MİLLİ SAVUNMA ÜNİVERSİTESİ
BARBAROS DENİZ BİLİMLERİ VE MÜHENDİSLİĞİ ENSTİTÜSÜ
DENİZ BİLİMLERİ VE MÜHENDİSLİĞİ DERGİSİ
NATIONAL DEFENSE UNIVERSITY
BARBAROS NAVAL SCIENCES AND ENGINEERING INSTITUTE
JOURNAL OF NAVAL SCIENCE AND ENGINEERING

Deniz Bilimleri ve Mühendisliği Dergisi (Journal of Naval Science and Engineering), hakemli, uluslararası düzeyde, Nisan ve Kasım aylarında olmak üzere yılda iki kez yayımlanan, çok disiplinli bilim ve teknoloji dergisidir. Dergide; Bilgisayar, Makine, Gemi İnşa, Elektrik/Elektronik, Endüstri Mühendisliği ile Temel ve Sosyal Bilimler alanlarında bilimsel nitelikli akademik yazılara yer verilmektedir. Dergi, Türk Silahlı Kuvvetlerinin artan ihtiyaçlarına bilimsel katkı sağlamayı amaçlamaktadır. Dergide yer alan makaleler İngilizce olarak yayınlanmaktadır.

Journal of Naval Science and Engineering is a peer reviewed, international, inter-disciplinary journal in science and technology, which is published semi-annually in November and April. It publishes full research papers, review articles, technical notes, short communications, book reviews, letters to the editor, and extended versions of conference papers. Topics of interest include the technological and scientific aspects of the following areas: **computer science and engineering**, **electrical and electronics engineering**, **naval/mechanical engineering**, **naval architecture and marine engineering, industrial engineering and basic/social sciences**. The papers in the journal are published in English.

İrtibat Noktaları / Subscription and Corresponding Address:
Emrah YAMAKOĞLU
Barbaros Deniz Bilimleri ve Mühendisliği Enstitüsü
MSÜ Deniz Harp Okulu
Tuzla 34942, Istanbul - Turkey
Phone: +90 (216) 395 26 30 / Fax: +90 (216) 395 26 58

MİLLİ SAVUNMA ÜNİVERSİTESİ
BARBAROS DENİZ BİLİMLERİ VE MÜHENDİSLİĞİ ENSTİTÜSÜ
DENİZ BİLİMLERİ VE MÜHENDİSLİĞİ DERGİSİ

CİLT : 13 SAYI : 1 NİSAN 2017 ISSN:1304-2025

İÇİNDEKİLER / CONTENTS

NATIONAL DEFENSE UNIVERSITY
BARBAROS NAVAL SCIENCES AND ENGINEERING INSTITUTE
JOURNAL OF NAVAL SCIENCE AND ENGINEERING

VOLUME: 13 NUMBER: 1 APRIL 2017 ISSN: 1304-2025

Journal of Naval Science and Engineering
2017, Vol. 13, No.1, pp.1-22
Elektrik-Elektronik Mühendisliği/Electric-Electronic Engineering

COMPARATIVE STUDY OF SOFT SWITCHING METHODS USED IN DC-DC CONVERTERS

Ali Saygun SAYGI[1]
Ersoy BEŞER[2]
Murat ÜNLÜ[3]

[1]*Electrical Engineering, Kocaeli University, Umuttepe, Kocaeli, Turkey, alisaygun@hotmail.com*
[2]*Electrical Engineering, Kocaeli University, Umuttepe, Kocaeli, Turkey, ebeser@kocaeli.edu.tr*
[3]*Electrical Engineering, Kocaeli University, Umuttepe, Kocaeli, Turkey, muratunlu@kocaeli.edu.tr*

Date of Receive: 19.02.2017 **Date of Acceptance: 26.03.2017**

ABSTRACT

High frequency switched-mode DC-DC converters are widely used in industry such as battery charging, renewable energy, fuel-cell, power factor correction, LED lighting applications, due to their low response time, easy controlling and high power density. However, at high switching frequency, switching losses, electromagnetic interference (EMI) and lower efficiency become substantial problem. These problems must be eliminated or reduced by using additional passive and active snubber cells in order to operate the converter with soft switching (SS) instead of hard switching (HS). In this paper, properties of soft switching methods named as zero voltage transition (ZVT), zero current transition (ZCT), and zero voltage zero current transition (ZVZCT) developed by combining the ZVT and ZCT, zero voltage switching (ZVS) and zero current switching (ZCS) are studied and discussed, simulations of soft switching DC to DC boost converters including these methods are accomplished for 500W and 1kW power at switching frequency of 100 kHz.

ÖZ

Yüksek frekanslı anahtarlamalı DC-DC dönüştürücüler, kontrol kolaylığı, süratli tepki verme ve yüksek güç yoğunluğu avantajları nedeniyle endüstride; batarya şarj istasyonları, yenilenebilir enerji sistemleri, yakıt pili, güç faktörü düzeltme, LED aydınlatma, gibi uygulamalarda yaygın olarak kullanılmaktadır. Ancak, anahtarlamalı DC-DC dönüştürücülerde anahtarlama frekansı arttıkça güç yoğunluğunun daha da artmasına rağmen anahtarlama kayıpları, elektromanyetik girişim (Electromagnetic Interference-EMI) gürültüleri ve düşük verim sorunları ortaya çıkmaktadır. Bu sorunların üstesinden; dönüştürücünün sert anahtarlama (Hard Switching-HS) ile çalıştırılması yerine, dönüştürücüye pasif ve aktif bastırma hücreleri ilave edilerek dönüştürücünün yumuşak anahtarlama (Soft Switching-SS) ile çalıştırılmasıyla gelinebilmektedir. Bu çalışmada, literatürde yumuşak anahtarlama teknikleri olarak yer alan; sıfır akımda geçiş (Zero Current Transition-ZCT) ve sıfır gerilimde geçiş (Zero Voltage Transition-ZVT) tekniklerinin birleştirilmesiyle geliştirilen sıfır gerilim ve akımda geçiş (Zero Voltage Zero Current Transition-ZVZCT) tekniği ile sıfır akımda anahtarlama (Zero Current Switching-ZCS) ve sıfır gerilimde anahtarlama (Zero Voltage Switching-ZVS) tekniklerini içeren aktif bastırma hücreli DC-DC dönüştürücüler incelenmiş, 500W-1kW güçlerinde ve 100 kHz anahtarlama frekansında yükseltici DC-DC dönüştürücülerin simülasyonları yapılmıştır.

Keywords: *Switched-mode DC-DC Converters, Hard Switching (HS), Soft Switching (SS), Zero Current Switching (ZCS), Zero Voltage Switching (ZVS), Zero Voltage Transition (ZVT), Zero Current Transition (ZCT), Zero Voltage Zero Current Transition (ZVZCT)*
Anahtar Kelimeler: *Anahtarlamalı DC-DC Dönüştürücüler, Sert Anahtarlama (HS), Yumuşak Anahtarlama (SS), Sıfır Akımda Anahtarlama (ZCS), Sıfır Gerilimde Anahtarlama (ZVS), Sıfır Akımda Geçiş (ZCT), Sıfır Gerilimde Geçiş (ZVT), Sıfır Gerilim ve Akımda Geçiş (ZVZCT).*

1. INTRODUCTION

The switched-mode DC-DC converters are widely used in the industry. They possess higher power density, faster transient response are derived and sizes of transformer, inductance and capacitor become smaller when they are operating at high frequency. However, by increasing frequency of the converter, switching losses and EMI noises increase accordingly. Therefore, to eliminate or reduce switching losses, EMI noises, current and voltage stresses, the converter need to be operated with soft switching instead of hard switching In literature, numerous soft-switching techniques have been proposed [1-8].

The switching losses in converter occur during semiconductors are turning off and on. When the semiconductors are turning on, its voltage decreases and it current increases at the same time. On the contrary, during the semiconductors are turning off, its voltage increases and its current decreases at the same time. In process of turning on, losses due to discharge of parasitic capacitor and reverse recovery of the main diode are added to switching losses [1]. Zero current switching (ZCS), zero voltage switching (ZVS), zero voltage transition (ZVT), zero current transition (ZCT) methods are commonly used for soft switching techniques.

As seen in Figure 1; ZCS limits the rising speed of the current flow through the switch in turning on process while ZVS limits the rise speed of the voltage across switch. In turning off process, ZCT makes switch's current down to zero for a short time in turning off process and ZVT makes switch's voltage down to zero for a short time in turning on process.

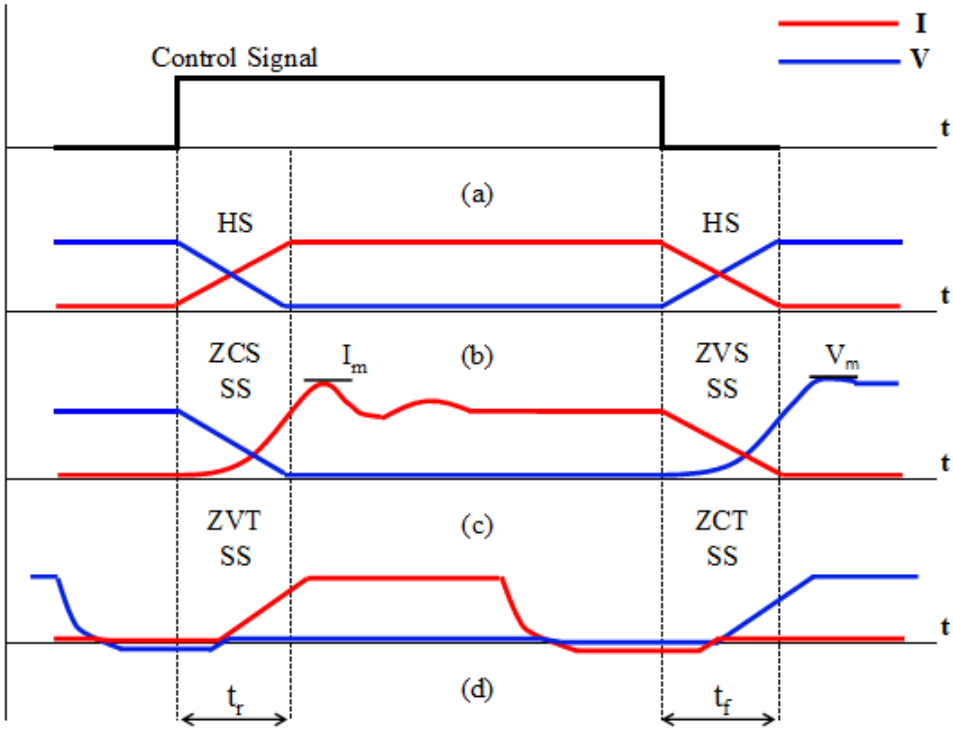


Figure 1. (a) Switching signal, (b) HS, (c) ZCS and ZVS, (d) ZCT and ZVT waveforms

The auxiliary circuits realizing soft switching techniques are called snubber cells. The snubber cells are divided into active or passive snubber cells according to whether or not additional one or more an auxiliary switches are used.

2. ACTIVE SNUBBER CELLS

The active snubber cell is used to perform ZVT and ZCT, and has been studied in the literature for about thirty years. This snubber cell contains one or more an auxiliary switches to operate the main switch with soft switching. In last years, it has been improved and proposed ZVZCT technique which obtained by combining ZCT and ZVT techniques. In this paper, ZVT, ZCT, two different ZVZCT active snubber cells are studied, and moreover boost DC-DC converter including two different ZVZCT active snubber cells analyzed and simulated respectively.

2.1. BASIC ZCT CONVERTER

In ZCT technique, it is aimed to make the main switch turn off when a current flows over it is zero, due to make transition without losses. In the basic ZCT converter shown in Figure 2, the snubber cell is consist of an auxiliary switch, resonant inductance and capacitor and an auxiliary diode. The general features of the converter are as follows [2].

- Low voltage/current stress on the main switch and diode.
- Minimum circulating energy.
- Operating at wide load range.
- Fixed switching frequency.

One of the disadvantages of this converter is, the main switch is turned on and the main diode is turned off simultaneously with HS, so a short circuit occurs at the same time. It is very difficult to realize the avoidance of this short circuit causing losses and EMI problems [3]. Besides, energy in the parasitic capacitor can not be recovered and the main diode turns off with HS, so that reverse recovery loss of this diode is large. The current stress of main switch increases cost of the converter [4].

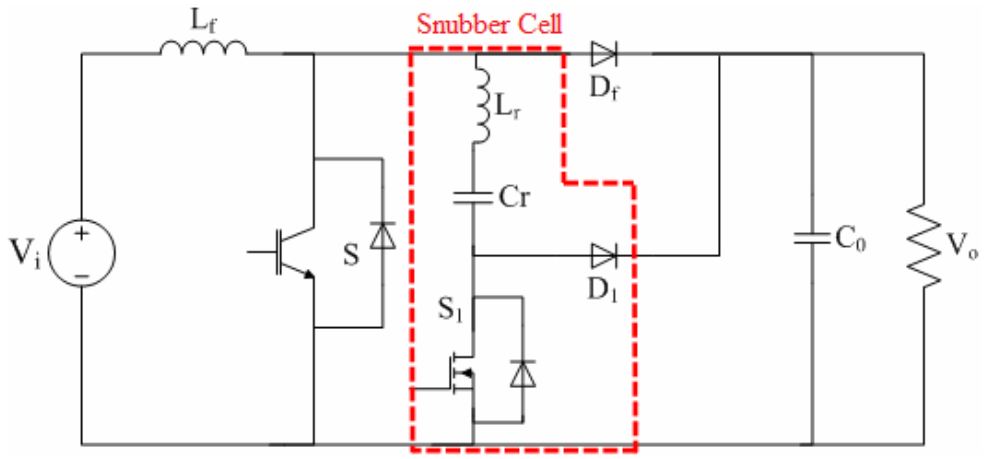


Figure 2. The basic ZCT converter circuit [2]

As shown in Figure 3, the main switch current is subjected to zero by the snubber cell in Figure 2 just before the main switch is in turn off position. and after that, switching signal of the main switch is removed. Thus, the main switch turns off without switching losses. In converter, the main diode turns on with ZVS whereas an auxiliary switch turns on with ZCS. Both of them turn off with HS [4].

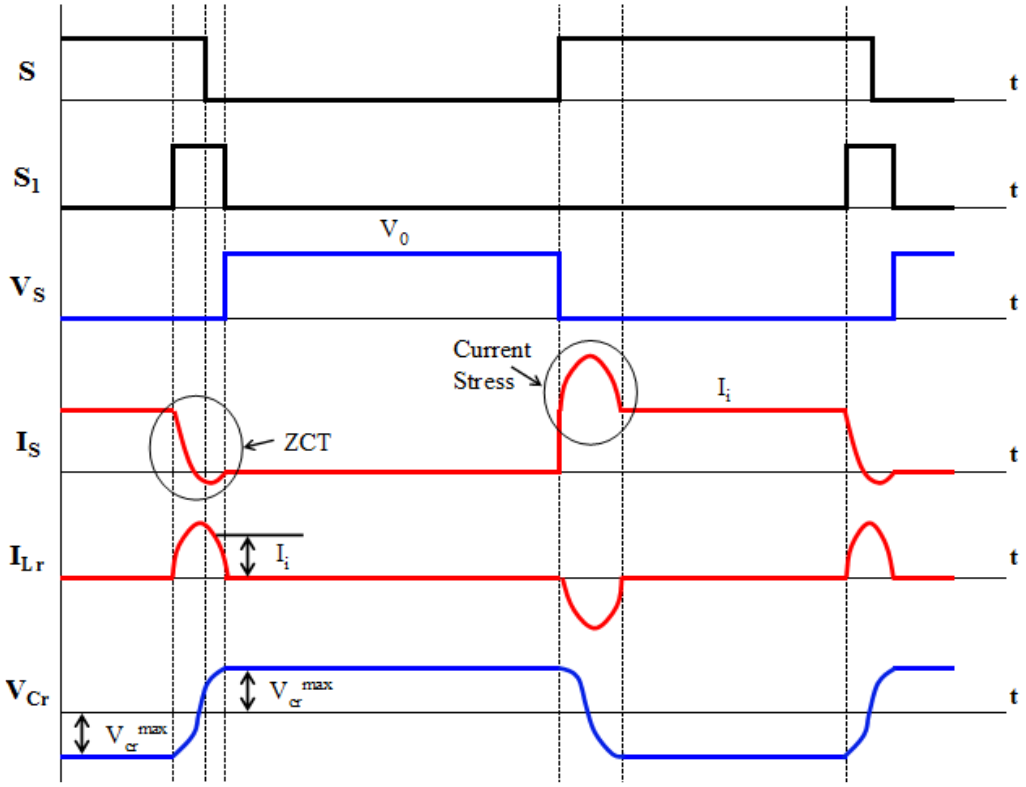


Figure 3. Switching signal of the main switch (S), switching signal of the auxiliary switch (S_1), the main switch voltage (V_S), the main switch current (I_S) and L_r inductance current (I_{Lr}), the voltage of C_r (V_{Cr}) [2].

2.2. THE BASIC ZVT CONVERTER

In ZVT technique, it is intended to make the main switch turn on from turn off state as voltage of switch is zero. As seen in Figure 4, the basic ZVT converter has a snubber cell including resonant capacitor and inductance, an auxiliary switch and two an auxiliary diodes connected in parallel to the main switch. The general features of the converter are;

- Both the main switch and diode with soft switching,
- Lowest voltage/current stress on the main switch and diode,
- Fixed switching frequency [5].

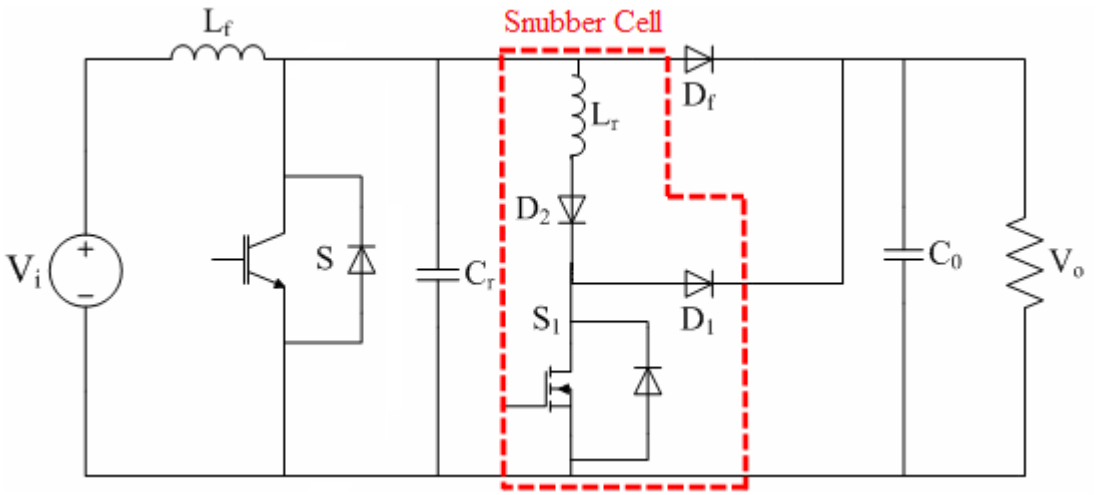


Figure 4. The basic ZVT converter circuit [5]

The waveforms in Figure 5 show that the snubber cell in Figure 4 makes the main switch turns on with ZVT, without losses and any voltage and current stress. Furthermore, the main switch turns off with ZVS by C_r capacitor. The main diode turns off with ZCS and turn on with ZVS by L_r inductance so that reverse recovery losses of the main diode are mostly reduced. Besides, the auxiliary switch turns on with ZCS and voltage or current stress does not occur in other components of the converter other than the acceptable current stress on the auxiliary switch [4,5].

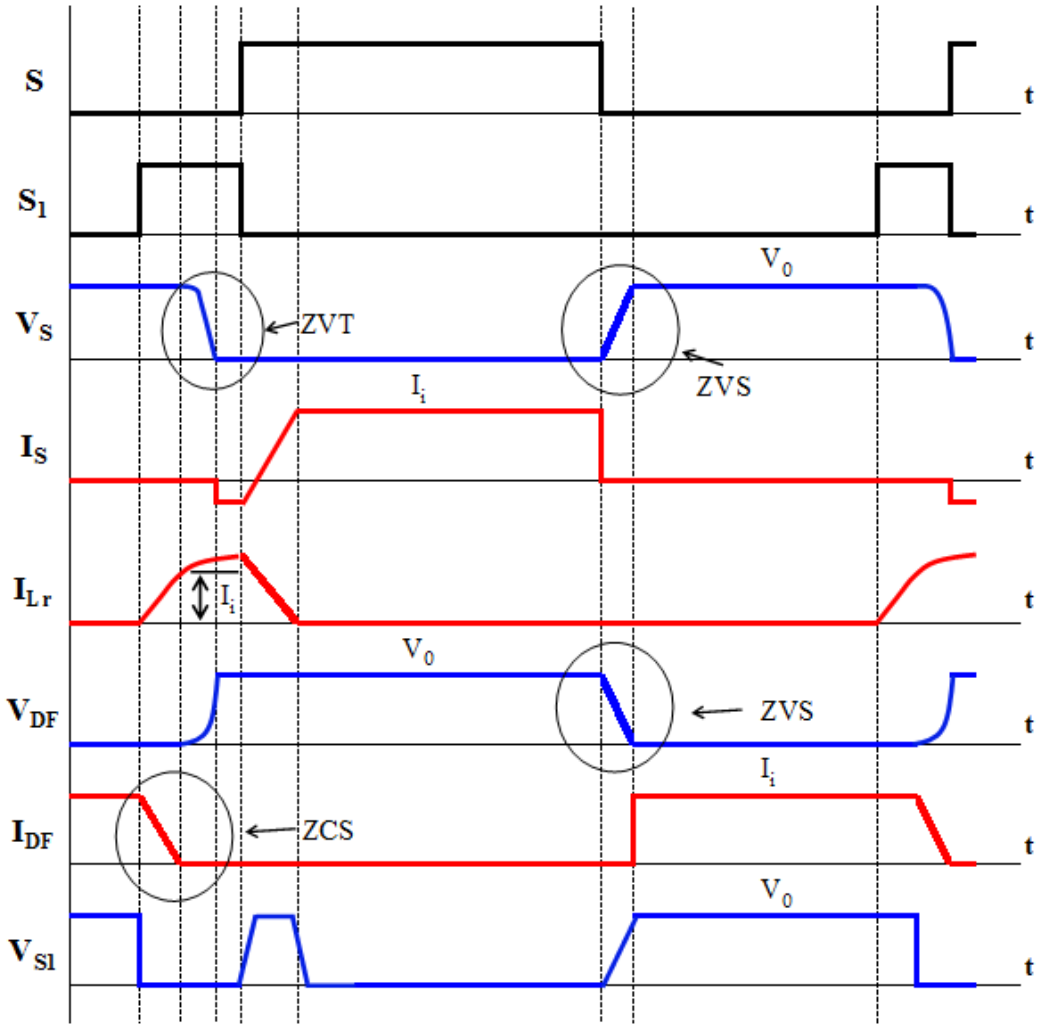


Figure 5. Switching signal of the main switch (S), switching signal of the auxiliary switch (S_1), the main switch voltage (V_S), the main switch current (I_S) and L_r inductance current (I_{Lr}), the main diode voltage (V_{DF}), the main diode current (I_{DF}), the auxiliary switch voltage (V_{S1}) [5]

The disadvantages of the converter are being dependent on load, the difficulty of the transferring of the energy stored in the inductance to the load and switching losses caused by the auxiliary switch turning off with HS [6].

2.3. ZVZCT DC-DC CONVERTER-I

The circuit in Figure 6 is designed in order to overcome most of the problems of the basic ZCT DC-DC converter. As seen in Figure 6, the snubber cell that is connected in parallel to the main switch consists of a snubber inductance L_s , a snubber capacitor C_s and an auxiliary switch which are connected in serial to each other. The capacitor C_p is the sum of the parasitic capacitor of the main switch and the other parasitic capacitors. ZVT and ZCT properties are obtained from the basic ZCT converter without any changing in the circuit topology. In this converter, the main switch turns on with ZVT and turns off with ZCT and all the other semi-conductors turns on and off with soft switching [7].

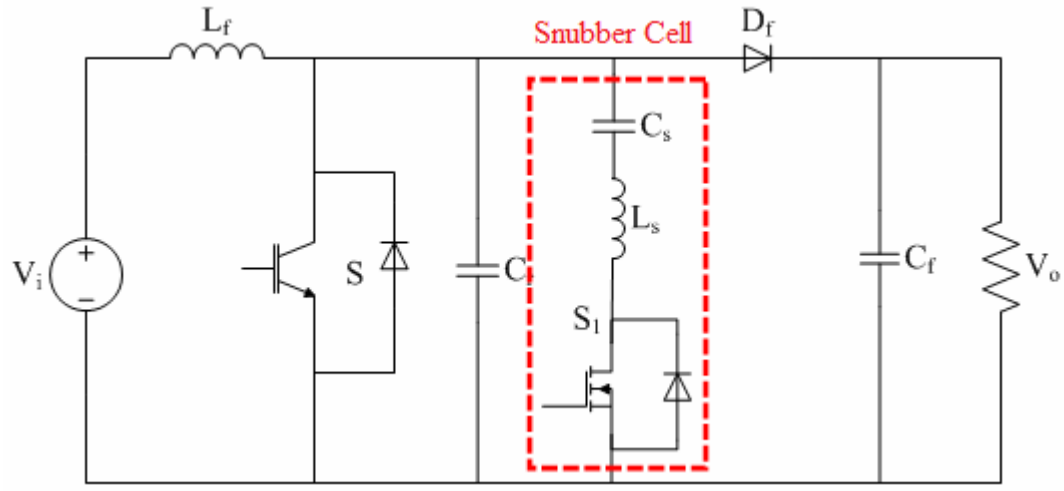


Figure 6. The ZVZCT DC-DC converter [7]

It can be seen from Figure 7 that as the auxiliary switch is in turn on position, switching signal of the main switch is applied so that the main switch turns on with ZVT. At this time, the main diode turns off with ZCS and ZVS. In this interval, there is a low voltage on the auxiliary switch. After that, the auxiliary switch turns on before the main switch turns off and then the main switch turns off with ZCT. The main diode turns on with ZVS after the main switch turns off.

Approximate output voltage occurs on the auxiliary switch until main switch turns on again [7].

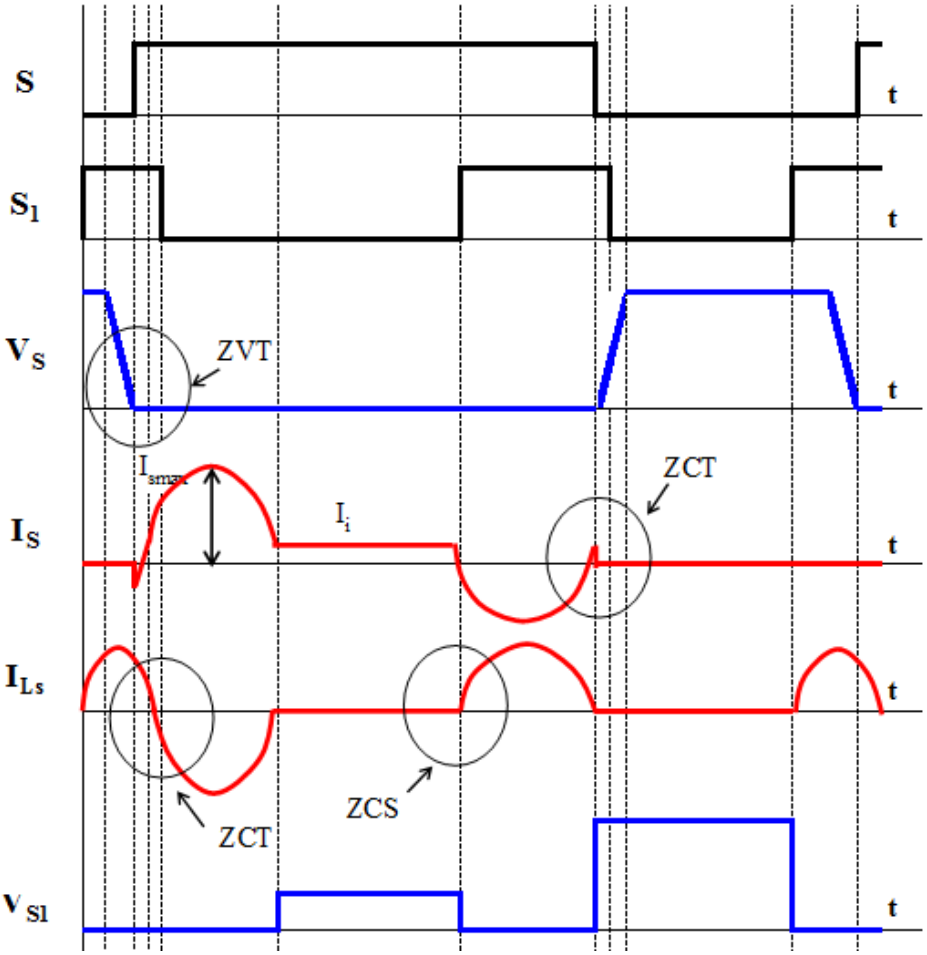


Figure 7. Switching signal of the main switch (S), switching signal of the auxiliary switch (S_1), the main switch voltage (V_S), the main switch current (I_S) and L_s inductance current (I_{Ls}), the auxiliary switch voltage (V_{S1}) [7]

For the converter shown in Figure 6, the main diode turns on with ZVS and turns off with ZCS-ZVS and is not exposed to voltage and current stress and also the other semi-conductors are not subjected to additional voltage stress. Soft switching is maintained at very wide load range. The auxiliary switch turns off with ZCT and turns on with ZCS. A small amount of circulation energy gets lost. The switching losses are not dissipated on the snubber cell, are transferred to the load [7].

2.4. ZVZCT DC-DC CONVERTER-II

As seen in the converter of Figure 8, the snubber cell that is connected in parallel to the main switch includes an auxiliary diode D_2, the resonant inductances L_a and L_b, a resonant capacitor C_s, and an auxiliary switch. The capacitor C_p that is connected in parallel to the main switch is the sum of the parasitic capacitor of the main switch and the other parasitic capacitors. The main switch turns on with ZVT, turns off with ZCT and the main diode turns on with ZVS and off with ZCS. Thus, reverse recovery losses of the main diode are minimized. The main switch and diode are not subjected to additional current or voltage stress. The auxiliary switch turns on and off with ZCS. The converter decreases EMI noise and operates even at a wide range of load and high frequency [8].

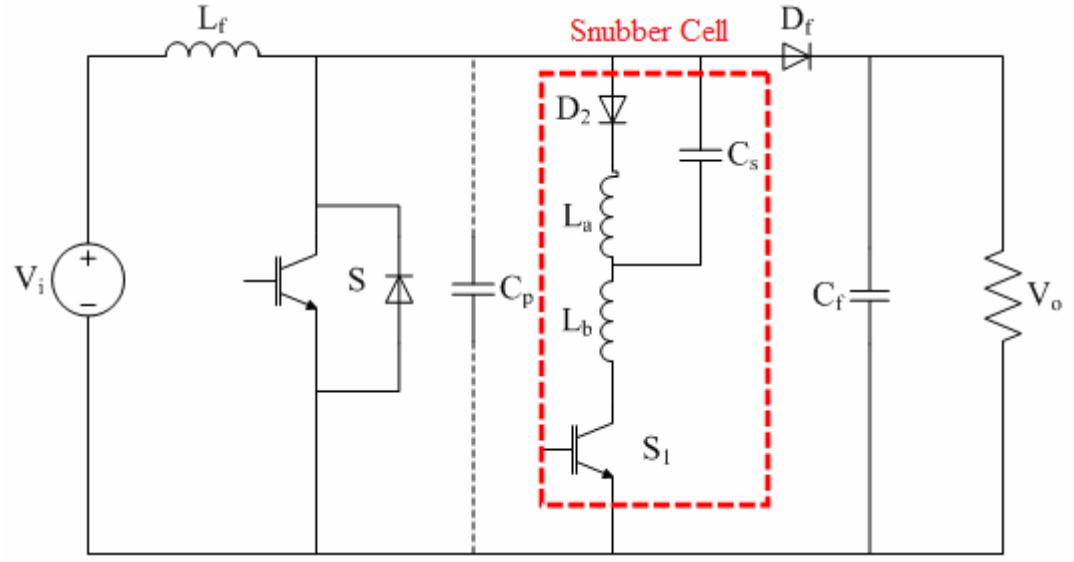


Figure 8. The ZVZCT DC-DC converter [8]

The voltage and current waveforms of the main switch, the auxiliary switch and the main diode are shown in Figure 9. In turning on interval, voltage of the main switch is reduced to zero by the snubber cell in Figure 8. The switching signal of the main switch is applied when voltage of the switch is zero and as its internal diode conducts. Thus, switching losses of the main switch as turning on are eliminated. During the turning off stage, the main switch current is reduced to zero by the snubber cell. After that the switching signal of the main switch is removed when its internal diode conducts. In this way, the main switch turns off without losses with ZCT [8].

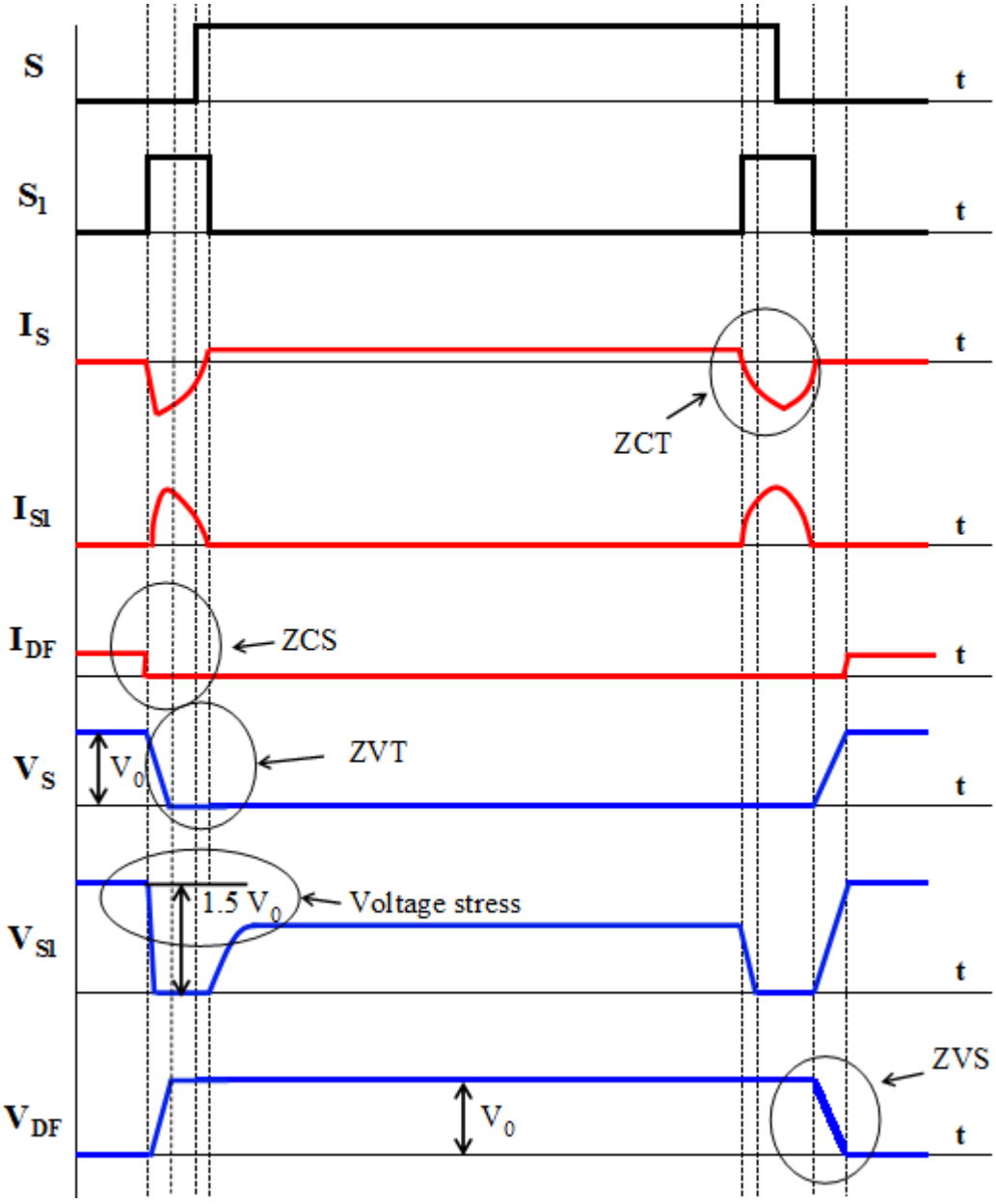


Figure 9. Waveforms of the semi-conductors in the converter [8]

Figure 9. Switching signal of the main switch (S), switching signal of the auxiliary switch (S_1), the main switch current (I_S), the auxiliary switch current (I_{S1}), the main diode current (I_{DF}), the main switch voltage (V_S), the auxiliary switch voltage (V_{S1}), the main diode voltage (V_{DF}) [8]

2.5. THE COMPARISON OF ACTIVE SNUBBER CELLS

A comparison of the modern soft switching techniques studied in Chapter 2 is given in Table 1. It is deduced from Table 1 that the ZVZCT techniques are more advantageous than the other soft switching techniques mentioned in Chapter 2.

Table 1. The features of soft switching techniques [1-8]

Feature	**Basic ZCT**	**Basic ZVT**	**ZVZCT-1**	**ZVZCT-2**
The main switch's turning on	HS	ZVT	ZVT	ZVT
The main switch's turning off	ZCT	ZVS	ZCT	ZCT
The aux. switch's turning on	ZCS	ZCS	ZCS	ZCS
The aux. switch's turning off	HS	HS	ZCT	ZCS
The main diode's turning on	ZVS	ZVS	ZVS	ZVS
The main diode's turning off	HS	ZCS	ZCS-ZVS	ZCS
Current stress	High	Low	No	No
Voltage stress	No	No	No	Low
Operating at wide load range	Yes	No	Yes	Yes

3. SIMULATIONS

The results are obtained by performing simulation of the boost DC-DC converters including the ZVZCT techniques, which featured in the soft switching techniques studied in Chapter 2.

3.1. SIMULATION OF ZVZCT CONVERTER-I

In Figure 10, the model of a 1 kW converter operating at 100 kHz frequency is demonstrated. The switching signal of the auxiliary switch S_1 is applied before about 150 ns and removed after about 400 ns regard to the turn on signal of the main switch. Similarly, the switching signal of the auxiliary switch is applied before about 300 ns and removed after about 300 ns considering the turn off signal of the main switch [7].

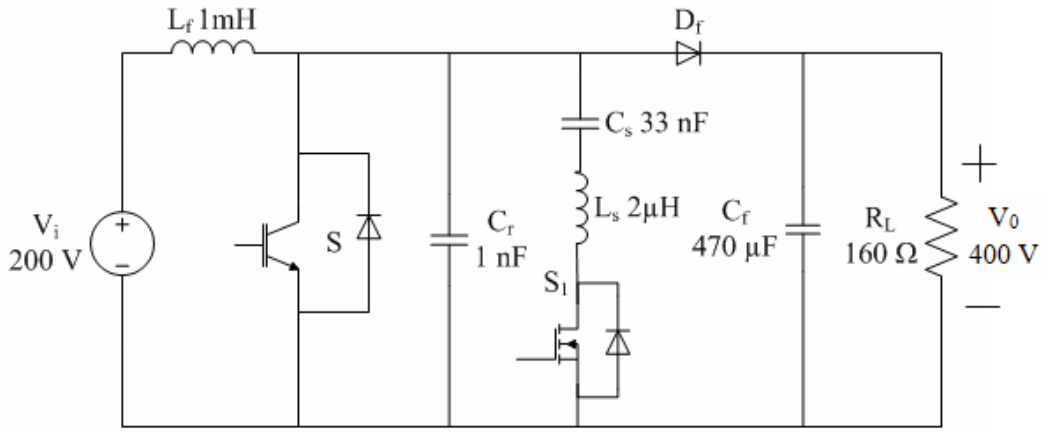


Figure 10. The model of ZVZCT Converter-I used in simulation [7]

Output voltage of the boost converter is 400 V, because of the duty cycle of the main switch is 0.5. As seen in Figure 11, the main switch turns off with ZCT and turns on with ZVT. The fall time of the main switch is 125 ns.

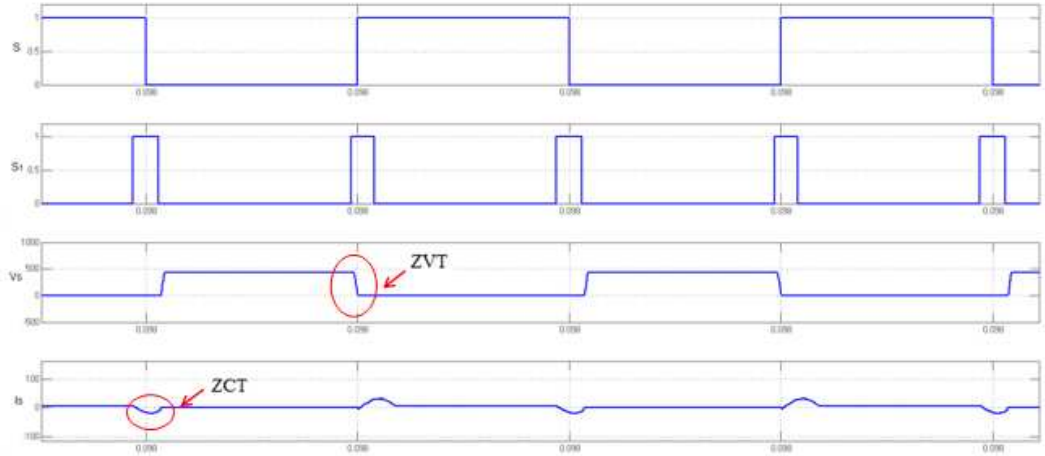


Figure 11. Switching signal of the main switch (S), switching signal of the auxiliary switch (S_1), the main switch voltage (V_S) the main switch current (I_S)

The waveforms of the auxiliary switch are shown in Figure 12. The auxiliary switch turns off with ZCT and turns on with ZCS. The fall time of the auxiliary switch is 58 ns.

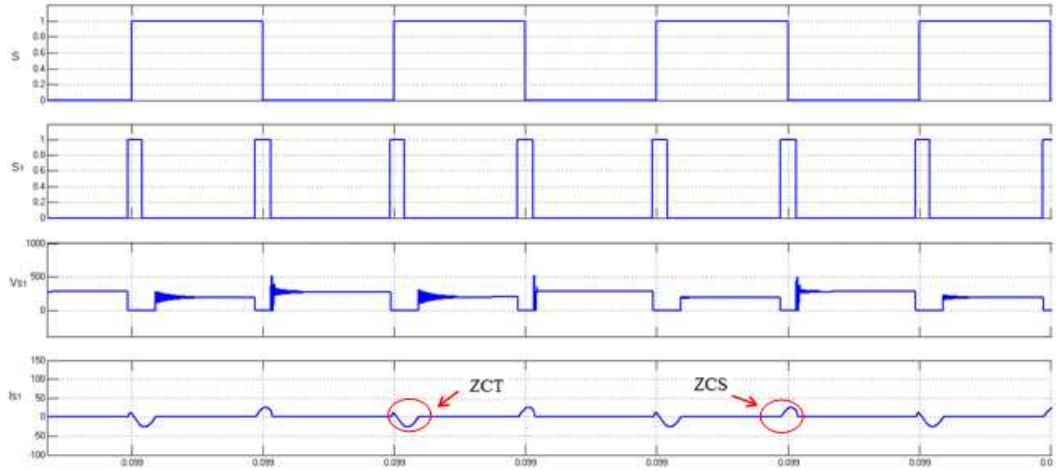


Figure 12. Switching signal of the main switch (S), switching signal of the auxiliary switch (S_1), the auxiliary switch voltage (V_{S1}) the auxiliary switch current (I_S)

3.2. SIMULATION OF ZVZCT CONVERTER-II

In Figure 13, the model of a 1 kW ZVZCT boost converter operates at 100 kHz frequency is shown. In simulation studies, the switching signal of the auxiliary switch S_1 is applied before about 200 ns and removed after about 50 ns regard to turn on signal of the main switch S. Correspondingly, the switching signal of the auxiliary switch is applied before about 200 ns and removed after about 200 ns considering turn off signal of the main switch. C_p is the sum of the parasitic capacitor of the main switch and the other parasitic capacitors [8].

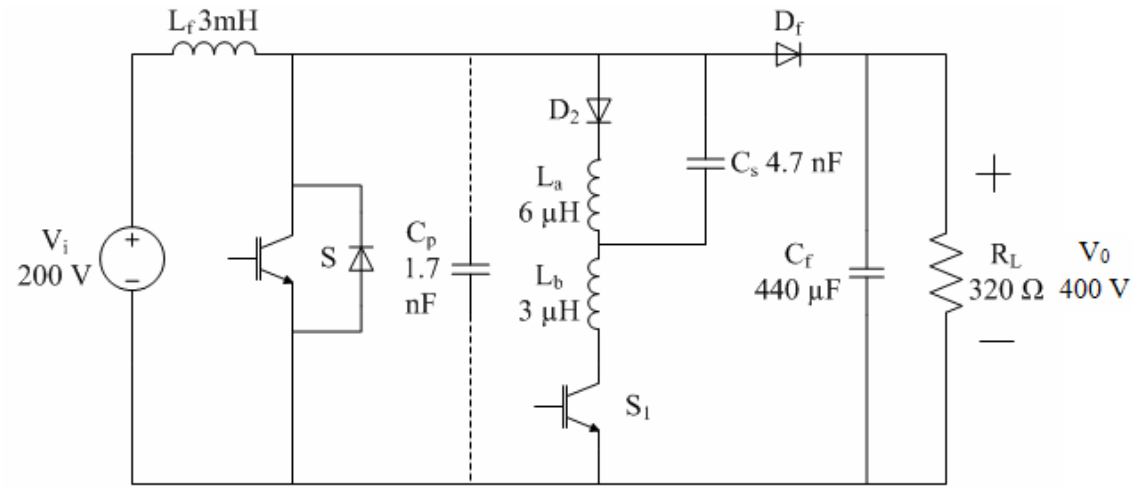


Figure 13. The model of ZVZCT Converter-II used in simulation [8]

Output voltage of the converter is 400 V because of duty cycle is 0.5. In Figure 14, the waveforms show that the main switch turns on with ZVT and turns off with ZCT. The fall time of the main switch is 40 ns.

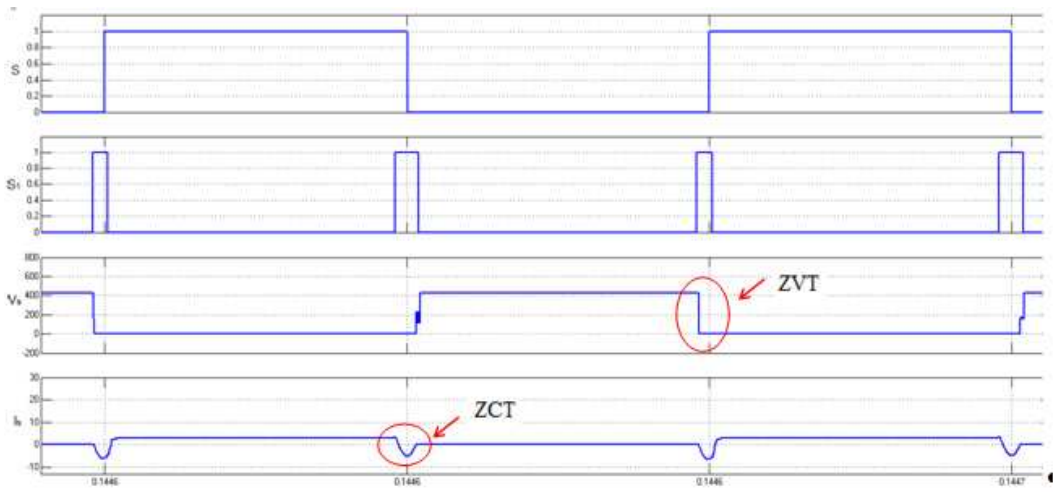


Figure 14. Switching signal of the main switch (S), switching signal of the auxiliary switch (S_1), the main switch voltage (V_S) the main switch current (I_S)

The waveforms of the auxiliary switch are shown in Figure 15. The auxiliary switch turns on and off with ZCS. A voltage stress about 1.5 times of the output voltage occurs on the auxiliary switch. The fall time of the auxiliary switch is 20 ns [8].

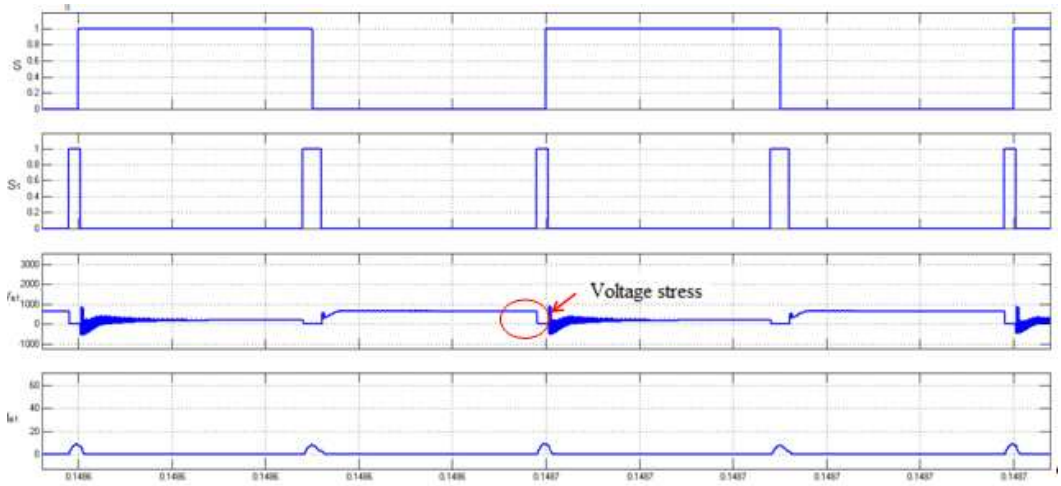


Figure 15. Switching signal of the main switch (S), switching signal of the auxiliary switch (S_1), the auxiliary switch voltage (V_{S1}) the auxiliary switch current (I_S)

In Figure 16, waveforms of the main diode are shown. The main diode turns on with ZVS, and it turns off with ZCS.

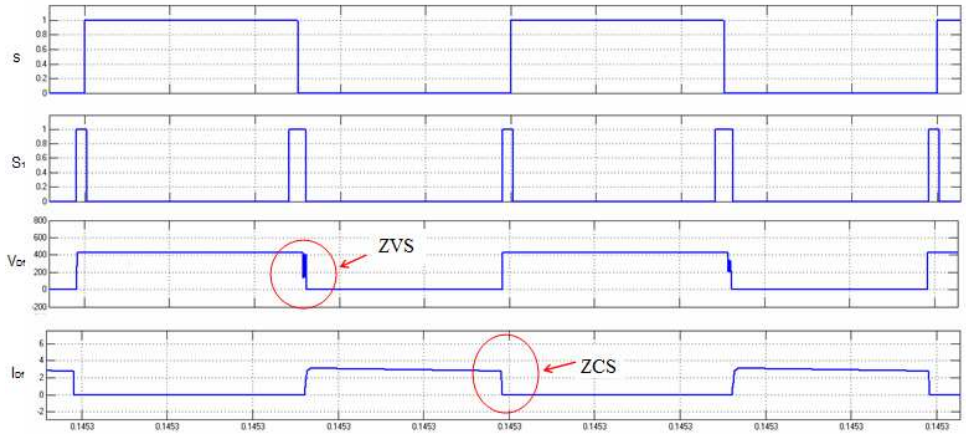


Figure 16. Switching signal of the main switch (S), switching signal of the auxiliary switch (S_1), the main diode voltage (V_{DF}), the main diode current (I_{DF})

4. CONCLUSION

Although size of the circuit elements become smaller when the converter operates at high frequencies, power losses and EMI noises increase. Many techniques have been developed that allow converters to operate with soft switching in order to solve this problem. In this paper, zero voltage transition (ZVT), zero current transition (ZCT), and zero voltage zero current transition (ZVZCT) that is developed by combining the ZVT and ZCT soft switching methods are studied. According to the results of the comparison in Table 1, the ZVZCT converters have many advantages so that the simulations of these converters are implemented.

In simulation of the first converter the main switch turns on with ZVT and turns off with ZCT, the auxiliary switch turns on with ZCS and turns off with ZCT. As seen in simulation of the second converter, the main switch turns on with ZVT and turns off with ZCT and a voltage stress about 1.5 times of the output voltage occurs on the auxiliary switch. The main diode turns off with ZCS and turns on with ZVS.

In both converters there is no extra voltage or current stress except for the acceptable voltage stress of the second converter.

5. REFERENCES

[1] H.Bodur, İ.Aksoy, B.Akın, "DC-DC Dönüştürücülerde Yumuşak Anahtarlama Teknikleri", Kaynak Elektrik, Jun.2002, vol. 158, pp. 100-108.

[2] G.Hua, E. X.Yang,Y. Jiang, and F. C. Lee, "Novel Zero-Current-Transition PWM Converters," IEEE Trans. Power Electron., vol. 9, pp. 601–606, Nov. 1994.

[3] H. Bodur and A. F. Bakan, "An Improved ZCT-PWM DC–DC Converter for High-Power and Frequency Applications," IEEE Trans. Power Electron., vol. 51, no. 1, pp. 89-95, Feb.2004.

[4] Y.Şahin, İ.Aksoy, N.S.Tınğ, "The Comparison of Methods Used in Soft Switching DC-DC Converters," Electric-Electronic-Computer and Biomedical Engineering Symposium, Bursa, Nov.2014, pp.235-238.

[5] G. Hua, C. S. Leu, Y. Jiang, and F. C. Lee, "Novel Zero-Voltage-Transition PWM Converters," IEEE Trans. Power Electron., vol. 9, no. 2, pp. 213–219, Mar. 1994.

[6] H. Bodur and A. F. Bakan, "A new ZVT-PWM DC-DC converter," IEEE Trans. Power Electron., vol. 17, no. 1, pp. 40–47, Jan. 2002.

[7] N.Altıntaş, A.F.Bakan, İ.Aksoy, "A Novel ZVT-ZCT-PWM Boost Converter," IEEE Trans. Power Electron., vol. 29, no. 1, pp. 256-265, Jan. 2014.

[8] Y.Şahin, İ.Aksoy, N.S.Tınğ, "A New Soft-Switched ZCZVT-PWM DC-DC Boost Converter," TUBİTAK Turkish Journal of Electrical Engineering & Computer Sciences, DOI:10.3906/elk-1508-258.

Journal of Naval Science and Engineering
2017, Vol. 13, No.1, pp.23-30
Endüstri Mühendisliği/Industrial Engineering

A CASE STUDY FOR PRE-POSITIONING A GLOBAL HUMANITARIAN RELIEF NETWORK

Ertan YAKICI

Industrial Engineering Department,
National Defense University, Turkish Naval Academy, Tuzla, Istanbul
eyakici@dho.edu.tr

Date of Receive: 14.01.2017 **Date of Acceptance: 27.03.2017**

ABSTRACT

In this case study, we have investigated the optimal design of a network of warehouses to be pre-positioned for humanitarian relief operations to be executed when expected disasters happen. A model which is previously introduced in the literature is applied with the most recent data. The model responds to decision requirements in both locations of warehouses and allocation of resources to these warehouses, assuming the disaster pattern of last decade will continue. A sensitivity analysis is also conducted to observe how the average response time changes as the allowed number of warehouses increases.

ÖZ

Bu çalışmada, beklenen doğal afetlere karşı insani yardım kapsamında önceden konumlandırılacak depolara ait şebekenin dizaynı incelenmiştir. Daha önce literatürde tanıtılmış olan bir model en son elde edilen veri ile uygulanmıştır. Model, son on yılda gerçekleşen doğal afet paterninin önümüzdeki yıllarda da gerşekleşeceği varsayımını esas alarak, depoların yerleşimi ve kaynakların bu depolara dağıtımı için ortaya çıkan karar ihtiyaçlarına beraberce cevap vermektedir. Açılabilecek depo sayısındaki artışın ortalama tepki zamanı üzerindeki etkisini görebilmek için bir duyarlılık analizi çalışması da yapılmıştır.

Keywords: *Pre-positioning, Humanitarian Relief Logistics, Warehouse Location.*
Anahtar Kelimeler: *Ön-konumlandırma; İnsani Yardım Lojistiği; Depo Yerleştirme.*

1. INTRODUCTION

In the last decades, with the effect of global warming, the number of natural disasters increases. This phenomenon requires fast and coordinated humanitarian relief operations. Unpredictability of demand in humanitarian logistics makes pre-disaster activities more important. One of these

activities is strategic positioning of warehouses built for supporting relief operations [1].

Pre-positioning can be defined as a tool to increase responsiveness by locating items which will be used in relief operations, like foods and medical material, closer to the regions under risk [2].

In this study we applied a model used by Duran et al. [3] with a data belongs to most recent decade (2007-2016) . In their paper, the authors report that they have supported the decision process in designing a pre-positioning network of warehouses. The employed model considers demand raised from 22 regions of the world, which is determined by United Nations, for relief supplies to be used after earthquakes, windstorms and floods. Candidate warehouse locations are determined by CARE International. It is assumed that, when inventory shortage occurs, main suppliers can send relief supplies to the regions with longer lead times. The model minimizes the weighted average response time.

To assign demand to discretized time periods, two-week time horizon is used in concordance with the estimation of CARE International suppliers [3]. Demand information is obtained from Emergency Events Database (EM-DAT) which keeps the data on the effects of disasters all around the world since 1900 [4].

This study is not the only one applying the model proposed by Duran et al. [3]. Bozkurt and Duran [5] observe three decades from 1977 to 2006 to see whether there is a significant change in the disaster locations and the number of affected people over this period. Our study can be considered as a follower of the work presented by Bozkurt and Duran [5], because we apply the same model with the data of the most recent decade.

In the following sections, the formulation of the problem is given and the results are reported. Finally, conclusion is given in the last section.

2. PROBLEM DEFINITION

Definitions of Index sets, variables and parameters are given below.

I set of canditate locations for warehouses,
D set of disaster types,
J set of demand points,
R set of relief items,
E set of demand instances,

y_i 1 if warehouse i is activated, 0 otherwise,
q_{ir} quantity of item r held at warehouse i,
x_{ijer} quantity of item r supplied to demand point j from warehouse i for demand instance e,
x'_{jer} quantity of item r supplied to demand point j from suppliers for demand instance e,

N maximum number of warehouses allowed to be activated,
Q total inventory,
P_e probability of occurring for demand instance e,
t_{ij} response time from warehouse i to demand point j,
t'_{jr} response time from suppliers to demand point j for item r,
d_{dje} number of affected people at demand point j by a disaster of type d for demand instance e,
p_{djr} probability of item r being required at demand point j by a person affected by a disaster of type d,
a_{djr} quantity of item r required by a person affected by a disaster of type d in demand point j,
d'_{jer} expected demand for item r at demand point j in demand instance e.

According to the notation given above, the mathematical formula of mixed integer programming model is given as follows:

$$z = \min \sum_{e \in E} P_e \left(\frac{\sum_{j \in J} \sum_{r \in R} x'_{jer} t'_{jr} + \sum_{i \in I} \sum_{j \in J} \sum_{r \in R} x_{ijer} t_{ij}}{\sum_{j \in J} \sum_{r \in R} d'_{jer}} \right) \quad (1)$$

$$d'_{jer} = \sum_{d \in D} a_{djr} p_{djr} d_{dje} \qquad j \in J, e \in E, r \in R \quad (2)$$

$$\sum_{i \in I} x_{ijer} + x'_{jer} \geq d'_{jer} \qquad j \in J, e \in E, r \in R \quad (3)$$

$$\sum_{j \in J} x_{ijer} \leq q_{ir} \qquad i \in I, e \in E, r \in R \quad (4)$$

$$q_{ir} \leq Q y_i \qquad i \in I, r \in R \quad (5)$$

$$\sum_{i \in I} \sum_{r \in R} q_{ir} \leq Q \quad (6)$$

$$\sum_{i \in I} y_i \leq N \quad (7)$$

$$x_{ijer}, x'_{jer}, q_{ir} \geq 0 \qquad i \in I, j \in J, e \in E, r \in R \quad (8)$$

$$y \in \{0,1\} \qquad i \in I \quad (9)$$

The travel of a relief item is normally equal to the fly time of a usual cargo aircraft between the warehouse and the demand point plus one additional

preparation day. However, if warehouse inventory is not sufficient to meet the demand, the global suppliers provide the relief items with a response time of two-weeks. Therefore, average response time which is reflected by objective function (1) is calculated as the weighted sum of these two response times, where weights are equal to the proportions of demand satisfied by each method.

Constraint set (2) assigns the value of expected demand of each relief item at each demand location for each disaster instance. Constraint set (3) ensures the requirement of demand satisfaction of each relief item at each demand point for each disaster instance. Constraint set (4) ensures that total amount of an item shipped from a warehouse cannot exceed the inventory of this warehouse of that item type. Constraint (5) set reflects that a warehouse should be activated to hold any inventory. Constraint (6) forces that total inventory cannot be exceeded. Constraint (7) satisfies the requirement of allowed number of active warehouses should not be exceeded. Remaining constraint sets (8-9) defines the variable domains.

3. APPLICATION AND RESULTS

Our case includes 22 demand points, 12 candidate locations for warehouses, seven types of relief items; cold tent, hot tent, household utensils, medical relief items, hygiene sets, sanitation sets and water as in the previous work of Bozkurt and Duran [5]. Since the detailed information about the used data is given in the thesis of Bozkurt [6] and the study of Bozkurt and Duran [5], if they are kept same, we do not mention the parameter details here.

As in the previous works [5, 6], each demand instance is created by grouping disasters occurred in two-week time periods in a region. This assumption creates 237 demand instances from the disaster data of the last decade. Each disaster type may require different combination of relief items per affected person according to the region of the world. Although model allows such a detailed level of analysis, since there is no evidence for differentiating the regions with respect to required relief items, we assume

all of the affected people regardless of their regions will demand the same combination of relief items.

In contrary to Bozkurt and Duran [5], we only used one demand level. To be on the safe side, we assume that all affected people are included in the demand and all disaster events have 100% probability of occurring. Total inventory is assumed to be the average demand of a demand instance.

A commercial solver, CPLEX 12.6.2.0, is run to the optimality. It is observed that the solver has provided the optimal solution in a few minutes depending on number of warehouses allowed to be activated.

To observe the sensitivity to the number of warehouses, we have expanded the warehouse network one by one. If we open one warehouse, it is optimal to open it in Denmark. If we increase the number of warehouses to two, it is optimal to open them in Kenya and Honduras. Optimal places for three warehouses are Denmark, Kenya and Honduras. Then, if we continue to increase the number to four and five, Hong Kong and Italy are added to the set, respectively. As observed from the graph in Figure 1, after four warehouses, there is no need to activate another, since its marginal contribution is insignificant.

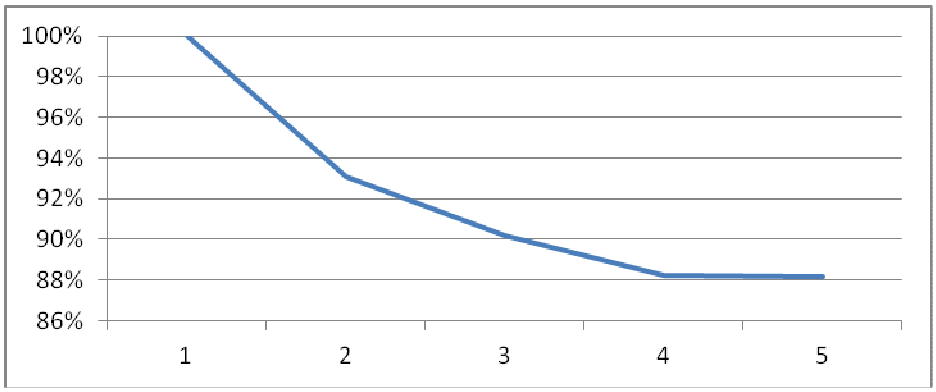


Figure 1. Decrease in response time as the number of warehouses increases

In Table 1, we give the allocation of items in each activated warehouse in percentages.

Table 1. Allocation of relief items to warehouses

	Cold Tent	Hot Tent	Household Utensils	Medical Relief Items	Hygiene Sets	Sanitation Sets	Water
Denmark	4%	4%	8%	21%	21%	24%	17%
Honduras	4%	4%	8%	20%	20%	21%	23%
Hong-Kong	5%	5%	9%	21%	21%	21%	19%
Kenya	4%	4%	8%	22%	21%	19%	22%

4. CONCLUSION

In this study, we have investigated the optimal design of a network of warehouses to be located for humanitarian relief operations. A model which is previously introduced in the literature is applied with the most recent data that belong to the period of 2007-2016. With the assumption of the disaster pattern of the last decade will continue, the model attempts to minimize the average response time, while supporting the decisions in both locations of warehouses and allocation of relief items to activated warehouses.

We have conducted a sensitivity analysis to observe how the average response time changes as the allowed number of warehouses increases. We have seen that, there is no need to activate fifth warehouse, because of its insignificant marginal contribution. We also present the suggested allocation of relief items to the four warehouses which are suggested to be activated.

REFERENCES

[1] Ergun O., Karakus G., Keskinocak P., Swann J., and Villarreal, M., (2008). Overview of Supply Chains for Humanitarian Logistics. In *Encyclopedia in Operations Research and Management Science*; Cochran, J., Ed.; John Wiley Sons: Hoboken, NJ, USA.

[2] Van Wassenhove L.N., (2006). *Blackett memorial lecture-humanitarian aid logistics: Supply chain management in high gear*, J. Oper. Res. Soc., 57, pp. 475–489.

[3] Duran S., Gutierrez M.A., and Keskinocak P., (2011). *Pre-positioning of emergency items for care international*, Interfaces, vol. 41(3), pp. 223–237.

[4] EM-DAT The International Disaster Database Homepage. Available online: http://www.emdat.be (accessed on 5 March 2017).

[5] Bozkurt M., and Duran S., (2012). *Effects of Natural Disaster Trends: A Case Study for Expanding the Pre-Positioning Network of CARE International*, Int. J. Environ. Res. Public Health, *9*, pp. 2863-2874.

[6] Bozkurt M., (2011). *The effects of natural disaster trends on the prepositioning implementation in humanitarian logistics networks*, MS Thesis, METU, Ankara.

Journal of Naval Science and Engineering
2017, Vol. 13, No.1, pp.31-42
Bilgisayar Mühendisliği/Computer Engineering

GENDER CLASSIFICATION FROM FACE IMAGES

Eyyüp YILDIZ [1]
Tolga ENSARİ [2]

[1]*Computer Engineering, Istanbul University, Istanbul, Turkey, 1306110012@ogr.iu.edu.tr*

[2] *Computer Engineering, Istanbul University, Istanbul, Turkey, ensari@istanbul.edu.tr*

Date of Receive: 12.03.2017 **Date of Acceptance: 28.03.2017**

ABSTRACT

In this article, we study on gender classification which is one of the important issue in security, statistics and related commercial areas. In the study, FEI face data set has been used that has 200 female and 200 male frontal face images. Principal component analysis (PCA) has been used for feature extraction process. We use all part of the face images instead of taking some part of them. Support Vector Machine (SVM) and k-nearest neighbor algorithms used for classification test phases. We compare the results which obtained in our experiments and give them in tables and graphs. According to the experiments, defined as hybrid method principal component analysis with k-nearest neighbor method gives better recognition accuracy then defined as hybrid method principal component analysis with support vector machine method.

ÖZ

Bu makalede, günümüzde güvenlik, istatistik ve ilgili ticari alanlarda önemli yer tutan konulardan biri olan, yüz resimlerinden cinsiyet sınıflandırma üzerine bir araştırma yapılmıştır. Çalışmada, 200 bayan ve 200 bay olmak üzere 400 adet ön yüz resmi bulunan FEI yüz veri kümesi, resimlerden özellik çıkarımı için ise temel bileşen analizi (TBA) kullanılmıştır. Özellik (feature) çıkarımında yüzün belirli bölümleri yerine tamamı alınmıştır. Sınıflandırma ve test için destek vektör makineleri (DVM) ve en yakın k-en yakın komşu (k-nearest neighbor k-nn) algoritmaları kullanılmıştır. Deneysel çalışmalarda elde edilen sınıflandırma doğruluk oranları karşılaştırılmış ve sonuçlar analiz edilerek tablolar ve grafikler şeklinde sunulmuştur. Buna göre, elde edilen sonuçlara göre, temel bileşen analiziyle hibrit metot olarak kullanılan k-nn algoritmasının, destek vektör makineleri yöntemine göre cinsiyet sınıflandırmada daha iyi sonuçlar verdiği tespit edilmiştir.

Keywords: *Gender classification, face recognition, principal component analysis, k-nearest neighbor.*
Anahtar Kelimeler: *Cinsiyet sınıflandırma, yüz tanıma, temel bileşen analizi, k-en yakın komşuluk.*

1. INTRODUCTION

Pattern recognition is one of the sub-part of artificial intelligence and machine learning. It is described as recognition of patterns which has some special numbers, letters and shapes. For this purpose, this system makes classification process, using patterns' important features. It is used speech and speaker (voice) recognition, fingerprint recognition, character and digit recognition, DNA/RNA (microRNA) classification, micoarray data classification/clustering, military applications, robotics, fault detection systems, image and signal processing, classification and more application areas. It will be more common in the future. Customer detection and classification, churn analysis are also among this systems. Therefore, gender classification process is one of the important area in pattern recognition.

Although, many researchers publish many studies in pattern recognition area, there are quite little papers related with gender classification in the literature. This concept is also important for psychological effects. Especially, artificial neural networks, principal component analysis, support vector machines and k-nearest neighbor methods has been used in the literature. First study for gender classification had been made in 1991 by Jain and Huang [1, 17]. Next research had been studied with artificial neural networks [2, 17]. On the other hand, principal component analysis has also been preferred in machine learning and pattern recognition community [4,17]. It has been developed by Hetelling [3]. Chervonenkis et al used hyperplane kernels for nonlinear classification [1].

K-nearest neighbor method was proposed in order to classify patterns, by Fix and Hodges in 1951. In [6], local binary pattern (LBP) was used for gender classification to measure the performance and get 95% success. On the other hand, genetic algorithms, linear discriminant analysis and artificial neural networks methods also have been studied in the literature [6]. L. Lu et al used two stages principal component analysis and support vector machines algorithms and reached 94% accuracy [7]. H. Hassasnpour et al tried fuzzy logic classification on principal component analysis and they reached 87% accuracy result [8]. M. Hu et al also published successful

approach based on principal component analysis [9]. In 2014, convolutional neural networks and support vector machine hybrid approach have been applied to determine the gender. 84% accuracy has been obtained in this article using Matlab programming [10]. T. Bissoon et al tested principal component analysis and linear discriminant analysis hybrid approach in their study, in 2013 [11]. At the end, support vector machines, principal component analysis, k-nearest neighbor and Fischer discriminant analysis algorithms have been used in [12].

2. APPLIED METHODS

In this article, we use FEI face data set. It has been collected in Artificial Intelligence laboratory-Brazil, 2006. According to the publications in this field; chap, eyebrow and distance between eyebrows are important features for gender recognition [13]. Therefore, we remove other parts from face images. Hair parts of face images also removed from faces. These images is used for feature extraction process of principal component analysis. We use k-nearest neighbor and support vector machine algorithms and compare the recognition results.

2.1 Principal Component Analysis (PCA)

Principal component analysis is one of the most used algorithm in image processing. The purpose of this method decrases the size of data without harm it. This is also called Karheunen-Loeve transform or Hotelling transform [14]. In this method, the projection is used to extract features. The variance is calculated and chosen with that direction. So, we can summarize it with these basic steps:

Let $W=\{X_1,X_2,X_3,X_4,\ldots\ldots,X_k\}$ is a sample data set, with each element X_k is NxN dimension. Firstly, mean of X is calculated with these formulas:

$$\mu_{\times} = \frac{1}{n}\left(\sum_{i=0}^{n} X_i\right) \qquad (2.1a)$$

$$\mu_{W} = \frac{1}{k}\left(\sum_{i=0}^{k} \mu_{\times_i}\right) \qquad (2.1b)$$

After finding the mean of data set, the axis is shifted by subtracting each element with mean value. Then, covariance matrix of new values is calculated. For example, if we have X values with amount of K, then covariance values will be $K!/[(K-2)! * 2]$. The covariance matrix is a symmetric and its diagonals give the variance of data X. Obtained this matrix coordinates contains all combinations of covariances. After that, eigenvalues and eigenvectors of covariance matrix is calculated :

$$[C - \lambda I] = 0 \qquad (2.2)$$

All eigenvalues of C covariance matrix and their correspondent eigenvectors is calculated with below equation:

$$[C - \lambda_{1\to k} I]\begin{bmatrix} \propto_1 \\ \vdots \\ \propto k \end{bmatrix}_{k,1} = 0 \qquad (2.3)$$

All lenghts of each eigenvectors are 1 and after this stage less important parts can be removed from data set. For this purpose, obtained eigenvalues and eigenvectors is organized from largest values to small values. Moreover, very small parts can be removed completely. Here, the largest value is chosen as first principal component. This process will make computations easy for covariance and finding eigenvector. The eigenvector matrix is obtained with organizing them from the minimum one to

maximum one. In this stage, small eigenvectors can be removed. So, the matrix can be formed.

$$[W]_{KxN^2}([C]^T)^{-1} = [\overline{W}]_{KxN^2} \qquad (2.4)$$

After that, when we use Eq. (2.4), new space is obtained. Data is converted the axis which names called first component and second component. In principal component analysis, each image is shown as row or column vector. This process can be called vectorization. We make computations with row vectors. Obtained matrix can be seen in Fig. 1.

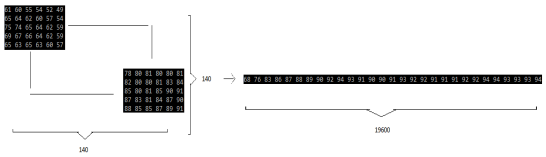


Figure 1. Forming a row vector with 140x140 size image
(Vectorization process)

After these conversion, data set wil be ready for implementing principal component analysis algorithm. Label is also ready for this process. After determining eigenvalues and eigenvectors, sample data is converted to new space. The largest 15 and 90 eigenvectors space has been chosen as two space.

2.2 Support Vector Machine (SVM) and k-nearest neighbor

In this study, we employ support vector machine and k-nearest neighbor classification algorithms. These are well known and widely used methods in machine learning area. Determining a line between two groups is main issue for support vector machine. It should be fitted according to data points. With this approach not only linear classification but also nonlinear classification can be implemented. On the other hand, k-nearest neighbor algorithm uses distance measures for classification with proper k

values [15]. But this method is very sensitive for distinct values. Classification is applied according to k values starting with 1 to other integer numbers. If the distance the same, in this condition one of class randomly selected [16].

3. EXPERIMENTAL RESULTS

We implement totally 400 faces from FEI face data set. k-fold cross-validation method is used to find error rate. We set this value as k=4. After reduction of dimension of data, we apply k-nearest neighbor algorithm. We show accuracy values for eigenvalues 15 and 30 in Table I. Mean recognition rates also can be seen from the table. We test the method 4 times and take their mean.

Figure 2. Organizing FEI face data set face images

The process on face images can be seen from Fig.2. Adjusting and preparing phases implemented on data set.

Experiments on k-nearest neighbor classifier show that 30 eigenvectors recognition is more successful than 15 eigenvectors. We can see this computations from Table 1.

k-fold cross validation method is also used for k-nearest neighbor algorithm to randomize the classification process and get their accuracies.

Table 1. The k-nearest neighbor accuracy rates for first 15 and 30 eigenvectors of FEI data set

KNN						
Eigenvector	k	TEST 1	TEST 2	TEST 3	TEST 4	MEAN
30	3	85	91	91	96	90.75
	4	85	89	86	93	88.25
	5	88	90	87	94	89.75
	6	86	85	83	93	86.75
	7	84	88	82	94	87
	8	86	87	82	92	86.75
	9	83	87	83	93	86.5
	10	84	86	83	91	86
	11	84	88	81	91	86
	12	83	88	81	92	86
	13	82	87	81	92	85.5
	MEAN	84.54	87.81	83.63	92.81	87.20
Eigenvector	k	TEST 1	TEST 2	TEST 3	TEST 4	MEAN
15	3	79	87	89	96	87.75
	4	77	85	86	93	85.25
	5	85	88	85	93	87.75
	6	83	85	85	92	86.25
	7	83	84	81	91	84.75
	8	83	82	81	90	84
	9	83	84	81	91	84.75
	10	83	84	82	92	85.25
	11	83	87	83	92	86.25
	12	81	85	83	91	85
	13	81	84	82	91	84.5
	MEAN	81.90909	85	83.45455	92	85.59

When we analyze the recognition results, number of eigenvectors is proportional to accuracies. But there is inverse proportion between k-values and accuracies. The highest accuracy is obtained for k=3. General recognition results reach their highest values at Test-4. At the end, we state that the recognition rate reach 85% for both eigenvector 15 and 30.

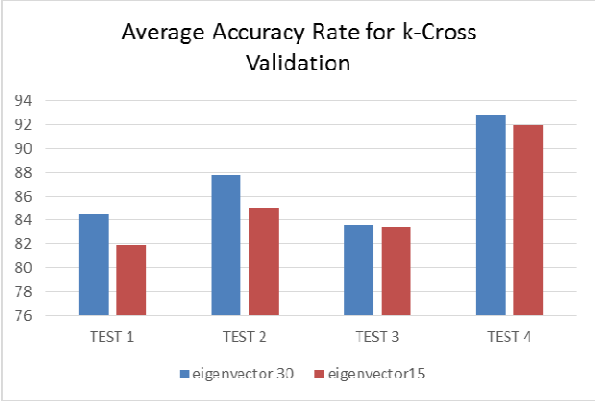
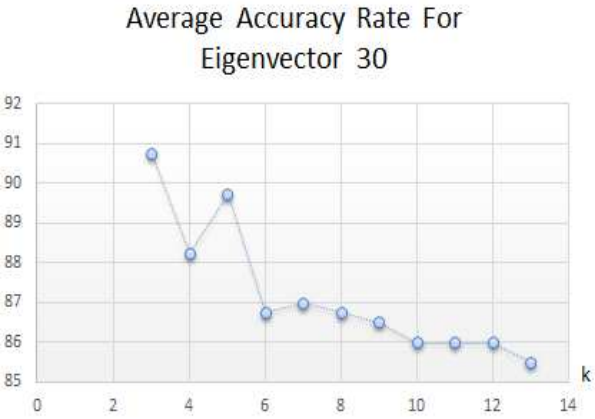


Figure 3. k-nearest neighbor classification rates graph for first 15 and 30 eigenvectors in FEI face data set.



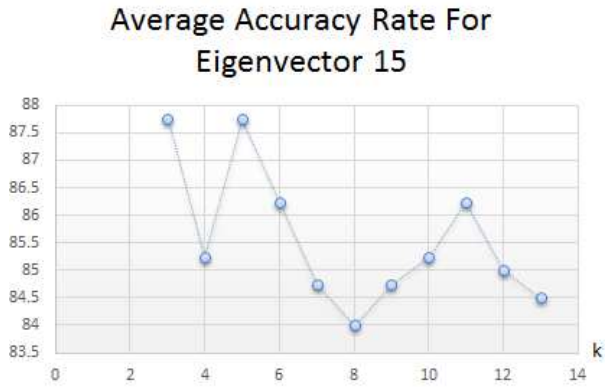


Figure 4. Classification accuracy rates according to k-values

Table 2. Support vector machine accuracy results for FEI face data set

Accuracy (%)				
0-80	80-160	160-240	240-320	320-400
85	85	75	77.5	82.5

Table 3. k-nearest neighbor and support vector machine accuracy results for FEI face data set

Accuracy (%)	
k-nearest neighbour	Support vector machine
86	80

When we compare the recognition performance of support vector machine and k-nearest neighbor, we can state k-nearest neighbor is more successful in accuracies about 6% (From Table 2 and Table 3).

5. CONCLUSION

In this article, we make gender classification to contribute image processing and machine learning research area. We analyze the advantages and disadvantages of techniques with previous published results. We focus

on determining gender on FEI face data set. Several conversions and pre-processing phases is used for the implementations. Some feature extraction and classification algorithms is tested on FEI. According to experimental results, we show that principal component analysis with k-nearest neighbor hybrid method is better than principal component analysis with support vector machine hybrid method. The main reason of this difference between two hybrid method is new space conversion of principal component analysis. The new places of converted data set via covariance matrix is more distinctive.

REFERENCES

[1] Hotelling, H.: Analysis of a complex of statistical variables into principal components, Journal of Educational Psychology, vol.. 24, (1933), 417–441 and 498–520.

[2] Alpaydın E.: Introduction to machine learning, The MIT Press, USA, (2015).

[3] Pearson, K.: On lines and planes of closest fit to systems of points in space, Philosophical Magazine, vol. 2, no.11, (1901), 559–572.

[4] Jain, A. ve Huang, J.: Integrating independent components and linear discriminant analysis for gender classification, International Conference on Automatic Face and Gesture Recognition, Seoul, Korea, (2004), 159-163.

[5] U. Turhal, A. Akbaş: Yüz örüntülerinden cinsiyet tespitinde hibrit özniteliklerle performans geliştirme, Elektrik-Elektronik ve Bilgisayar Sempozyumu, (2016), 361-365.

[6] Z. Sun, G. Bebis: X. Yuan, S. J. Louis, Genetic Feature Subset Selection for Gender Classification: A comparison study, IEEE Workshop on Applications
of Computer Visions, (2002), 165-170.

[7] L. Lu, P. Shi: A novel fusion-based method for expression-invariant gender classification, IEEE International Conference on Acoustic, Speech and Signal Processing, (2009) 1065-1068.

[8] H. Hasassnpour, H. Dehghan: Neonate facial gender classification using PCA
and fuzzy clustering, Iranian Conference of Biomedical Eng., (2010), 1-5.

[9] M. Hu, Y. Zheng, F. Ren, H. Jiang: Age estimation and gender classification
of facial images based on local directional pattern, IEEE International Conference on Cloud Computing and Intelligent Systems, (2014), 103-107.

[10] A. Verma, L. Vig: Using Convolutional Neural Networks to discover cognitively validated features for Gender Classification, International Conference on Soft Computing and Machine Intelligence, (2014), 33-37.

[11] T. Bissoon, S. Viriri: Gender classification using Face Recognition, International Conference on Adaptive Science and Technology, (2013), 1-4.

[12] S. A. Khan, M. Nazir, N. Naveed, N. Riaz: Efficient gender classification methodology using DWT and PCA, IEEE International Conference on Multitopic Conference, (2011), 155-158.

[13] R. Brunelli, T. Poggio: Hyber BF networks for gender classification, DARPA
Image Understanding Workshop, (1992).

[14] Pearson, K.: On lines and planes of closest fit to systems of points in space,
Philosophical Magazine 2 (6), (1901), 559-572.

[15] Fix, E., Hodges, J. L.: Discriminatory analysis nonparametric discrimination:
Consistency properties, Technical Report 4, (1951).

[16] Wiesner V., Evers L.: Statistical data mining, University of Oxford, (2004).

[17] Ozbudak O., "Gender classification from pictures of human faces", MSc thesis, Electronics and Communication Eng., Istanbul Technical University, (2009).

Journal of Naval Science and Engineering
2017, Vol. 13, No.1, pp.43-59
Gemi İnşa Mühendisliği/Marine Engineering

SUBMARINE SHELL ELEMENT STATIC LINEAR DEFORMATION ANALYSIS

İsmail BAYER [1]
Kerem YILMAZ [2]

[1]*Faculty of Naval Architecture and Marine Engineering, Yildiz Technical University, bayer@ytu.edu.tr,*
[2] *National Defense University Barbaros Naval Sciences and Engineering Institute, keremyilmaz6146@gmail.com*

Date of Receive: 01.03.2017 **Date of Acceptance: 24.03.2017**

ABSTRACT

In this paper; a submarine vessel's shell element's deformation has been investigated due to hydrotatic pressure. Eleven different pressure value for eleven depth has been accounted. A doubly curved shell element within different radius and different lenghts of edges is analysed by using numerical method solution of static linear equilibrium equation of shell element. In the solution part, Navier Solution method with double Fourier series is used for solution of final differantial equations. Identical shell element has been analysed in a package program ANSYSTM in order to verification of solution. Following of verification, cylindrical shell element has been analysed with numerical method. In numerical analysis a MATLABTM code is written for easy solution for different curvature radiuses and different lenghts of edges. After all solution analyses, stres components of shell elements has been compared with Turkis Loyd permitted stress components for design of a submarine. As a result, it's studied on deformation of isotropic shell element according to different length-thickness ratio and length values.

ÖZ

Bu makalede, dalmış durumdaki bir denizaltı kabuki elemanı üzerinde hidrostatik basınç nedeniyle oluşan deformasyonu incelenmiştir. On bir farklı derinlikteki basınç değeri için kabuki üzerinde oluşan deformasyon hesaplanmıştır. Denizaltıya ait çift taraflı eğimli bir kabuki eleman farklı eğrilik yarıçap değerleri ve farklı kenar uzunlukları için static lineer denge denklemlerinin sayısal çözümü ile deformasyon analizi yapılmıştır. Denge denklemlerinin çözümünde kurulan diferansiyel denklemlerin çözümünde Navier yöntemi ile çift Fourier serileri analizi kullanılmıştır. Yapılan çözümün kontrolü kapsamında yanı özelliklere sahip kabuk eleman ticari paket program ANSYSTM ile lineer deformasyon analizi yapılmıştır. Çözüm doğrulamanın ardından bir silindirik kabuki

elemanın aynı derinliklerdeki deformasyon analizi gerçekleştirilmiştir. Sayısal çözümler esnasında elde edilen deklemlerin çözümü için MATLABTM kodu kullanılmmıştır. Bu kod ile farklı eğrilik yarıçapları ve farklı kenar uzunlukları için kabuki elemanın deformasyon analizi kolaylaşmıştır. Tüm analizlerin devamında kabuki üzerinde meydana gelen gerilme bileşenleri Türk Loydu içerisinde denizaltı dizaynında izin verilen gerilme değerleri ile karşılaştırılmıştır. Sonuç olarak; izotropik bir denizaltı kabuğunun farklı eğrilik yarıçap ve kenar uzunlukları için deformasyon analizi yapılmıştır.

Keywords: *Thin shell, doubly curved shell, Fourier analysis, submarine shell, deformation of thin shell.*
Anahtar Kelimeler: *İnce kabuki, çift eğrili kabuki, Fourier analizi, Denizaltı kabuğu, İnce kabuki deformasyonu.*

1. INTRODUCTION

HY-80, HY-100 steels are used in submarine vessels widely. These steels are highly strong and durable under high pressures. Submarine vessels consist of shell elements. Shell elements of submarines are mostly take part in engineering as thin shells due to ratio of length and thickness. It's an important point to make deformation, buckling analysis in design section. For numerical problem solution of isotropic shell deformation analysis it's been seen the similar equations for static lineer equilibrium equation suggested by Köksal [1], Ventsel and Krauthammer [2].

2. PROBLEM DEFINITION

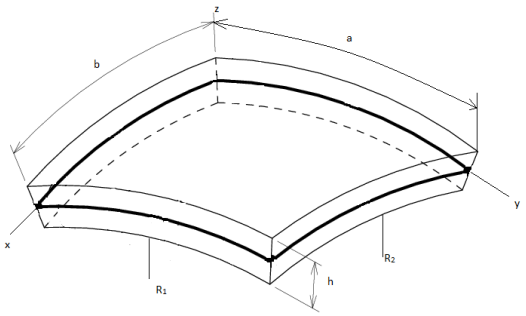


Figure 1. Doubly curved shell element

A doubly curved shell with R_1, R_2 curvature radiuses, a and b lengths of edges, h thickness values.

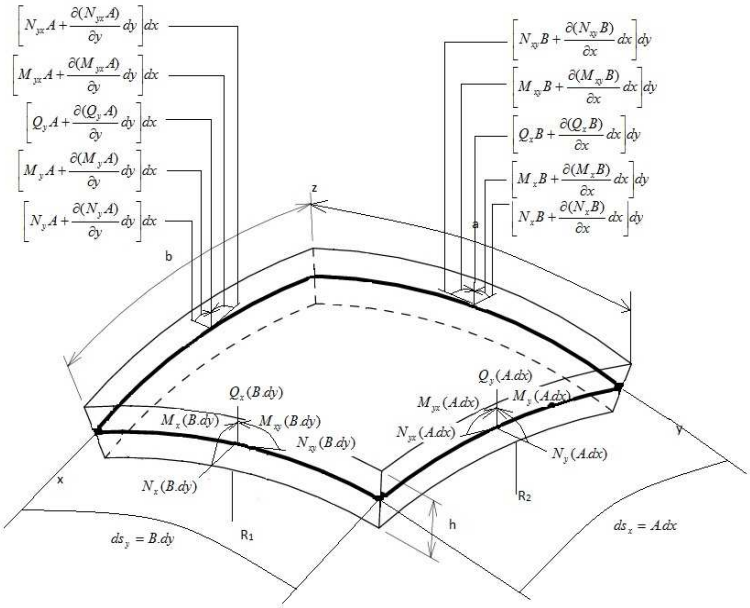


Figure 2. Forces and moments on shell element

All force and moment components take part in figure 2. N_x and N_y are normal force components, N_{xy} and N_{yx} are shear force components, M_x and M_y are bending moment components, Q_x and Q_y are shear force components.
When total forces and total moments are equated zero according to axis x,y and z, we get to equilibrium of shell element.

$$\frac{1}{AB}\left[\frac{\partial(N_x B)}{\partial x}+\frac{\partial(N_{xy}A)}{\partial y}-\frac{\partial B}{\partial x}N_y+\frac{\partial A}{\partial y}N_{xy}\right]-\frac{Q_x}{R_1}+q_x=0$$

$$\frac{1}{AB}\left[\frac{\partial(N_y A)}{\partial y}+\frac{\partial(N_{xy}B)}{\partial x}-\frac{\partial A}{\partial y}N_x+\frac{\partial B}{\partial x}N_{xy}\right]-\frac{Q_y}{R_2}+q_y=0$$

$$\frac{1}{AB}\left[\frac{\partial(Q_x B)}{\partial x}+\frac{\partial(Q_y A)}{\partial y}\right]+\frac{N_x}{R_1}+\frac{N_y}{R_2}+q_z=0$$

$$\frac{1}{AB}\left[\frac{\partial(M_x B)}{\partial x}-\frac{\partial B}{\partial x}M_y+\frac{\partial A}{\partial y}M_{xy}+\frac{\partial(M_{xy}A)}{\partial y}\right]-Q_x=0$$

$$\frac{1}{AB}\left[\frac{\partial(M_y A)}{\partial y}-\frac{\partial A}{\partial y}M_x+\frac{\partial B}{\partial x}M_{xy}+\frac{\partial(M_{xy}B)}{\partial x}\right]-Q_y=0$$

(1)

q_x, q_y and q_z symbolize the forces or loads according to axis. At this point; q_x and q_y equals zero since no force or load at these axis. In these equations; A and B are lame parameters for definition of surface form.
Eqs (1) can be eased by reducing five equation into three by replacing Q_x and Q_y components with M_x, M_y, M_{xy} components. In addition; derivations of lame parameters are negligible compared to force or moment derivations.

$$\frac{1}{AB}\left[\frac{\partial N_x}{\partial x}B+\frac{\partial N_{xy}}{\partial y}A\right]-\frac{1}{ABR_1}\left[\frac{\partial M_x}{\partial x}B+\frac{\partial M_{xy}}{\partial y}A\right]=0$$

$$\frac{1}{AB}\left[\frac{\partial N_y}{\partial y}A+\frac{\partial N_{xy}}{\partial x}B\right]-\frac{1}{ABR_2}\left[\frac{\partial M_y}{\partial y}A+\frac{\partial M_{xy}}{\partial x}B\right]=0$$

$$\frac{1}{AB}\left[B\left(\frac{\partial^2 M_x}{\partial x^2}\frac{1}{A}+\frac{\partial^2 M_{xy}}{\partial x\partial y}\frac{1}{B}\right)+A\left(\frac{\partial^2 M_y}{\partial y^2}\frac{1}{B}+\frac{\partial^2 M_{xy}}{\partial x\partial y}\frac{1}{A}\right)\right]+\frac{N_x}{R_1}+\frac{N_y}{R_2}+q_z=0$$

(2)

Let us replace N and M components with displacement components for solution of these equations. Isotropic shell linner elasticity relation for N and M components in the following equations.

$$\begin{Bmatrix} N_x \\ N_y \\ N_{xy} \\ M_x \\ M_y \\ M_{xy} \end{Bmatrix} = \begin{bmatrix} C & \nu.C & 0 & 0 & 0 & 0 \\ \nu.C & C & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1-\nu}{2}.C & 0 & 0 & 0 \\ 0 & 0 & 0 & D & \nu.D & 0 \\ 0 & 0 & 0 & \nu.D & D & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1-\nu}{2}.D \end{bmatrix} . \begin{Bmatrix} \varepsilon_x \\ \varepsilon_y \\ \gamma_{xy} \\ k_x \\ k_y \\ k_{xy} \end{Bmatrix}$$

$$C=\frac{Eh}{(1-\nu^2)}$$

$$D=\frac{Eh^3}{12(1-\nu^2)}$$

(3)

C represents elongation rigidity, D represents flexure rigidity, E is elasticity module, h is thickness of shell, v is poisson ratio. We can write the following equations for isotropic thin shell [1];

$$\varepsilon_x = \frac{1}{A}\frac{\partial u}{\partial x} + \frac{w}{R_1} \qquad k_x = -\frac{1}{A^2}\frac{\partial^2 w}{\partial x^2}$$

$$\varepsilon_y = \frac{1}{A}\frac{\partial v}{\partial y} + \frac{w}{R_2} \qquad k_y = -\frac{1}{B^2}\frac{\partial^2 w}{\partial y^2}$$

$$\gamma_{xy} = \frac{1}{B}\frac{\partial u}{\partial y} + \frac{1}{A}\frac{\partial v}{\partial x} \qquad k_{xy} = \frac{\partial^2 w}{\partial x \partial y}$$

Rewriting N and M components with given displacement and curvature equations.

$$N_x = C\left[\frac{1}{A}\frac{\partial u}{\partial x} + \frac{w}{R_1} + \nu\left(\frac{1}{B}\frac{\partial v}{\partial y} + \frac{w}{R_2}\right)\right]$$

$$N_y = C\left[\frac{1}{B}\frac{\partial v}{\partial y} + \frac{w}{R_2} + \nu\left(\frac{1}{A}\frac{\partial u}{\partial x} + \frac{w}{R_1}\right)\right]$$

$$N_{xy} = C\frac{1-\nu}{2}\left[\frac{1}{A}\frac{\partial v}{\partial x} + \frac{1}{B}\frac{\partial u}{\partial y}\right]$$

$$M_x = -D\left[\frac{1}{A^2}\frac{\partial^2 w}{\partial x^2} + \nu\left(\frac{1}{B^2}\frac{\partial^2 w}{\partial y^2}\right)\right]$$

$$M_y = -D\left[\frac{1}{B^2}\frac{\partial^2 w}{\partial y^2} + \nu\left(\frac{1}{A^2}\frac{\partial^2 w}{\partial x^2}\right)\right]$$

$$M_{xy} = -D(1-\nu)\left[\frac{\partial^2 w}{\partial x \partial y}\right]$$

(4)

Using Eqs (4) in Eqs (2) we get following equations.

$$\frac{C}{AB}\left[B\left(\frac{1}{A}\frac{\partial^2 u}{\partial x^2}+\frac{1}{R_1}\frac{\partial w}{\partial x}+v\left(\frac{1}{B}\frac{\partial^2 v}{\partial x\partial y}+\frac{1}{R_2}\frac{\partial w}{\partial x}\right)\right)+A\frac{1-v}{2}\left(\frac{1}{A}\frac{\partial^2 v}{\partial x\partial y}+\frac{1}{B}\frac{\partial^2 u}{\partial y^2}\right)\right]$$

$$-\frac{1}{R_1 AB}\left[-DB\left(\frac{1}{A^2}\frac{\partial^3 w}{\partial x^3}+v\left(\frac{1}{B^2}\frac{\partial^3 w}{\partial x\partial y^2}\right)\right)-DA(1-v)\frac{\partial^3 w}{\partial x\partial y^2}\right]=0$$

$$\frac{C}{AB}\left[A\left(\frac{1}{B}\frac{\partial^2 v}{\partial y^2}+\frac{1}{R_2}\frac{\partial w}{\partial y}+v\left(\frac{1}{A}\frac{\partial^2 u}{\partial x\partial y}+\frac{1}{R_1}\frac{\partial w}{\partial y}\right)\right)+B\frac{1-v}{2}\left(\frac{1}{A}\frac{\partial^2 v}{\partial x^2}+\frac{1}{B}\frac{\partial^2 u}{\partial x\partial y}\right)\right]$$

$$-\frac{1}{R_2 AB}\left[-DA\left(\frac{1}{B^2}\frac{\partial^3 w}{\partial y^3}+v\left(\frac{1}{A^2}\frac{\partial^3 w}{\partial x^2\partial y}\right)\right)-DB(1-v)\frac{\partial^3 w}{\partial x^2\partial y}\right]=0$$

$$\frac{1}{AB}\left\{\begin{array}{l}B\left[-D\frac{1}{A}\left(\frac{1}{A^2}\frac{\partial^4 w}{\partial x^4}+v\frac{1}{B^2}\frac{\partial^4 w}{\partial x^2\partial y^2}\right)+\frac{1}{B}\left(-D(1-v)\frac{\partial^4 w}{\partial x^2\partial y^2}\right)\right]\\+A\left[\frac{1}{B}\left(\frac{-D}{B^2}\frac{\partial^4 w}{\partial y^4}-Dv\frac{1}{A^2}\frac{\partial^4 w}{\partial x^2\partial y^2}\right)-\frac{1}{A}D(1-v)\frac{\partial^4 w}{\partial x^2\partial y^2}\right]\end{array}\right\}$$

$$+\frac{C}{R_1}\left[\frac{1}{A}\frac{\partial u}{\partial x}+\frac{w}{R_1}+v\left(\frac{1}{B}\frac{\partial v}{\partial y}+\frac{w}{R_2}\right)\right]+\frac{C}{R_2}\left[\frac{1}{B}\frac{\partial v}{\partial y}+\frac{w}{R_2}+v\left(\frac{1}{A}\frac{\partial u}{\partial x}+\frac{w}{R_1}\right)\right]=-q_z$$

(5)

3. DOUBLE FOURİER SERIES

Using double Fourier series with Naiver Solution on Simply-Supported elements. In Fourier series, assigning u,v and w displacements according to boundary condition with following series;

$$u(x,y)=\sum_{m=0}^{\infty}\sum_{n=1}^{\infty}U_{mn}\cos\alpha x\sin\beta y \qquad 0\le x\le a\ ,\ 0\le y\le b$$

(6.a)

$$v(x,y)=\sum_{m=1}^{\infty}\sum_{n=0}^{\infty}V_{mn}\sin\alpha x\cos\beta y \qquad 0\le x\le a\ ,0\le y\le b$$

(6.b)

$$w(x,y)=\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}W_{mn}\sin\alpha x\sin\beta y \qquad 0\le x\le a\ ,\ 0\le y\le b$$

(6.c)

In Eqs (6);

$$\alpha=\frac{m\pi}{a}$$

$$\beta=\frac{n\pi}{b}$$

Now the displacement values in Eqs (5) must be replaced with proper derivatives of Eqs (6).

Example for derivatives;

$$\frac{\partial^2 u}{\partial x^2}=-\sum_{m=0}^{\infty}\sum_{n=1}^{\infty}U_{mn}\alpha^2\cos\alpha x\sin\beta y$$

$$\frac{\partial^2 u}{\partial y^2}=-\sum_{m=0}^{\infty}\sum_{n=1}^{\infty}U_{mn}\beta^2\cos\alpha x\sin\beta y$$

After replacement final equations we obtain the following:

$$\sum_{m=1}^{\infty}\sum_{n=0}^{\infty}\sin\alpha x\cos\beta y\begin{Bmatrix} C\alpha\beta\left[-\frac{\nu}{AB}-\frac{(1-\nu)}{2AB}\right]U_{mn} \\ C\left[-\frac{\beta^2}{B^2}-\frac{(1-\nu)\alpha^2}{2A^2}\right]V_{mn} \\ \frac{C\beta}{B}\left[\frac{1}{R_2}+\frac{\nu}{R_1}\right]+\frac{D\beta}{R_2}\left[-\frac{\beta^2}{B^3}-\frac{\nu\alpha^2}{A^2B}-\frac{(1-\nu)\alpha^2}{A}\right]W_{mn} \end{Bmatrix}=0$$

$$\sum_{m=0}^{\infty}\sum_{n=1}^{\infty}\cos\alpha x\sin\beta y\begin{Bmatrix} C\left[-\frac{\alpha^2}{A^2}-\frac{(1-\nu)}{2B^2}\beta^2\right]U_{mn} \\ \frac{C\alpha\beta}{AB}\left[-\nu-\frac{(1-\nu)}{2}\right]V_{mn} \\ \frac{C\alpha}{A}\left(\frac{1}{R_1}+\frac{\nu}{R_2}\right)-\frac{D\alpha}{R_1}\left(\frac{\alpha^2}{A^3}+\frac{\nu\beta^2}{AB^2}+\frac{(1-\nu)\beta^2}{B}\right)W_{mn} \end{Bmatrix}=0$$

(7)

$$\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}\sin\alpha x\sin\beta y\begin{Bmatrix} C\alpha\left[-\frac{\nu}{AR_2}-\frac{1}{AR_1}\right]U_{mn} \\ C\beta\left[-\frac{\nu}{BR_1}-\frac{1}{BR_2}\right]V_{mn} \\ D\left[-\frac{\alpha^4}{A^4}-\frac{2\nu\alpha^2\beta^2}{A^2B^2}-\frac{2(1-\nu)\alpha^2\beta^2}{AB}-\frac{\beta^4}{B^4}\right] \\ +C\left[\frac{1}{R_1^{\,2}}+\frac{2\nu}{R_1R_2}+\frac{1}{R_2^{\,2}}\right]W_{mn} \end{Bmatrix}=-q_z$$

4. PROBLEM SOLUTION

In chapter 3 we have final equations need to be resolved (Eqs(7)). The Fourier coefficient W_{mn} gives us the deformation in axis z after solving W_{mn} with Navier Solution. In this step a MATLAB^{TM} code is created for solution Eqs (7) and W_{mn}. With similar geometric features same problem solved in ANSYS^{TM} with Shell91 input data to correct numerical solution. In the following table ANSYS^{TM} and MATLAB^{TM} results are located.

Table 1. Deformation analyse in ANSYS and MATLAB

		Deformation(mm)			
Depth (m)	*Hydrostatic pressure (kPa)*	**MATLAB**	**ANSYS**	**MATLAB**	**ANSYS**
		a/h=10 a/b=1		*a/h=15 a/b=1*	
100	1005.525	**0.456**	**0.482**	**1.600**	**1.630**
150	1508.2875	**0.685**	**0.723**	**2.401**	**2.445**
200	2011.05	**0.913**	**0.964**	**3.201**	**3.261**
250	2513.8125	**1.141**	**1.205**	**4.001**	**4.076**
300	3016.575	**1.370**	**1.446**	**4.802**	**4.891**
350	3519.3375	**1.598**	**1.687**	**5.603**	**5.707**
400	4022.1	**1.827**	**1.928**	**6.403**	**6.523**
450	4524.8625	**2.055**	**2.169**	**7.203**	**7.337**
500	5027.625	**2.283**	**2.410**	**8.004**	**8.153**
550	5530.3875	**2.512**	**2.652**	**8.805**	**8.969**
600	6033.15	**2.740**	**2.893**	**9.605**	**9.785**

The analysis made with length-thickness ratio; a/h=10, 15 values.It's seen that our numerical solution and ANSYS analysis results close enough to be sure that numerical solution is correct and valid. Now we can get the different curvature radiuses and different lengths of edges shell deformation results using numerical solution. Following tables contain these solutions.

Table 2. Solution of a/h=10,15,20 shell element deformations

		Deformation (mm)		
Depth (m)	*Hydrostatic pressure (kPa)*	*a/h=10 a/b=1*	*a/h=15 a/b=1*	*a/h=20 a/b=1*
100	1005.525	**0.456**	**1.600**	**4.009**
150	1508.2875	**0.685**	**2.401**	**6.015**
200	2011.05	**0.913**	**3.201**	**8.022**
250	2513.8125	**1.141**	**4.001**	**10.025**
300	3016.575	**1.370**	**4.802**	**12.031**
350	3519.3375	**1.598**	**5.603**	**14.038**
400	4022.1	**1.827**	**6.403**	**16.045**
450	4524.8625	**2.055**	**7.203**	**18.047**
500	5027.625	**2.283**	**8.004**	**20.054**
550	5530.3875	**2.512**	**8.805**	**22.060**
600	6033.15	**2.740**	**9.605**	**24.067**

Table 3. Solution of a/h=10-a/b=1,0.8 and a/h=15-a/b=1,0.8 shell element deformations

		Deformation (mm)			
Depth (m)	*Hydrostatic pressure (kPa)*	*a/h=10 a/b=1*	*a/h=10 a/b=0.8*	*a/h=15 a/b=1*	*a/h=15 a/b=0.8*
100	1005.525	**0.456**	**0.689**	**1.600**	**2.464**
150	1508.2875	**0.685**	**1.034**	**2.401**	**3.698**
200	2011.05	**0.913**	**1.379**	**3.201**	**4.931**
250	2513.8125	**1.141**	**1.723**	**4.001**	**6.162**
300	3016.575	**1.370**	**2.068**	**4.802**	**7.396**
350	3519.3375	**1.598**	**2.413**	**5.603**	**8.629**
400	4022.1	**1.827**	**2.758**	**6.403**	**9.863**
450	4524.8625	**2.055**	**3.103**	**7.203**	**11.094**
500	5027.625	**2.283**	**3.448**	**8.004**	**12.347**
550	5530.3875	**2.512**	**3.793**	**8.805**	**13.561**
600	6033.15	**2.740**	**4.138**	**9.605**	**14.794**

Table 4. Solution of a/h=20 and a/b=1,0.8 shell element deformations

		Deformation (mm)	
Depth (m)	*Hydrostatic pressure (kPa)*	*a/h=20 a/b=1*	*a/h=20 a/b=0.8*
100	1005.525	**4.009**	**6.369**
150	1508.2875	**6.015**	**9.557**
200	2011.05	**8.022**	**12.745**
250	2513.8125	**10.025**	**15.927**
300	3016.575	**12.031**	**19.115**
350	3519.3375	**14.038**	**22.303**
400	4022.1	**16.045**	**25.491**
450	4524.8625	**18.047**	**28.673**
500	5027.625	**20.054**	**31.861**
550	5530.3875	**22.060**	**35.049**
600	6033.15	**24.067**	**38.237**

These results are for isotropic doubly curved shell element. Now in the following table we have a cylindrical shell element deformation results.

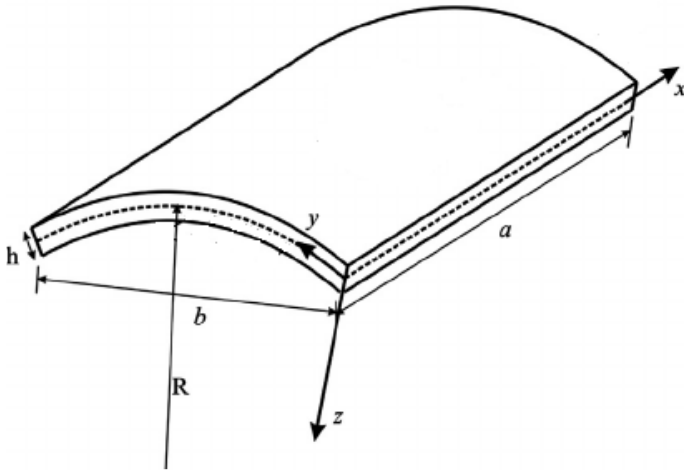


Figure 3. A cylindrical shell element

Table 5. Solution of a/h=10-a/b=1,0.8 and a/h=15-a/b=1,0.8 cylindrical shell element deformations

		Deformation(mm)			
Depth (m)	*Hydrostatic presure (kPa)*	*a/h=10 a/b=1*	*a/h=10 a/b=0.8*	*a/h=15 a/b=1*	*a/h=15 a/b=0.8*
100	1005.525	**1.608**	**1.608**	**5.427**	**5.429**
150	1508.2875	**2.413**	**2.413**	**8.144**	**8.146**
200	2011.05	**3.218**	**3.219**	**10.860**	**10.864**
250	2513.8125	**4.021**	**4.022**	**13.572**	**13.579**
300	3016.575	**4.826**	**4.827**	**16.288**	**16.294**
350	3519.3375	**5.631**	**5.632**	**19.005**	**19.013**
400	4022.1	**6.436**	**6.438**	**21.721**	**21.729**
450	4524.8625	**7.239**	**7.241**	**24.432**	**24.441**
500	5027.625	**8.044**	**8.046**	**27.149**	**27.158**
550	5530.3875	**8.849**	**8.852**	**29.866**	**29.876**
600	6033.15	**9.654**	**9.657**	**32.582**	**32.593**

5. PERMITTED STRESSES

Submarine design criterion Türk Loydu Part E Chapter 111-Naval Ship Technology, Submarines (2007) gives the permitted stresses on submarine hull. According to Türk Loydu rules, permitted stresses can be found with following instructions.

$\frac{R_{m,20}}{A^1}$ and $\frac{R_{eH,t}}{B^1}$ $R_{m,20}$ is maximum tensile strength [N/mm^2], $R_{eH,t}$ is yield point or %0.2 proof stress [N/mm^2]. A^1 and B^1 are safety coefficients[6]. The lower one is used for permitted stresses.
For HY-100 steel [6], [7];
$R_{m,20}$=820 MPa
$R_{eH,t}$=690 MPa
A^1=2.7
B^1=1.7

$$\frac{R_{m.20}}{A^1} = 303.7 MPa$$

$$\frac{R_{eH,t}}{B^1} = 405.8 MPa$$

Permitted stress=303.7 MPa

We need to determine the maximum stresses on each depth. Determined maximum stresses for three different length-thickness ratio are in the following table.

Table 6. Maximum stresses accordint to a/h=10,15,20

		Maxiumum stresses (MPa)		
Depth (m)	*Hydrostatic pressure (kPa)*	*a/h=10*	*a/h=15*	*a/h=20*
100	1005.525	**22.61**	**66.79**	**187.56**
150	1508.2875	**33.93**	**100.09**	**281.44**
200	2011.05	**45.25**	**133.48**	**375.23**
250	2513.8125	**56.54**	**166.80**	**469.51**
300	3016.575	**67.67**	**200.18**	**564.21**
350	3519.3375	**78.81**	**233.57**	**658.42**
400	4022.1	**89.12**	**266.96**	**752.76**
450	4524.8625	**91.56**	**300.28**	**844.33**
500	5027.625	**113.11**	**333.65**	**938.80**
550	5530.3875	**124.32**	**366.92**	**1033.12**
600	6033.15	**135.74**	**400.44**	**1126.29**

It can be seen in foregoing table;

- For a/h=10; 303.7 MPa permitted stress value is not exceeded,
- For a/h=15; at 500m, 550m and 600m depths permitted stress is exceeded.
- For a/h=20; after 150m depth permitted stress is exceeded.

6. CONCULUSION AND RECOMMENDATIONS

In this paper submersed submarine shell deformation has been investigated due to hydrostatic pressure. Deformation analysis are made for isotropic doubly curved and cylindrical shell element. Neglecting lame parameters derivatives in numerical solution facilitated problem and neglecting did not influence the result that seen at numerical solution and FEM analysis comparison. In relation to deformation investigation of doubly curved shell element, emerging stress components in our problem compared with permitted stresses in Türk Loydu Rules. About this comparison, different exceeding occurred at different length-thickness ratio of shell element that tells us the importance of determination thickness of the shell.

REFERENCES

1) Köksal, E., Köksal, M.K., Kabuk ve Plakların Statik Stabilite ve Dinamik Analizi Örnek Çözümler ve Tablolar, Literatür Yayıncılık, İstanbul.

2) Ventsel, E., Krauthammer, T., (2001). Thin Plates and Shells Theory, Analysis and Applications, Marcel Dekker, Inc., New York-Basel.

3) Timoshenko, S. ve Woinowsky-Krieger, S., (1959). Theory of Plates and Shells, McGraw-Hill Book Co..

4) Alankaya, V., (2011). Süreksiz Sınır Şartları Etkisindeki Katmanlı Kompozit Kabukların Yüksek Mertebeli Kayma Deformasyon Teorisi ile Analizi, Doktora Tezi, YTÜ Fen Bilimleri Enstitüsü, İstanbul.

5) Goldenveizer, A.L., (1961). Theory of Elastic Thin Shells, Pergamon Press Ltd., London.

6) Türk Loydu Part E Chapter 111-Naval Ship Technology, Submarines (2007).

7) Ritter, J.C. ve Baldwin, N.J. (1988), Properties of HY-100 Steel For Naval Construction, DSTO, Melbourne

Journal of Naval Science and Engineering
2017, Vol. 13, No.1, pp.60-72
Savunma Bilimleri/Defense Sciences

PROHIBITION AGAINST THE USE OF FORCE AND THE COERCIVE USES OF THE CYBERSPACE

Hakan Selim CANCA[1]

Social Sciences Department
National Defense University, Turkish Naval Academy, Tuzla, Istanbul
hcanca@dho.edu.tr

Date of Receive: 01.02.2017 **Date of Acceptance: 19.03.2017**

ABSTRACT

The use of force is resorted by States as a form of dispute settlement generally as a last resort. But Article 2(3) of the United Nations (UN) Charter states that all members shall settle their international disputes by peaceful means. Article 2(4) bans the unilateral use or threat of force by States. In the customary international law, Article 2(4) is interpreted as a prohibition against the use of force focusing on restricting the use of military instruments. This instrument-based interpretation of the use of force causes the responsibility of States which deploys cyber instruments to cause physical damage in the target States' critical infrastructures, remain outside the scope of Article 2(4).

There are doctrinal difficulties in examining current international law on use of force and self-defense in cyberspace, while the legal frameworks for defining the parameters of operations in cyberspace are not clear. As being unforseen until this age of information and cyber technology, the prohibition of the use of force interpreted from Article 2(4) should be evolved to cover coercive uses of cyber instruments being used to have destructive effects in the enemy's physical infrastructures such as telecommunications, transportation, power systems, finance and emergency services.

Categorizing the cyber attacks as having physical effects to critical infrastructure and not having any physical effects can be the first step to solve the problem of evolving the article to cover cyber attacks within the concept of use of force. Then the efforts may be concentrated on the cyber attacks having physical effects on the enemy's infrastructures to be considered as a use of force. The main problem is that there would be an unwillingness of the powerful States which are

[1] Assistant Professor of Law, Commander (Navy), Head of Social Sciences Department, National Defense University, Turkish Naval Academy-Istanbul, hakancanca@gmail.com. All the opinions, considerations, proposals and mistakes in this text belong to the writer and do not reflect any opinion, consideration, proposal or policy of any institution. All the informations in this text are provided from unclassified sources. While every effort has been made to ensure that the information contained in this text correct, neither the author nor the publisher can accept any responsibility for any errors or omissions or for any consequences arising therefrom.

likely to use the opportunities of cyberspace in Inter-State coercion to evolve the interpretation of the article, while the technology-dependent or powerless States would have a volition to evolve the Article.

ÖZ

Kuvvet kullanımına, devletler tarafından anlaşmazlıkların çözümünde genellikle son çare olarak başvurulmaktadır. Ancak Birleşmiş Milletler Şartının 2(3) maddesinde, tüm taraf devletlerin uluslararası anlaşmazlıklarını barışçı yollarla çözmesi gerektiği ifade edilmektedir. Madde 2(4), devletler tarafından tek taraflı kuvvet kullanımı ya da kuvvet kullanma tehdidinde bulunulmasını yasaklamaktadır. Uluslararası örf adet hukukunda Madde 2(4), askeri araçların kullanımını kısıtlamaya odaklanan bir kuvvet kullanımı yasağı olarak yorumlanmaktadır. Kuvvet kullanımı yasağına ilişkin söz konusu araç-temelli yorum, hedef devletlerin kritik tesisleri üzerinde fiziksel hasara neden olacak şekilde siber araçları kullanan devletlerin sorumluluklarının Madde 2(4)'ün kapsamı dışında kalmasına neden olmaktadır.

Siber uzayda kuvvet kullanımı ve meşru müdafaaya ilişkin mevcut uluslararası hukukun incelenmesinde doktrinsel güçlükler olmakla birlikte, siber uzayda yürütülen harekatların parametrelerinin tanımlanmasına ilişkin hukuki çerçeveler de açık değildir. Günümüz bilgi ve siber teknoloji çağına kadar göz önüne alınmamış olmakla beraber, Madde 2(4)'te söz konusu kuvvet kullanma yasağı, siber araçların, düşmanın telekomünikasyon, ulaştırma, güç sistemleri, finans ve acil durum servisleri gibi fiziki altyapısına yıkıcı etkiler meydana getirecek şekilde cebri kullanımını da kapsayacak şekilde yeniden düzenlenmelidir.

Siber saldırıların kritik altyapılar üzerinde fiziksel etkileri olanlar ve olmayanlar şeklinde kategorize edilmesi, söz konusu maddenin kuvvet kullanımı konsepti kapsamında siber saldırıları kapsayacak şekilde yeniden düzenlenmesi probleminin çözümü için ilk adım olabilir. Daha sonra çabalar, düşman altyapısı üzerinde fiziksel etkileri olan siber saldırıların kuvvet kullanımı olarak kabul edilmesi üzerinde yoğunlaştırılabilir. Temel sorun, teknoloji bağımlı veya güçsüz devletlerin, maddenin yeniden düzenlenmesi konusunda istekli olacak olmalarına rağmen, devletler arası zorlama yöntemi olarak siber uzay fırsatlarını kullanma ihtimali olan güçlü devletlerin, maddenin yeniden düzenlenmesi konusunda isteksiz davranacak olmalarıdır.

Keywords: *Use of Force, Self Defence, Cyberspace, Cyber Attacks, Cyberspace Operations, Act of Aggression.*

Anahtar Kelimeler: *Kuvvet Kullanımı, Kuvvet Tehdidi, Meşru Müdafaa, Siber Uzay, Siber Saldırı, Siber Uzay Harekatları, Saldırı Eylemi.*

1. Introduction

States are willing to keep the cyberspace open for the social, economic and security interests of their country and their citizens. Everyday we see that all aspects of life are getting more dependent to cyber instruments. While the use of the cyberspace is getting more comprehensive, the vulnarability of States increases because of the exploitation of the cyber instruments. It is a big question whether a State can use armed forces in self defense under a cyber attack to its critical infrastructures. There are doctrinal difficulties in examining current international law on use of force and self-defense in cyberspace, while the legal frameworks for defining the parameters of operations in cyberspace are not clear.

2. Definition of Cyberspace

Definiton of various cyber capabilities and aspects of cyberspace is important to develop policies, doctrines and responses for the use of cyber capabilities. Current U.S. Department of Defense Dictionary of Military and Associated Terms defines the term "cyberspace" as "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." The term "cybersecurity" is also defined in this doctrine as "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."[2]

The international community and all States shall clearly define the terms like cyberspace, cybersecurity and cyberattack to develop successfull strategies to handle with the gaps while securing the crucial infrastructures and the public uses of internet. Characterizing

[2] The doctrine defines the term "cyberspace operations" as "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."; U.S. Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, 8 November 2010 (As Amended Through 15 February 2016), p.57-58, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, last visited April 17, 2016.

the cyber activity will lead to determine the organizations having authority to conduct any activity, funds that may be used to pay for the resources and operations, oversight procedures applicable to the activity and approval procedures.[3]

3. The Prohibition Against the Use of Force

The question whether the *jus ad bellum* and the *jus in bello*[4] bodies of law apply to the activities in cyberspace needs to be considered very carefully. But we can say that the *jus ad bellum* as currently structured is inadequate in containing and responding to the strategic threat posed by cyber capabilities to international peace and security.[5]

Article 2(3) of the United Nations (UN) Charter states that all members shall settle their international disputes by peaceful means. But the use of force is resorted by States as a form of dispute settlement generally as a last resort. Article 2(4) bans the unilateral use or threat of force by States providing "The Organization and its members, in pursuit of the purposes stated in Article 1, shall act in accordance with the following principles: .... (4) All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations."[6]

In the customary international law, Article 2(4) is interpreted as a prohibition against the use of force focusing on restricting the use of military instruments. This instrument-based interpretation of the

---

[3] Commander Todd C. Huntley, "Controlling the Use of Force in Cyberspace: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare", Naval Law Review, Vol.60, 2010, p.6.

[4] *jus in bello* are the principles designed to limit suffering and destruction once an armed conflict has begun, and *jus ad bellum* are the principles governing when a State may legitimately use force. The term *"law of armed conflict"* includes both *jus ad bellum* and *jus in bello* principles.

[5] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law*, Vol.37, 1999, p.885.

[6] Article 2(4), U.N. Charter, http://www.un.org/en/sections/un-charter/chapter-vii/, last visited April 17, 2016.

use of force causes the responsibility of States which deploys cyber instruments to cause physical damage in the target States' critical infrastructures, remain outside the scope of Article 2(4).

The U.N. Charter also recognizes two different instances in which a State may use force:

The first instance is explained by Articles 39, 41 and 42 of the Charter. Article 39 states that "The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security."[7] Article 41 provides that "The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."[8] If the measures listed in Article 41 are inadequate or have proved to be inadequate, the Security Council, pursuant to Article 42, "may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security and such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations."[9]

The second instance where a State may also use force is to defend itself and others against an armed attack. Article 51 of the Charter states that "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take

[7] Article 39, U.N. Charter, loc.cit.

[8] Article 41, U.N. Charter, loc.cit.

[9] Article 42, U.N. Charter, loc.cit.

at any time such action as it deems necessary in order to maintain or restore international peace and security."[10] Thus, the use of force by States in individual or collective self-defense is recognized by the Charter. Article 51 limits the use of force in self-defense only if an armed attack occurs.

4. Cyber Attacks and the Prohibition Against the Use of Force

Whether a cyber attack constitutes a use of force is a complex issue. At the same time, it is very difficult to attribute cyber attacks to a specific individual, organization or State or a geographic location. Any removal or replication of valuable economic information and other forms of cyber espionage and exploitation in this area continue to remain outside the *jus ad bellum*.[11] Using the cyberspace to cyber espionage, manipulation of financial or personal data in a financial system, gain access to the control systems of critical infrastructure facilities, etc. may not reach to a level of use of force but they may cause greater damage to the security of any State or to the collective securty of the international community.

In the document named "An Assessment of International Legal Issues in Information Operations"[12] and published by the U.S. Department of Defense Office of General Councel which is dated May 1999, briefly explanations are given about "International Law Concerning the Use of Force among Nations", "Application to Computer Network Attacks" and "An "Active Defense" against Computer Network Attacks". After these explanations in this document, there is an assessment about "International Legal Regulation of the Use of Force In Peacetime" as:

> "It is far from clear the extent to which the world community will regard computer network attacks as "armed attacks" or

[10] Article 51, U.N. Charter, loc.cit.

[11] Jack M. Beard, "Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law", Vanderbilt Journal of Transnational Law, Vol.47, 2014, p.131.

[12] An Assessment of International Legal Issues in Information Operations, http://www.au.af.mil / au / awc / awcgate / dod-io-legal / dod-io-legal.pdf; last visited April 17, 2016.

> "uses of force," and how the doctrines of self-defense and countermeasures will be applied to computer network attacks. The outcome will probably depend more on the consequences of such attacks than on their mechanisms. The most likely result is an acceptance that a nation subjected to a State-sponsored computer network attack can lawfully respond in kind, and that in some circumstances it may be justified in using traditional military means in self-defense. Unless the nations decide to negotiate a treaty addressing computer network attacks, which seems unlikely anytime in the near future, international law in this area will develop through the actions of nations and through the positions the nations adopt publicly as events unfold. U.S. officials must be aware of the implications of their own actions and statements in this formative period."[13]

By this assessment it is underlined that the international community is not clear about the computer network attacks to be defined as armed attacks or use of force as prohibited by the Article 2(4) of the U.N. Charter. The U.S. officials are also noticed to be aware of the implications of their actions and statements during this period of which there is no exception in the near future about nations to negotiate a treaty addressing computer network attacks.

Commander Huntley of U.S. Navy argues that today the majority of cyber attacks conducted do not rise to a level of a use of force or an armed attack and continues: "There is a general agreement that for a cyber attack to be considered as an armed attack, the consequences of the cyber activity must be equivalent to those of a kinetic attack, that is, the activity must cause physical damage, injury or death. Such an attack would justify the use of armed force by the victim in self-defense, with the accompanying duty to abide by law of armed conflict (LOAC) in the use of that force. A State that found itself the victim of a cyber attack equivalent to a use of force, but not an armed attack, would be prohibited from using force to defend itself,

[13] An Assessment of International Legal Issues in Information Operations, http://www.au.af.mil / au / awc / awcgate / dod-io-legal / dod-io-legal.pdf; last visited April 17, 2016, p.27.

but might take diplomatic or economic measures in response to the activity."[14]

So one State under a cyber attack should consider the level of the attack and give reaction depending on the level of that attack. An entry into computer systems to obtain and observe information without causing any effect resulting destruction or modification of the system does not constitute either an armed attack or use of force, while it may constitute a violation of the territorial integrity of the State of the target computer or system.[15] So in specific circumstances in cyberspace it is very hard to determine that a cyber attack constitutes an armed attack or use of force.

Cyber threats have fundamentally different nature. In most of the cyber intrusion cases the responsible persons or organizations cannot be identified. In some cases the general geographic location from where the malicious activity eminated can be identified but one cannot be sure whether the activity had been routed through that location in an effort to shift blame or throw off investigators.[16]

Cyberspace also facilitates information operations such as psychological operations and military deception. The term "information operations" is defined in the U.S. Department of Defense Dictionary of Military and Associated Terms as "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[17]

When a multi-week wave of cyberattacks in April to May 2007 disrupted the websites of the Estonian President and Parliament, the vast majority of Estonian ministries, three of the country's six largest

[14] Huntley, op.cit., p.43.

[15] CDR Vida M. Antolin-Jenkins, Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?", Naval Law Review, Vol.51, 2005, p.9.

[16] Huntley, op.cit., p.12.

[17] U.S. Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, 8 November 2010 (As Amended Through 15 February 2016), p.110, http://www.dtic.mil / doctrine / new_pubs / jp1_02.pdf, last visited April 18, 2016.

news organizations, and two of its major banks, the country shut down.[18]

The Stuxnet event showed us how a malware can gain control, target or destroy a critical infrastructure without using any kinetic weapons. The discovery of a malware that targeted the control systems at the Natanz nuclear facility of Iran was reported in June 2010. A malware called Stuxnet which was a 500-kilobyte computer worm had infected the software of at least 14 industrial sites in Iran, including a uranium-enrichment plant.[19] The worm attacted in three phases. In the first phase, it targeted Windows machines and networks, repeatedly replicating itself. In the second phase, it sought out Windows-based Siemens software, which is used to program industrial control systems that operate equipment such as centrifuges. In the last phase, the worm compromised the programmable logic controllers and thus, unbeknownst to the human operators at the plant, the worm's authors could spy on the industrial systems and cause the fast-spinning centrifuges to tear themselves apart.[20]

Stuxnet was designed and executed as a direct malware attack[21] targeting specific software or information technology. The other type of malware attack targets specific company or organization. Stuxnet's payload targeted specific Supervisory Control and Data Acquisition Systems (SCADA Systems).[22] Stuxnet's attack occured in diffirent approaches: a. Taking control of the centrifuge systems and begin to spin them faster and slower to crack and destroy them; b. Taking control of the nuclear fuel cascade process and begin to manipulate the process causing damage to the system; c. Deceiving

---

[18] Kelly A. Gable, "Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent", Vanderbilt Journal of Transnational Law, Vol.43, 2010, p.61.

[19] David Kushner, "The Real Story of Stuxnet; How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program"; http:// spectrum.ieee.org / telecom / security / the-real-story-of-stuxnet, erişim tarihi: 13.04.2016.

[20] loc.cit.

[21] A targeted attack is designed to attack a specific unit. A direct attack is designed to attack a single system within a specific unit.

[22] Andrew Moore, "Stuxnet and Article 2(4)'s Prohibition Against the Use of Force: Customary Law and Potential Models", Naval Law Review, Vol.64, 2015, p.2.

the engineers in the control room by sending them false data; d. Compromising digital safety systems preventing the automated systems from halting an unsafe process.[23] Thus, through the attacks of Stuxnet, the centrifuge systems and fuel cascade systems got out of control; the engineers in the control room got false data and digital safety systems compromised.

All unauthorized cyber activities are commonly referred by the terms "cyber warfare" or "cyber attack", regardless of the nature of the activity, the consequences of the activity or the person conducting the activity.[24] Current legal regimes fail to explain the legal framework to provide guidance to any State's offensive cyber operations or responses to cyber attacks. The law of armed conflict[25] do not adequately deter the States or non-State actors from using cyber attacks and intrusions to pursue their interests in a manner harmful to the national interests of another State.

The critical point is what will happen if such a complex and sophisticated malware attack would be created, tested and monitored in a well-coordinated manner by a terrorist organization or by a terror-sponsoring State? The international community shall deal with such an important issue.

All States shall investigate their cyberspace infrastructure and develop a cyber security strategy in order to prevent any attack towards critical infrastructure, networks and systems. After U.S. President Obama took office, his first acts was to order a comprehensive sixty-day review of U.S. cyberspace policy.[26]

[23] ibid, p.3.

[24] Huntley, op.cit., p.3-4.

[25] In the "U.S. Department of Defense Dictionary of Military and Associated Terms", the terms "law of armed conflict" and "law of war" are defined as "That part of international law that regulates the conduct of armed hostilities" and the term "rules of engagement" is defined as "Directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered. Also called ROE.", U.S. Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, 8 November 2010 (As Amended Through 15 February 2016), p.139, 207, http://www.dtic.mil / doctrine / new_pubs / jp1_02.pdf, last visited April 17, 2016.

[26] White House Press Statement, President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review (Feb. 9, 2009)

Furthermore the U.S. Congress introduced three different bills addressing various aspects of cyber security in April 2009.[27] The developed States shall aid the technology-dependent States to counter cyber attacks and intrusions to provide collective security throughout the globe.

5. Conclusion

As being unforseen until this age of information and cyber technology, the prohibition of the use of force interpreted from Article 2(4) should be evolved to cover coercive uses of cyber instruments being used to have destructive effects in the enemy's physical infrastructures such as telecommunications, transportation, power systems, finance and emergency services. Categorizing the cyber attacks as having physical effects to critical infrastructure and not having any physical effects can be the first step to solve the problem of evolving the article to cover cyber attacks within the concept of use of force. Then the efforts may be concentrated on the cyber attacks having physical effects on the enemy's infrastructures to be considered as a use of force.

The main problem is that there would be an unwillingness of the powerful States which are likely to use the opportunities of cyberspace in Inter-State coercion to evolve the interpretation of the article, while the technology-dependent or powerless States would have a volition to evolve the Article.

The international community has much work to do in developing an international legal framework dealing with the cyber instrument threatening the security throughout the world. Cyber attacks continuously occur in daily bases not reaching to the level of use of force. States may not realize the real threat of a cyber attack until a critical situation occurs.

The international legal framework can be developed to reach to a point that enable States to use armed forces dealing with the threats

---

available at http://www.whitehouse.gov / the_press_office / advisorstoconductimmediate-cybersecurityreview/.; Huntley, op.cit., p.1.

[27] Ben Bain, Lawmakers Attack Cybersecurity on Multiple Fronts, Federal Computer Week, May 1, 2009, available at http://www.fcw.com / Articles / 2009/05/04/ news-congress-cybersecurity.aspx.; Huntley, loc.cit.

of cyber attacks, but this approach may lead to more complex situations and violent actions. Thus the mechanism to deal with the malicious uses of cyberspace should cover the operations made in the basis of cyberspace. The U.N. and other affiliated international organizations must deal with cyber warfare and develop strategies to prevent the malicious uses of the cyberspace. Very rapid mechanisms must be developed by the Security Council to react to cyber attacks intended to be used to threat the security of an individual State or the collective security of the international community.

REFERENCES

[1] Andrew Moore, "Stuxnet and Article 2(4)'s Prohibition Against the Use of Force: Customary Law and Potential Models", ***Naval Law Review***, Vol.64, 2015, p.1-25.

[2] Jack M. Beard, "Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law", ***Vanderbilt Journal of Transnational Law***, Vol.47, 2014, p.131.

[3] Kelly A. Gable, "Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent", ***Vanderbilt Journal of Transnational Law***, Vol.43, 2010, p.61.

[4] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", ***Columbia Journal of Transnational Law***, Vol.37, 1999, p.885.

[5] Todd C. Huntley, "Controllıng the Use of Force in Cyberspace: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare", ***Naval Law Review***, Vol.60, 2010, p.1-40.

[6] Vida M. Antolin-Jenkins, Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?", ***Naval Law Review***, Vol.51, 2005, p.9.

[7] An Assessment of International Legal Issues in Information Operations , http://www.au.af.mil / au / awc / awcgate / dod-io-legal / dod-io-legal.pdf; last visited April 17, 2016.

[8] David Kushner, "The Real Story of Stuxnet; How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program"; http:// spectrum.ieee.org / telecom / security / the-real-story-of-stuxnet, erişim tarihi: 13.04.2016.

[9] U.S. Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, 8 November 2010 (As Amended Through 15 February 2016), p.57-58, http://www.dtic.mil / doctrine / new_pubs / jp1_02.pdf, last visited April 17, 2016.