ISSN 2395-1621

Design and Analysis of Structural Frame Based on Design Codes for Subsea Applications

[#1]Ajinkya Kulkarni, [#2]RatnakarGhorpade

[1]kulkarni.ajinkya38@gmail.com
[2]ratnakar.ghorpade@mitpune.edu.in

[#12]Mechanical Engineering Department, MIT,
Kothrud, Pune 411038,
Maharashtra, India

ABSTRACT

Subsea Technology in offshore oil and gas production is a highly specialized field of application with particular demands on Engineering and Simulation. Oil and gas fields reside beneath many inland waters and offshore areas around the world. Various components and subsystems are required to be lifted, transported and deployed to seabed for subsea applications. Different structural frames and baskets are used to carry these subsea components as payloads. A structural frame to carry the Flying lead of 1200m length and weighing 2500kg is designed, and analyzed to evaluate the efficiency ratio according to DNV 2.7-3 and Eurocode 3 using FEA. In different phases, the effect of environmental loads, accidental loads and permanent loads is studied. Different load cases according to DNV 2.7-3 - Normal Lifting, Sea Transport, Impact, Drop and Retrieval are performed and the member verification is carried out. The structural integrity of different connections or joints within the structure is checked. Finally, the Optimization is carried out to minimize the efficiency ratio and to reduce the weight. The structure was analyzed in Autodesk RSA and calculations were performed in PTC Mathcad. For different load cases the efficiency ratio of the structure was in between 0.220 to 0.904 but the efficiency ratio for drop case was beyond limit i.e. 1.045 before optimization and 0.809 after optimization.

ARTICLE INFO

Article History

Received :18th November 2015

Received in revised form :

19th November 2015

Accepted : 21st November , 2015

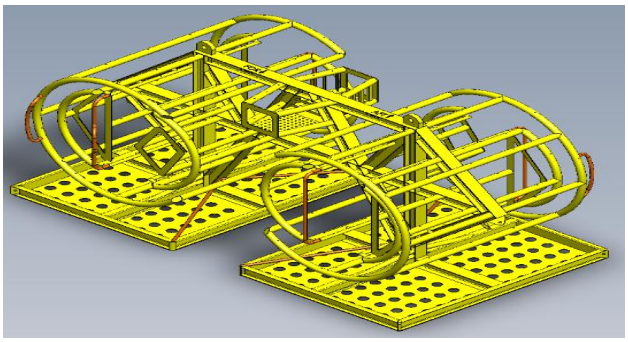
Published online :

22nd November 2015

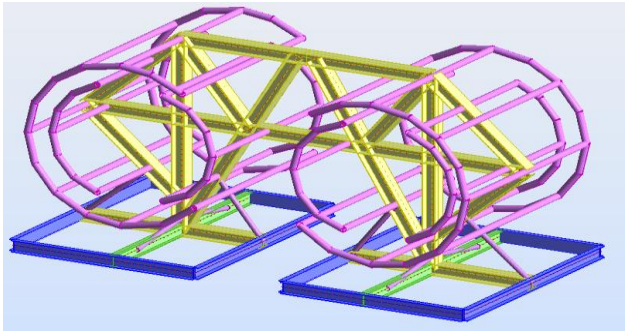
Keywords- **Subsea, FLDF, Lifting analysis, Sling cables, Joints, PO unit, Retrieval**

I. INTRODUCTION

Subsea is a term to refer to equipment, technology and methods employed in offshore oil and gas development industries. Oil and gas fields reside beneath many inland waters and offshore areas around the world.Different equipmentare to be deployed to the sea bed for this purpose and structures (frames or baskets) are needed to carry those equipment. For a structure to be used for subsea applications, its lifting analysis is important before sea-going. Structure has to go through stages like Lifting, Transportation and Deployment. Lifting analysis involves the study of effects of environmental loads, accidental loads and permanent loads in all these stages. DNV (Det Norske Veritas) establishes the rules and guidelines regarding classification, quality assurance and certification of sea going structures.DNV 2.7-3 addresses all types of Portable Offshore (PO) units.The acceptance criteria according to DNV 2.7-3 is the stress in any member of unit should not increase the 0.85 times the yield stress value. It is also the intention that PO unit certified according to DNV 2.7-3 will meet all relevant requirements in DNV rules for planning and execution of marine operations.In the Past, Authors have analyzed structures such as skids using DNV 2.7-1 regulations. Authors did the analysis for normal lifting case and impact load case. [7]This paper presents design and analysis of FLDF (Flying Lead Deployment Frame) as per DNV regulations. Various lifting analysis operations such as Normal Lifting, Sea Transport, Impact, Drop and Retrieval have been formulated with the help of FEA (Finite Element Analysis) using Autodesk RSA (referred to as Robot). Robot is an integrated graphic program for modeling, analyzing and designing various types of structures.



(a)



(b)

Fig. 1 FLDF Model (a) CAD Model in SOLIDWORKS (b) FE Model in Autodesk RSA

I. FLDF

Flying Leads are used to link subsea trees to main umbilical termination arrangements, manifolds and subsea distribution units. These are frequently deployed by ROVs. The FLDF is designed to provide an easy method of deploying flying leads to the sea floor. It overcomes the problem of leaving flying leads lying on the sea floor during equipment deployment.Here, The Flying lead with 1200 m length and 50mm diameter is to be deployed to the sea bed. The geometric limitations of the frame were, height should not be above 4m and width should not be above 4m. The ultimate bending radius of pipe is 1.5m. And weight of the frame should not increase above 20T. The material used for frame is S355 steel.The CAD model drawn using SOLIDWORKS and FE model drawn in Autodesk RSA are shown in fig. 1. The FE model of FLDF is simplified by removing all secondary structure members. Primary structure includes all members that participate in global structural strength of the PO unit, padeyes, lashing points, panels, while secondary structure includes parts which are not essentially load carrying.

II. OPERATIONAL CLASS DECISION

A “PO Unit” (Portable Offshore Unit) is a package or unit intended for repeated or single offshore transportation and installation or lifting. PO Units typically carry equipment (or any kind of installation) intended for a service function offshore. The equipment could be an integrated part of the PO unit or detachable.DNV 2.7-3 groups the PO unit into five types, namely type A, B, C, D and E. FLDF is a type A PO unit as it is a PO unit with primary structure frame. It includes skids arranged with crash frame. It shares many characteristics with offshore containers.PO Units shall be assigned to an operational class for the offshore lift. The class should be selected based on the basis of weight/mass, risk evaluation and type of structure. [1]Risk level should normally be defined as “High” if at least one of the risk elements listed in Table I is fully applicable or at least two are partially applicable; otherwise risk level should be ”Low” Here, two elements are clearly applicable and one element is partially applicable, thus the Risk level should be HIGH. Type of PO unit is type A and Weight of PO unit is below 25T, thus the class of frame is R 45.

TABLE I
RISK EVALUATION

Risk Element		Not Applicable	Clearly Applicable	Partially Applicable
A	Installed Equipment specially sensitive to impact loads	√		
B	Crane hook could catch in protruding parts	√		
C	Protruding parts may stuck on transported items or transport vessel	√		
D	Lack of Roof Protection, Crane hook may accidently hook onto items inside PO units		√	
E	Lift Points in positions where they could be damaged by the impacts	√		
F	Lack of proper crash framing		√	
G	PO units of exceptional geometry or unhandy (big) size			√
H	Sling sets include loose spreader bars	√		
I	Other (Describe)	√		
Clearly applicable risk elements : 2 Partially applicable risk elements : 1 **RISK LEVEL : HIGH**				

I. MASS ESTIMATION

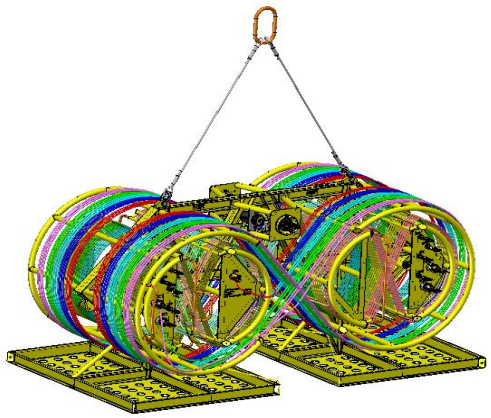


Fig. 2 Equally Distributed Payloads on FLDF

Maximum Gross Weight (MGW) is the maximum mass of the PO unit including payload. MGW is the sum of Tare Weight and the Payload. Where, Payload is the mass of the equipment carried by the PO unit and Tare Weight is the mass of an empty unit and equals to the combined mass of primary and secondary structure. For FLDF the Tare Weight of the original model is 10.5T and Payload is 2.5T. Out of these 2.5T, Outer drums carry 1400kg; Inner drums carry 1100kg weight. Thus MGW becomes 13T.After completing the FE model, its mass is measured and compared with the original design. The weight of the FE model is 5.57T and the Tare weight of original frame is 10.5T. This difference is because of removing secondary structure. The Tare weight value is matched by scaling the density of the material. The force density of the material S355 is increased from 75,550N/m^3 to 142,413N/m^3. Mass estimate based on CAD model may differ from the mass of an actual real structure, so mass contingencies should be included to account for inaccuracies and uncertainties in the mass estimates. Here, 10% contingency (CF=1.1) is used for mass estimation. [1]

TABLE II
MASS ESTIMATES AND CONTINGENCY

	Basis	**Original Mass (T)**	**CF**	**Mass used in calculations (T)**
Tare Weight	Solid Works	10.5	1.1	11.55
Outer Drum Payload	Input	1.4		1.54
Inner Drum Payload		1.1		1.21
MGW		13.0		14.3

III. LIFTING ANALYSIS

According to DNV 2.7-3, three different methods are available for design analysis. Those are Eurocode, Elastic FEA and Limit FEA method. In this paper, Eurocode analysis method is used. Design calculations are performed according to Eurocode 3 (EN-1993-1-1) for steel structures. DNV says, The vonMises stress produced due to the design loads shall not exceed 0.85 times the yield stress, i.e. The Partial safety factor value γ_{M0} = 1.18 or 1/0.85 shall be used for Eurocode calculations purpose. [2]

A. Normal Lifting

The Design loading on all elements in a lift with lifting slings are calculated based on F (in kN). For all PO units, F is given by,

*F = Max {DF*MGW*g, 2.5*MGW*g}*

Where, DF is design factor. For R45 operational class and MGW less than 50T, the value of the Design factor is-calculated based on [5], based on geometry to weight relation and wave conditions. Details of this calculation are not in the scope of this paper.

DF = 4.91

Thus, the new mass estimates are tabulated in Table III.

TABLE III
MASS ESTIMATES FOR LIFTING CASE

	Mass value after contingency (T)	**DF**	**Mass used in calculations for Normal Lifting (T)**
Tare Weight	11.55	4.91	56.71
Outer Drum Payload	1.54		7.56
Inner Drum Payload	1.21		5.94
MGW	14.3		70.213

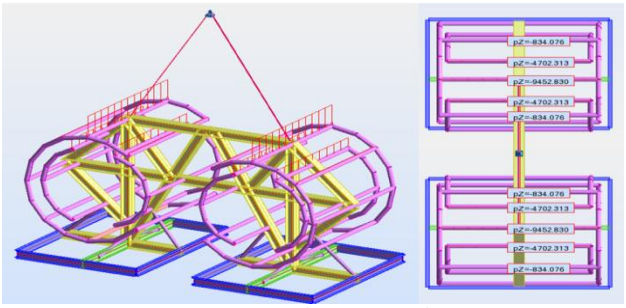


Fig. 3 FE Modelling for Normal Lifting case

For Normal Lifting case, the sling angle with the vertical is 30˚, length of the cable is 4m, diameter of the cable section is 18mm and material used is steel. Sling strength and selection is not the scope of this work. The master link is pinned.

After calculations, the maximum vonMises stress is obtained at upper bar of the outer drum and it is 345MPa.

B. Impact Loading

Impact loads may occur during lift off or set down of PO Units and they are a result of the relative velocitiesbetween transport vessel deck and the hanging load. Impacts loads occur randomly and are of very shortduration. Due to the inherent uncertainties in the input parameters it is not considered feasible to calculate these loads accurately.For R45 operational class, [1]

$F_{HI} = 0.08*2.5*MGW*g = 28.05kN$

$FVI = 0.08*F = 55.084kN$

To study the Impact loads, the cables are removed and fixed support is applied at the position of padeyes. The vertical impact force is applied at the middle of the horizontal bar at the bottom and horizontal impact force is applied at the outermost bar of the outer drum.

For vertical impact, the global maximum von Mises stress is obtained at upper bar of the outer drum. It is 70.5MPa.

And local maximum von Misesstress value in a bar carrying impact load is 11.6MPa. For Horizontal impact, the maximum vonMises stress is in the bar carrying impact load. It is 153.5MPa.

C. Sea Transport

If the PO unit is transported by sea, it should be designed for this purpose. The securing arrangement could include lashing ropes, stops welded to the deck to prevent sliding of the PO unit. The stability of all PO Units shall be checked for loads due to the maximum accelerations and wind pressure that could occur duringsea transport. The vertical and horizontal accelerations for the sea transportation are taken from DNV 2.7-3. For sea transport purpose, eight lashing ropes are used. Four long cables are of length 4m and four short cables are of length 0.7 m. Long cables make 30˚ angle with platforms and short cables make 10˚ angle with platform.

Horizontal Component = A_H = g =9.81

*Max Vertical component=AV_{max} = 1.3*g = 12.753m/s^2*

*Min Vertical component = AV_{min} = 0.7*g = 6.867m/s^2*

Wind load is calculated by considering the wind pressure P_{wind} = 1.0kN/m^2 acting in the same direction as in the horizontal acceleration. An equivalent horizontal acceleration for wind load is given by, [1]

$A_{wind} = (P_{wind} * A_{proj})/MGW$

Here, A_{proj} value is calculated as in the fig 6. Projected area for FLDF is 29.15m^2 and wind load acceleration is A_{wind} = 2.038m/s^2.

The maximum vonMises stress is obtained in the vertical bars. It is 315.09MPa.

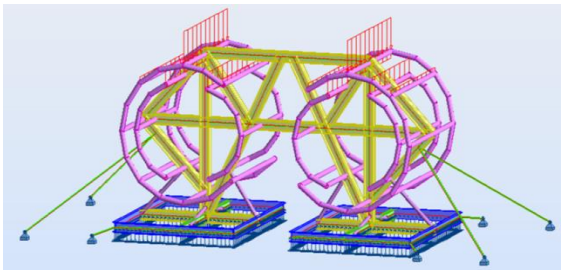
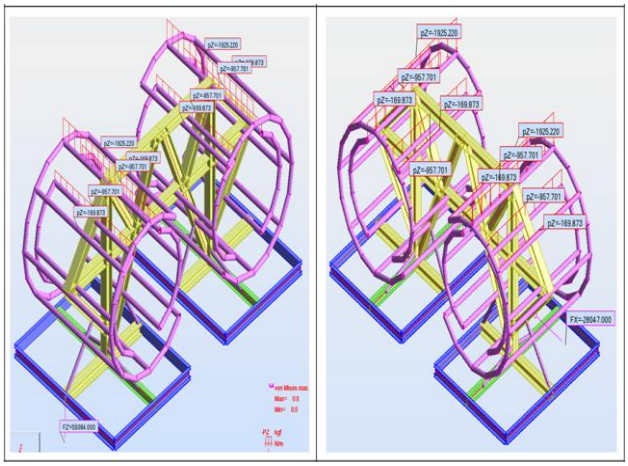


Fig. 4 FE Modelling for Sea Transport case



(a) (b)

Fig 5 FE Modelling (a) Vertical Impact Test (b) Horizontal Impact Test

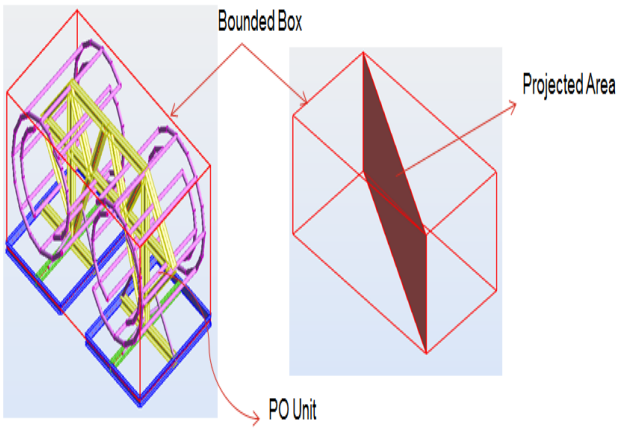


Fig 6. Projected area for the calculation of wind load

D. Drop Case

In a general case, drop event can be divided into four phases as shown in fig. 8: Free Fall i.e. the PO unit falls freely and gains speed and kinetic energy, Rigid Body Rotation i.e. if the initial impact is only on the one corner, the PO unit will start rotating as a rigid body, Deceleration i.e. once the PO unit touches the ground with at least three points, the kinetic energy will be converted into internal energy (strain energy) in a structure and Rebound i.e. after all the kinetic energy is taken by the structure, the structure will start to oscillate around the static deflections.

Acceptance criteria for the structure should be evaluated when the loads on the structure are highest i.e. at the end of the deceleration phase and the beginning of the rebound. The design factor for drop case is 4.5. [6]

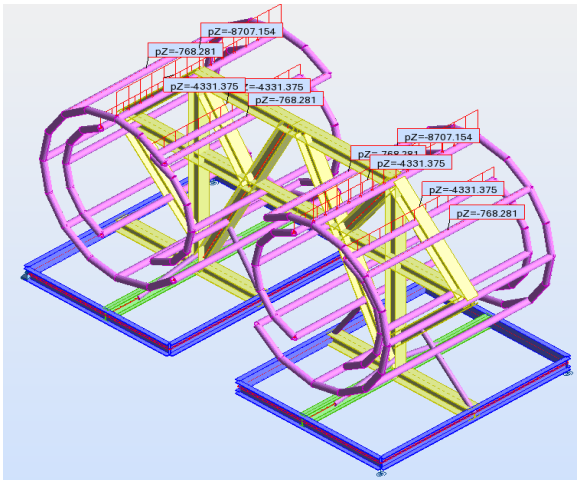
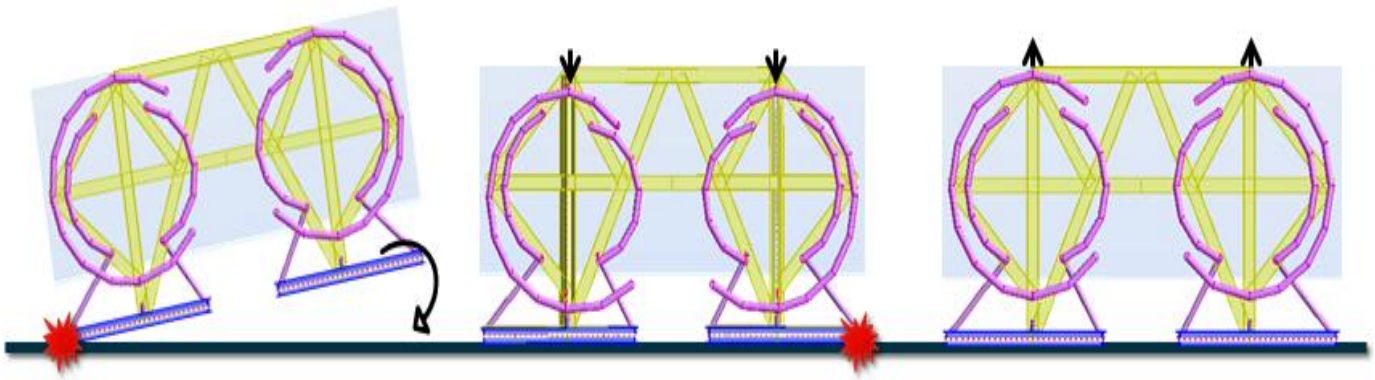


Fig. 7 FE Modelling for Drop case



(a) (b) (c)

Fig. 8 Different phases in drop event (a) Rigid body rotation (b) Deceleration (c) Rebound

E. Retrieval Load Case

Retrieval load is a force required to pull out a PO unit from a soil or seabed. For retrieval load case, the retrieval load in the direction of cables local x axis is 412701.519N and cables are removed. The support condition is a foundation support with kz = 9979.969N/m. [4]

The maximum vonMises stress is in a bar at bottom and it is 221MPa.

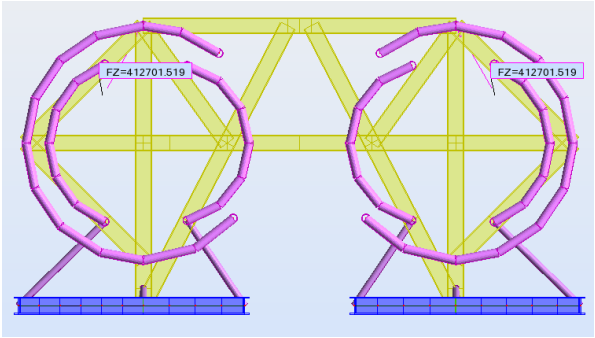


Fig. 9 FE Modelling for Retrieval case

I. STEEL DESIGN

Autodesk RSA is code based software. It is possible to do steel design using different National codes. In this paper, Eurocode (Steel code EC3 EN 1993-1-1) is used for steel design purpose.

Eurocode first classifies members according to their cross sections. The role of cross section classification is to identify the extent to which the rotation capacity is limited by its local buckling resistance.

In the fig. 11 the cross sections classification is given with the help of moment vs rotation capacity graph. Class 1 is plastic cross section, class 2 is compact, class 3 is semi compact and class 4 is slender cross section. Class 1 and 2 are least susceptible to local buckling while class 3 and 4 are most susceptible to local buckling. In class 1 and 2 plastic moment resistance can be developed while in class 3 and 4 the failure is due to local buckling. [2]

During steel design calculations, plastic section modulus is used for class 1 and 2while elastic section modulus is used for class 3 and 4. The classification of cross section depends on width to thickness ratio of the parts subject to compression and material yield strength.

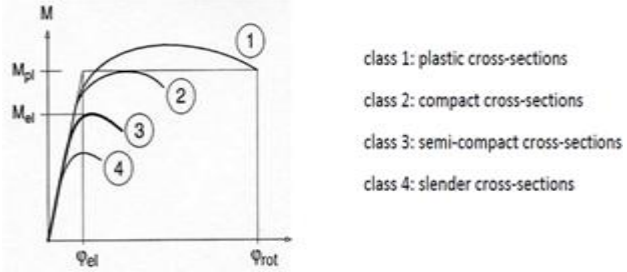


Fig. 11 Moment Rotation curve depending on cross section classes 1 to 4

After classification of cross section, resistance of cross section isfound out and efficiency ratio of members is calculated. The efficiency ratio should be below 1. Eurocode does not calculate vonMises stress.It calculates the efficiency ratio for tension, compression, bending, shear, and torsion, whichever loads are present, independently. If more than one type of loads is present then it will calculate design resistance considering effect of all the loads. And then calculate the efficiency ratio for that combination. Out of all these efficiency ratios, whichever value is maximum that would be the efficiency ratio of that particular member. [2]

II. OPTIMIZATION

Optimization is used here to obtain minimum weight while keeping the efficiency ratio below unity. From the table IV, it is seen that the structure is not safe for drop case. The intention of optimization is to bring the efficiency ratio below 1 and also to reduce the weight of the structure.

For Optimization purpose, first the efficiency ratio of all the members in different cases according to Eurocode is found out. And the members having less efficiency ratio in all the cases are listed separately in table V; these members will not contribute in load carrying and can be removed. When efficiency ratio of different members in all cases are compared, bar 8 and bar 40 are having least efficiency ratio in all cases and these members can be removed.After removing the members, once again the efficiency ratios are calculated.

TABLE IV
EFFICIENCY RATIO FOR DIFFERENT STAGES IN LIFTING ANALYSIS

Sr. No.	Stage	S, Mises		Eurocode		Run Time (Sec)
		Stress (MPa)	Efficiency ratio	Class of section	Efficiency ratio	
1	Normal Lifting	345	1.15	1	0.672	42
2	Sea Transport	315	1.051	1	0.886	71
3	Horizontal Impact	153.5	0.511	1	0.287	36
4	Vertical Impact	70.5	0.235	3	0.220	34
5	Drop	375	1.247	1	1.045	39
6	Retrieval	221	0.735	1	0.904	97

TABLE V
MEMBERS HAVING LEAST EFFICIENCY RATIO IN ALL CASES

Bar No.	Normal Lifting	Sea Transport	Vertical Impact	Horizontal Impact	Drop	Retrieval
8	0.043	0.007	0.026	0.05	0.076	0.04
40	0.043	0.007	0.021	0.055	0.076	0.04

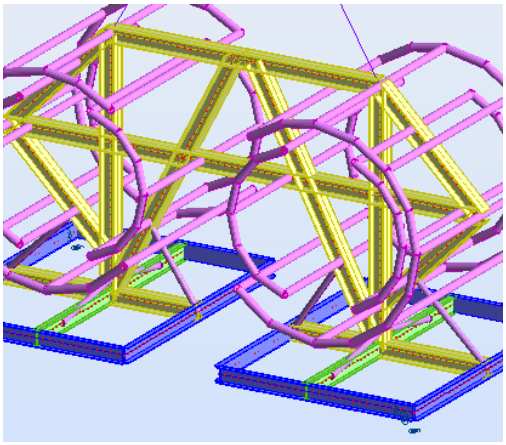


Fig. 12 Structure after optimization

TABLE VI
EFFICIENCY RATIO BEFORE AND AFTER OPTIMIZATION

Load Case	Before Optimization	After Optimization
Normal Lifting	0.672	0.671
Sea Transport	0.886	0.853
Horizontal Impact	0.287	0.287
Vertical Impact	0.220	0.232
Drop	1.045	1.029
Retrieval	0.904	0.929

From Table VI, it is seen that for drop case, still the efficiency ratio is above one. To bring it below 1, code group design operation is performed using Autodesk Robot.

First the members having efficiency ratio above 1 are listed. From analysis of drop case, it is seen that C section bars at the bottom are having maximum efficiency ratio. Thus all the bars having C section are grouped together.All the channel sections in the Eurocode database i.e. UAP, UPE, UPN and UPAF are selected and asked for calculation of efficiency ratio of the group members for each of the sections selected.

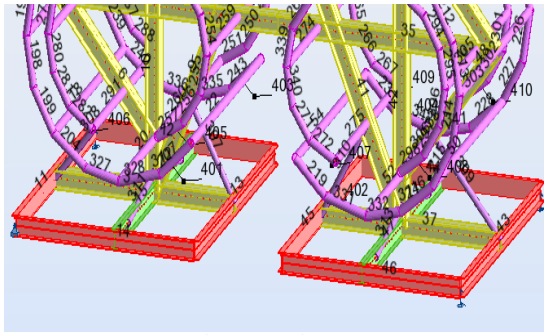


Fig. 13 Group of members for code group design

After optimization, UAP 250 is finalized to substitute the current C section members. As it reduces the efficiency ratio to 0.797 and weight of the structure is increased by 2.31%. But, 10% contingency for mass is already provided.

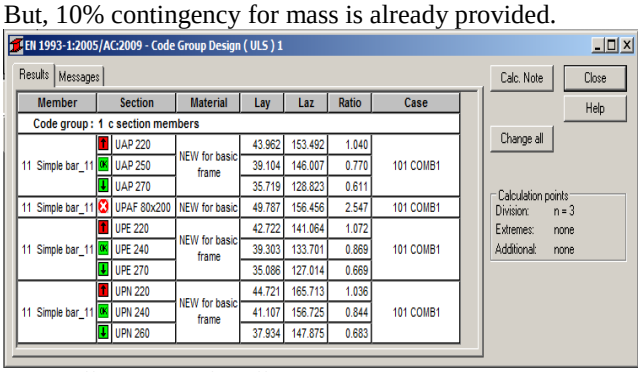


Fig. 14Efficiency ratio for different cross sections under code group design

IV.

FLDF is an R45 class structure, with MGW = 13T. The efficiency ratio is calculated according to Eurocode using Autodesk RSA tool. Initially the efficiency ratio for drop case is above 1. Thus, optimization process is performed and efficiency ratio for drop case brings to 0.801

The results are summarized in table VII.

TABLE VII
S, MISES AND RUN TIME AFTER OPTIMIZATION AND EFFICIENCY RATIOS BEFORE AND AFTER OPTIMIZATION

Sr. No.	Load Case	S, Mises		Eurocode		Run Time (Sec)
		Stress	Efficiency ratio	Efficiency ratio before optimization	Efficiency ratio after optimization	
1	Normal Lifting	344.65	1.14	0.672	0.671	42
2	Sea Transport	301.45	1	0.886	0.887	67
3	Horizontal Impact	152.63	0.5	0.287	0.287	32
4	Vertical Impact	70.065	0.23	0.220	0.229	33
5	Drop Case	284.64	0.95	1.045	0.801	34
6	Retrieval	210	0.7	0.904	0.896	65

V. CONCLUSION

The structural frame FLDF is designed and analyzed for subsea applications, by Lifting analysis process according to DNV 2.7-3. The efficiency ratio according to code (Eurocode EN 1993) and according to S, Mises values are different. According to Eurocode, design is safe for subsea applications.

ACKNOWLEDGEMENT

The Authors are grateful to thank Mr. Satyajit Lonkar and Mr. Amey Bhide from Aker Solutions for their invaluable help in this thesis process. We would also like to thank Prof. Dr.S. T. Chavan, M.E. Designcoordinator from MIT Pune. Thanks are also due to WOS team of Aker Solutions and Mechanical Engineering Dept., MIT, Pune.

REFERENCES

[1] DNV 2.7-3 Standard for certification Portable offshore Unit, May 2011
[2] Eurocode 3 BS 1993-1-1_2005 Design of steel structures - General rules and rules for buildings
[3] Eurocode 3 BS EN 1993 -1-8_2005 Design of steel structures – Design of joints
[4] API RP 2GEO Geotechnical and foundation design considerations, First Edition, April 2011
[5] DNV RP H103 Modelling and Analysis of Marine Operations, April 2011
[6] Eurocode 1991-1-7 Actions on structures - Accidental Actions

Web delivered services and applications have increased in both popularity and complexity over the past few years. Daily tasks, such as banking, travel, and social networking, are all done via the web. Such services typically employ a web server front end that runs the application user interface logic, as well as a back-end server that consists of a database or file server. Due to their ubiquitous use for personal and/or corporate data, web services have always been the target of attacks. These attacks have recently become more diverse, as attention has shifted from attacking the front end to exploiting vulnerabilities of the web applications in order to corrupt the back-end database system (e.g., SQL injection attacks).

A plethora of Intrusion Detection Systems (IDSs) currently examine network packets individually within both the web server and the database system. However, there is very little work being performed on multitier Anomaly Detection (AD) systems that generate models of network behavior for both web and database network interactions. In such multitier architectures, the back-end database server is often protected behind a firewall while the web servers are remotely accessible over the Internet. Unfortunately, though they are protected from direct remote attacks, the back-end systems are susceptible to attacks that use web requests as a means to exploit the back end.

To protect multitier web services, Intrusion detection systems have been widely used to detect known attacks by matching misused traffic patterns or signatures. A class of IDS that leverages machine learning can also detect unknown attacks by identifying abnormal net-work traffic that deviates from the so-called "normal" behavior previously profiled during the IDS training phase. Individually, the web IDS and the database IDS can detect abnormal network traffic sent to either of them. However, we found that these IDSs cannot detect cases wherein normal traffic is used to attack the web server and the database server.

For example, if an attacker with non admin privileges can log in to a web server using normal-user access credentials, he/she can find a way to issue a privileged database query by exploiting vulnerabilities in the web server. Neither the web IDS nor the database IDS would detect this type of attack since the web IDS would merely see typical user login traffic and the database IDS would see only the normal traffic of a privileged user. This type of attack can be readily detected if the database IDS can identify that a privileged request from the web server is not associated with user-privileged access. Unfortunately, within the current multithreaded web server architecture, it is not feasible to detect or profile such causal mapping between web server traffic and DB server traffic since traffic cannot be clearly attributed to user sessions.

We present Double Guard, a system used to detect attacks in multitier web services. Our approach can create normality models of isolated user sessions that include both the web front-end (HTTP) and back-end (File or SQL) network transactions. To achieve this, we employ a light-weight virtualization technique to assign each user's web session to dedicated container, an isolated virtual computing environment. We use the container ID to accurately associate the web request with the subsequent DB queries. Thus, Double Guard can build a causal mapping profile by taking both the web server and DB traffic into account.

II. RELATED WORK

Double guard and its classification:-

Double Guard is a system used to detect attacks in multitier web services [1] [2].A network Intrusion Detection System can be classified into two types: anomaly detection and misuse detection. Anomaly detection first requires the IDS to define
and characterize the correct and acceptable static form and dynamic behaviour of the system, which can then be used to detect abnormal changes or anomalous behaviours. The boundary between acceptable and anomalous forms of stored code and data is precisely definable. Behaviour models are built by performing a statistical analysis on historical data or by using rule-based approaches to specify behaviour patterns. An anomaly detector then compares actual usage patterns against established models to identify abnormal events [1] [2] [3].

Methodology:-

This approach can create normality models of isolated user sessions that include both the web front-end (HTTP) and back-end (File or SQL) network transactions [1] [3]. It employs a light-weight virtualization technique [1] [3] to assign each users web session to a dedicated container, an isolated virtual computing environment. It uses the container ID to accurately associate the web request with the subsequent
DB queries. Double Guard forms container-based IDS with multiple input streams to produce alerts. The correlation of input streams provides a better characterization of the system for anomaly detection because the intrusion sensor has a more precise normality model that detects a wider range of threats[1] [2] [3] [4].

Possible Attacks:-

Some of the important attacks are generally used by attackers for hacking i.e. SQL injection, Direct DB Attack ,Hijack future session attack, Privilege escalation[1] [2] [3] [5]and D-DOS attack [1].

Algorithm Used:-

In order to detect such attacks algorithms which are being used are Static model building algorithm [1] [2] [3] [4].

Limitations:-

Vulnerabilities Due to Improper Input Processing :-

Once the malicious user inputs are normalized, Double Guard cannot detect attacks hidden in the values [1].

Possibility Of Evading Double Guard :-

It is possible for an attacker to discover the mapping patterns by doing code analysis or reverse engineering, and

issue expected web requests prior to performing malicious database queries [1].

Distributed DOS attacks:-

Previous Double Guard system was not designed to mitigate D-DOS attacks. These attacks can also occur in the server architecture without the back-end database. Denial-of-service attacks are common and fashionable these days. In denial-of service attack, attacker tries to prevent legitimate users from using a service or shutting down a service owing to some implementation vulnerability crashing the machine [1].

III.DOUBLE GUARD SYSTEM ARCHITECTURE

System architecture:-

This is the system architecture design. In this, first the client sends a request for price and other information related to a particular product then that request is analyzed in order to identify if the request is HTTP request or a query and this is done using static model building algorithm.

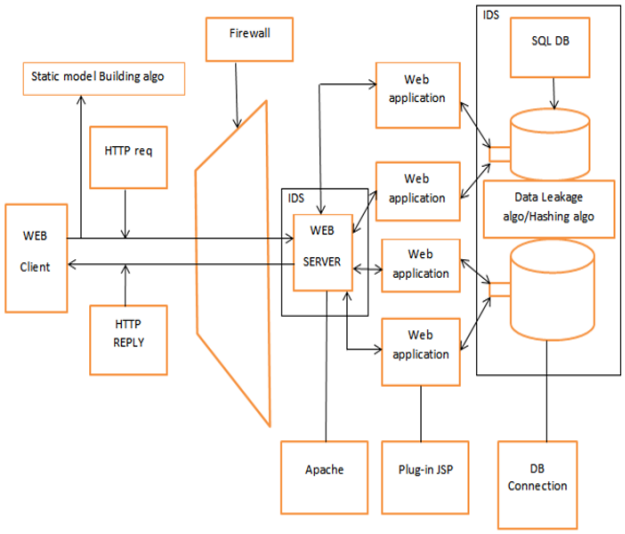


Figure 3.1: System Architecture diagram

After the request is categorized if the request is HTTP request then that request is passed through firewall and web server receives that request and that request is send as a query to database server and response is sent accordingly but the request is handled only after user authentication is satisfied .If the values in database is changed then data leakage occurs and that's when data leakage algorithm works and saves the
records of unauthorized user and sends it to admin. If a particular authorized user requests for hacked data then previous data is provided to that user and this is done using hashing algorithm.

Attacks scenario:-

1. ***SQL-Injection Attacks:-***

Attacks such as SQL injection do not require compromising the web server. Attackers can use existing vulnerabilities in the web server logic to inject the data or string content that contains the exploits and then use the web server to relay these exploits to attack the back-end database [fig 2]. Since our approach provides a two-tier detection, even if the exploits are accepted by the web server, the relayed contents to the DB server would not be able to take on the expected structure for the given web server request.

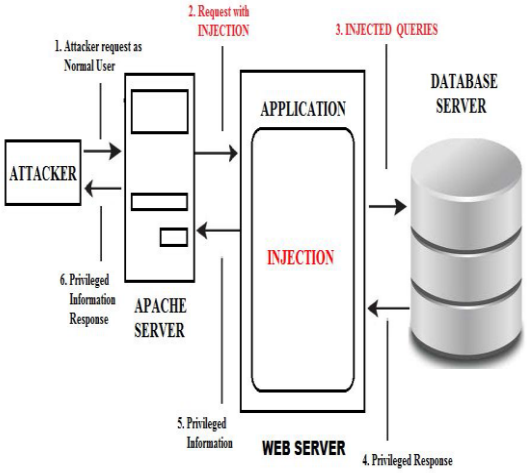


Fig 3.2 SQL- injection attack [5]

Attacks such as SQL injection do not require compromising the web server. Attackers can use existing vulnerabilities in the web server logic to inject the data or string content that contains the exploits and then use the web server to relay these exploits to attack the back-end database. Since our approach provides two-tier detection, even if the exploits are accepted by the web server, the relayed contents to the DB server would not be able to take on the expected structure for the given web server request. For instance, since the SQL injection attack changes the structure of the SQL queries even if the injected data were to go through the web server side, it would generate SQL queries in a different structure that could be detected as a deviation from the SQL query structure that would normally follow such a web request.

2. ***D-Dos Attacks:-***

Double Guard is not designed to mitigate D-DoS attacks [fig 3]. These attacks can also occur in the server architecture without the backend database. In computing, a denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the internet. A distributed denial-of-service (D-DoS) is where the attack source is more than one–and often thousands–of unique IP addresses. Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web server such as banks, credit card payment gateways; but motives of revenge, blackmail or activism can be behind other attacks. A distributed denial-of-service (D-DoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted

system, usually one or more web servers. Such an attack is often the result of multiple compromised systems flooding the targeted system with traffic.

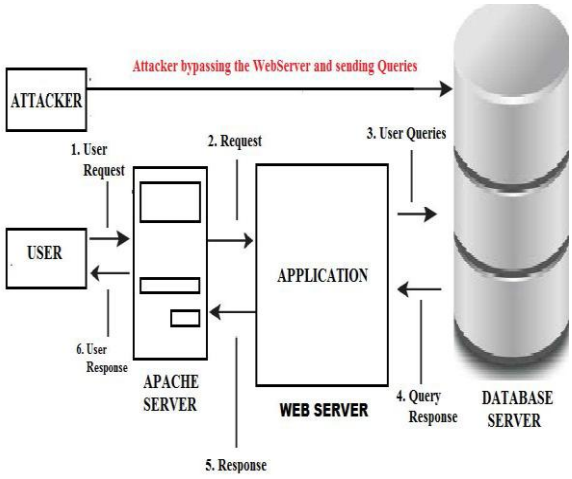


Fig 3.3 D-DoS attack

When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This after all will end up completely crashing a website for periods of time. Malware can carry D-DoS attack mechanisms; one of the better-known examples of this was My Doom. Its DoS mechanism was triggered on a specific date and time. This type of D-DoS involved hard coding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.

IV.ALGORITHM

Static Model Building Algorithm (I):-

Ensure: The Mapping Model for static website

Input: Set AQ for database query. Set AR for server request.

Step 1: Identify the input type of HTTP request whether it is a query or a request.

Step 2: for each different request do, if r is a request to static file.

Step 3: Store the input in hash table as per their type AQ for query and for request AR.

Step 4: The key for hash table entry will be set as the input itself.

Step 5: Forward AQ and AR to virtual server to validate.

Step 6: If attack identified then virtual system automatically terminate the HTTP request.

Step 7: Else HTTP request is forwarded to the original server.

Step 8: Display information.

Step 9: Exit.

Data leakage algorithm (II):-

Input: Input data D = D1, D2, D3,.., Dn saves into the hash table.
Step 1: Arrange all input data into matrix format (save into log files).
Step 2: Consider m as a selected data act as a new selected data.
Step 3: m position gets changed after allocated time period.
Step 4: If Ms data get hacked.
Step 5: Data leakage is occurs.
Step 6: We have to check the leakage data and prevent
Step 7: Using Revert back function we have to get original data.
Step 8: When user calls that corrupted file, hash function gives to user a previous data.
Step 9: Return True.

MD5 Hashing algorithm (III):-

MD5 which stands for Message Digest algorithm 5 is a widely used cryptographic hash function The idea behind this algorithm is to take up a random data (text or binary) as an input and generate a fixed size hash value as the output The input data can be of any size or length, but the output hash value size is always fixed

Step 1: Start

Step 2: For each candidate set element.

Step 3: For PV (i) and CV (i) compare attributes and detect which fields are corrupted.

Step 4: get who and when of corruption event.

Step 5: Prepare a report.

Step 6: Stop

V.FUTURE SCOPE

The basic idea is provide two tier security to for web applications. The aim is to secure the web server from the

attacker client and to secure the data from the internal authorized persons in the data care centres. This security model can be further extended to provide security against other attacks.

VII.CONCLUSION

This paper States the design level approach taken by team for the project. In this document, a fair amount of elaboration has been done on the project scenario pointing out the most of the important detail. The goal for the final product has become
apparent as the scenario and the desired user interface is visually explained. Additionally, this report defines proposed system architecture and is discussed with attacks scenario. Further information on the technical design is given and progress is summarized. In this the system architecture is designed for detecting intrusions like SQL injection and D-Dos attacks.

REFERENCE

[1].Mixing Le, Angelos Stavros, Member, IEEE, and Brent ByungHoon Kang, Member, IEEE, IEEE Transactions on dependable and secure computing, Double Guard: Detecting Intrusions in Multitier Web Applications, VOL. 9,NO. 4, March, 2014.

[2]. Mr. Chaudhari Hitesh Kumar, Prof. Ajay V. Nadargi, Mr. Bodade Narendra, Mr. Shinde Sushil , Double Guard: Detecting Intrusions in Multi-tier Web applications, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 2, February 2015.

[3].K.Karthika, K.Sripriyadevi, To Detect Intrusions in Multitier Web Applications by using Double Guard Approach., International Journal of Scientific and Engineering Research Volume 4, Issue 1, January-2013.

[4]. ShapnaRani.E, G.Sathesh Kumar, Mythili.R, Karthick.R. Intrusion Detection System for Multitier Web Applications Using Double Guard, International Journal of Engineering And Computer Science ISSN: 2319-7242 Volume 2 Issue 7 (July 2013), Page No. 2162-2166.

[5].Niraj Gaikwad, Swapnil Kandage, Dhanashri Gholap, Double Guard: Detecting and Preventing Intrusions in Multitier Web Applications, Networks and Systems, 2(2), February March 2013, International Journal of Networks and system.

