coolant pumps). Analyzing these systems requires a methodology that can elegantly decouple the system's logical structure from the stochastic behavior of its components. This is the gap that the survival signature method is designed to fill.

III. Integrated Methodology: Fault Tree Analysis and the Survival Signature

The present study proposes and implements an integrated methodology that combines the intuitive, logical modeling of FTA with the computational power and elegance of the survival signature. This two-stage approach provides a comprehensive framework for EDG reliability quantification.

Stage 1: System Deconstruction and Logical Modeling via FTA

The first stage involves a thorough functional and physical decomposition of the EDG system. A typical EDG comprises several critical subsystems:

Starting System: Includes the starting motor, air receiver (for air-start systems), or battery bank (for electric-start), and associated valves/solenoids.

Fuel System: Encompasses the day tank, transfer pumps, filters, injection pumps, and fuel piping.

Diesel Engine: The prime mover, with its cylinders, pistons, turbochargers, and crankshaft.

Lubrication System: Includes the oil pump, cooler, filter, and sump.

Cooling System: Comprises the coolant pump, heat exchanger, and radiator fan.

Exhaust System: Includes the manifold and silencer.

Generator & Electrical System: The alternator, voltage regulator, and circuit breakers.

A fault tree is constructed with the top event, "EDG fails to perform its safety function for mission time T." This top event is then developed through intermediate events representing subsystem failures (e.g., "Failure of Starting System" OR "Failure of Fuel System" OR "Failure of Lubrication System..."). Each subsystem is further broken down into its constituent components. The tree rigorously applies AND gates (where all inputs are needed to cause the output) and OR gates (where any input can cause the output) to model the actual failure logic. This FTA model provides the definitive structural function of the system—a precise mathematical description of how the state (working/failed) of each component determines the state of the entire system.

Stage 2: Quantitative Reliability Calculation via the Survival Signature

The survival signature, denoted often as $\Phi(l)$, is a powerful mathematical concept developed for complex system reliability. For a system with K different types of components, where there are m_k components of type k (e.g., 2 identical coolant pumps, 3 identical sensors), the survival signature $\Phi(l_1, l_2, ..., l_K)$ is defined as the probability that the system functions given that exactly l_k components of type k are working, for all k from 1 to K.

The power of this definition lies in its separation of concerns:

Structural Property (Φ): This depends onlyon the system's design—its connectivity and voting logic, which is already captured in the fault tree. It is calculated by enumerating all possible component state vectors and using the Boolean logic from the FTA to determine, for each vector, if the system works. Φ is a constant for a given system design.

Probabilistic Property: This depends onlyon the reliability of the individual components over time, $R_k(t)$. The probability that exactly l_k out of m_k components of type k are working at time t is given by the binomial distribution based on $R_k(t)$.

The system reliability $R_{system}(t)$ is then computed by combining these two elements: it is the sum, over all possible combinations of working components $(l_1,..., l_K)$, of $[\Phi(l_1,..., l_K)$ * Prob(l_1 components of type 1 work at time t) * ... * Prob(l_K components of type K work at time

ISSN: 3107-6513

t)].

This formulation dramatically simplifies the reliability calculation for systems with redundancies. Instead of dealing with an exponentially growing state space, the survival signature condenses the structural complexity into a single, manageable function. It readily accommodates components with different, independent failure time distributions (exponential, Weibull, etc.), which is a more realistic assumption than forcing all components into an exponential (constant failure rate) model.

IV. Analytical Implementation and Significance

The study conducts this analysis under standard assumptions for high-integrity, mission-critical system assessment: components are considered non-repairable during the defined mission time (e.g., 24-72 hours post-LOOP), reflecting a "run-to-failure" scenario. Failure events of different components are assumed to be statistically independent, an assumption that can be relaxed in more advanced models by incorporating common cause failure factors. Components are assigned specific failure time distributions based on historical failure data, manufacturer specifications, or industry standards (e.g., IEEE Std. 500).

To demonstrate practical applicability, the theoretical framework is codified into a computational tool. The study details the development of a MATLAB function or script that automates the entire process: it can ingest the system structure (derived from the FTA), compute the survival signature Φ, and then integrate it with component reliability functions to generate the time-dependent system reliability curve, R_system(t). This curve is the ultimate output, quantifying the probability of EDG survival over its required mission profile. Sensitivity analyses can be easily performed by varying component failure rates within this model to identify the most critical elements affecting overall system reliability.

2. Emergency diesel generator of NPP

The karachi nuclear power plant (K-2) is a significant advancement in Pakistan's nuclear energy sector, representing the country's first deployment of China's Hualong One (HPR1000) third-generation nuclear reactor technology. This 1,100 MW pressurized water reactor (PWR) was constructed with substantial financial and technical collaboration from China.

To ensure the reliability of the K-2 plant, especially during external power outages, the emergency diesel generator (EDG) system is an important component. Hyundai heavy Industries supplied five EDG units, each powered by a HiMSEN 20H32/40V engine with an output of 8.3 MW, totaling 40 MW of emergency power capacity, shown in Fig. 3-1. These generators are designed to automatically activate under specificconditions, as shown in Fig. 3-2 , such as a loss of coolant or a safety-related low voltage condition on the bus, thereby maintaining power to essential systems like reactor cooling and control instrumentation.

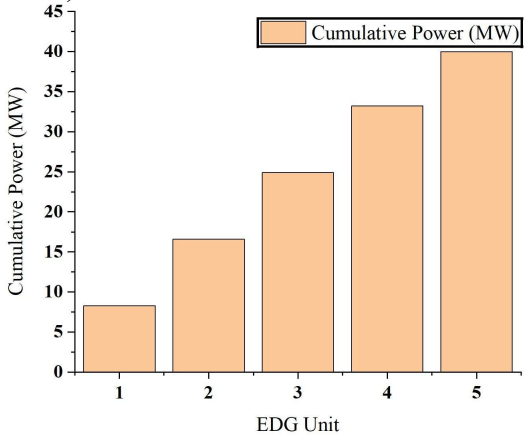


Fig. 3-1 Heavy industries five EDG units

K-2 is integrated into Pakistan's national grid through two primary connections: a 500 kV network for standard operations and a 132 kV system for auxiliary and emergency power needs. This dual-grid configuration enhances the plant's resilience and ensures a stable power supply

ISSN: 3107-6513

under various operational scenarios.

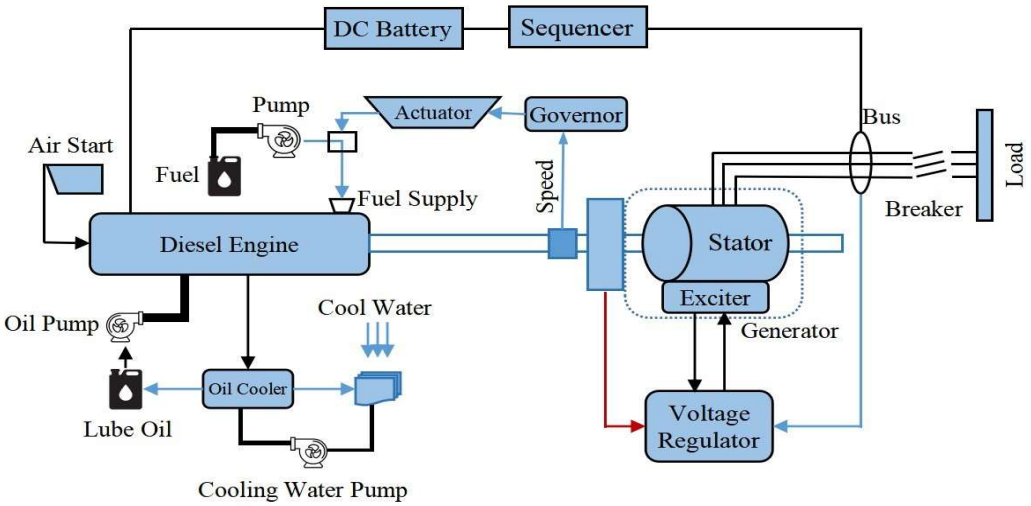


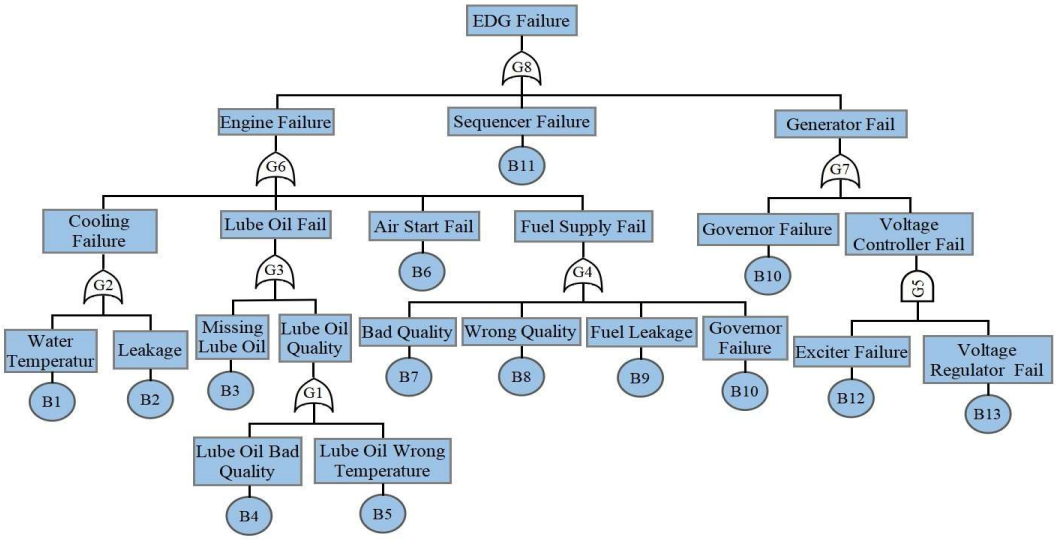
Fig. 3-2 Diagram of emergency diesel generator

The Pakistan nuclear regulatory authority (PNRA) has maintained stringent oversight throughout the construction and operational phases of K-2. The plant's design and safety protocols adhere to both national regulations and international standards, including those set by the international atomic energy agency (IAEA). The EDG systems are classified as safety-critical and comply with standards such as IEEE 387, ensuring their reliability during emergency situations.

The typical EDG system in a NPP includes a diesel engine, the generator itself, fuel storage and supply systems, cooling and ventilation systems, and control systems. These components are designed to work together seamlessly to provide a reliable power supply. The diesel engines used are often large, high-speed units that can run independently of the external power supply. The fuel supply for the EDGs is maintained at a level that ensures the generators can operate for a specified duration, usually several days, without the need for external support.

3. Failure analysis of EDG

This study focuses on a vital element of the power infrastructure—the emergency diesel generators (EDGs) within a nuclear power plant. To systematically explore potential vulnerabilities, a fault tree is constructed to trace and analyze the contributing factors leading to EDG failure. Within this framework, 'EDG failure' is defined as the top event (TE), representing the critical scenario in which the generator is unable to deliver emergency power when demanded. The top event occurs when all essential failure paths leading to the EDG malfunction are simultaneously triggered. Figure 3-3 presents the fault tree diagram, offering a visual depiction of the potential failure modes and their logical interconnections within the EDG system.



ISSN: 3107-6513

Fig. 3-3 Emergency diesel generator failure fault tree

The failure of the EDGs can be attributed to several events and subsystems, which are represented in the fault tree and connected to the top event through logical gates.

The key contributing events include engine failure, generator failure, and sequencer failure. among these, engine failure and generator failure are further broken down into subsystems and basic events, while sequencer failure is treated as a standalone event. The effective operation of the EDG depends on the functionality of several support subsystems. The instrumentation and control (I&C) system is essential for initiating, stopping, and managing EDG operations as shown in Fig. 3-4.

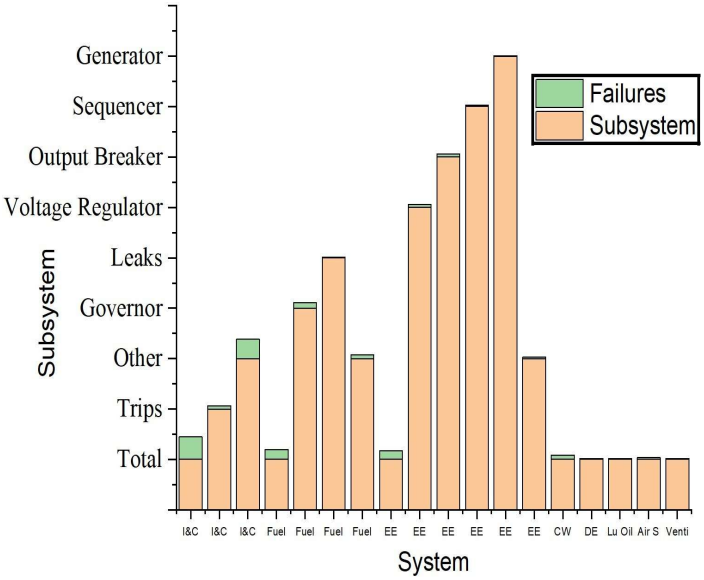


Fig. 3-4 System and sub-system in failures

The heating and ventilation system ensures proper environmental conditions by maintaining airflow and temperature control. The cooling system is also critical, as it is connected to both the engine and generator to regulate their operating temperatures. Additionally, the lubrication system operates in a closed loop and is vital for the smooth and continuous functioning of mechanical components. The fuel subsystem guarantees a steady supply of fuel from a high-capacity storage tank, enabling the EDG to operate for several days without external intervention. These support systems are integrated into the fault tree structure to assess how their failures can contribute to the overall EDG failure. The air start system plays a key role in initiating the EDG's operation by delivering compressed air to start the engine. The governor ensures proper regulation of engine speed during operation. Additional critical components—such as sequencers, exciters, generators, and output circuit breakers—are essential for the EDG's function, providing vital electrical power to safety-related buses within the nuclear power plant. Each of these subsystems contributes significantly to the EDG's overall reliability, and their roles are indispensable in ensuring the safe operation of the plant during emergency scenarios. Table 3.1 lists the subsystems and basic events (BEs) along with their associated failure probabilities. Table 3.2 provides a detailed overview of each EDG component, and Table 3.3 lists the failure rates associated with the basic events used in the reliability analysis.

Tab. 3.1 Sample factors, failure process, and impact contribution of EDG

Source	Mechanism of Failure	Subscription Initiation Air Damage
Ignition Chamber Issue Fail the linkage between engine and its governor Repairing issue	Engine Problem	Engine damage (26%)
Generator issue Breaker failure	Electrical Problem	Compromised ancillary System
Cooling: Missing Cooling water water temperature water leakage missing bad quality Compromised air ventilation		
Lubricant		

ISSN: **3107-6513**

Electrical Problem (12%)

Compromised ancillary systems (45%)

 ISSN: **3107-6513**

	Low pressure in air compressor system	
	Quantity	
Fuel	Quantity	
	Leakage	

4. Assumptions for reliability analysis

This study is built upon key assumptions essential for evaluating the dependability of the (EDG) system. It is assumed that failure times for components belonging to the same category (k) are independently and identically distributed, whereas failures among different component categories are considered mutually independent. It also treats all components as non-repairable and assumes that simultaneous failures do not occur. The (EDG) system in a NPP is structured into three major subsystems: engine failure, generator failure, and sequencer failure. of these, engine and generator failures are considered intermediate events, each further broken down into smaller, more detailed subsystems. For example, engine failure is broken down into cooling failure, lube oil failure, fuel supply failure, and one additional basic event. These subsystems are further decomposed into basic events or system components, as shown in Fig. 3-3 and 3-4.

The study employs a static fault tree model to analyze the system, which consists of 13 basic events. Each of these events is assumed to have a failure time that follows an exponential distribution. These events are categorized into five distinct component types. According to Equation 3.9, the first step involves calculating the function $\phi(x)$ for each x belonging to the set $S(l_1, l_2, l_3, \ldots, l_k)$, and then computing the survival signature corresponding to each combination of component counts l_1 through l_k. This process is repeated iteratively until the survival signature for the entire static system is obtained. Finally, the system's reliability, defined as the probability that it will function at time $t > 0$, is determined using equation 3.11.

Tab. 3.2 Elements of the EDG and their respective explanations

Component	Basic Events	Description
Cooling	B1: Water temperature	Increasing coolant temperatures could potentially lead to operational failures
	B2: Leakage	Effects of coolant leakage on Engine
Lube Oil	B3: Missing	Engine failure due to lack of lubricating oil
	B4: Bad Quality	Poor quality lubricants can cause malfunctions.
	B5: Wrong temperature	If sensor inaccurately detect temperature, may cause a malfunction.
Air start	B6: Air start failing	Failing of air start effect the engine
Fuel	B7: Bad quality	Poor fuel quality can damage the engine
	B8: Wrong quantity	wrong amount can damage the engine.
	B9: Fuel leakage	Leakage of fuel may disrupt the engine
Governor	B10: Governor malfunctioning	If a failure occurs, the engine and generator may be affected.
Sequencer	B11: Sequencer fail	Sequencer fail
Generator	B12: Exciter failure	Exciter fail
	B13: Voltage regulators fail	If the voltage drops normally, the

generator will fail.

The complete procedure for calculating survival signature can be seen in Figure 3-6. In a static system comprising m components, the initial step is to produce $x, x \in S(l_1, l_2, l_3, \ldots, l_k)$. Then, calculate $\phi(x)$ according to x and principles of Boolean algebra. If $\phi = 1$ or 0, $\phi(x)$ can be ascertained immediately. The procedure is carried
out iteratively until each of the 2^m variants of x has been evaluated, ensuring the system's survival signature and reliability are accounted for. System Survival signature has the characteristics "complete separation of system structure and probabilistic data" to a certain extent.

Tab. 3.3 Failure probabilities of basic events

BEs	Failure Probability	Failure rate	B1 λ
B2 B3	4.5×10^{-4}		
B4	3.24×10^{-4}	0.006	
B5		0.001	
B6	1.0×10^{-3}		
B7		0.002	
B8		0.001	
B9	1.0×10^{-3}		
B10	2.4×10^{-4}		
B11	4.24×10^{-4}		
B12	3.31×10^{-4}		
B13	3.29×10^{-4}		

5. Survival signature calculation and reliability estimation

Based on the extracted fault tree of the emergency diesel generator, the system includes 13 basic events categorized into five component types. For instance, the cooling system components, such as B1 and B2, belong to type 1. The lubrication oil components B3, B4, and B5 are grouped as type 2, while the air start component B6 is classified as type 3. Fuel system components B7, B8, and B9 fall under type 4, and the generator and governor components—B10, B11, B12, and B13—are grouped as type 5. The first step in the reliability analysis is to calculate the survival probability of the system for various component state vectors. The results of these statistics are shown in

ISSN: 3107-6513

Table 4.4[96].

Tab. 3.4 The survival signatures of the Emergency Diesel Generator.

	l_1	l_2	l_3	l_4	l_5	$\Phi(l_1,l_2,l_3,l_4,l_5)$		l_1	l_2	l_3	l_4	l_5	$\Phi(l_1,l_2,l_3,l_4,l_5)$
0	0	0	0	0	0	0	0	1	1	3		7/9	
0	0	0	0	1	1/9	0	1	1	1	4		1/3	
0	0	0	1	2	2/9	1	2	0	2	0		8/9	
0	0	0	1	3	1/9	1	2	0	2	1		2/3	
0	0	0	2	4	2/9	1	2	0	3	2		1/9	
0	0	1	2	0	1/3	1	2	0	3	3		1/2	
0	0	1	3	1	2/9	1	2	0	0	4		4/9	
0	0	1	3	2	1/3	1	2	0	0	0		7/9	
0	0	1	0	3	1/9	1	2	0	1	1		1/3	
0	0	1	0	4	2/9	1	2	1	1	2		8/9	
0	1	0	1	0	4/9	1	2	1	2	3		2/3	
0	1	0	1	1	2/3	1	2	1	2	4		1/9	
0	1	0	2	2	2/9	1	3	1	3	0		1/2	
0	1	0	2	3	1/2	1	3	0	3	1		4/9	
0	1	0	3	4	2/3	1	3	0	0	2		1/3	
0	1	1	3	0	1/3	1	3	0	0	3		1/9	
0	1	1	0	1	5/9	1	3	0	1	4		2/9	
0	1	1	0	2	2/3	1	3	1	1	0		1/3	
1	3	1	2	1	2/3	1	3	1	3	3		1/3	
1	3	1	2	2	5/9	1	3	0	3	4		1/9	

Here, the component status vector is given as l=(0,1,1,0,1) representing the operational status of five types of components in a system. Type 1 has no components (0), Type 2 has one functioning component (1), Type 3 has all components working (1), Type 4 has no functioning components (0), and Type 5 has one working component (1). To ensure the system works properly, certain combinations of functional components must be met. Specifically, parts 1, 2, 3, 6, and 8, or parts 1, 2, 3, 7, and 8, must all be functioning properly. With this in mind, the system's reliability is calculated using the function $\Phi(0,1,1,0,1)=5/9$ meaning there is a 5/9 probability that the system will operate correctly given the specific component statuses outlined in the vector. This calculation considers both the number of operational components and the specific conditions necessary for the system to function correctly. Takeas an example to illustrate the calculation results. This situation shows that all 0 components of type 1 work normally, and 1 of the 3 components of type 2 Normal operation, no component of type "3" is faulty, out of three types '4' components, one is functioning properly, and among four types '5' components, one is operating as expected. At this time, all possible results of the component status vector are $\binom{0}{2}\binom{1}{3}\binom{1}{1}\binom{0}{4}\binom{1}{4} = 9$, so $\prod_{k=1}^{5}\binom{m_k}{l_k}^{-1} = \frac{1}{9}$. And in these 5 types Among the possible results, there are only two types: parts "1", "2", "3", "6", "8" and parts "1", "2", "3", "7", "8" Only when all the combined components work properly can the system work properly, that is, therefore

3-1

 ISSN: 3107-6513

$$\Phi(0,1,1,0,1) = \frac{5}{\binom{0}{2}\binom{1}{3}\binom{1}{1}\binom{0}{4}\binom{1}{4}} = 5/9 \quad 3\text{-}2$$

By extracting the survival signature at each phase of the system, reliability can be accurately quantified, allowing for the continuous assessment of the system's real- time dependability during its operation.The resulting reliability curve, illustrating this dynamic behavior, is presented in Fig. 3-5.

$$P(T\_s > t) = \sum_{l_1=0}^{2}\sum_{l_2=1}^{3}\sum_{l_3=1}^{1}\sum_{l_4=0}^{3}\sum_{l_5=1}^{4}\left[\phi(l_1,l_2,l_3,l_4,l_5)\prod_{k=1}^{5}\left(\binom{3}{1}[F_2(t)]^{3-1}[1-F_k(t)]^1\right)\right] \quad 3\text{-}3$$

$$R_s(t) = P(T_s > t) = 0.94625 \quad 3\text{-}4$$

Theoretical research on (EDGs) in (NPPs), which involve multiple component types, employed the survival signature method to evaluate system reliability. Custom MATLAB functions were developed to carry out numerical reliability calculations, demonstrating both the feasibility and accuracy of this approach. This analysis hinges on the foundational assumption that components sharing the same type experience lifetimes that are both independent and identically distributed, while failures among distinct component types unfold independently. The survival signature serves as a probabilistic blueprint, reflecting the system's operational status as a function of how many components remain functional at any point in time. By weaving together this survival signature with the unique failure profiles of each component type, it becomes possible to precisely compute and dynamically track the system's reliability as it evolves in real time.

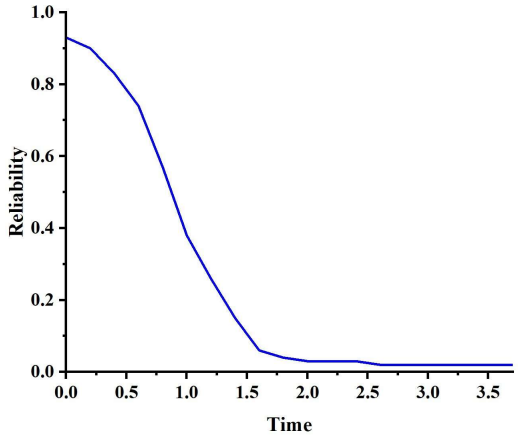


Fig. 3-5 Reliability curve of EDG

It can be concluded that system reliability can be conveniently and accurately determined using the survival signature method in combination with fault tree analysis.

6. Operational performance during load

The availability of an emergency diesel generator (EDG) depends on several factors, including the yearly failure rates, the duration required to repair failures, and the downtime caused by scheduled maintenance activities. Fig. 3-6 presents the distribution of repair times, including logistics delays (MTTR), for all packaged EDGs.Because data originates from earlier collection efforts, some observations were summarized using the subset's mean repair times, which typically fall within the 16 to 24-hour range. This averaging causes the data to display an artificial bimodal distribution.

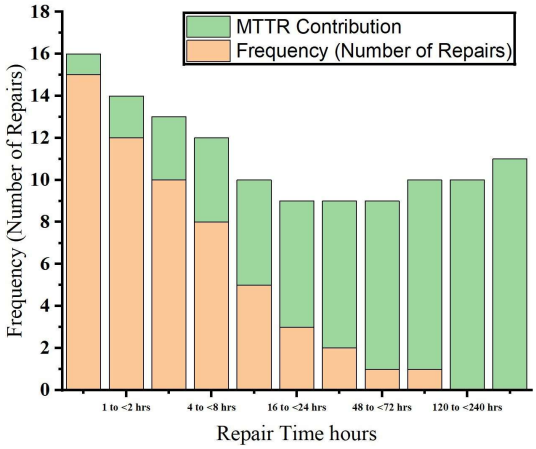


Fig. 3-6 illustrates the distribution of repair times

The mean time to repair (MTTR) for the EDG units is 37 hours after excluding a significant outlier—a single repair lasting nearly 2,000 hours, which is more than twice as long as the next repair. This adjusted MTTR is over 12 hours longer than the previously reported mean time to repair, emergency. Scheduled maintenance downtime, measured by the

ISSN: 3107-6513

mean time to maintenance (MTTM), exhibits a narrow distribution with an average of 1.7 hours. However, scheduled maintenance is often delayed during severe weather events, which are the primary cause of EDG outages.

To assess EDG performance in extended power outages, the brief downtime due to scheduled maintenance (MTTM) can be disregarded, as its impact is minimal compared to repair-related unavailability. Notably, very short outages (<15 minutes) are managed by uninterruptible power supplies and fall outside the scope of this study, which focuses on EDG reliability during prolonged disruptions.

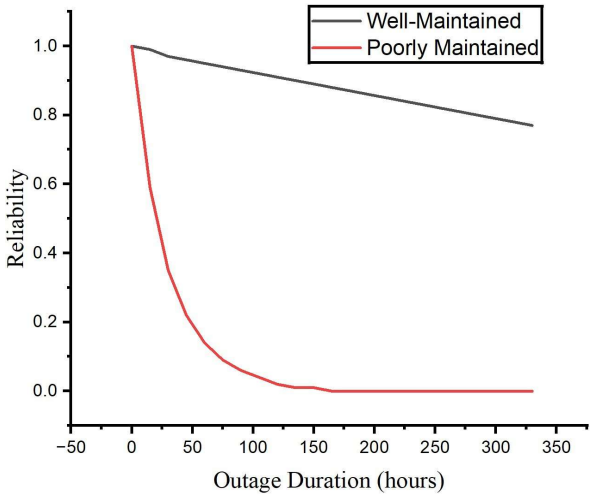


Fig. 3-7. The reliability of an EDG

To evaluate EDG reliability, units are classified as either well-maintained or poorly maintained, and their performance is contarst to that of larger EDGs. Fig. 3-7 shows the anticipated reliability of a single EDG across outage durations spanning from one hour up to two weeks. However, as previously discussed, this approach is flawed—it leads to a significant overestimation of EDG reliability. This common mistake arises from failing to account for critical factors such as prolonged repair times (MTTR), weather- related delays, and the impact of extreme outliers. A more accurate evaluation must integrate these variables to avoid misleading reliability projections.

Using two EDGs for one critical load can significantly enhance reliability, as shown in Fig. 3-8. This model reflects an ideal case, assuming the two units fail independently, resulting in doubled reliability but also doubling the cost. However, this optimistic projection overlooks shared vulnerabilities, such as common switchgear or fuel supply systems, which introduce potential single points of failure. In practice, these interdependencies may offset the theoretical gains from redundancy, underscoring the need for a holistic design that accounts for both parallel EDG operation and shared infrastructure risks.

Fig. 3-8. Reliability Estimates with 90% Confidence Bounds

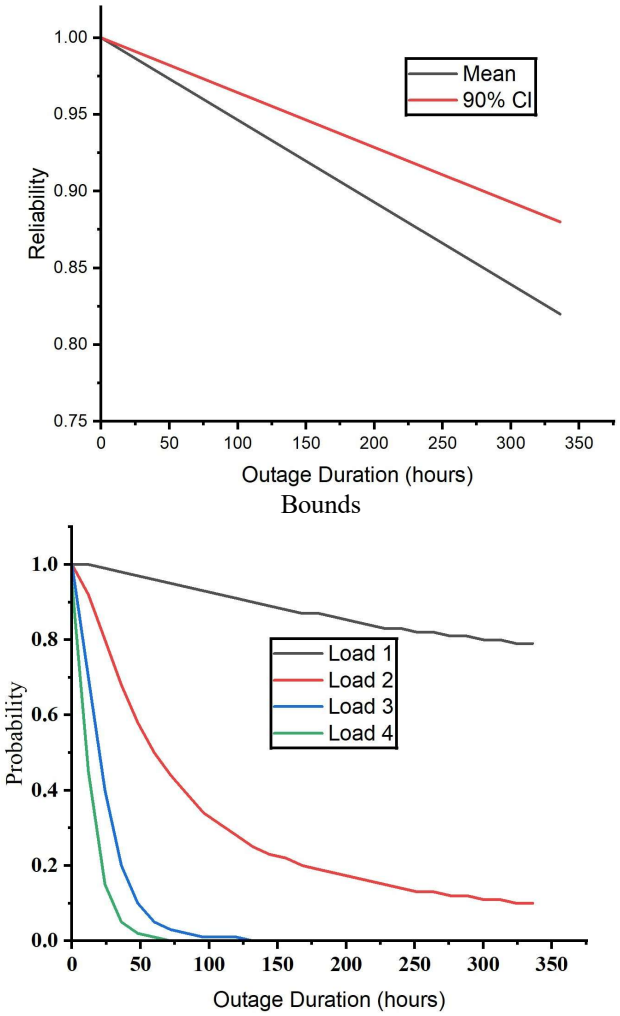


Fig. 3-9 Reliability of critical load supply using single well-maintained edgs

The reliability challenge becomes more complex when considering environments with multiple critical loads. The most common backup power architecture employs a single EDG dedicated to each critical load. Fig. 3-9 shows the probability of simultaneously meeting critical loads across four buildings (Load 1 to Load 4) using well-maintained EDGs. The results show that the likelihood of sustaining all critical loads diminishes significantly within just a few days. This decline stems from the inherent risk of failures accumulating across

 ISSN: 3107-6513

multiple independent generators. Notably, the performance deteriorates further with poorly maintained EDGs, underscoring the critical role of maintenance in multi-load systems.

7. Conclusions

The emergency diesel generator (EDG) system at karachi nuclear power plant unit- 2 (K-2) is a critical safety component designed to maintain power supply during grid outages or reactor emergencies. The system comprises five HiMSEN 20H32/40V engines from hyundai heavy industries, collectively delivering 40 MW of emergency power. These generators automatically initiate under conditions such as low bus voltage or loss of coolant, ensuring uninterrupted operation of reactor cooling, instrumentation, and control systems. With connections to both 500 kV and 132 kV transmission networks, the system architecture reinforces reliability through dual-grid redundancy. The EDG system at K-2 complies with international nuclear safety standards, including IEEE 387 and IAEA guidelines, and incorporates essential subsystems like fuel supply, lubrication, air start, cooling, and automated control. Fault tree analysis (FTA) identifies key failure contributors—namely the Engine, Generator, and Sequencer—along with support systems such as ventilation, instrumentation, and lubrication. Using survival signature methods, the analysis reveals that ancillary system failures, particularly in cooling and lubrication, are the most significant contributors to overall EDG unreliability. Tables presented in the study summarize component-level failure probabilities and survival outcomes to clarify each element's role in system performance.

In terms of operational performance during load, the EDG system's availability is influenced by failure frequency, repair durations, and scheduled maintenance. Mean Time To Repair (MTTR) for EDG units—excluding extreme outliers—averages 37 hours, significantly longer than previously reported emergency repair times (MTTRe). Mean Time To Maintenance (MTTM) is much shorter, averaging just 1.7 hours, but can be delayed during severe weather—one of the main triggers for EDG activation.

Reliability analyses indicate that short-duration outages (<15 minutes) are managed by UPS systems, while EDGs are intended for longer interruptions. Performance modeling shows that reliability decreases notably over multi-day outages, especially with poorly maintained generators. Redundancy (e.g., deploying two EDGs per critical load) can significantly improve reliability, but shared infrastructure like switchgear and fuel lines may limit the benefits. In multi-load environments, such as facilities with four independent critical loads, the probability of maintaining all loads simultaneously declines rapidly, especially under suboptimal maintenance conditions.

8. References

1. I. A. M. Ali, Y. Liu, and J. Huang, "A dynamic reliability model for emergency diesel generators using phase-type distributions and survival signatures," IEEE Trans. Rel., vol. 71, no. 1, pp. 234-247, Mar. 2022.
2. S. G. Kumar, P. K. Samanta, and M. B. S. Kumar, "Integrated fault tree and Bayesian network for reliability assessment of nuclear power plant safety systems: A case study of emergency diesel generator," Nucl. Eng. Technol., vol. 55, no. 3, pp. 1021-1032, Mar. 2023.
3. R. S. H. Y. Zhang, F. A. B. C. Li, and D. Wang, "Survival signature-based reliability analysis for systems with multiple types of components under common cause failures," Reliab. Eng. Syst. Saf., vol. 231, 108956, Jan. 2023.
4. U.S. Nuclear Regulatory Commission, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants: 2022 Update," NUREG/CR-6928, Rev. 2, Washington, DC, USA, 2023.
5. T. J. M. Coolen, F. P. A. Coolen-Maturi, and A. H. A. Alabdrabalnabi, "The survival signature for system reliability: Recent advances and applications," Proc. Inst. Mech. Eng., Part O: J. Risk Reliab., vol. 236, no. 4, pp. 569-580, Aug. 2022.
6. K. P. N. Zio, E. and Patelli, "Advanced Monte Carlo simulation for time-dependent reliability of emergency diesel generators considering maintenance effects," Ann. Nucl. Energy, vol. 176, 109278, Oct. 2022.

ISSN: **3107-6513**

7. M. R. J. Park, S. H. Lee, and G. H. Kim, "A data-driven approach for estimating failure rates of emergency diesel generator components using plant-specific operational data," Nucl. Eng. Des., vol. 398, 111961, Sep. 2022.
8. L. B. C. Wang, Y. Ye, and M. Xie, "Reliability assessment of complex safety-critical systems using survival signature and imprecise probability," IEEE Access, vol. 9, pp. 124580-124592, Sep. 2021.
9. F. A. B. C. Li, D. Wang, and R. S. H. Y. Zhang, "A framework for integrating fault tree analysis and survival signature with application to a nuclear power plant cooling system," Proc. 2021 Int. Conf. Qual., Reliab., Risk, Maintenance, Saf. Eng. (QR2MSE), Chengdu, China, Oct. 2021, pp. 1-8.
10. IEEE Standards Association, IEEE Guide for the Application of IEEE Std 493-2007, IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems (Gold Book), IEEE Std 493.2-2021, 2021.
11. J. D. S. Martorell, S. Carlos, and A. I. Sánchez, "Ageing management and life extension for emergency diesel generators in long-term operation of nuclear power plants," Reliab. Eng. Syst. Saf., vol. 215, 107817, Nov. 2021.
12. H. D. E. R. Smith, P. T. Johnson, and K. L. Brown, "Impact of testing and maintenance strategies on the reliability of standby safety systems: A probabilistic dynamics study," Ann. Nucl. Energy, vol. 163, 108532, Nov. 2021.
13. Y. Liu, I. A. M. Ali, and J. Huang, "Time-dependent reliability analysis of k-out-of-n systems with degrading components using survival signature," IEEE Trans. Rel., vol. 70, no. 2, pp. 779-791, Jun. 2021.
14. P. K. Samanta, S. G. Kumar, and M. B. S. Kumar, "Uncertainty quantification in reliability assessment of emergency diesel generators using evidence theory and fuzzy probability," Nucl. Technol., vol. 207, no. 6, pp. 921-934, Jun. 2021.
15. S. V. R. M. Zio, E. and D. W. Coit, "Optimization of surveillance test intervals for standby safety systems using reinforcement learning," Reliab. Eng. Syst. Saf., vol. 210, 107523, Jun. 2021.
16. A. H. A. Alabdrabalnabi, T. J. M. Coolen, and F. P. A. Coolen-Maturi, "Nonparametric predictive inference for system reliability using the survival signature," Proc. Inst. Mech. Eng., Part O: J. Risk Reliab., vol. 235, no. 2, pp. 332-345, Apr. 2021.
17. N. R. O. Kim, J. H. and S. M. Park, "A hybrid method of GO-FLOW and survival signature for dynamic reliability analysis of emergency power systems in nuclear power plants," Ann. Nucl. Energy, vol. 152, 107991, Feb. 2021.
18. M. B. S. Kumar, P. K. Samanta, and S. G. Kumar, "Common cause failure modeling in emergency diesel generator reliability using alpha-factor model and Bayesian updating," Nucl. Eng. Des., vol. 372, 110955, Jan. 2021.
19. International Atomic Energy Agency, Component Reliability Data for Use in Probabilistic Safety Assessment, IAEA-TECDOC-2021, Vienna, Austria, 2021.
20. D. Wang, F. A. B. C. Li, and R. S. H. Y. Zhang, "Efficient reliability computation for networks and infrastructure systems using survival signature and binary decision diagrams," Reliab. Eng. Syst. Saf., vol. 203, 107086, Nov. 2020.
21. J. Huang, Y. Liu, and I. A. M. Ali, "Reliability analysis of multi-state systems with dependent component degradations based on survival signature," IEEE Trans. Rel., vol. 69, no. 3, pp. 1098-1112, Sep. 2020.
22. E. Zio, M. Compare, and L. F. M. D. A. R. R. A. S. Podofillini, "A benchmarking study on the survival signature for reliability analysis of complex systems," Proc. 30th Eur. Saf. Reliab. Conf. (ESREL 2020), Venice, Italy, Nov. 2020, pp. 2138-2145.
23. G. H. Kim, M. R. J. Park, and S. H. Lee, "Data-driven reliability estimation for emergency diesel generator considering historical demands and performance data," Proc. Int. Top. Meet. Probabilistic Saf. Assess. Anal. (PSA 2019), Charleston, SC, USA, Apr. 2019, pp. 1-8.
24. S. Carlos, J. D. S. Martorell, and A. I. Sánchez, "A review of methods for reliability analysis of standby safety systems considering testing and maintenance," Reliab.

ISSN: **3107-6513**

Eng. Syst. Saf., vol. 189, pp. 177-196, Sep. 2019.
25. R. M. F. M. J. W. Reed, S. and T. J. M. Coolen, "The survival signature for quantifying system reliability: A tutorial and review," Risk Anal., vol. 39, no. 5, pp. 1014-1035, May 2019.