해양 시추설비 안전시스템의 신뢰성, 가용성 및 유지보수성 분석

민준호*, 장광필, 김준홍, 이세중
현대중공업 산업기술연구소 에너지・환경연구실
(jhmin@hhi.co.kr*)

RAM Study on Safety Systems of an Offshore Drilling Platform

Joonho Min*, Kwangpil Chang, Junhong Kim, Sejoong Lee
Hyundai Industrial Research Institute of Hyundai Heavy Industries
(jhmin@hhi.co.kr*)

Introduction

The main purpose of the study is to ensure whether safety systems of an offshore drilling platform maintain their integrity and perform their duty under credible accident scenarios. This assurance can be completed via reliability and availability analysis of the systems, verifying the design outcomes and recommending design and operational changes. It is envisaged that only critical safety systems will be analyzed in this study. The scope is limited to determining the reliability and availability for continuous systems, and only the reliability, often represented probability of failure on demand (PFD), for stand-by systems. Qualitative analysis is to be carried out to identify each failure mode and the sequence of events associated with it for the seven critical safety systems within the scope. Based on the result of qualitative analysis, failure scenarios are logically constructed to comprise of basic events and failure effects through fault tree analysis (FTA). The failure data will be taken from generic references such as the offshore reliability data handbook (OREDA).

Scope of Study

The seven critical safety systems of the offshore drilling platform under construction in the northern Pacific region are listed as following:

- Emergency shutdown (ESD) system,
- Fire detection system,
- Gas detection system,
- Fire fighting system,
- HVAC fire damper system,
- Public address and general alarm (PA/GA) system, and
- Emergency power system.

Failure Modes

A failure mode is defined as the way an item of equipment fails to function as intended. The failure effects describe the loss of required functions that result from failures. The failures considered have been restricted to hardware components and systems, with human reliability information excluded.

Failure modes are divided into the following three main types [1]. The failure rate used in this analysis accounts for critical failure modes, which could immediately cause an abnormal shutdown of the system. Failures classified as degraded or

incipient (non-critical), which may result in off-specification operation but not in immediate shutdown, are not included:

- *Critical Failure*
  A failure that causes sudden cessation of one or more fundamental functions. This failure requires immediate corrective action in order to return the item to a satisfactory condition.
- *Degraded Failure*
  A failure that is gradual, partial or both. Such a failure does not cease the fundamental functions, but compromises one or several functions. The function may be compromised by any combination of reduced, increased or erratic out puts. In time, such a failure may develop into a critical failure.
- *Incipient Failure*
  An imperfection in the state or condition of an item of equipment that a degraded or critical failure can be expected to result if corrective action is not taken.

Safety Instrumented System (SIS)

For any facility where flammable or toxic materials are present, personnel in the vicinity will be exposed to some risks. The complete way to remove them is only to remove the hazardous sources fundamentally. It is impossible, however, not to treat the risky materials in offshore processes/platforms. Such risks may be managed through safety management systems (SMS) including the provision of systems to prevent an accident or to control the accident should it occur. Safety instrumented systems (SIS) are such systems, designed to reduce the likelihood or magnitude of an accident to personnel or the facility itself. The criticality of each SIS in preventing/controlling the hazards is reflected in the performance requirement placed upon each system. The performance requirement is generally defined in the form of a safety integrity level (SIL).

Safety Integrity Level (SIL)

In order to determine the performance requirements of a SIS, a safety integrity level (SIL) is assigned to each SIS (e.g., ESD system and F&G detection system). The SIL states the required system availability (for systems in continuous operation) or the probability to fail on demand (for systems which are only activated once the hazard has occurred). The SIL is split over categories or levels, representing various degrees of stringency, depending on the system criticality in protecting personnel or the facility. Safety integrity levels are defined in four categories with associated performance requirements in the ANSI/ISA, as outlined in Table 1. The SIL requirements of the SIS considered in this study will be based on these categories.

Table 1. SIL Performance Requirements

SIL	Performance Requirements	
	Availability, %	PFD, per demand
1	> 99.99	10^{-5}~10^{-4}
2	99.90~99.99	10^{-4}~10^{-3}
3	99.00~99.90	10^{-3}~10^{-2}
4	90.00~99.00	10^{-2}~10^{-1}

Applied Data

Failure data can be directly derived through statistical analysis of historical operation data. In case of lack of specific data, however, surrogate data are reliably applied to estimation of reliability/availability. The data in this study have been primarily taken from the offshore reliability data handbooks (OREDAs) [1, 2, 3]. If data for mechanical or electrical parts are not available in OREDAs, other references such as NPRD [4] and EPRD [5] are referred. Applied data to the emergency power system, for example, are represented in Table 2.

Table 2. Failure and Repair Rate Data Used for Emergency Power System

Device	Failure rate, $\times 10^6$ hr^{-1}	MTTF, hr	MTTR, hr	Source
Emerg. power generator	1.36E+04	7.36E+01	5.3	OREDA-2002 2.1.1.2
Diesel engine (emerg.)	6.65E+03	1.50E+02	5.5	OREDA-2002 1.4.1.3
UPS system	-	4.42E+04	11.6	Individually calculated
UPS battery charger	9.00E+00	1.11E+05	10.0	OREDA-1992 4.2.4
UPS battery bank	8.50E-01	1.18E+06	18.0	OREDA-1992 4.2.5
UPS circuit breaker	8.40E-01	1.19E+06	6.5	OREDA-1992 4.2.6.2
Inverter	1.20E+01	8.33E+04	12.0	OREDA-1992 4.2.2
Control system	2.18E+01	4.59E+04	2.0	OREDA-1997 4.1.1.3.1
Manual button	1.00E+00	1.00E+06	4.0	NPRD-91

General Assumptions and Considerations

This section summarizes the assumptions and considerations that have been made in the analysis. For all the systems considered, these have been commonly applied to assessment of failure modes and reliability/availability modeling as follows:

- It is assumed that the lifetime of all systems considered is generally 20 years.
- The support systems without information are assumed to be 100% available.
- The availability of utilities, e.g. instrument air and instrument gas, is taken to be 100% since loss of utilities will result in total platform shutdown.
- Sparing identified, e.g. standby/duty equipment, has been taken into account.
- The ESD philosophy and cause & effect diagrams have been used to identify the criticality of the safety systems to the overall system availability.
- Maintenance intervals for lifetime are not taken into account.
- Preventive maintenance, e.g. periodic shutdown, has been not considered since the preventive repair time does not affect the availability actually.
- Corrective maintenance can be conducted immediately upon equipment failure, i.e. the applicable spares and maintenance personnel are always available. The active repair times in references can be regarded as the actual repair times.
- Corrective maintenance is assumed to restore all equipment to an as-good-as new condition.
- Human error, e.g. making a wrong decision, is not considered.

Results and Conclusion

Fault tree analysis (FTA) is a technique widely applied to describing logical relationships between the circumstances, equipment failures, operating conditions, etc. from the viewpoint of failure scenarios. In the study, after qualitative analyses of each system to identify specific failure modes and effects, FTA was carried out to comprise of the failures with the system configurations and operating philosophies. Figure 1 shows fault trees of the emergency power system for a simple case.

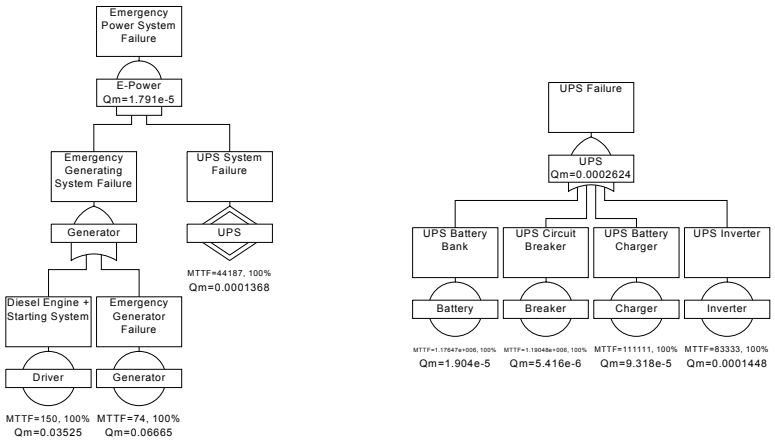

Figure 1. Fault Trees of Emergency Power System

The reliability/availability of the safety systems considered are evaluated using Monte Carlo simulation, based on appropriate and relevant failure rates and maintenance data taken from the generic references. The final results are presented in Table 3. It is considered that the analysis results for the systems assessed are broadly acceptable for general safety requirements of offshore drilling facilities.

Table 3. Overall Results of RAM Study for the Safety Systems

System	Unavailability	Availability	MTTR, hr	MTTF, hr	Failure rate, hr^{-1}
ESD system	7.71E-03	0.9923	5.656	734	1.36E-03
Fire detection system	2.98E-04	0.9997	2.281	7,647	1.31E-04
Gas detection system	2.79E-04	0.9997	1.979	7,108	1.41E-04
Fire fighting system	4.21E-03	0.9958	7.809	1,853	5.40E-04
Fire damper system	3.92E-03	0.9961	3.926	1,001	9.99E-04
PA/GA system	0.00E+00	1.0000	0.000	175,200	5.71E-06
Emergency power system	1.79E-05	0.9998	4.023	224,600	4.45E-06

References

1. DNV and SINTEF, *Offshore Reliability Data Handbook (OREDA)*, 4th Ed., 2002.
2. DNV and SINTEF, *Offshore Reliability Data Handbook (OREDA)*, 3rd Ed., 1997.
3. DNV and SINTEF, *Offshore Reliability Data Handbook (OREDA)*, 2nd Ed., 1992.
4. Reliability Analysis Center, *Non-Electric Parts Reliability Data (NPRD)*, 1991.
5. Reliability Analysis Center, *Electric Parts Reliability Data (EPRD)*, 1991.