SWISS GERMAN UNIVERSITY

MASTER OF INFORMATION TECHNOLOGY

THE ANNUAL MIT CONFERENCE

Applied Research and Innovation Empowers and Inspires People towards Economic Growth

April 30, 2016

Volume 3

Preface

Serpong, Swiss German University, 30th of April 2016

In the name of God The Most Supreme and Most Merciful,

It is with great honour that the Annual Conference on Management and Information Technology a.k.a. ACMIT is conducted to reach the highest academic achievement and research contribution. At this moment I am standing here, on behalf of esteemed ACMIT Committee, would like to honourably greet our keynote speakers, special guests, lecturers, students and friends, hence, we will enjoy our achievement and endless learning journey together. Congratulations to you all and thank you for such valuable opportunities, efforts and supports given.

The theme of research, i.e. "Applied Research and Innovation Empower and Inspire People towards Economic Growth" is selected rigorously; therefore, we would set ourselves to achieve research focusing toward innovations where applicable and benefitting the society, international community, particularly Indonesia. Eventually creative innovations obtained from research would then generate business and industries in which strengthen the economy.

This year we have succeeded in papers being submitted; almost 300 % increased from previous years ACMIT. Now we can all celebrate it in ACMIT 2016. Thank God … Big applause to everyone who has contributed. We have accepted this year in ACMIT 35 papers. Some have been categorized as poster papers. Though this situation perhaps not yet met our expectation; however, we should never stop: our dreams, our struggles and our fulfilment to exceed beyond our own credo academic excellent. Please allow me to quote wisdom from Ernest Hemingway: "But man is not made for defeat …". That's all courage we need our dear honourable guest, colleagues, students and friends.

Finally, have fun and see you next year in 4th Annual Conference MIT, 2017. May God bless us all. Thank you.

Chairman of Annual Conference on Management and Information Technology,

(signed)

Dr. Mohammad. A. Amin Soetomo

ACMIT Committee

Commissioner	**:**	Rector, Dr. rer. nat. Filiana Santoso Vice Rector of Non Academic Affairs, Edward B.P. Manurung, M.Eng. Dean Faculty of Engineering & IT, Dr. Ir. Gembong Baskoro, M.Sc.
Steering Committee	**:**	Dr. Dr. Dipl.-Ing. Rachman Sjarief, MM, MH (BBA)
Organizing Committee	**:**	MIT & MME, SGU
Chairman	**:**	Dr. Ir. Mohammad A. Amin Soetomo, M.Sc.
Secretary	**:**	Khoriyah, S.Pd.
Treasurer	**:**	Sakinah Ardiana Bunda, S.E. (Finance)
Communication & P.R.	**:**	Deni Hutajulu, S.S. (Dir. of Comm. & PR)—Photographer Irzan Fahmi, S.Kom. (Dir. Of Comm. & PR)—Visual Designer Ilham Akbar, S.Ikom—Website
Program Support	:	Yunus Nugraha (ASC & ExO)--projector, mics, speakers
IT Infrastructure	**:**	Angga Anugrah, B.Sc (ISS) Dipl.-Ing. Iqbal Yasin, S.Kom, M.Kom (ISS) Billy Siagian, S.Kom (ISS)
Fundraiser	**:**	Herry Ahmadi, (PT. DGE) Wita Susilowaty, S.I.Kom. (PT. JSK) Musdi Soleh, S.Kom (NTMC POLRI) Dodik Novianto, S.Ak. (PT. JSK)
Facility	**:**	Rina Rahayu (FM)--room, HVAC and physical security
Procurement	**:**	Latifah Bachrum (GA)
Paper Reviewer	**:**	Charles Lim, M.Sc., ECSA, ECSP, ECIH, CEH, CEI (Coordinator) Dr. Eng. Handri Santoso, S.Si., M. Eng. Dena Hendriana, BSc., S.M., Sc.D Dr. Tanika Sofianti, S.T., M.T. (BIE) Dr. Maulahikmah Galinium, S.Kom., M.Sc. (BIT) Dr. Eka Budiarto, S.T., M.Sc. (BMT) Ir. Heru Ipung, M.Eng. (BIT) Dr. Adhiguna Mahendra, S.Kom, M.Kom, MSc., MSV, MSR Dr. Ir. Nuki A. Utama, M.Sc Asep S. Suntana, S.Hut, M.A., Ph.D Dr. Mulya R. Mashudi, S.T., M.Sc Dr. Rusman Rusyadi Dr. Edy Sofyan, B.Eng., M.Eng. Leonard P. Rusli, B. Sc, M. Sc, Ph. D
Moderator	**:**	Dr. Dr. Dipl.-Ing. Rachman Sjarief, MM, MH Dena Hendriana, BSc., S.M., Sc.D Dr. Eka Budiarto, S.T., M.Sc. Dr. Ary Syahriar, BSc., MSc., DIC Charles Lim, M.Sc., ECSA, ECSP, ECIH, CEH, CEI Dr. Edy Sofyan, B.Eng., M.Eng. Ir. Heru Ipung, M.Eng.
Proceeding	**:**	Emanuel Ade Crisna Putra, S.T., M.T.
Registration & Certificate	**:**	Anis Choirunnisa, S.T. Rachmawati, S.Sos (BMT) Byan Haqi Mupitra, S.Kom Eldorado Vasco Pradana (ASC)
Food & Beverage	**:**	Oqke Prawira Triutama, S.ST, M.Si.Par (HTM) Dapur Selvy Catering

Time	**Rundown** **ACMIT Conference April 30, 2016,** **SGU Campus, BSD City, Tangerang**
08:00 – 08:30	Greeting and Registration Prayers
08:30 – 08:50	ACMIT Report by Chairman (Dr. Ir. Moh. A. Amin Soetomo, M.Sc.) Welcoming Speech by Dean FEIT SGU (Dr. Ir. Gembong Baskoro, M.Sc.) Opening Speech by Rector SGU (Dr. rer. nat. Filiana Santoso)
08:50 – 09:20	Keynote Speaker I: Dr. Ary Syahriar, BSc., MSc., DIC, Dean at University al Azhar
09:20 – 10:20	Keynote Speaker II: Dr. Ir. Neni Sintawardani, Chief of Bureau at Indonesia Research Institute (LIPI)
10:20 – 10:25	Photo Session (afterword VIP Guest may be excused from event)
10:25 – 12:00	Parallel Research Presentation First Session
12:00 – 13:00	Lunch/Prayer
13:00 – 15:20	Parallel Research Presentation Second
15:20 – 15:40	Session Break
15:40 – 17:15	Parallel Research Presentation Third Session
17:15 – 17:30	Reception and Closing

The Annual Conference on Management and Information Technology (ACMIT) 2016

Application Low Cost Sensor MG-811With Real-time System to Maintain Concentration of CO2 inside Car Cabin

Sudarto
Swiss German University, EduTown BSD City, Tangerang 15820, Indonesia

Abstract

Respiration effect from passenger in cabin car, the concentration of CO2 will rise into number which causing drowsiness. Investigated method to control the CO2 concentration are by using on-off control and fractional control. Fractional control developed most reliable control than on-off control. The fan speed of air conditioner become the most influencer to create smooth control and successfully extend the range of time operation of circulation flap but have not yet developed into auto control. Using the low cost CO2 sensor, the author developed an automatic system to control to maintain the concentration of CO2 below the 1000 ppm as recommended by organization that concern to human safety OSHA and ASHRAE.

Keywords: CO2; fractional; drowsiness;ASHRAE;auto control

1. Introduction

Modern cars are designed to provide comfort to its passengers, less fuel consumption and pollution. The cars have to be well sealed to block the fine particle and other gas entering the car cabin. Air conditioning system also have objective to produce the comfort, while the air condition in operation, it is need to block the outside air from entering the cabin by recirculate the air inside the cabin for fuel consumption efficiency.

The main issue with having full recirculation is that it drives up different gas concentration in the vehicle. From the study, it was found that recirculating the air causes an increase in carbon dioxide (CO2) concentrations inside the vehicle's cabin. This is due to passengers continuous exhaling without introduction of outside air into the car cabin. Increased levels of CO2 are known to have negative side effects drowsiness and headaches [5]. Zhu et al. [2] demonstrated that CO2 focuses ascend to 4500 ppm in 10 min for a passenger car with 3 travelers amid air-recirculation mode. This is far above the 400 ppm concentration that is in normal air. Mathur [6] refered to ASHRAE standard 62 which indicates the security level of CO2 in adapted space. The ASHRAE standard is 700 ppm over surrounding conditions on a constant premise.

This paper describes the application of low cost CO2 sensor as input into controller system that will programmed to maintain the outside air flap to maintain the concentration level of CO2 in car cabin.

2. Related Works

2.1. On-Off Air Control

Mathur [6] tried to control the level of carbon dioxide by changing between full recirculation and no recirculation. Full recirculation mode drives the concentration up while no outside air flow into cabin. Mathur's objective was to keep the concentration lower than 1000 ppm to keep with the ASHRAE standard. Figure 1 demonstrates the concentration as a function time with four passengers. With a specific end goal to keep the carbon dioxide beneath 1000 ppm, the recirculation must be switched every 2 minutes. This recurrence reduces with the number passengers. With one and only passenger this recurrence is reduces to 6 minutes.

This is a great way to control the carbon dioxide concentration levels, but it is not feasible because if a vehicle has a recirculation door that moves this often, it is only a matter of time before the recirculation door motor fails.

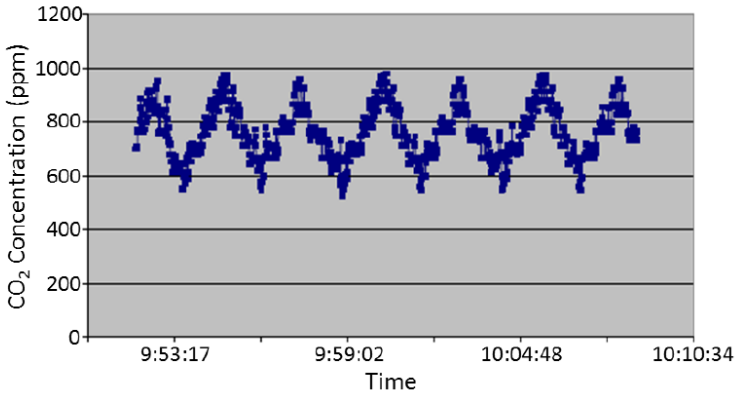


Figure 1. Cabin concentration levels for carbon dioxide as a function of time. Recirculation alternates between on and off, with four passengers. Figure from [25]

2.2. Fractional Air Control

Differ from On-Off control method, Grady [1] has do CO2 control cycle for attainability test starts with full recirculation and after that opens the recirculation door somewhat to keep up the upslope at slightly positive value. The test then cycles with a second recirculation door point which shows the slight downslope. This is to keep up the CO2 fixation at an objective scope of focuses. Distinctive ventilation speeds make shifting measures of outside air entering cabin. This outcomes in the requirement for the division of air recirculation, which is controlled by the recirculation door point, to be acclimated to an alternate level. For instance a quicker ventilation fan speed results in more body leakage flow. Along these lines the division of outside air should be less contrasted with that of a slower ventilation fan speed.

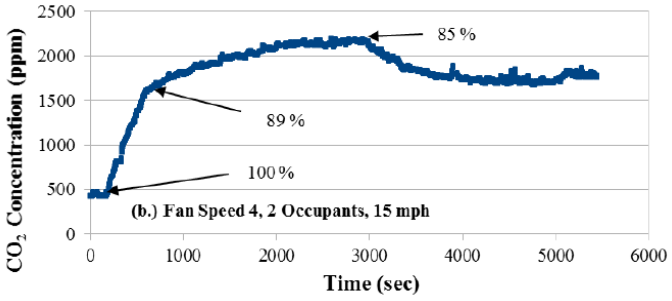


Figure 2. Feasibility test to control cabin CO2 concentration at a target level of 2000 ppm, at 15 mph with two passengers.

Figure 2 demonstrates cabin CO2 concentration that are kept up inside of an objective scope of concentration for various ventilation fan speeds. The procedure portrayed above is utilized to accomplish the same level of CO2 fixation. The door point cycles at regular intervals contrasted with Mathur's 600 seconds, making a more powerful.

2.3. Carbon Dioxide Build Up Modelling

Jung [4], has working for study to express how the CO2 build up inside the cabin car. Figure 3 shows a schematic diagram of the vehicle cabin system. *Qi* is a flow through the inlet duct system and this should balance with *Qo* which is a flow through the body vent. Passengers are the source of CO2 within the cabin. The normal human breath exhales CO2 at levels ranging from 38,000 ppm to 56,000 ppm with rates ranges from 220 ml/min when idle to 1650 ml/min during moderate sport [7].

This high concentration exhale can lead to high levels of the CO2 concentration in enclosed spaces like the vehicle cabin unless it is well ventilated. The outside CO2 concentration is fixed at the ambient CO2 level which is around 385 to 395 ppm [8]− 390 ppm was used for all fits- while the in-cabin CO2 concentration can vary as a function of the strength of the source term (i.e. number of passengers), cabin volume (*Vc*) and body leakage flow (*Ql=Qi=Qo*). *Ql* can vary as a function of other parameters like ventilation fan speed, vehicle speed, and geometry of the ducting system.

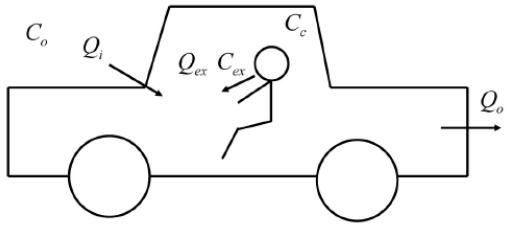


Figure 3. The schematic diagram of vehicle cabin air system by Jung

3. System Design and Methodology

Structure of the flap controller offers need to minimal effort, solidness and simplicity of installation. The case depends on the choice of sensors, power supply and show of measurement results be a noteworthy concern

3.1. The Choice of Component and Part

Carbon Dioxide Sensor chose in this controller is MG - 811 which is a sensor with a basically chemical response. The sensor utilized is as a part of the type of a module that is incorporated with the analog to digital converter. This sort of DT-Sense module has two information interfaces are UART and I2C. I2C underpins the utilization of more than one sensor and in parallel. The sensor utilizes power between 5V - 12V is suitable to utilize existing power supply in the vehicle.

Arduino Mega utilized as a controller for the read sensor comes about and perform figuring and produce yield for controlling the operation of a motor mounted on the ventilation flap mechanism. The results of sensor readings showed by the LCD as information readings from every sensor and its highest value.

3.2. Hardware Design

Hardware circuit diagram of the system shown in Figure 3. The system in mainly composed main controller and sensors

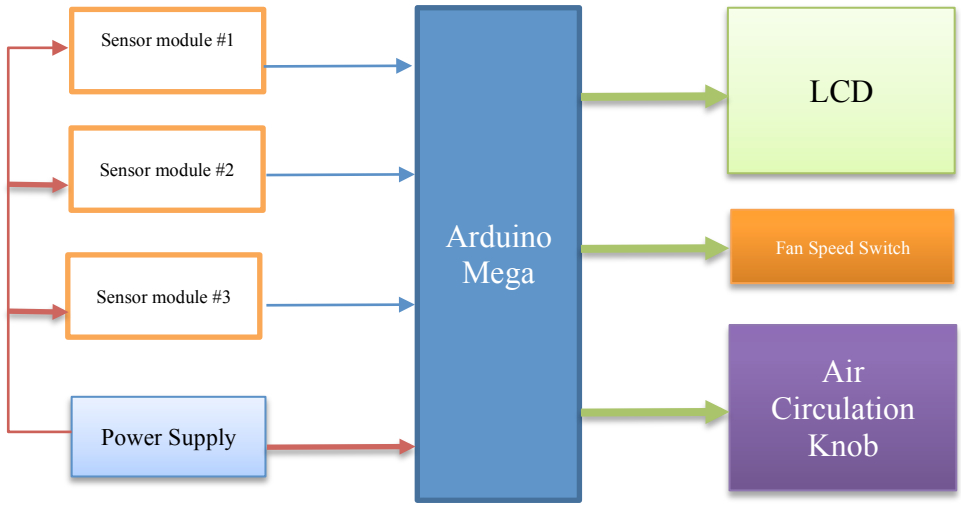


Figure 4. Simple Diagram for hardware configuration

3.3. Software Design

3.3.1. Real-time Diagram

Adjustment of the schematic outline for the diagram made by Samar Abdi [3], utilizing a single processor to perform various thread with an alternate assignment. Results from a producer thread that common information utilized by another thread, must be place in available area in system that openly for other thread with a specific end goal to keep away from delays. Outline of continuous procedures can be found in figure no. 3 below:

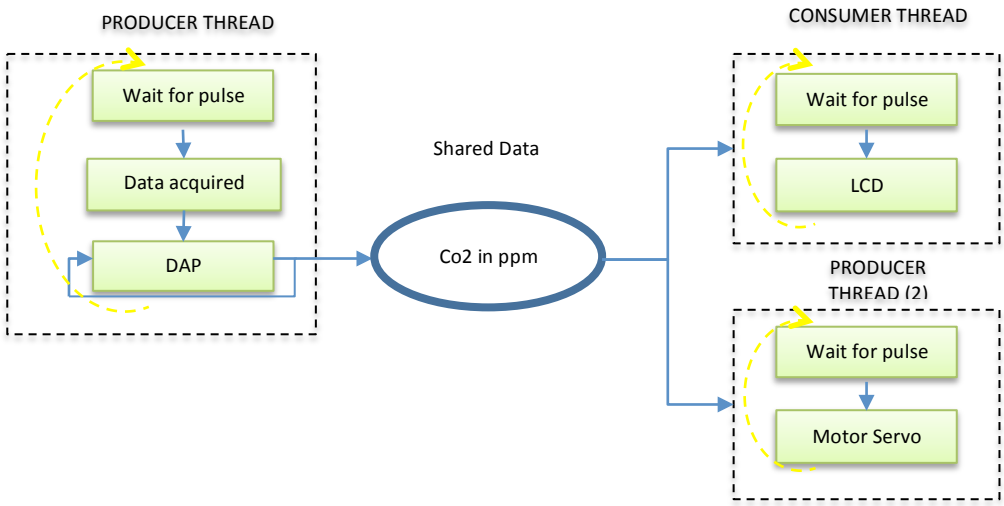


Figure 5. Realtime System Diagram

3.3.2. Control Servo Motor

The controller equipped with two motor servo that have different task, to control opening the valve circulation and the other hand to control the fan speed switch. Servo has chosen because the movement both knob and switch can calculate easily by measuring angle of servo movement. The servo has limitation in energy in hold position. The study also about to find the suitable motor like linear motor or step motor.

4. Experiment Result

4.1 Sensor Position

In the cabin, air circulation happens in the close recirculation and open course. In order to know comprehensive estimations for dispersion of grouping of CO2 sensor located on three areas: the front, centre, and rear side of the cabin. The concentration of co2 will be recorded under several combination of possible scenarios of vehicle operations. The collected data will be analysed to get the parameter that will be written into the controller unit.

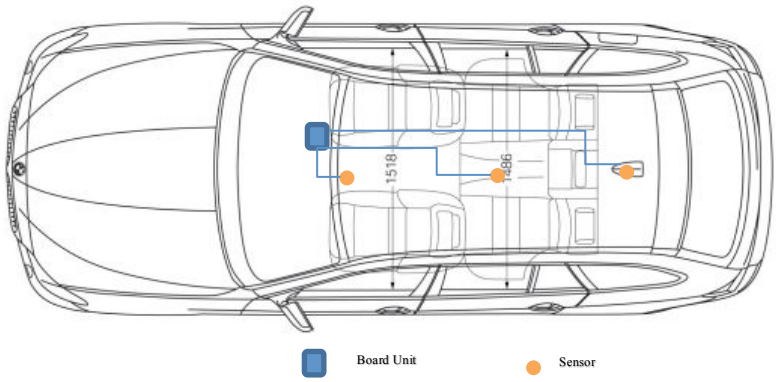


Figure 6. Illustration of board unit and sensor placement.

4.2. Data Collection

The concentration of CO2 will record under several combines scenario of circumstance that may happens in actual operation of vehicle. The circumstances to combine are:

- Number of passenger 1-4 passenger
- Vehicle speed 20 km/h, 40 km/h and 60 km/h
- Air conditioner fan speed 1, 2, 3, and 4.
- Sensor location.

The collected data will be analyze to get the parameter that will be write into controller programming.

5. Conclusion

Carbon dioxide in certain amount can causing drowsiness and headache. Principle of maintain concentration level by allowing outside air entering the cabin either by on-off method or fractional control that keeping air flap open in various position. To design automatic system, it requires data about concentration level and distribution of carbon dioxide.

References

[1] Grady, M. L., Jung, H., chul Kim, Y., Park, J. K., & Lee, B. C. (2013).*Vehicle Cabin Air Quality with Fractional Air Recirculation*. tech. rep., SAE Technical Paper.

[2] Zhu, Y., Eiguren-Fernandez A., et al. (2007). "In-Cabin Commuter Exposure to Ultrafine Particles on Los Angeles Freeways" Environmental Science & Technology 41(7):2138-2145.

[3] Abdi, Samar (2012) "Introduction to Real-Time Systems" Lecture Notes, Concordia University.

[4] Jung, Heejung.(2013) "Modeling CO2 Concentrations in Vehicle Cabin" SAE Technical Paper

[5] NIOSH. (1975) Criteria for a Recommended Standard Occupational Exposure to Carbon Dioxide (Pub. No. 76-194). Cincinnati, NIOSH.

[6] Mathur, G.(2009), "Field Tests to Monitor Build-up of Carbon Dioxide in Vehicle Cabin with AC System Operating in Recirculation Mode for Improving Cabin IAQ and Safety,"*SAE Int. J. Passeng. Cars - Mech. Syst.* 1(1):757-767.

[7] U.S. Department of Labor, Occupational Safety and Health Administration. Code of Federal Regulations, Title 29, Part 1910.1000-1910.1450. www.osha.gov.

[8] U.S. Department of Labor, Occupational Safety and Health Administration. OSHA Technical Manual. TED 01-00-015. www.osha.gov.

Definitions/Abbreviation

OSHA - Occupational Safety and Health Administration

ASHRAE - American Society of Heating, Refrigerating, and Air-Conditioning Engineers

The Annual Conference on Management and Information Technology (ACMIT) 2016

Risks Mitigation of Defacement Attack Vectors on Educational Institution Websites by Using OWASP and Risk IT Frameworks

Mohammad Amin Soetomo, Rio Asepta
Information Technology Department
Swiss German University
Edutown Kav II.1, BSD City, Tangerang 15339, Indonesia.
mohammad.soetomo [at] sgu.ac.id, rio.asepta [at] student.sgu.ac.id

Abstract

According to an article published by The Hacker News in 2006 [1] 21.549 websites defaced by Turkish hacker team, Iskorpitx. It was the largest defacement in web history. Zone-h, the largest defaced website archives [2] listing 11.107.846 websites became the victims of defacement attack. So how about educational institution websites? Are they become the target of defacement attack?
In point of fact, University of Maryland, North Dakota University, Butler University, Indiana University and Arkansas State University became the victims of data breach by malicious attacker, the data breach was larger than data breach attack on Sony [3]. After analysing the data filtered from Zone-h archives, we retrieved that the defaced websites belong to educational institution in ASEAN countries; Indonesia (11.615 websites), Malaysia (3.512 websites), Singapore (312 websites), Vietnam (3.294 websites), Thailand (9.860 websites), Brunei Darussalam (30 websites), Cambodia (65 websites), LAO PDR (9 websites), Myanmar (6 websites), Philippines (978 websites) have been defaced in 2015. This paper will analyse the motive, attack methods, risks, impacts and mitigations of defacement attack in educational institutions. MECEES, OWASP and Risk IT will be used as framework. Hacked educational institutions will lead to critical risks.

Keywords: Website defacement ; motive; method ; risks ; impacts ; mitigation ; OWASP ; Risk IT

1. Introduction

Zone-h lists 11.107.846 websites became the victims of defacement attack in 2015. After analysing the data filtered from Zone-h archives, we collected that the defaced websites belong to educational institution in ASEAN countries; Indonesia (11.615 websites), Malaysia (3.512 websites), Singapore (312 websites), Vietnam (3.294 websites), Thailand (9.860 websites), Brunei Darussalam (30 websites), Cambodia (65 websites), LAO PDR (9 websites), Myanmar (6 websites), Philippines (978 websites) have been defaced in 2015.

This paper will analyse the motives by using MECESS, attack methods, risks and impacts by using OWASP and mitigation of defacement attack in educational institution by using Risk IT framework. In the table 1 below, we filtered the defaced ASEAN countries' websites from Zone-h website with these conditions:

Table 1. Filtering conditions to retrieve defaced websites belong to educational institution in Zone-h website

No	Country	Educational Institution Domain	Filtering Options			Date*
			Special defacement Only	Fulltext/Wildcard	Onhold (Unpublished) only	
1	Indonesia	ac.id	No	Yes	No	All
2	Malaysia	edu.my	No	Yes	No	All
3	Singapore	edu.sg	No	Yes	No	All

4	Vietnam	edu.vn	No	Yes	No	All
5	Thailand	ac.th	No	Yes	No	All
6	Brunei Darussalam	edu.bn	No	Yes	No	All
7	Cambodia	edu.kh	No	Yes	No	All
8	LAO PDR	edu.la	No	Yes	No	All
9	Myanmar	edu.mm	No	Yes	No	All
10	Philippines	edu.ph	No	Yes	No	All

*Date: All →from 01-January-2015 – 07-November-2015.

Figure 1 below shows an example of defaced educational institution website:

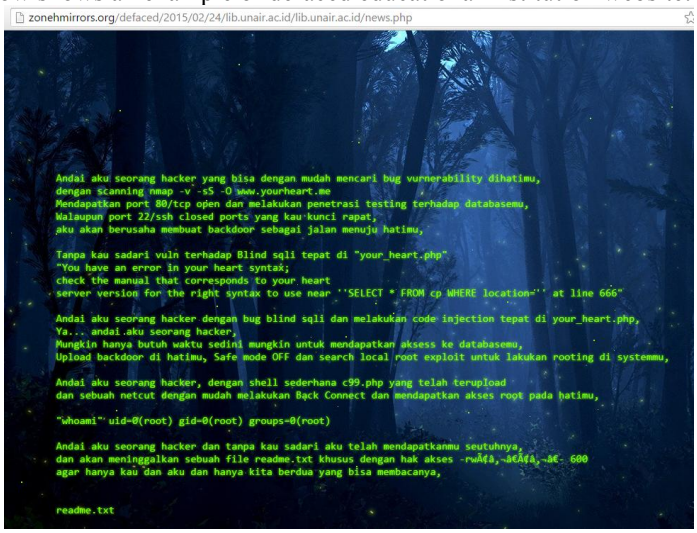


Fig. 1. Sample of mirrored defaced educational institution website [4]

The comparison of defaced websites belong to educational institution in ASEAN countries filtered from Zone-h website shows in the figure 2 below:

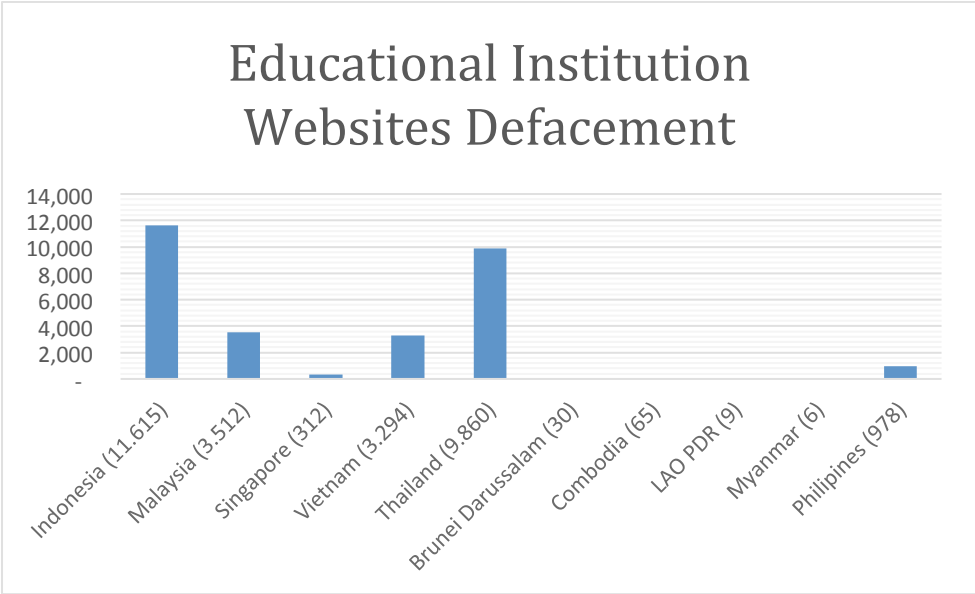


Fig 2. Defaced websites comparison in ASEAN Educational institution [5]

1.2. Overview

1.2.1. Website Defacement

Website Defacement is an attack on a website that modify the visual appearance [6] . Website defacement usually change the entire webpage. This page usually put the defacer's pseudonym or the defacer's hacking team. Sometimes, the website defacer makes fun of the system administrator for failing to login to the hacked system.

1.2.2. Educational Institution Website

Educational institution is defined as an entity which organize to conduct and maintain its identity where people of different ages receive an education. Where website means a set of interconnected webpages in World Wide Web [7] . Educational institution website refers to the interconnected web pages to deliver information about education.

1.2.3. OWASP

OWASP, Open Web Application Security Project was found in December 1st 2001 as non-profit organization [8]. The purpose of OWASP is to conceive, develop, acquire, operate and maintain the applications. The approach is based on attack vectors to deliver the secure web application. In the figure 3 below shows OWASP risks to business impact due to malicious attack vectors:

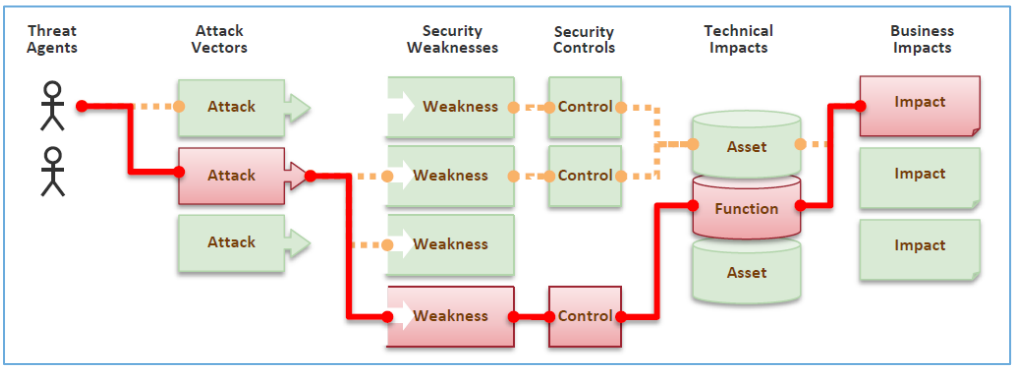


Fig. 3. OWASP Top 10 2013 risks to business impact [9]

1.2.4. MEECES

Attacker will leave a message in any defaced website. Any message is motive. MEECES will be used to analyze this motive. MEECES is an acronym for Money, Entertainment, Ego, Cause, Entrance to Social Group and Status which stated as general hacking motives by Max Kilger in one of Honeynet Project publication [10]. MEECES will be used to find the probability motive in defacing educational institution website.

1.2.5. Risk IT Framework

Risk IT is designed by ISACA to assists enterprise company to manage any risk related to information technology threats [11]. In the figure 4 below describes the Risk IT components consist of Risk Governance, Risk Response and Risk Evaluation [12]. Manage Risk points in Risk Response component will be used to build attack mitigation in handling website defacement attack vector especially for educational institution website. Figure 4 below shows the Risk IT components those are mentioned above:

Fig. 4. Risk IT Components [13]

1.2.6. Zone-h

Zone-h is the largest global website defacement archives [14] that was found in Estonia on March 2, 2002. Once a defaced website is submitted to Zone-H, it will be mirrored on the Zone-H servers, the administrator of Zone-h will crosscheck which is the submitted defaced websites valid or not. This portal contains of IT security news, digital trend news, geo-politics, analyses, forums and researches.

1.3. Problem Statement

The objective of this paper is to answer these below questions:

1. Website Defacement motives in Educational Institution
2. What is the method used by the hackers to deface educational institution?
3. What is the risk and impact to the defaced websites belong to educational institutions
4. What is the mitigation to this attack?

1.4. Expected Outcome

After analyze the questions above, we expects the result of this analysis will get many advantages for educational institutional as their reflection on their own IT infrastructure security to indicate the weakness points based on OWASP and build mitigation procedure based on Risk IT Framework. The works is also intended to bridge the gap between technical level and managerial level in understanding the risks and mitigations.

1.5. Theoretical Framework

We will use below data and knowledge resources in this work:

1. Website defacement motives – **MEECES**
2. Website defacement methods - **OWASP**
3. Website defacement risks and impacts – **OWASP**
4. Website defacement mitigations – **Risk IT Framework**

1.6. Related Works

Vulnerability impact of website hacking is very dangerous [15], concept and framework to mitigate the issues should be developed to decrease the impact and risk. Marcius et. al has developed Ontological approach [16] to a risk mitigation to reduce gaps between developer and security knowledge. Information security in not only engineer and consultant responsibility, CIO is also need to understand the business requirements for information security [17]. To eliminate the gaps between the operational and managerial level understanding in risk mitigation regarding website hacking especially in educational institution website, we develop the mitigation concept to mitigate the risk by bridging the OWASP Top 10 2013 and Risk IT framework.

2. Methods

2.1. Defacement Motives

By analyze more than 100 HTML pages of mirrored defaced website randomly from educational institution websites in ASEAN countries, we filtered the defaced websites from http://www.zone-h.org, we found that the attacker left message(s) in defaced websites. This motives will be mapped in to MEECES. We have results as shown in the table 2 below:

Table 2. Defacement motives in educational institution websites in ASEAN

Motives	Result	Motives Count
Money	No	0
Entertainment	Yes	77
Ego	No	0
Cause	Yes	20
Entrance to Social Group and Status	Yes	62

Graphically as shown in figure 5 below as the result of table 2 above:

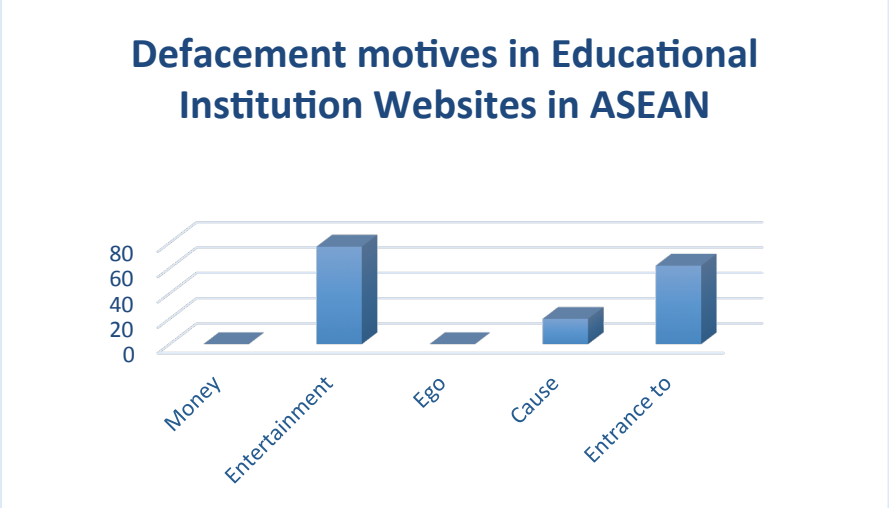


Fig. 5. Defacement motive in educational institution websites in ASEAN

From the 100 defaced educational institution websites we found that a template can interpret more than one motives. The description of the result can be described as below:

- **Motives: Money**

There is no motives found which the attacker asked the educational institution to transfer money after the attack.

- **Motives: Entertainment**

In this analyzed defacement educational institution websites we found funny messages, funny images, no clear message, personal defacing in the defaced websites. This criteria will be included in Entertainment motives. Sample of this messages:

"*Admin'e Ojo Ngopi Ae… wkwkwkwkwk*",
"*Tidak akan pernah ada bangsa* diantara kami!",*
"*Sorry Admin websitenya kurang aman …*",
"*… Aku kangen kamu lho …*",
"*By defacer tersakiti".*

- **Motives: Ego**

Ego motives is regarding intellectual challenge, not interest in any recognition. As this defaced websites show the trace and message, this motive is not valid.

- **Motives: Cause**

Cause motive consist of any message to deliver protest regarding a policy, religion, political contains. Sample of this messages:

"*pertandingan dikit aja tawuran pake teriak2 slogan gituan. Duh tong malu ane tong …*",
"*Negara Malaysia sekarang sudah gegar dengan pelbagai kekotoran ... Najib sudah buat kepada rakyat! …*",
"*OpChina action must fail*",
"*ISIS Doesn't represent Islam …*",
"*Save KPK …*",
"*Turunkan harga kenderaan. Kami tak mampu nak tunggu …*",

- **Motives: Entrance to Social Group and Status**

This motive is motivated by the attacker community acts to show their skill to their rival, the attacker country vs other countries. Sample of this messages:

"*Hacked by "*, where the attacker is All_Indonesian_Hackers (Indonesia) and the victim is www.amc.edu.my (Malaysia)
"*Thanks to: All Crew",* where the attacker: JayZet (Indonesia) and the victim is www.rks.ac.th (Thailand)
"*... Turkish Hacker*", where the attacker is BorLak (Turkish) and the victim is www.kibi.edu.kh (Cambodia)

2.2. Methods Used to Deface Educational Institution Websites

According to Prof. Vivek Richariya, the most common method of defacement is by using SQL injection which is in web application area [18]. Since this statement, we used Open Web Application Security Project (OWASP) Top 10 – 2013 attack vectors in the table 3 below [19] will be used as the framework to find more methods used to deface a website.

Table 3 below will describe OWASP Top 10 - 2013 Attack and description:

Table 3. OWASP Top 10 - 2013 Attack and description [20]

Attacks	Description
A1 – Injection	Attacker will be able to access data without proper authorization.
A2 – Broken Authentication and Session Management	It allows attackers to compromise passwords.
A3 – Cross-Site Scripting (XSS)	XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions.
A4 – Insecure Direct Object References	Attackers can manipulate to access unauthorized data.
A5 – Security Misconfiguration	Any defaults settings are often insecure, it should be updated and patched.
A6 – Sensitive Data Exposure	Attackers may steal or modify such weakly protected data to steal credit card, identity, or other crimes.
A7 – Missing Function Level Access Control	Attackers will be able to forge requests in order to access functionality without proper authorization.
A8 - Cross-Site Request Forgery (CSRF)	This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
A9 - Using Components with Known Vulnerabilities	If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover.
A10 – Unvalidated Redirects and Forwards	Attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

The mapping results of OWASP Top 10 -2013 attack vectors by using CVE Mitre and known vulnerability exposures as shown in the table 4 below:

Table 4. Attack mapping for website defacement [21]

Attacks	Used to deface a website	Sample of vulnerability leads to website defacement
A1 – Injection	Yes	- Joomla JNews (com_jnews) - SQL Injection - PHP-Fusion <= v7.02.07 - SQL Injection
A2 – Broken Authentication and Session Management	Yes	- Ultimate PHP Board 2.2.7 Broken Authentication Management
A3 – Cross-Site Scripting (XSS)	No	- Not available
A4 – Insecure Direct Object References	Yes	- ZTE ZXDSL 831CII - Insecure Direct Object Reference
A5 – Security Misconfiguration	Yes	- Password in public files
A6 – Sensitive Data Exposure	Yes	- Directory listing of system files and folders
A7 – Missing Function Level Access Control	Yes	- IBM WebSphere - Insufficient Access Control
A8 - Cross-Site Request Forgery (CSRF)	No	- Not available
A9 - Using Components with Known Vulnerabilities	Yes	- Java 7 Applet Remote Code Execution
A10 – Unvalidated Redirects and Forwards	No	- Not available

2.3. Defacement Risks (OWASP) and Mitigation (Risk IT)

Based on the risk methods and its impacts by using OWASP (low level), the risk of defaced websites belong to educational institutions will face the risks in table 5 below, the risks to business impacts will be translated to business term by using Risk IT framework (high level) and finally the required mitigations those comply with Risk IT framework in the result chapter:

Table 5. Website defacement Risk (OWASP Top 10 2013) and the mitigation (Risk IT)

Attack Vectors	Risks to Business Impacts	Risks Translated to Business Terms
	(OWASP Top 10 2013)	(Risk IT - IT Risk in Business Term)
(A1) Injection	All data could be stolen, modified, or deleted. Reputation could be harmed.	- Confidentiality (COBIT) - Customer (BSC) - Customer Services (Ext.BSC) - Operations (COSO ERM) - Reputation (FAIR)
(A2) Broken Authentication & Session	Business impact of public exposure of the vulnerability.	- Confidentiality (COBIT) - Customer (BSC) - Customer Services (Ext.BSC) - Reputation (FAIR)
(A3) Cross-Site Scripting (XSS)	Not included	- Not included
(A4) Insecure Direct Object References	Consider the business value of the exposed data.	- Confidentiality (COBIT) - Customer (BSC) - Customer Satisfaction (Ext.BSC) - Strategic (COSO ERM) - Reputation (FAIR)
(A5) Security Misconfiguration	The system could be completely compromised without detected. All of the data could be stolen or modified. Recovery costs could be expensive.	- Confidentiality (COBIT) - Customer (BSC) - Customer Services (Ext.BSC) - Operations (COSO ERM) - Reputation (FAIR)
(A6) Sensitive Data Exposure	Consider the business value if the lost data has impact to the reputation. What is the responsibility if this data is exposed? Also consider the damage to the reputation.	- Availability (COBIT) - Confidentiality (COBIT) - Customer (BSC) - Customer Satisfaction (Ext.BSC) - Reputation (FAIR)
(A7) Missing Function Level Access Control	Consider the business value of the functions those exposed and the data they process.	- Confidentiality (COBIT) - Customer (BSC) - Customer Satisfaction (Ext.BSC) - Reputation (FAIR)
(A8) Cross-Site Request Forgery (CSRF)	Not included	- Not included
(A9) Using Components with Known Vulnerabilities	Consider each vulnerability might impact to the business management by the affected application. At worst, it will complete compromise.	- Availability (COBIT) - Customer (BSC) - Operations (COSO ERM)
(A10) Unvalidated Redirects and Forwards	Not included	- Not included

4.1.1 Results

3.1 Attacker Motives in Defacing Educational Institution Websites

As the result after analyzed 100 defaced education institution websites, **Entertainment** motive is the most motive used by the attacker in performing educational institution website defacement (77), then **Entrance to Social Group** motive (62) and **Status** motive (20). This Entertainment motive becomes the highest motives due to most of universities use published website templates [22] and share them [23] where the fact is the published templates have many vulnerabilities comparing to self-developed website template, self-developed University website template will encourage the University to develop and authorize the security aspects of their website template [24].

3.2 Risk Mitigation for Defacing Educational Institution Websites

During this work, we have combined OWASP and RISK IT. The flow process of the combined frameworks as below figure 6:

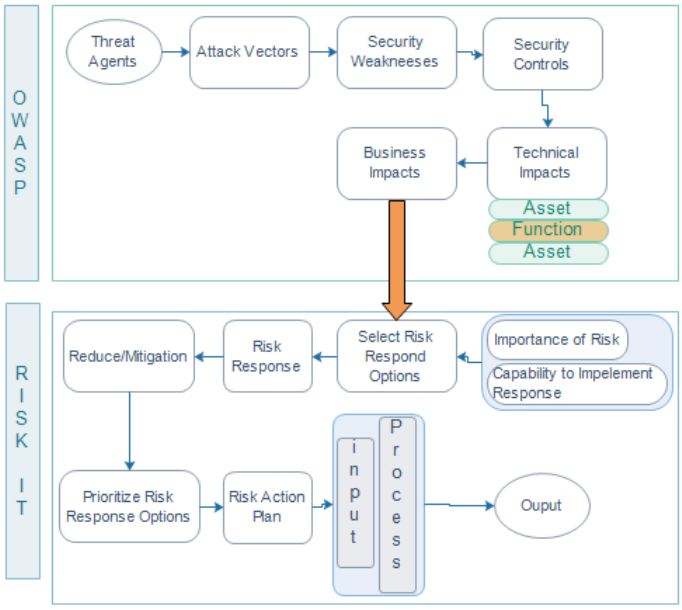


Fig. 6. OWASP and RISK IT combination

Based on the figure 6 above, we complied the data from table 5 above as the Input and Impact and the risk mitigation (Output) by using RR3.1 - Maintain incident response plans. The result is as described in the table 6 below:

Table 6 Risk Mitigation

Input (Attack vectors)	Impact	Process (Mitigation)	Output (Goal)
(OWASP TOP 10 2013)	Security threats and vulnerabilities(RiskIT)		
A9	**Availability**	- Maintain open communication about risk acceptance	COBIT DS4
A1, A2, A4, A5, A6, A7	**Confidentiality (COBIT)**	- Risk management activities	COBIT DS4
A1, A2, A4, A5, A6, A7	**Customer (BSC)**	- Analysis techniques and results available to assist with plan preparation	COBIT DS4
A1, A2, A5	**Customer Services (Ext.BSC)**	- How long the enterprise may be exposed and how long it may take to recover	COBIT DS4
A4, A6, A7	**Customer Satisfaction (Ext.BSC)**	- Define pathways of escalation across the enterprise, from line management to executive committees	COBIT DS4
A1, A5, A9	**Operations (COSO ERM)**	- Verify that incident response plans for highly critical processes are adequate	COBIT DS4
A1, A2, A4, A5, A6, A7	**Reputation (FAIR)**		COBIT DS4
A4	**Strategic (COSO ERM)**		COBIT DS4

4.1.2 Conclusion

Attack on Educational institution websites such as defacement usually performed by newbie (attacker with lower skill) to show off or entertainment, just for fun, motivated by the community and some fundamental cause such as a protest to a policy, religion or political. The impact is high, where the reputation of academic institution which is defaced will be devastated. Based on the analysis of motives, methods, risks, impacts and mitigation faced by defaced educational institution websites, we conclude that risk mitigation should be performed to decrease the risk impacts.

References:

[1] "World Record : 404907 websites hacked by Iskorpitx (Turkish Hacker) !" .

[2] A. Bartoli, G. Davanzo, and E. Medvet, "The reaction time to web site defacements," *Internet Comput. IEEE*, vol. 13, no. 4, pp. 52–58, 2009.

[3] "5 Colleges With Data Breaches Larger Than Sony's in 2014," 15-Jan-2015. .

[4] "lib.unair.ac.id hacked," 13-Apr-2015. .

[5] "Zone-h." .

[6] T. Kanti, V. Richariya, and V. Richariya, "Implementing a Web browser with Web defacement detection techniques," *World Comput. Sci. Inf. Technol. J. WCSIT*, vol. 1, no. 7, pp. 307–310, 2011.

[7] V. K. Grover, "INTELECTUAL INERTIA: FRIEND AND FOE FOR AN EDUCATIONAL INSTITUTION TO GROW."

[8] D. Patil and M. Phil, "Challenges & Problems in Security Testing of Web based Applications: A study of software companies in Pune city."

[9] T. OWASP, "Top 10–2013," *Ten Most Crit. Web Appl. Secur. Risks*, p. 5, 2013.

[10] M. Kilger, O. Arkin, and J. Stutzman, "Profiling," *Honeynet Proj. 2 Nd Ed Know Your Enemy Addison Wesley Prof.*, 2004.

[11] ISACA, *The Risk IT Framework*. Information System Audit and Control Association (ISACA) IL, 2009.

[12] ISACA, *The Risk IT Framework ISACA*. Information System Audit and Control Association (ISACA) IL, 2009.

[13] ISACA, *The Risk IT Framework*. Information System Audit and Control Association (ISACA) IL, p. 15, 2009.

[14] O. Oriola, A. Adeyemo, and A. Robert, "Distributed Intrusion Detection System Using P2P Agent Mining Scheme," *Afr. J. Comput. ICT*, vol. 5, no. 2, pp. 3–10, 2012.

[15] A. P. P. V. Ami and A. P. S. Malav, "Top Five Dangerous Security Risks over Web Application," *Int. J. Emerg. Trends Technol. Comput. Sci.*, vol. 2, no. 1, pp. 41–43, 2013.

[16] M. Marques and C. G. Ralha, "An Ontological Approach to Mitigate Risk in Web Applications," *Proc. SBSeg*, 2014.

[17] A. Passori, "Selecting the risk assessment method of choice," *Delta*, vol. 2911, p. 17, 2004.

[18] T. Kanti, V. Richariya, and V. Richariya, "Implementing a Web browser with Web defacement detection techniques," *World Comput. Sci. Inf. Technol. J. WCSIT*, vol. 1, no. 7, pp. 307–310, 2011.

[19] T. OWASP, "Top 10–2013," *Ten Most Crit. Web Appl. Secur. Risks*, 2013.

[20] T. OWASP, "Top 10–2013," *Ten Most Crit. Web Appl. Secur. Risks*, p. 6, 2013.

[21] "CVE - Common Vulnerabilities and Exposures (CVE)." [Online]. Available: http://cve.mitre.org/. [Accessed: 20-Oct-2015].

[22] K. Peterson, "Academic web site design and academic templates: Where does the library fit in?," *Inf. Technol. Libr.*, vol. 25, no. 4, pp. 217–221, 2013.

[23] D. Gibson, K. Punera, and A. Tomkins, "The volume and evolution of web page templates," in *Special interest tracks and posters of the 14th international conference on World Wide Web*, 2005, pp. 830–839.

[24] S. Nicholson, "An investigation into the management of a university web site," *Retrieved Novemb.*, vol. 20, p. 2013, 2002.

The Annual Conference on Management and Information Technology (ACMIT) 2016

Analysis of Light Influence on The Camera Measurement for Better Calibration Process in Electronic Industry

M Adib Arif Hartadi [1]*
[a]*Swiss German University, BSD City, Tangerang, 15339, Indonesia*

Abstract

Machine vision systems have been used in the automatic inspection of connector product in electronic industry. Everyday the condition of automatic inspection machine must be checked by using a master product to make sure that the result of measurement is according to requirement. When the result is out of specification, the inspection machine must be re-calibrated. Time that is required for once calibration is about 8 hours. Light is one of factor that influence measurement result. In this study first of all, this paper set up the experimental platform for measure dimension of object by using camera. Pixel equivalent that is got by calibration experiment is 0.044 mm / pixel with measurement range of 0.044 ~ 21.956 mm. Secondly, analysing experimental data of measurement result by changing light intensity. This paper try to find correlation between light intensity and dimension result of the machine vision result to get a better formula that can be used to calibrate a machine vision in order to make less frequency of calibration process.

keyword : camera, inspection, calibration, light.

1. Introduction

Size measurement is important at the stage of product inspection in the world of industry. Appropriately and accurately measurement on the inspection of a product is important that all products produced in accordance with the quality standards desired by consumers and provides benefits for producers by reducing production time and cost saving production may be done.

The inspection process which is usually done manually by the human senses, start from viewing, measuring and comparing the sample or a standard product and then record and documenting the result obtained. Those entire manual inspection is done by manually contact measurement.

For small size of product, manually contact measurement is easy to destroy the surface and change their relative position, thereby affecting the measurement accuracy. For mass production, sampling can only be used. In inspection process, using the quality of the sample can be used to be the standard of the entire batch product [1]. Meanwhile, a long-term work can cause the fatigue of the body and eyestrain, which in turn brings stability problems, and poor working condition will also affect health and mood the operator. thus in certain aspects, such as measurement speed, accuracy, automation and security, the limitation of traditional measurement method which is unable to meet modern manufacturing time online, non-contact measurement, high-speed precision development is needed.

Size measurement must be done by measuring tools, which have gone through several stage of mechanical, optical and electrical type and so on. Nowadays, digital image process by using camera inspection is applied widely in visual inspection method. The visual inspection using a camera inspection as a measurement tools offers several advantages over manual based inspection. There are

1

* Corresponding author. Tel.: +62-818-927-297
E-mail address: adibarif_h@yahoo.com.

advantages include minimize set up time, real-time scanning, reduce inspection time and more widely data saving capability.

2. Automated Visual Inspection

In the manufacturers of connectors in electronic industry have to conduct the inspection of the product. Machine vision will provide information OK if the results of measurements according to the limits specified dimensions and will provide information NG (Not Good) if the results of measurements outside the limits specified dimensions. Method checks are performed depends on the level of requirements expected by customers. Among the several existing methods of inspection performed should be measured one by one in certain parts of the product. This is necessary because it relates to the function of the product for example lead coplanarity inspection on connector for computer hard drive. Lead coplanarity is the the distance between the lead connector and the PCB to be soldered. The required distance is maximum 0.1mm. If the distances are greater than 0.1mm there is the potential occurrence of a failure in the soldering process performed by the customer, resulting in a product malfunction. Examination manually using a measuring instrument such as a projector or a measuring microscope is very time consuming and has the potential for measurement error due to be done by humans due to fatigue and condition factor of the human. Examples of machine vision applications are shown in Fig. 1.

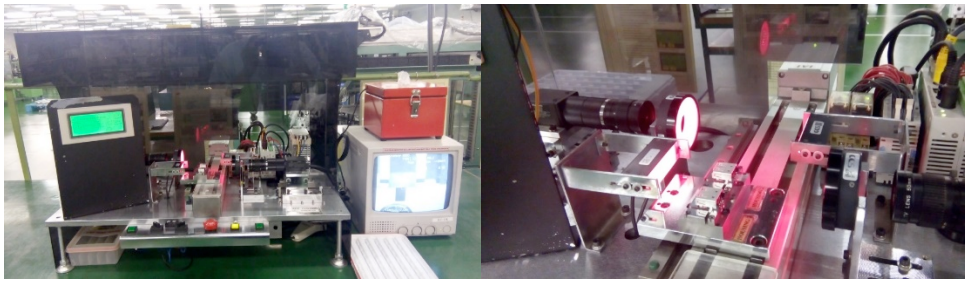


Figure 1. Example of automated visual inspection that is applied in electrical industry

The surface shape of the measured lead connector is a flat field but on the edges are curved or radius field that is caused by cutting process of the connector lead through a stamping process. In the production process, machine vision that is used to measure the connector product must be verified daily to ensure that the conditions are still able to work in accordance with the checked by comparing the measurement results using the product master. Difference permitted ie 0.04mm or equivalent to two pixels as one pixel calibration measurements in machine vision that is worth to 0.02mm. If the difference between the actual and the results dimension measurements using machine vision greater than 0.04mm machine vision then it should be recalibrated. The time required to re-calibrate approximately 8 hours so that this condition interfere production process.

Based on historical data of production in the PT. JST Indonesia, the average calibration process is done every single week. From the results of investigations and inspections conducted by the maintenance acquired that distance and the angle between a product with a camera no great changes, the maximum changes are only about 0.2 mm caused by linear bearings on a carrier product that is always moving back and forth during the examination process and clearance among the products with the holder of products to facilitate the process of laying and retrieval product during the process. Cameras is fastened using bolts firmly enough with a fixed position. Setting the camera focus was no change and locked in the starting position. The surface of the lens on the camera is in clean condition because cleaning process is carried out every day to avoid dirt or dust that may result in noise in the image when it is done by a machine vision process. One among several factors affecting the change in the measurement results that is done by machine vision is the light intensity factor.

3. Calibration system

The definition of calibration according to ISO/IEC Guide 17025:2005 and Vocabulary of the International Metrology (VIM) is a series of activities that establish a link between the value indicated by the measuring instrument or measuring system, or values represented by a material measure, with values already known relating the magnitude measured under certain conditions. The purpose of

calibration is to achieve measurement traceability. Calibration should be carried out periodically. The time interval is influenced by the type of calibration of measuring instruments, frequency of use, and maintenance.

The size in pixels is converted to the physical of the space. This process is completed by the system calibration. Specific steps are as follows:

- Select a standard part whose size has been known. Size is : S
- When the measurement system is working correctly and measurement of environmental is steady, this standard part is measured using the measurement system to obtain the size in pixels: Sp.
- Calibration factor is calculated according to the formula

$$K = \frac{S}{Sp} \quad (1)$$

K express that the measurement system transformation between pixel size and actual physical dimensions [1].

4. Design of Experiment

Object that is used to check dimension result of machine vision is a bolt that has 17.76 mm length. Web camera with specification 2 mega pixels is set 35mm in front of the object for capture the object image. Light Emitting Diode (LED) is set 50mm behind the camera for giving light to object. Light controller is used to change intensity of light from LED. Digital light sensor type BH-1750 is set 55mm behind the object in order to measure intensity of light that exist in the system and connected to Arduino (single-board microcontroller) that receives input signal from light sensor. Intensity of light is then forwarded to computer by using serial communication between Arduino and computer. Equipment and setting position of design of experiment can be seen in figure 2.

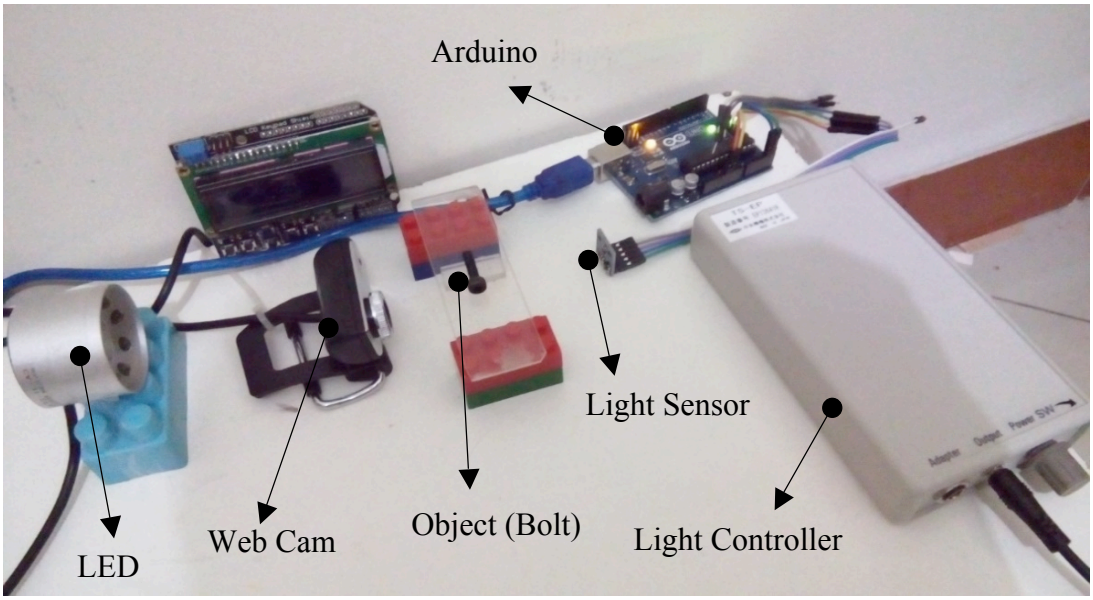


Figure 2. Equipment and setting position of design of experiment

This experiment uses Qt application software for processing the image. First, image is captured every 100 ms. This original image then is processed by using a median filter. This filter is particularly useful to combat salt and peeper noise and has advantage of preserving the sharpness of the edges. It operates on a pixel's neighbourhood in order to determine the output pixel value. The pixel and its neighbourhood form a set of values and, as the name suggests, the median filter will simply compute the median value of this set, and the current pixel is then replaced by this median value [2].

Second, image after filtering is processed to find edges of the object. There are many method that can be used to find edges in image processing. In this experiment used Canny edge detector because it result sharp of edges better [3]

Algorithm in designing of this experiment can be made according to the step below:

1. Start

2. Define length of object and set it in front of camera.
3. Set light intensity until the object can be seen clearly between object and background.
4. Take size of object length in Pixels and calculate object length in mm by using formula to find calibration factor.
5. Input calibration factor in calculation for displaying the measurement result in mm.
6. Check stability of the system by taking data 10 times.
7. If result of the system is stable continue to set light intensity to find correlation between light and measurement dimension of the system.
8. If result of system is not stable back to step 3.
9. Set light intensity step by step from low level to high level.
10. Record the result of measurement for each step of light intensity level.
11. Find correlation between the change of light intensity and measurement result as a factor that must be included in calculation of calibration formula.
12. Input additional calibration factor of light in calculation.
13. Set light intensity step by step from low level to high level.
14. Record the result of measurement for each step of light intensity level.
15. If measurement result is stable it conclude that measurement system can work more stable although light intensity is changed.

Algorithm of QT programming can be seen below.

```
    Mat capture, smooth, edge ;
    timer->start(100);
     // Blur the image so that edges detected by Canny due to noises
will reduced
     medianBlur(capture, smooth, 5);
     for( int i = 0; i < 10; i++)
        medianBlur(smooth, smooth, 5);
     // Edge detection
      Canny(smooth, edge, 80, 80, 3);
        int c=0;
        int y=245;
        for (int x=50; x<edge.cols; x++)
           {
            if(x<550)
              {
                  if(edge.at<uchar>(y,x)>240)
                     {
                      c=c+1;
                      if(c==1)
                         {
                          o=x;
                          p=y;
                         }
                      else
                         {
                          s=x;
                          t=y;
                         }
                     }
               }
             countPixel=s-o;
             dim=countPixel/22.69;
```

First this paper try to set light intensity that is received by light sensor at 14 Lux. Two edge points of object can be seen clearly. In the calibration environment of this experiment it found that length of object is 403 pixels. By using formula above we know that calibration factor of this system is K = 0.044 mm / pixel, it is used as pixel equivalent when it measure the length of the object. Second this

paper try to find stability of result from this measurement system by taking data every 100ms. Stability result can be seen in table.1.

Table 1. Stability result

No.	Light Intensity (Lx)	Size in Pixel	Size in mm
1	10	403	17.76
2	10	403	17.76
3	10	403	17.76
4	10	403	17.76
5	10	403	17.76
6	10	403	17.76
7	10	403	17.76
8	10	402	17.72
9	10	403	17.76
10	10	403	17.76

5. Experiment Result

In order to know correlation between light intensity and measurement result of this system, object that has 17.76mm length is used. According to experiment result, when light intensity is less than 4 (Lx), size of object is less than 17.72 mm. This condition happened because light intensity is poor and it caused edges detection on the object become wrong or miss. The different conditions of light intensity can be seen in figure 3.

(a) (b) (c)

Figure 3. Light intensity 4 Lx (a), Light intensity 10 Lx (b), Light intensity 59 Lx (c).

According to trial that have been done, result of measurement is tend stable when light intensity is above 5 Lx. There is deviation about 1 pixel or 0.04mm when giving light intensity 40 Lx. Data of trial can be seen in Table 2.

Table 2. Measurement result of changing light intensity.

No.	Light Intensity (Lx)	Size in Pixel	Size in mm
1	0	6	0.26
2	1	331	14.59
3	2	392	17.28
4	3	397	17.50
5	4	402	17.72
6	5	403	17.76
7	10	403	17.76
8	21	403	17.76
9	40	402	17.72
10	59	403	17.76

6. Conclusion

Webcam, light sensor, light controller, arduino and PC are used to build the image measurement system. Based on Qt integrated development environment, the measuring interface is designed and the image processing algorithm is written. Length of object is measured based on the system calibration, and the accuracy of the measurement is within 0.09 mm range. Results of system is steady but still failed to get a correlation between the light intensity and the measurement results in this experiment. This research plans to continue by using objects that has radius at the edges, in order to create conditions that similar to actual measurements on connector product.

Acknowledgements

This paper is made possible through the help and support from my advisors and contributors. First and foremost, I would like to thank Dedy Loebis, ST, MBA, M.Sc., Ph.D. for his most support and encouragement. Second, I would like to thank Dena Hendriana, BSc., S.M., Sc.D. and Dr. Ir. Gembong Baskoro, M.Sc.that provide valuable advices,

References

[1] Zang, Weiei, Lulu Yuan (2014). *Applied Study of Size Measurement Based on Image.* Department of electrical engineering, Henan Polytechnic Institute, Nan yang China.

[2] Robert Laganière (2011). *Open CV 2 Computer Vision Application Programming, Cookbook*. PACKT publishing

[3] C. Russ, John (2007). *The Image Processing Handbook, Fifth Edition.* Taylor and Francis Group

The Annual Conference on Management and Information Technology (ACMIT) 2016

Measuring Quality of Service for Real Time Gross Settlement (RTGS) gen 2 Application by Telkomsigma using SERVQUAL

Rosmawati Dwi
Swiss German University, BSD City, Serpong
GSB Arcadia G17 Tangerang 15322
Indonesia
Rosmawati.dwi@gmail.com

Abstract

A service based company has to realize that quality of service and customer satisfaction is a major aspect of the continuity of company's business. It is important for a service company to maintain the satisfaction of their customer. To measure quality service of company like Telkomsigma as one of service based company, we use SERVQUAL. SERVQUAL as an effective and proven approach use to analyze the gaps between customer expectations with the perceptions that indicate the customer satisfaction of Telkomsigma's services especially in Real Time Gross Settlement (RTGS) gen 2. From the research analysis below, we get 92.67 % of SERVQUAL percentage, which means the satisfactory of RTGS gen 2 is very high.

Keywords:SERVQUAL, service, expectations, quality

1. Literature Review

As one of the IT service solutions company, Telkomsigma has to focus on performance improvement of the product so that it can fulfill customer needs. In delivering IT solutions to the customer, it is a must that the services are customer-focused. One of the businesses IT services of telkomsigma is providing core banking systems called Alphabits. One of the products of core banking systems that is developed by Telkomsigma is RTGS (Real Time Gross Settlement). Recently, Bank Indonesia as the central bank in Indonesia, issue the new regulation related to RTGS. So, every bank must change their application to comply with the regulation. This project is called as RTGS gen 2.

Compare with the previous RTGS, there are several differences, like the format of text file, the procedure of sending money within the member, and the process of each steps. Due to the differences of regulations, each employee of banks should adapt and learn this new application and procedure to help them use it.

Question arises when we try to measure how this new concept is adapted:

- Is the product that we delivered is comply with the customer needs?
- How satisfied the customer to have our services?
- Is there any gap between customer needs and our solutions/services?

To answer those questions above, we better get a good understanding about what is service quality, services gaps, and the approach of measuring it.

1.1 Service Quality

Service quality is the extent to which a service meets customer's needs or expectations[1]. It can also be defined as the difference between customer expectations of service and real service. If the expectations are higher than the performance, then the quality of service is less than satisfactory and gaps of quality occurs[2]. We need the tool to measure the quality of cloud services for BPR and to know the gaps between the expectations and the perceived services. SERVQUAL is one of the approach uses for analyzing factors of quality services. It has been using as an instrument to measure the quality of services since 1988.

1.2 Model of Service Quality Gaps

There are seven gaps in the service quality concept, which are shown in Figure 1:

- **Gap 1 : Customers' expectations vs management perceptions :** a result of lack of marketing research orientation, inadequate communication and too many step of management.
- **Gap 2: Management perceptions vs service specifications:** a result of lack commitment to quality, a perception of unfeasibility, insufficient task standardisations and lack of goal setting.
- **Gap 3: Service specifications vs service delivery :** a result of role ambiguity and conflict, poor employee-job fit and poor technology-job fit, not suitable control systems, lack of perceived control and insufficiency of teamwork.
- **Gap 4: Service delivery vs external communication :** a result of inadequate horizontal communications and prosperity to over promise.
- **Gap 5: The gap between customer expectations and their perceptions of the service delivered :** the result of the influences exerted from customer side and the gaps on the part of service provider. In this case, the customer expectations are influenced by the personal needs, word of mouth recommendation and past experiences.
- **Gap 6: The difference between customer expectations and employees' perceptions :** the result of the differences in the concept of customer expectations by service providers.
- **Gap 7: The gap between employee's perceptions and management concept:** the result of the differences in the concept of customer expectations between managers and providers.

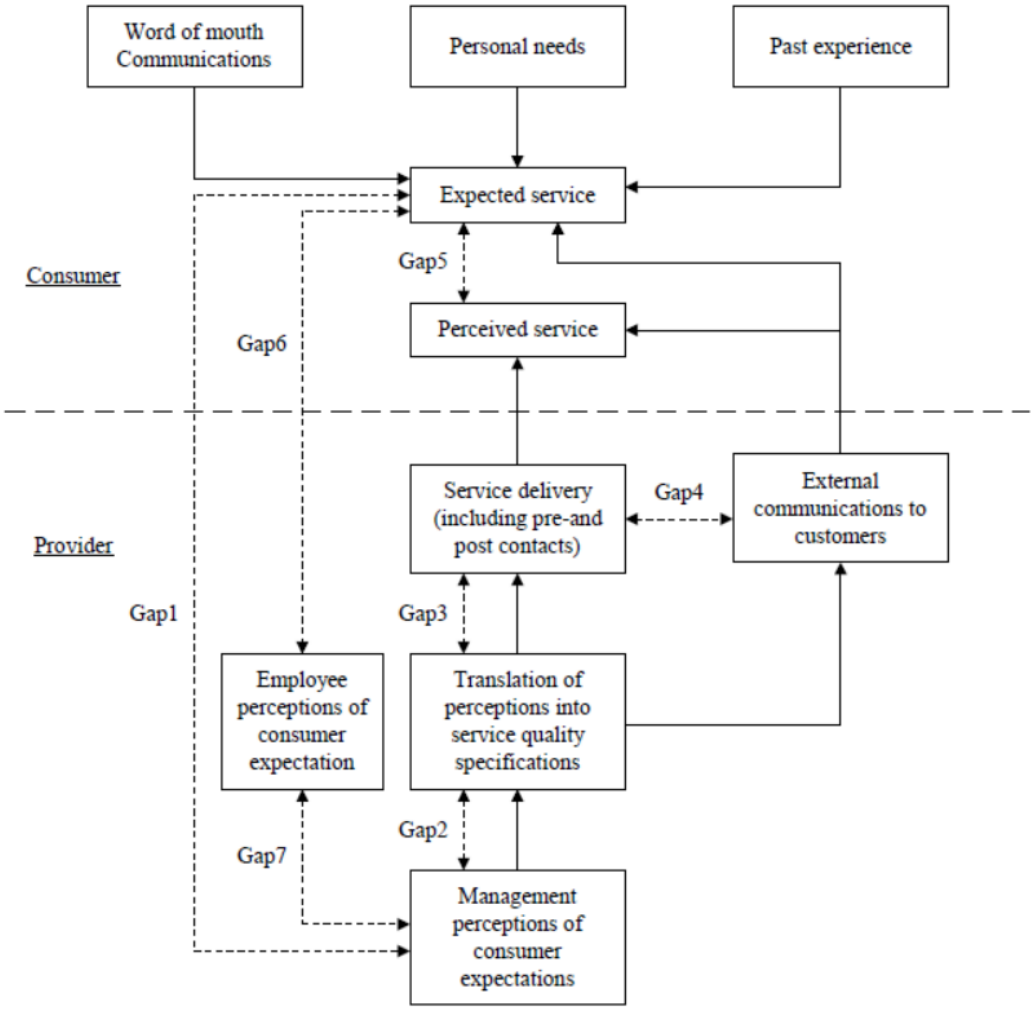


Figure 1. Models of service quality gaps (Parasuraman et al., 1985; Curry, 1999; Luk and Layton, 2002)

The model identifies seven key discrepancies relating to managerial perceptions of quality of service, and tasks related with service delivery to customers. The six gaps (Gap 1, Gap 2, Gap 3, Gap 4, Gap 6 and Gap 7) are identified as functions of the way in which service is delivered, whereas Gap 5 mentions to the customer and is considered to be the valid measurement of service quality. The Gap that the SERVQUAL methodology has influence is Gap 5.

2. Research Methodology and Framework

Measurement of quality services has become interesting research and opinions about how the perspective of services value is being measured. One service quality measurement model that has been applied is the SERVQUAL model. The SERVQUAL tool has been the main method used to measure customers' perceptions of service quality. It has five factors and are stated as follows (van Iwaarden *et al.*, 2003)[3]:

(1) *Tangibles* . Facilities, equipment and appearance of employee.
(2) *Reliability*. Ability to perform the stated service reliably and accurately.
(3) *Responsiveness*. Compliance to help customers and provide fast service.
(4) *Assurance.* Knowledge and modesty of employees and their ability to inspire belief and confidence.
(5) *Empathy* (including communication, access, understanding the customer). Caring and individualized attention that the company provides to its customers.

In the SERVQUAL tool, 22 list of statements (Appendix I) measure the performance over these five factors, using a seven points of weight measuring customer expectations and perceptions (Gabbie and O'neill, 1996). It is noted that without adequate information on the quality of services expected and perceptions received then feedback from customer surveys can be potentially misleading from both a policy and an operational perspective**.**

4.1.3 Data Sampling and Analysis

3.1. Data Input

According to the member of banks that become Telkomsigma's customer, there are 11 banks that use RTGS gen 2 applications. To collect the data, the author gives the questioners to these representatives. There are 15 questioners from member banks of telkomsigma that are answered the 22 questions. The questions focus on the RTGS gen 2 application that they are tested and how the support of our employees of this application. The questioner range is converted into likert scale (1-5).

3.2. Data Processing

In servqual method, there are two variables X and Y, where Y is a score of expectation aspect of the services and X is the score of the consumer perceptions. Below are the formulas of these two variables[4]:

$$X = \frac{\sum_{I=1}^{N}}{K} Xi \quad \text{..... (1)} \qquad \text{and} \qquad Y = \frac{\sum_{I=1}^{N}}{K} Yi \quad \text{.....2)}$$

Note: K is the numbers of attributes or questions that can influence the customer's satisfactions

There is also the formula to measure the average of the customer satisfaction:

$$\overline{X} = \frac{\sum Xi}{n} \quad \text{..... (4)} \qquad \overline{Y} = \frac{\sum Yi}{n} \quad \text{..... (5)}$$

To measure the percentage of quality services, below is the formula:

$$\mathbf{Q} = \frac{\overline{X}}{\overline{Y}} x100\% \text{.....(3)}$$

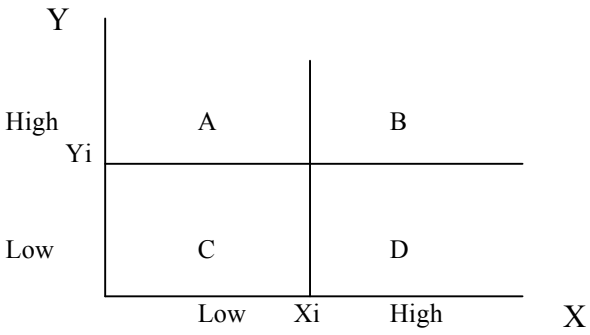
Note: Q = The percentage of quality services
$\overline{X}$ = Score of customer's perception

$\overline{Y}$ = Score of customer's expectation

Minnesota Satisfaction Questionnaire (MSQ) use the format of Likert scales to get the satisfaction score in some criteria (Steers, 1993). The criteria of scoring percentage are:

1. 20- 40 % : Low Satisfaction
2. 41- 79 % : Middle Satisfaction
3. 80 - 100 % : High Satisfaction

Below is the cartecius diagram of the range of customer perception and customer expectation:



Note:

- A shows us the attribute that influent the customer's satisfaction, including the services that is assumed as important to the customer but the management or employee doesn't comply the customer needs well.
- B has shown us that the services are successfully delivered to the customer by the service provider company, so this quality of service should be maintained. It is very important and very satisfying.
- C shows us some factors that are less important to the customers, and the services are very common. So it is less important and less satisfying.
- D shows us the factors that are less important for customers, but the execution of services is too high. So it is less important but very satisfying.

3.3. Result and Analysis

From the questioners, the author measures the customer satisfaction using RTGS gen 2 from 15 samples, so:

The average customer perception ($\ddot{X}$) = $\frac{59.12}{15}$ = 3.94

The average customer expectation ($\overline{Y}$) = $\frac{63.8}{15}$ = 4.25

From these two results, we can get the quality of services (QoS) or the average of customer satisfactions:

$$Q = \frac{3.94}{4.25} \times 100\% = \mathbf{92.67\ \%}$$

Based on steers criteria, the result of the average customer satisfaction is on the range of 80 – 100%, which means the average satisfaction of this RTGS gen 2 application is **very high**. Now, we measure each instrument of the questioners to find out the gaps of each service. Below is the table of the result analysis of RTGS gen 2 applications to the customer:

Table 1. Table of Gaps Analysis of Each Instrument of the Questioners of RTGS gen 2

Variable	Items	Average Score		Gaps	Quadrant
		Perception	Expectation		
Tangibles					
1	Tools & Technology of RTGS 2	3.95	4.29	-0.34	B
2	Connection	4.05	4.29	-0.24	B
3	Feature & Friendly Application	3.57	4.29	-0.72	A
4	Functional Application	3.86	4.29	-0.43	A
Reliability					
5	Delivery time	4.1	3.57	0.52	D
6	Reliable to support of the issue	4.05	3.57	0.48	D
7	Delivering support	4.05	4.29	-0.24	B
8	Appropriate Solution offers	3.71	5	-1.29	A
9	Accuracy of problem analysis	3.86	4.29	-0.43	A
Responsiveness					
10	Cooperation in delivering Apps	3.81	3.57	0.24	C
11	Always responds all the issue	3.9	5	-1.1	A
12	Customer perspective goal	4	5	-1	B
13	Giving best suggestion	4.05	5	-0.95	B
Assurance					
14	Trusted and has credibility	4.24	4.29	-0.05	B
15	Secure to use the application	3.86	4.29	-0.43	A
16	Professionalisms	4.1	4.29	-0.19	B
17	Helpful	4	4.29	-0.29	B
Empathy					
18	Giving full focus	3.76	4.29	-0.53	A
19	Personal approach	4	3.57	-0.43	D
20	Knowing customer needs	3.81	3.57	0.24	C
21	Treat the customer seriously	4.14	4.29	-0.15	B
22	24 hours support	3.86	4.29	-0.43	A
TOTAL		86.71	93.57		
AVERAGE		**3.94**	**4.25**		

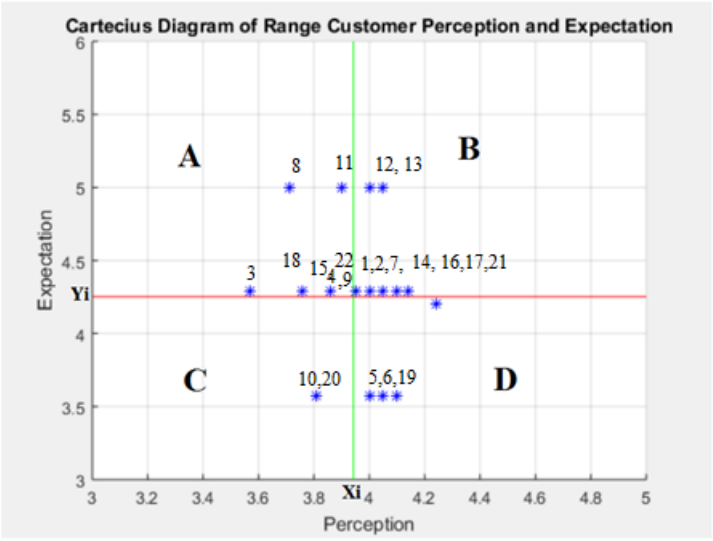


Figure 2. Cartecius Diagram of Range Customer Perception and Expectation of RTGS gen 2

From the table above, we can see that there are some negative gaps and positive gaps between customer's perspective and customer's expectations. The highest gap comes from the responsiveness. The customer's expectation of RTGS support response is very high. So it needs more effort for the employee to support all the RTGS issue that comes from customer. This solution can be provided by

adding the number of employee that support the RTGS and adding the skill to support the RTGS apps so that the handling of all issue can be as fast as possible.

If we see the quadrant of the customer satisfaction, the most shown is in quadrant B. It means most of services in RTGS gen 2 applications is important and been delivered satisfactorily. But, there are also some factors that from the customer point of view is very important but the company give less effort on it (A); **these factors should be the most priority** of the company to improve the quality of service so that it can comply the customer expectation.

4. Conclusion

From the analysis based on the data above, we can conclude that:

a. Based on Steers criteria of customer satisfaction, the service of RTGS gen2 application lays on the range of 80-100 %; which is 92.67 %. That means the customer's satisfactory of the service is very high.
b. There are still gaps between the customer's perception and customer's expectation; those gaps arise from the different between customer needs and the service that has been delivered like in quadrant A. The company should take more attention to improve the services so that it can meet the customer's expectation.

5. Future Work

To improve this research about quality of services, we can use another method beside SERVQUAL methods, like Analytic Hierarchy Process (AHP). We can also combine SERVQUAL methods with other methods like Lean Six Sigma methods to get better result of this research and adding value to the Quality of Service.

Beside the methods, we also can improve this research by using another technique of collecting data. We can use more sample of data, and spread the questioners to all of officers of banks not only to the IT officers in order to get another perspective and opinion about the applications.

References

[1] A. Shahin, SERVQUAL and model of service quality gaps: A framework for determining and prioritizing critical factors in delivering quality services. Andhra Pradesh: ICFAI University Press, 2006.
[2] A. Parasuraman, V. A. Zeithaml, and L. L. Berry, "Servqual," J. Retail., vol. 64, no. 1, pp. 12–40, 1988.
[3] J. van Iwaarden, T. van der Wiele, L. Ball, and R. Millen, "Applying SERVQUAL to web sites: An exploratory study," Int. J. Qual. Reliab. Manag., vol. 20, no. 8, pp. 919–935, 2003.
[4] H. J. Astuti, "ANALISIS KEPUASAN KONSUMEN (SERVQUAL Model dan Important Performance Analysis Model)," Media Ekon., vol. 7, no. 1, 2007.

Appendix A. Questioner Paper

QUISIONER RTGS GEN 2

Quisioner ini diberikan untuk memudahkan penulis dalam menganalisa kepuasan pelanggan atas Aplikasi RTGS gen 2 yang akan dideliver oleh sigma ke beberapa bank member Sigma. Tujuan dibuat quisioner ini adalah untuk pemenuhan tugas kuliah penulis di SGU. Data-data yang diberikan dijamin kerahasiaannya oleh penulis dan tidak akan disebarluaskan tanpa ijin. Mohon untuk dapat mengisi quisioner ini dengan sejujur-jujurnya dan sebenar-benarnya agar data yang diolah valid.
Petunjuk pengisian quisioner:
Jawab pernyataan-pernyataan dibawah ini dengan tanggapan 1-7 (1= Sangat tidak setuju, 2 = Kurang setuju, 3 = Agak kurang setuju , 4 = agak setuju, 5 = setuju , 6 = setuju sekali, 7 = sangat setuju sekali).

	No	Tanggapan
1. Aplikasi RTGS gen 2 yang akan dideliver sudah memenuhi standar aplikasi yang BI persyaratkan termasuk server dan network.	1	
2. Koneksi applikasi sigma dengan BI terhubung dengan baik dan stabil.	2	
3. Tampilan aplikasi RTGS gen 2 sudah user friendly dan mudah dimengerti	3	
4. Tampilan aplikasi RTGS gen 2 sudah sesuai dengan fungsinya untuk memprovide transaksi antar bank peserta	4	
5. Dari sisi delivery time, Sigma sudah berusaha mendelivery aplikasi RTGS gen 2 sesuai dengan waktu yang ditentukan bahkan lebih cepat	5	
6. Ketika ada issue atau masalah terkait aplikasi RTGS gen 2, tim sigma memberikan masukan dan jawaban dengan simpati dan meyakinkan	6	
7. Tim support sigma dapat diandalkan dalam mendeliver aplikasi RTGS gen 2	7	
8. Tim sigma memberikan solusi thd permasalahan yang ada sesuai dengan yang diharapkan	8	
9. Analisa terhadap masalah yang ada cukup akurat	9	
10. Tim support RTGS sigma kooperatif dalam memberitahukan kapan aplikasi RTGS siap dipakai	10	
11. Tim support RTGS sigma selalu merespon setiap pertanyaan/permintaan dari customer	11	
12. Tim support RTGS sigma selalu bertujuan untuk membantu customer di setiap permasalahan yang ada	12	
13. Tim support RTGS sigma merespon setiap issue dengan sigap dan tanggap dan berusaha mencarikan solusi terbaik untuk customer	13	

14. Anda percaya akan kredibilitas tim support RTGS sigma	14	
15. Anda merasa aman menggunakan aplikasi RTGS gen 2 ini dalam bertransaksi	15	
16. Tim support sigma bersikap professional selama project RTGS gen 2	16	
17. Anda merasa terbantu dengan adanya tim support RTGS sigma untuk bertransaksi menggunakan aplikasi RTGS gen 2	17	
18. Tim RTGS sigma memberikan perhatin penuh terhadap customernya	18	
19. Tim RTGS sigma melakukan pendekatan personal guna menjaga hubungan baik dengan customer	19	
20. Tim RTGS sigma tahu kebutuhan customernya	20	
21. Anda suka dan menghargai kesungguhan tim support RTGS sigma	21	
22. Tim RTGS sigma siap 24 jam untuk melayani keluhan pelanggannya terkait RTGS gen 2	22	

Terimakasih atas kesediaan saudara untuk mengisi quisioner ini.

The Annual Conference on Management and Information Technology (ACMIT) 2016

A Study on Customer's Perception of Internet Banking Services using Risk Apetite Framework

Dr. Ir. Moh. A. Amin Soetomo, M.Sc.[2], Arief Kusuma, BBA[b]*
[a]*Swiss German University, EduTown BSD City, Tangerang 15339, Indonesia*
[b]*Swiss German University, EduTown BSD City, Tangerang 15339, Indonesia*

Abstract

There are many technology breakthroughs today so that for banking delivery channel could cover people from the big city even rural areas today. The advancement of both technology and telecommunication has stimulated transaction for banking industry in overall. Internet Banking is becoming a trend in banking industry. One of the multi channel distribution of financial services industry is through internet streams. It helps the banks to open up new channel, reduce the costs, improve the services, enlarge customer portfolios and creates innovative products. The Internet Banking is being used as a strategic weapon to gain and retain customers. The paper covers customer's Perception on Internet Banking services using risk appetite & tolerance framework in accordance with management decision (IT Steering Committee)

Keywords: Internet Banking; Risk Apetite; Risk Tolerance; IT Steering Commitee;

1. Introduction

Today, Indonesia has more than one hundred banks existing under fierce competition from local banks and foreign banks. The Banks are looking for new way of optimizing and maximizing their profits through new and cost effective delivery channel streams. In addition, the Banks are offering the added value services to their customers in order to retain and attract more customers. Banking industry is offering customer experience with the customers through alternating delivery channel. Banking technology plays important and strategic role in the advancement of the alternating channel and the interactions between customers and banks. The Internet Banking is transforming the banking sector to run its business through inline platform so called Internet Banking or online banking. The Internet Banking offers personalized services to the customers through portals. The Internet Banking involves the usage of internet for delivery of products and services. The Internet Banking provides customers do the transactions at anytime and at anywhere with cost efficient and cost effective. The paper highlights the user's perception towards the Internet Banking using the risk appetite & tolerance framework. The decision makers for Internet Banking policy comprising of management of the Bank. Any implementations of the IT systems within the Banks will the responsibility of the respected Banks at Leles, Garut.

4.1.4 Statement of the Problem

The Banking industry focus on the customer excellence by providing a fast and satisfied services to the customers as customers play important role in banking industry. The old traditional functions of banking are limited and being left by most banks today. With Economic reforms initiated by the government of Indonesia in the mid 1990's have brought big change on how Indonesia banks operate and functions in the financial services industry. There are much more customers demand faster services

* Corresponding author. Tel.: +62 21 3045 0045 ; fax: +62 21 3045 0001
E-mail address: mohammad.soetomo@lecturer.sgu.ac.id, arief.kusuma@student.sgu.ac.id

from Bank's delivery channel streams in timely manner and cost effective/cost effective. Most banks worldwide have implemented mission critical core banking systems which is scalable, available and also provide online banking to the customers. Internet Banking provides new wave opportunities for banks in order to grow the markets and services locally and regionally. The Internet Banking has provided ease and flexibility in banking operations to the benefit of customers. The Internet Banking has made the customers forget the old traditional banking which has limited time banking and with a local area operation only. Hence, most customers prefer Internet Banking services due to its enormous benefits.

This study is provides an opportunity to know role of Internet Banking services in commercial banks and how customer satisfaction is analyzed. This study is also to measure of risk appetite & tolerance in regarding to customer's Perception of Internet Banking services (six commercial banks) at Leles, Garut

4.1.5 Scope of the Study

The conventional banking stays the most common operation for banking transaction. However, the technology advancement of internet has transformed the banks to deliver personal services to the customers drastically. Today, Commercial banking is introduced Internet Banking system to improve and reduce operational costs in overall. Despite the banks are endeavouring to establish better and easier Internet Banking system, these systems remain unnoticed by the customer. Hence, there is an urgency to recognize end user or so called business requirements of Internet Banking and a need to identify the determinants of the implementation of the Internet Banking. In addition, it includes the measurement of risk appetite and tolerance of commercial banks at Leles, Garut whereby the decision makers involving IT engineers, Group Head of IT, CEO, and IT Steering Committee.

4.1.6 Review of Literature

"Customer satisfaction through information technology in commercial banks' highlighted that, customers are satisfied with banking services to some extent and the bankers should try to improve services at an affordable cost with the help of information technology [11].

The paper explained the advantages and the security concerns about Internet Banking. According to him, improved customer access, offering of more services, increased customer loyalty, attracting new customers are the primary drivers of Internet Banking. But in a survey conducted by the online banking association, member institutions rated security as the most important concern of online banking [2].

Collected customers' opinions regarding the importance of e-Banking and the adoption levels of different e-Banking technologies in Indonesia and Kenya [1]. The study focuses on the latest of Internet Banking trends in both countries. The overall result indicates that customers in two countries that have establish a positive sign as they give much importance to the emergence of e-banking.

4.1.7 Objective of the Study

The objectives of the study comprising of:

- To analyze the reasons for bank account's opening.
- To find out the reasons for choosing Internet Banking services
- To understand the facilities mostly benefited by the respondents and the opinion on the services.
- To measure the customer satisfaction level.
- To measure risk appetite and risk tolerance which involve the decision makers of the IT policy ranging from IT engineers, Group Head of IT, CEO, and IT Steering Committee

4.1.8 Hypothesis

The objectives of the studies is developing the following null hypothesis.

1. There is no relationship between the socio economic and customer satisfaction
2. There is a relatiohip berween the risk appetite & tolerance level and the implementation of IT Banking Policy & IT Governance of the Banks.

4.1.9 Research Methodology

Data is a critical component in any study has been gathered through various resources. The researcher is using primary data for this study.

Primary Data
Primary Data are being collected from the study questionnaire taken from 300 respondents.

4.1.10 Tools for Analysis

The researcher is exercising the Percentage, Correlation and GAP Analysis, Risk Apetite & Tolerance Framework while probing and translating the data.

The governance process is the means of mechanism done by an organization structure in order to do the functions and to do the tasks in order to realize its commitments and governance structure in order to achieve governance outcome in accordance to Good Corporate Governance Guidance Principles.

Governance process comprising of :

1. Annual General Meeting Shareholders
2. The implementation of functions, job description, and roles & responsibilities of Board of Commissioners and Board of Directors
3. The implementation of the activity of Bank's business
4. The management of human resources
5. The responsibility of corporate social responsibility and environment
6. IT *governance*
7. The management of company's subsidiaries
8. The socialization programme of Bank's policy
9. Process documentation

The implementation of Risk Apetite & Tolerance whereby the IT Internet Banking Policy shall be based on the results of IT Steering Committee decision making process. The analysis of Risk Apetite and Tolerance can be seen in the below table.

4.1.11 Sampling Design

Leles, Garut West Java is so called "Dates" (Dodol) and "Leather City". Leles, Garut, West Java is known as a agriculture city generating rice. Most of these products (dates and leather) are exported to various countries such as Europe and United States. Similarly it's also known for Örange City in around 1970's. These industries are providing more business opportunities to the people more than the other areas in Leles, Garut. To facilitate the entrepreneur and other people six commercial banks are available with the Internet Banking Services. The numbers of Internet bank users are increasingly higher these days. So the researcher has adopted convenient sampling method and selects the 300 respondents from the all six banks.

4.1.12 Analysis and Interpretation

1.1. KIND OF ACCOUNT

Today banks offer variaties of account for different types of customer. The collection of data (type of account) depicted in Table 1.1.

Table 1.1
Type of Account

NO	Kind of Account	Number of Respondents	Percentage
1	Savings	62	20.67
2	Current	152	50.67
3	Payroll	48	16.00
4.	Cash Credit	38	12.66
	Total	300	100.00

Source: Primary Data (Banks at Leles, Garut, March 2015)

It is shown on the Table 1.1 which is out of 300, 20.67 percent respondents have savings bank account, 50.67 per cent owning current account, 16 percent of the persons being interviewed own salary accounts, and the remaining 10 percent of own time-deposit account.

1.2. INFORMATION SOURCES ABOUT INTERNET BANKING

The banks provide kinds of services to the customer occasionally. For most part, the current services provided by the bank is properly socialized to the customers. Hence, the researcher gathers the information directly through the respondents in regarding to Internet Banking services. The statistics shown in Table 1.2.

Table 1.2
INFORMATION ORIGINATION ABOUT INTERNET BANKING SERVICES

NO	Sources	Number of Respondent	Percentage
1	Advertisement	120	40.00
2	Friends and Families	63	21.00
3	Bank Employee	86	28.67
4	Bank Website	31	10.33
	Total	300	100.00

Source: Primary Data (Banks at Leles, Garut, March 2015)

It is shown the Table 1.2 which is out of 300 respondents, 40 percent have known from advertisement, 21 per cent the origination of information got from friends and families, 28.67 percent of the customers acknowledge the Internet Banking service via bank staff and the remaining 10.33 percent of the respondents obtained information from the website.

1.3. REASONS FOR THE USE OF INTERNET BANKING FACILITIES

Internet Banking provides charm faculties to the respondents. The investigator compiled all information in regarding to the elements which drive the respondents to transact online banking facilities. Table 1.3 shows the major reasons for utilizing the electronic banking.

Table 1.3
REASONS FOR THE USE OF INTERNET BANKING FACILITIES

NO	Reasons	Number of Respondents	Percentage
1	Fund transfer	144	48.00
2	Electronic Bill display and payment	44	14.67
3	Checking Accounts balance	64	21.33
4	Electronic bill payment	36	12.00
5	Purpose of Business	12	4.00
	Total	300	100.00

Source: Primary Data (Banks at Leles, Garut, March 2015)

It is shown from Table 1.3 that out of 300 respondents those who use Internet Banking services, 48 percent of the respondents use for Inter account fund transfer, 14.67 percent of the customers for Electronic Bill presentation and payment use of the Internet Banking, 21.33 percent choose for checking account balance, 12 percent use for online settlement of the bill, the remaining 4 percent choose to Deposit and withdraw money.

1.4. OPINIONS ABOUT SERVICE CHARGES OF INTERNET BANKING

The bank gathers service charges from the accounts owners for accomodating Internet Banking services. The researcher gathered information of service charges regulated the bank and shown in the Table 1.4.

Table 1.4
OPINION ABOUT THE SERVICE FEES

NO	Level Of Service Charges	Number of Respondents	Percentage
1	Very high	24	8.00
2	High	88	29.33
3	Mild/Modest	116	38.67
4	Low	72	24.00
	Total	300	100.00

Source: Primary Data (Banks at Leles, Garut, March 2015)

It is shown from the Table 1.4 that out of 300 respondents, 8 percent give opinions about are very high, and 29.33 percent stated that the charges are high, 38.67 percent say moderate and the remaining 24.00 percent say that services charges are relatively low.

1.5. Problems faced by the Respondents

Even though the bank furnishes type of Internet Banking services of to customers, somehow it creates inferior problems. The researcher saw some common matters faced by the respondents while transactiong Internet Banking. It is shown in the Table 1.5.

Table 1.5
PROBLEMS

NO	Problems	Number of Respondents	Percentage
1	Network failure	87	29.00
2	Error in operation	61	20.33
3	No security for internet dealing	83	27.67
4	No Authenticated records	52	17.33
5	Low Speed and Delay	17	5.67
	Total	300	100.00

Source: Primary Data (Banks at Leles, Garut, March 2015)

It is shown from Table 1.5 that out of 300 respondents 29 percent of the respondents experience network problems, 20.33 percent of the respondents experience error in operation, 27.67 percent of the respondents say that there is no security in Internet Banking transaction, 17.33 percent feel that there is no authentication logs and the remaining 5.79 percent of the respondents feel that network delay.

1.6. GAP ANALYSIS ON THE RESPONDENTS PERCEPTION

The expectations of respondents data in regarding to service quality dimension ranging from effficiency, fullfillment, system availability, privacy, assurance & trust, responsiveness, contact, and website aesthetics [19] were meant to measure the 'gap' that is existing on the respondent's perception. The gap analysis was done for eight dimensions of service quality. This level is meant to measure the mean. As a reference that the means value of '5' was considered to be the maximum value to accomplish the gap, i.e. the discrepancy between the expected and the experienced mean score is so called the "service gap". Table 1.5 shows the service gap on all eight service quality dimensions of Internet Banking.

Table 1.6
GAP ANALYSIS OF THE SATISFACTION LEVEL OF RESPONDENT ON INTERNET BANKING SERVICE

Dimensions	Expected Mean Scor	Experienced Mean Score	Service GAP
IB Confident	5	4.081081	0.918919
IB Login	5	3.932432	1.067568
IB Information	5	3.972973	1.027027
IB Satisfied	5	3.986486	1.013514
IB Security	5	3.648649	1.351351

Source: Primary Data (Banks at Leles, Garut, March 2015)

Scale of 2.5 of Service GAP was treated as critical area for improvement of the dimensions. A scale of 1.5 of service GAP was treated less significant and hence it does not require remedy and the discprepancy of scale of 1.5 to 2.5 was considered as crucial and it needed further improvement. It has been shown that the following services need further improvements.

The above GAP analysis showed that, the customer are content with the all the dimension of Internet Banking Services.

1.7. Satisfaction Level of the customer

The researcher has aggregated information about the Internet Banking users' satisfaction level and shown at the Table 1.7.

Table 1.7
SATISFACTION LEVEL

NO	Level of Satisfaction	Number of Respondents	Percentage
1	Highly Satisfied	123	41.00
2	Satisfied	89	29.67
3	Moderate	55	18.33
4	Unsatisfied	21	7.00
5.	Highly unsatisfied	12	4.0
	Total	300	100.00

Source: Primary Data (Banks at Leles, Garut, March 2015)

It is shown from the Table 1.7 that out of 300 respondents, 41 percent of the respondents are highly satisfied with the Internet Banking services and 4 percent of the users are not content with the Internet Banking services.

Reviewing of Hypothesis

There is no relationship between socio economic and customer satisfaction. To review the hypothesis, the researcher has applied correlation analysis.

Table 1.7 (A)
RELATIONSHIP BETWEEN SOCIO ECONOMIC AND INTERNET BANKING SERVICE

Variables	Gende	Age	Qualification	Employed	Sex	Income	Marita
Internet Banking	-.151	.065	-.134	-.041	.172	-.255	.103

Table 1.7 (A) indicates that Internet Banking services do not have high positive correlation with the socio-economic factors. The correlation analysis points out positive relationship with age (0.065), category (.172), marital status (.103) and negative relationship with gender(-.151), qualification (-.134), employment (-.041), income (-.255). Hence, the hypotheses are being rejected. In summary, the socio economic factors ranging from gender, qualification, employment and income coorelate with the customer satisfaction level base on the study as those factor mentioned above are negative.

The analysis of Risk Apetite and Tolerance

Table 1.8

PROCESS

Level	RG1.1 Perform enterprise IT risk assessment.	Score	Weight	WeightXlevel
0	Sponsor workshops with business management to discuss the broad amount of risk that enterprise is willing to accept in pursuit of its objectives (risk appetite).	0.25	0.01562	0
	Help business managers understand IT risk in the context of scenarios that affect their busin and the objectives that matter most in their daily lives	0.5	0.03125	0
	Take a top-down, end-to-end look at business services and processes and identify the ma points of IT support	0.5	0.03125	0
	Identify where value is generated and needs to be protected and sustained	0.5	0.03125	0
	Identify IT-related events and conditions that may jeopardize value, affect enterpr performance and execution of critical business activities within acceptable bounds, or otherw affect enterprise objectives (e.g., business, regulatory, legal, contracts, technology, trading partn human resources, and other operational aspects).	0.25	0.01562	0
	Map them to a business-driven hierarchy of risk categories (e.g., IT benefit/value enableme IT programme and project delivery, IT operations and service delivery) and subcategories (IT r domains) derived from high-level IT risk scenarios.	0.25	0.01562	0
	Break up IT risk by lines of business, product, service and process.	0.5	0.03125	0
	Identify potential cascading and coincidental threat types and the probable effect of r concentration and correlation across silos.	0.25	0.01562	0
	Understand how IT capabilities contribute to the enterprise's ability to add value and withsta loss.	0.25	0.01562	0
	Compare management's perception of the importance of IT capabilities to their current state	0.5	0.03125	0
	Consider how IT strategies, change initiatives and external requirements (e.g., regulati contracts, industry standards) may affect the risk profile	0.5	0.03125	0
	Identify risk focus areas, scenarios, dependencies, risk factors and measurements of risk t require management attention and further examination and development.	0.25	0.01562	0
Level	RG1.2 Propose IT risk tolerance thresholds.			
1	Establish the amount of IT-related risk a line of business, product, service, process, etc., willing to take to meet its objectives (risk appetite).	0.5	0.03125	0.03125
	Express limits in measures similar to the underlying business objectives and against accepta and unacceptable business impacts.	0.25	0.01562	0.015625
	Consider any trade-offs that may be required to achieve key objectives in the context of ri return balance	0.5	0.03125	0.03125
	Propose limits and measures in the context of IT benefit/value enablement, IT programme a project delivery, and IT operations and service delivery, and over multiple time horizons (e immediate, short-term, long-term).	0.25	0.01562	0.015625
Level	RG1.3 Approve IT risk tolerance.			
2	Evaluate proposed IT risk tolerance thresholds against the enterprise's acceptable risk a opportunity levels.	0.25	0.01562	0.03125
	Take into account the results of enterprise IT risk assessment and trade-offs required to achie key objectives in the context of risk-return balance	0.5	0.03125	0.0625
	Consider the potential effects of IT risk concentration and correlation across lines of busine product, service and process. Determine whether any unit-specific tolerance thresholds should applied to all business lines.	0.5	0.03125	0.0625
	Define the types of events (internal or external) and changes to business environments	0.25	0.01562	0.03125

	technologies that may necessitate a modification to the IT risk tolerance.			
	Approve IT risk tolerance thresholds.	0.5	0.03125	0.0625
Level	RG1.4 Align IT risk policy.			
3	Codify IT risk appetite and tolerance into policy at all levels across the enterprise	0.5	0.03125	0.09375
	Recognize that IT risk is inherent to enterprise objectives and document how much IT risk desired and allowed in pursuit of those objectives	0.25	0.01562	0.046875
	Document risk management principles, risk focus areas and key measurements	0.25	0.01562	0.046875
	Adjust IT risk policy based on changing risk conditions and emerging threats	0.25	0.01562	0.046875
	Align operational policy and standards statements with risk tolerance.	0.5	0.03125	0.09375
	Perform periodic or triggered reviews of operational policy and standards against IT risk pol and tolerance	0.5	0.03125	0.09375
	Where there are gaps, set target dates based on acceptable risk exposure time limits a required resources	0.25	0.01562	0.046875
	Where appropriate, propose adjustments to risk tolerance instead of modifying established a effective operational policy and standards.	0.25	0.01562	0.046875

Table 1.8

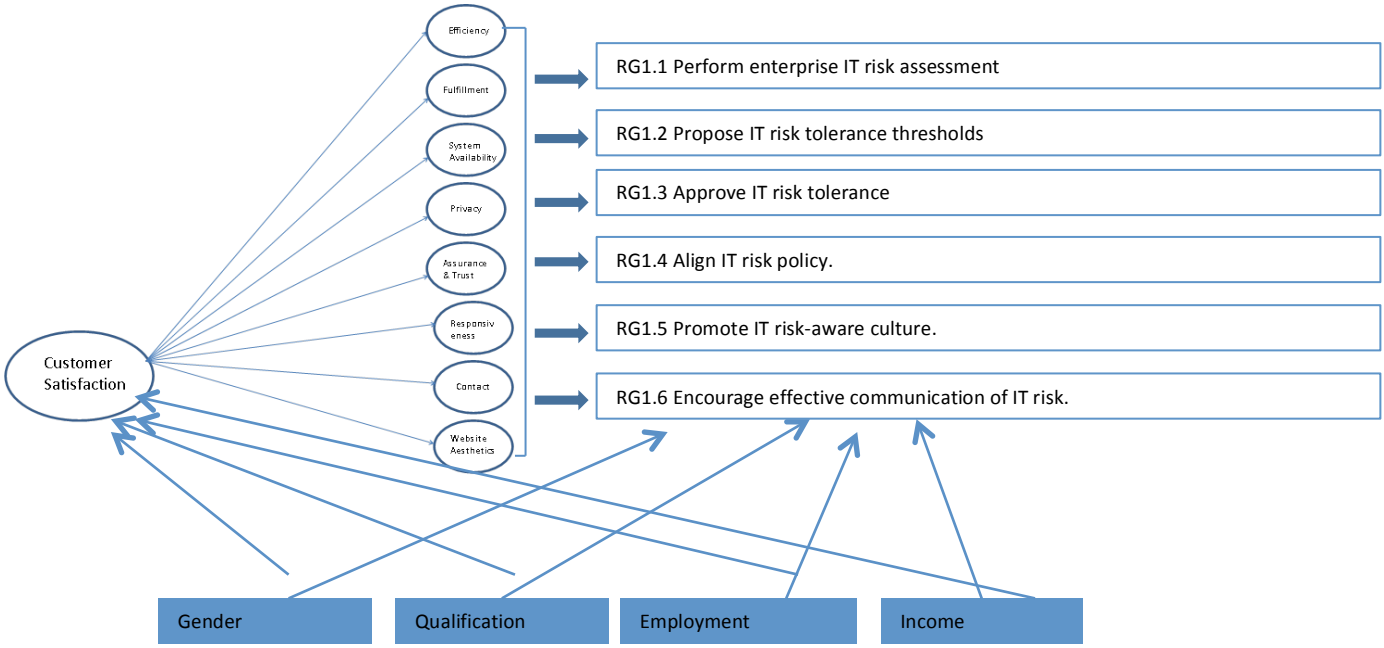
PROCESS

Level	RG1.5 Promote IT risk-aware culture.	Score	Weight	WeightXlevel
4	Based on an understanding of the current risk culture, empower the enterprise to proactiv identify IT risk, opportunity and potential business impacts	0.5	0.03125	0.125
	Encourage employees to address IT risk issues before serious escalation is required. Tr business and IT staff on threats, impacts and the enterprise's planned responses to specific r events	0.5	0.03125	0.125
	Communicate the 'why you should care' message for risk focus areas, and explain how to ta risk-aware actions for situations not specified in policies	0.25	0.01562	0.0625
	Walk through scenarios for areas not directly covered by policy, and reinforce expectations understanding general policy direction and using good judgment	0.25	0.01562	0.0625
	Demonstrate an attitude that encourages discussion and acceptance of the appropriate amou of risk	0.25	0.01562	0.0625
	Be positive about promoting a risk culture appropriate for IT and aligned with enterprise ri aware culture.	0.5	0.03125	0.125
Level	RG1.6 Encourage effective communication of IT risk.			
5	Establish and maintain a risk communication plan that covers IT risk policy, responsibiliti accountabilities and the risk landscape (e.g., threats, controls, impacts, root causes, busin decisions).	0.5	0.03125	0.15625
	Feature filters in the plan so it is clear, concise, useful and directed to the right audience.	0.5	0.03125	0.15625
	Perform frequent and regular communication between IT management and business leaders regarding IT risk issue status, concerns and exposures.	0.25	0.01562	0.078125
	Align IT risk communication with enterprise risk terms	0.25	0.01562	0.078125
	Consistently priorities in a manner that aligns with the enterprise definition of business risk	0.25	0.01562	0.078125
	Express IT Risk in business strategic and operational terms	0.5	0.03125	0.15625
	Clearly communicate how IT adverse IT related events may affect business objectives	0.5	0.03125	0.15625
	Enable senior managers and IT executives to understand the actual amount of IT Risk to h steer the right resources to respond to IT risk in line with the appetite and tolerance	0.25	0.01562	0.078125
	TOTAL	16	1	**2.359375**

Source: Primary Data (Banks at Leles, Garut, March 2015)

The above Table 1.8 points out that Internet Banking services has risks in security systems, risks in banking transactions, risks in customer authentication, and risks in power failures.

4.1.13 Results



Based on the results of the study that the customer satisfaction comprising of eight service dimensions namely efficiency, fulfillment, system availability, privacy, assurance & trust, responsiveness, contact and website aesthetics [19] whereas it is determined by the socio economic circumstances with the key determinants comprising of gender, qualifications, employment, and income and it is straigh relate while transacting Internet Banking transaction especially from the security point of view. In short, the customers with socio economic factors (gender, qualifications, employment, and income) are very concerned with the security and network failures when doing Internet Banking transactions. (please see the tables mentioned above).

Hence, there is a relationship between the socio economic factors of the respondents and the customer satisfaction level. Therefore, the risk appetite and tolerance level is at **2.3593752.** This risk appetite and tolerance level means that the implementation of IT Banking Policy is not up to the required IT Governance of the Banks.

The results of the study show that the Banks still need to improve on the aspects of **ELECTRONIC BANKING SERVICE QUALITY NAMELY EFFICIENCY, FULFILMENT, SYSTEM AVAILABILITY, PRIVACY, ASSURANCE AND TRUST, RESPONSIVENESS, CONTACT AND WEBSITE AESTHETICS. IT IS RECOMMENDED THAT THE BANKS NEED TO IMPROVE ON THOSE AREAS MENTIONED ABOVE AS THE TRENDS THE CUSTOMERS DO THE ONLINE BANKING. THOSE ASPECTS OF ELECTRONIC BANKING SERVICE QUALITY ARE VERY IMPORTANT TO THE CUSTOMERS AS THEY BANKS MUST LIVE AND SURVIVE UP TO THE CUSTOMER EXPECTATIONS FOR ONLINE BANKING**

Note:

Risk appetite and tolerance below than 2.8 needs attention and it is not up to minimum level of IT Banking Policy and IT Governance of the Banks.

4.1.14 Suggestions

There are some suggestions in order to improve the customer satisfaction of Internet Banking services.

1. Most customers are concerned about about the Security system of the Banks. Hence, the banks shall implement the followings.
   - Bank should install system supported by software and firewalls. It should be configured the highest security setting with the level protection in accordance with the customers' needs.
   - Bank should increase their ability to control and manage the various risks inherent to the Internet Banking transaction activities.
   - Bank should implement more security to minimize the risk and increase customer authentication such as PIN, Eectronic Signature, audit trail (of transactions), etc.

2. The Banks should focus on quality of Internet Banking and should charge a descent service charges (of transactions).
3. The major issues are connectivity and power failure problems (from customer point of view). Hence, the Banks should have a necessary measures such as Business Continuity Plan.
4. Banks should have inter connection with other banks so that the customers could transact among accounts of the Banks.

If any complaint is received by the Banks it must be addressed properly. Hence, Bank staff must eradicate concerns of the customers in common languages

4.1.15 Further Study

Based on the study, we may suggest other interesting areas for further study include:

- A comparison between online banking service quality with traditional banking service quality
- Further investigation of difference in customer expectations and perceptions between online banking environment and traditional banking environment.

However there might be three possible resistances in further study as follows:

- The first resistance is based on data on how the research align the data of service quality of internet of online banking and tradional banking. This will have misleading conclusion if the parameter and alignment of data is not properly set up.
- The second resistance is customers are reluctant to change their behaviour. The behaviour of online banking and tradional banking is rather different as the traditional banking focus on cleanliness and responsivess whereby the online banking focus on efficiency and assurance & trust.
- The third resistance is security. There are many educated customers still do not use online banking merely they do not trust the level security of Internet Banking from each Banks. There many cases whereby malware misuse personal information of the customers by stealing or tapping credit card information through Internet Banking transactions.

At last for further study, it should focus on the security and compensation dimensions as they are not explored in details in the current study. The purpose of future study is to get different Perception how the customer Perception relate to the service quality of Internet Banking focusing on the security and compensation dimensions in more scientific way.

4.1.16 Conclusion

Banking system in Indonesia emphasizes the need for automated banking. Internet Banking allows the customers to satisfy many needs with minimum human intervention. Because of the fierce competition the Banks must cut their costs and also gain the customer back by offering Internet Banking services. Internet Banking is a unique weapon for survival of banks and retains the customers' loyalty. But the security under Internet Banking is always questionable one. If the bank creates trust

about the securities system among the customers it easily accomplishes its milestones. Furthermore, all the bank's policy (IT Banking Policies) shall be consulted to the respected committee, IT Steering Committee. The IT Governance must be complying with the regulators (Otoritas Jasa Keuangan).

References

[1] Akinci, S., Aksoy, S. and Atilgan E., "Adoption of Internet Banking among sophisticated consumer segments in an advanced developing country", International Journal of Bank Marketing, Vol. 22, No. 3, 2004, pp. 212-232

[2] Maureen Grace, David Kiragu, Patrick Ngumi " A Literature Survey on Internet Banking Survey, 21 Jan 2013

[3] Indjikian, R. and Siegel, D.S., "The Impact of Investment in IT on Economic Performance: Implications for Developing Countries ", World Development (33: 5), 2005, pp. 681-700.

[4] Odedra-Straub, M. "E-commerce and Development: Whose Development?" Electronic Journal on Information Systems in Developing Countries, (11:2), 2003, pp 1-5.

[5] Sam, T.L. and Eam, L.H. (2011). 'Estimating The Determinants of B2B e -Commerce Adoption Among Small & Medium Enterprises'. *International Journal of Business and Society*, Vol. 12(1), pp. 15-30

[6] Poon, S. and Swat man, P.M.C. (1998). 'A Combined-Method Study of Small Business Internet Commerce'. International Journal of Electronic Commerce, Vol. 2(3), pp. 31-46.

[7] Dedrick, J., Goodman, S. & Kraemer, K. "Little Engines that could: Computing in Small Energetic Countries", *Association of Computing Machinery, (35),* 1995, pp.21-26.

[8] APJII – Asosiasi Penyelenggara Jasa Internet Indonesia, Statistik APJII, 2005.

[9] TKTI – Indonesian Telematics Coordinating Team. Five-Year Action Plan for the Development and Implementation of Information and Communication Technologies (ICT) in Indonesia, 2001.

[10] Unhelkar, B., "Understanding the Impact of Cultural Issues in Global e-Business Alliances", 4th International We-B Conference, 24-25 Nov, 2003, Perth, Western Australia

[11] Dr. C Paramasivan (2011) , "Customers' Satisfaction through Information Technology in Commercial Banks", Journal of Commerce and Management of Research in Commerce & Management, Volume 2, Issue no. 4, July, 2011 pp. 509-522.

[12] Turban, E. et al. Electronic Commerce: A Managerial Perception, 2006, Prentice Hall.

[13] Bromiley, P (1991), 'Testing A Causal Model of Corporate Risk Taking and Performance', Academy of Management Journal, vol. 34, no. 1, pp. 37-59,

[14] Denrell, J (2004), 'Risk Taking and Aspiration Levels: Two Alternative Null-Models', Academy of Management Best Conference Paper, and pp.J1- J6.

[15] Ford, G (2009), Remuneration, Risk Appetite and Financial Crisis, Macquarie Graduate School of Management, Sydney

[16] Devlin, J.F. (1995). Technology and innovation in retail banking distribution. International Journal of Bank Marketing, Vol. 13 No. 4, pp. 19-25.

[17] Altintas, M. H., and Gürsakal, N. (2007). Phishing Attacks and Perceptions of Service Quality: A Content Analysis of Internet Banking in Turkey. Journal of Internet Banking and Commerce, August, vol. 12, no. 2.

[18] An, M., and Teo, T.S.H. (2000). Factors influencing the adoption of Internet Banking. Journal of the Association for information Systems, Vol. 1 No. 5, pp. 1-42.

[19] Parasuraman A, Zeithamal V.A & Malhotra A. 2005. E-S-QUAL: A Multiple-Item Scale for Assessing Electronic Service Quality. *Journal of Service Research*, 7(3):213-233. Available from Emerald: http://www.emeraldinsight.com/ [Accessed: 2006-08-08].

The Annual Conference on Management and Information Technology (ACMIT) 2016

Ultrasonic Sonar Object and Range Detection Measurement Display using HC-SR04 Sensor on Arduino ATMEGA 2560

Hendryg Sansury[1]
Mechanical engineering (mechatronic) Swiss German University BSD,15119,Indonesia

Abstract

Ultrasonic sonar object and range detection measurement using Hc-sr04 display can be use in every application. Ultrasonic sonar popular to use due to low cost, availability, no radiation for human applied in more industry such as medicine, robotic, automation. Ultrasonic sensor is a measurement device that consist of two transducer one for transmitting an ultrasonic wave and the other for receiving the reflective wave. We use HC-SR04 ultrasonic sensor can detect lower range from 1cm to 2.5 meter with precession about 0.1 cm and frequency up to 40Khz. The target must be proper orientation and perpendicular to the direction propagation of pulse. The amplitude of receive signal decrease depend on the medium and the distance between transmitter and the target. The transmitter converts electrostatic energy from a vibrating membrane to an ultrasonic waveform whilst the receiver converts the reflected ultrasonic waveform back into electrical energy. This electrical energy combine with motor servo to see the angle of sweeping and ultrasonic waveform using arduino atmega 2560 then be interpreted by a computer display in two dimension for measurement angle and distance of object. Conversion between electrical energy to an ultrasonic waveform use electrostatic transducer or normally we call piezoelectric transducer.

Keyword : Object detecsion ;Ultrasonic sensor HC-SR04 ; Arduino atmega 2506 ; Interfase that connect to computer ; two dimension display ;

1. Introduction

Ultrasonic has been a research area for many years. It covers a variety of fields including underwater mapping, robot navigation and object recognition. In the context of object recognition significant research has been conducted using Time of flight sensors. An ultrasonic pulse is generated in a given direction. The same principle can be used for obstruction detection by electronic means as it is very simple to produce ultrasonic signals using electronic circuitry and ultrasonic transducers. For measuring the distance, time of flight for reflected ultrasonic signals is calculated. Ultrasonic signals have good directionality, and they are easily reflected by solid objects. By finding the time taken for ultrasonic signals to reflect, the distance traveled by sound can be easily calculated, as velocity of sound is a known quantity. This is known as pulse echo technique, which is used here for distance measurement. If there is an object in the path of this pulse, part or all of this pulse will be reflected back to the transmitter as an echo and can be detected through the receiver path. By measuring the difference in time between the pulse being transmitted and the echo being received, it is possible to determine how far away the object is. The speed of sound in air is approx. 346m/s at 24 degrees C. At 40KHz the wavelength is 8.65mm. Base on the International Journal of advance research in electrical electronic and instrumentation engineering about range detection base on ultrasonic principle at February 2014 the recent development just until how to detect and measure some object. The problem come that rare for ultrasonic system to be display so will be easy for people to be utilized with low cost, easy availability and no radiation for human. With the utilized of arduino microcontroller , HC-SR04Ultrasonic Range Finder , high Speed Servo and put on display two dimension mode.

Nomenclature

ToF	time of flight
Khz	kilo hezt
m/s	meter per second
SCL	serial clock line
SDA	serial data line
PWM	pulse width modulation
US	ultrasonic sensor
SCM	standard capacitor microphone
Amp	amplifier
FC	frequency counter
OSC	oscillator
L	object distance
C	velocity of sound
T	time
Pa	sound of pressure
Po	reference sound of pressure

2. Design object detection

To display two dimension on computer we need to understand all the system that working on this ultrasonic sensor equipment. HC-SR04 high performance ultrasonic low range finder is compact and measures low range from 1 cm to 2.5 m, working in 40khz frequency at working voltage 5vdc on working current 15mA on 2mA standby current.

Start measurement with the HC-SR04 ultrasonic rangefinder trig of SR04 should receive pulse of 5vdc at least 10us, this will initiate the sensor transmit of 8 cycle of ultrasonic burst at 40 kHz and wait the reflective of ultrasonic burst. Sensor detected ultrasonic from receiver and will set the echo pin on high 5vdc and delay for period width that is proportion to distance measure the width of echo pin. The ultrasonic propagation is subject to the temperature and medium in the air is about 340 m/s at 15^0C

Time = Width of echo pulse in microsecond
Distance in centimeter = Time /58
Distance in inch = Time / 148
V = 340 + 0.6 (T-15) m/s where T is Temperature in ^{0}C

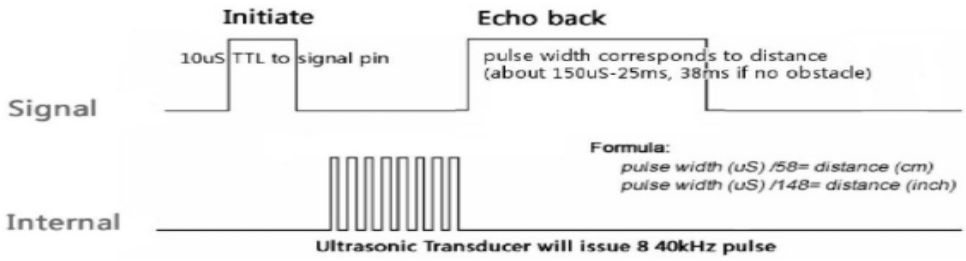


Figure 1. Produk User Manual HC-SR04 Ultrasonic Sensor

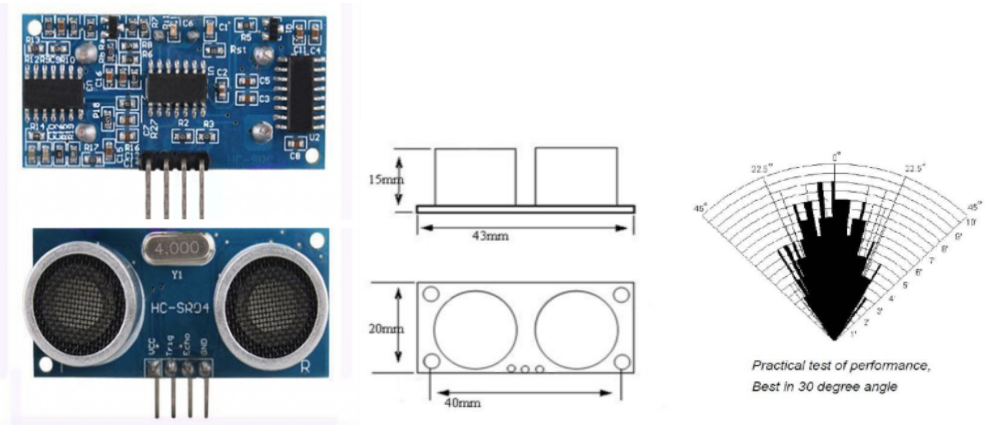


Figure 2. HC-SR04 Ultrasonic sensor Dimension

HC-SR04 Electrical Parameter:

Description	Value
Working Voltage	DC 5V
Working Current	15mA
Working Frequency	40Hz
Max Range	4M
Min Range	2Cm
Measuring Angle	15 degree
Trigger Input Signal	10us TTL Pulse
Echo Output Signal	Input TTL lever signal and the range on proportion

High speed MG995 servo can rotate 120^0 (60 inch in each direction) weight for 55g , operating speed is about 0.2 s/ 60^0 (4,8V) or 0,16s/ 60^0 (6 V). There are three output pin from the servo, PWM on orange calor, Vcc red color (+) and ground in brown color (-).Servomotor is a servomechanism. It is a closed-loop servomechanism that uses position feedback to control its motion and final position. The input to its control is some signal, either analogue or digital, representing the position commanded for the output shaft. The motor is paired with some type of encoder to provide position and speed feedback. In the simplest case, only the position is measured. The measured position of the output is compared to the command position, the external input to the controller. If the output position differs from that required, an error signal is generated which then causes the motor to rotate in either direction, as needed to bring the output shaft to the appropriate position. As the positions approach, the error signal reduces to zero and the motor stops.

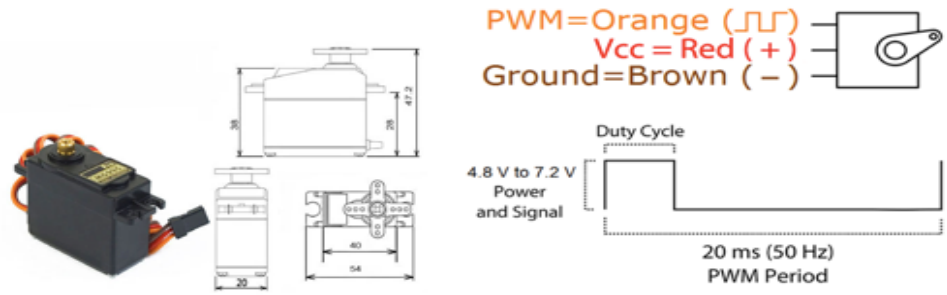


Figure 3. Servo Motor

3. Hardware Design

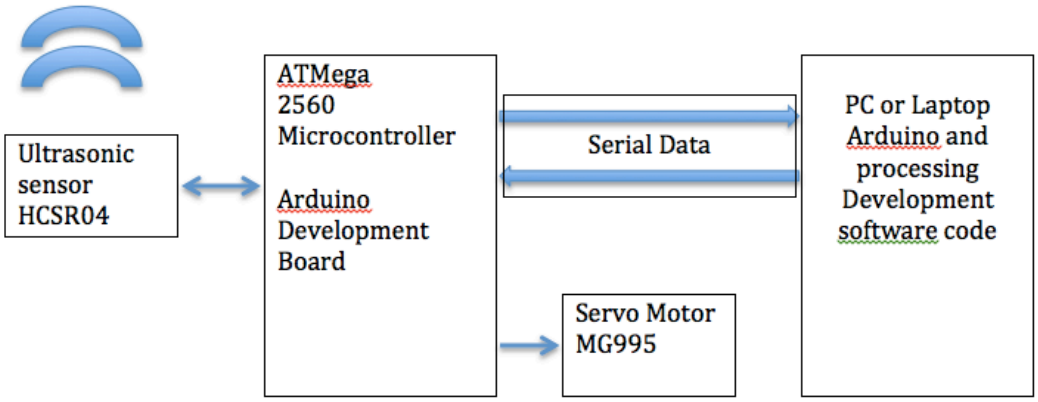


Figure 4. Hardware

The hardware section classified into two section a). Analog section and b). Digital section we can see above on Figure 4. On analog section the ultrasonic sensor module transmit some ultrasonic signal pick up its echo and measured the time elapse between echo and trigger waveform and modulated by the measured time which is proportional to the distance. Initialized sent 10um TTL signal trigger pulse and that transmit 40kHz and than pulse with correspondent distance not below 50ms we can this as the cycle period. Another part of analog section is servo motor MG995 working as mechanical movement to scan the object in front and working on sequence every 15^0. The HC-SR04 will doing scanning up to 165^0. On Digital section we have arduino atmega 2560 and as our development board for microcontroller to processing of distance calculate of object, timing calculation, give order to the servo motor to move every 15^0 up to 165^0 for scanning the object in front of ultrasonic sensor. Another digital section is processing I3 software I use to communicate serial data between arduino atmega 2560 so we can see the object , distance, measuring angle in PC or Laptop.

4. Software Design

On Pc display will have distance measure, angle color red if the ultrasonic HC-SR04 sensing object and color green if no object sensing. we need to draw the arc lines and angle lines function.

```
void drawRadar() {
  pushMatrix();
  translate(960,1000); // moves the starting coordinats to new location
  noFill();
  strokeWeight(2);
  stroke(98,245,31);
  // draws the arc lines
```

```
  arc(0,0,1800,1800,PI,TWO_PI);
  arc(0,0,1400,1400,PI,TWO_PI);
  arc(0,0,1000,1000,PI,TWO_PI);
  arc(0,0,600,600,PI,TWO_PI);
  // draws the angle lines
  line(-960,0,960,0);
  line(0,0,-960*cos(radians(30)),-960*sin(radians(30)));
  line(0,0,-960*cos(radians(60)),-960*sin(radians(60)));
  line(0,0,-960*cos(radians(90)),-960*sin(radians(90)));
  line(0,0,-960*cos(radians(120)),-960*sin(radians(120)));
  line(0,0,-960*cos(radians(150)),-960*sin(radians(150)));
  line(-960*cos(radians(30)),0,960,0);
  popMatrix();
```

To draw the line with out object I use means the line moving along the scanning area use lines function with green color and line with object use red color.

```
void drawLine() {
  pushMatrix();
  strokeWeight(9);
  stroke(30,250,60);
  translate(960,1000); // moves the starting coordinats to new location
  line(0,0,950*cos(radians(iAngle)),-950*sin(radians(iAngle))); // draws the line according to the angle
  popMatrix();
}
```

And we need to draw the distance and angle that according to ultrasonic sensor that sense the object.

```
void drawObject() {
  pushMatrix();
  translate(960,1000); // moves the starting coordinats to new location
  strokeWeight(9);
  stroke(255,10,10); // red color
  pixsDistance = iDistance*22.5; // covers the distance from the sensor from cm to pixels
  // limiting the range to 40 cms
  if(iDistance<40){
    // draws the object according to the angle and the distance
  line(pixsDistance*cos(radians(iAngle)),-
pixsDistance*sin(radians(iAngle)),950*cos(radians(iAngle)),-950*sin(radians(iAngle)));
  }
  popMatrix();
}
```

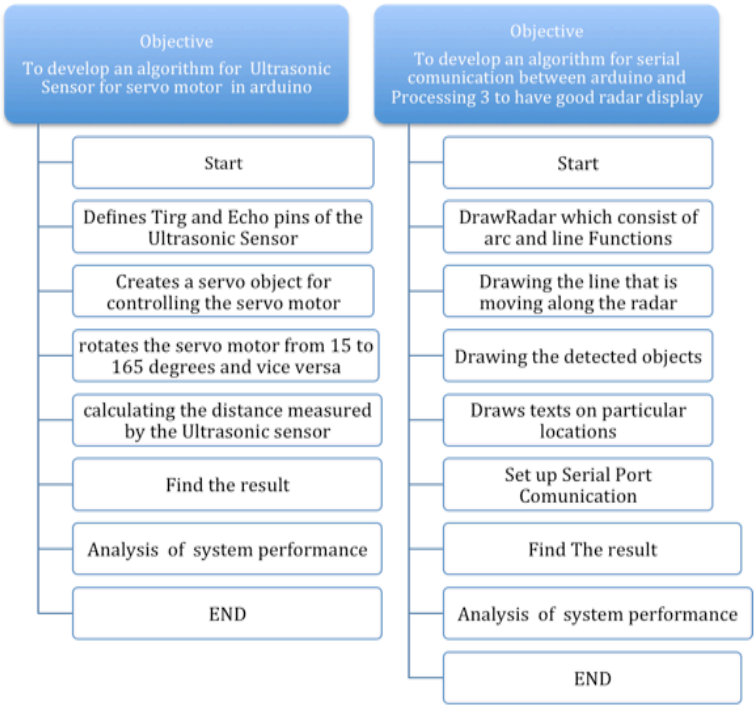


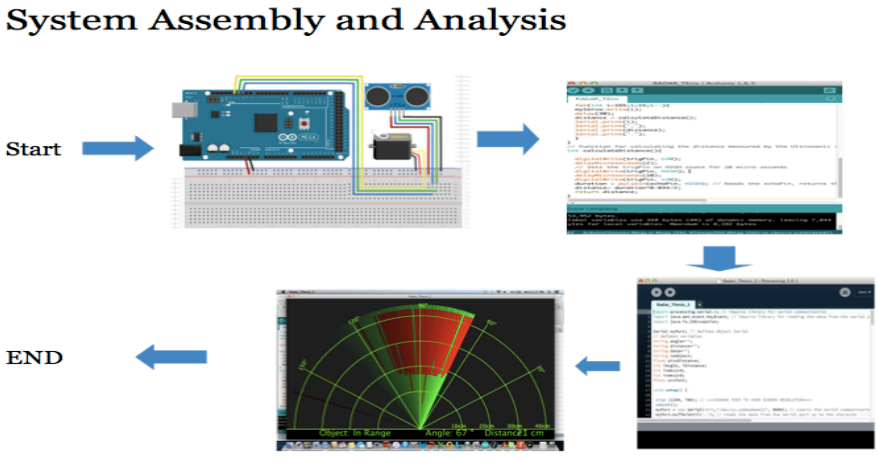
Figure 6. Software Design

5. Experiment and Progress

The principles of measuring distance and is called the "pulse reflection method" which makes it possible to count the number of reference pulses. This method is used to measure reflection time up to the object between transmitting pulse and receiving pulse of the ultrasonic wave.The relationship between the distance up to the object L and the reflecting time T is expressed by the following formula

$$L=C \cdot T/2$$

where C is the velocity of sound. That is, the distance to the object can be ascertained by measuring the reflection time involved in reaching the object.How to display the object in two dimension we use software help from arduino code and processing 3 DrawRadar Using consist of arc and line function, DrawLine moving along the Radar, DrawObject Function get the distance from ultrasonic sensor, Using Arduino IDE and Processing IDE, Modification for Port comunication to computer



6. Conclusion

A low-cost, low power and simple system for distance measurement. The precision of the result high compared to other conventional methods. Above figure shows the model of this paper implemented. It is certainly a reliable and efficient method for instantaneous measurement of distance and put it into a two dimension display in PC. This system will have high application in civil and mechanical field of engineering where it has been a bigger challenge for precise measurement of small and physically unreachable distances. It will surely have influence on small and large technicians who find measurements challenging in different severe environments. The future modification may include on three dimension display

Reference

[1] F L. Corp "Ultrasonic Transmitters vs. Guided Wave Radar for Level Measurement by FLO-CORP (Flow Line Options Corp.),2011 ,

[2] Dontabhaktuni Jayakumar , A. Pravalika, K. Purnachandra Rao ' Model Radar Implementation Using Ultrasonic Sensor' , paper published in November 2014.

[3] S. D. Gupta , A.A. Haque, A. R. Sudip Majumder, "Design and Implementation of Water Depth Measurement

[4] S. D. Gupta , A.A. Haque, A. R. Sudip Majumder , "Object Detection Model Using Ultrasonic Signal " , paper published in October 2012

[5] S.G.N. M urthy, B.Sangoju, H.Wiggenhauser, N.R.Iyer , "Application of Radar and Ultrasonic Pulse Echo for Testing Concrete Structures , paper, July 2009.

[6] Md. Shamsul Arefin, Tajrian Mollick , "Design of an Ultrasonic Distance Meter" , paper ,published in March 2013.

[7] L. Sambuelli, L. Valentina Socco, A. Godio ," Ultrasonic Electric and radar measurements for livening trees assessment" paper , published in Desember 2006.

[8] A. Luciano, M.Vicente, T.Carlos, " Ultrasonic Sensors in Urban Traffic Driving-Aid Systems" , paper published January 2011.

[9] Springer Handbook for Robotic http://www.springer.com/978-3-540-23957-4

[10] Arduino Instructable at www.instrutable.com

[11] ControllerSatish Pandey, Dharmendra Mishra, Anchal Srivastava, Atul Srivastava, "Ultrasonic Obstruction Detection and Distance Measurement Using AVR Micro Controller "Departement of Physics, University of Lucknow, Lucknow,

[12] Rajan P Thomas, Jithin K K, Hareesh K S, Habeeburahman C A,Jithin Abraham, " Range Detection base on ultrasonic Principle"

The Annual Conference on Management and Information Technology (ACMIT) 2016

Managing Risks of Managed Webhosting Outsourcing

Kalpin Erlangga Silaen[a], Dr. Mohammad A. Amin Soetomo[b]
[a]*Swiss German University, EduTown BSDCity, Tangerang 16339, Indonesia*
[b]*Swiss German University, EduTown BSDCity, Tangerang 16339, Indonesia*

ABSTRACT

Outsourcing managed webhosting to the provider can give benefits from cost savings point of view. With outsourcing webhosting, company can focus with their core business without worrying how to manage their webhosting, backup, hardware, software and licenses. Unfortunately, this also raised security issues and impact business. This paper provides another insight about risks in webhosting outsourcing and a model to manage those risks based on NIST SP800-30.

Keyword: *Managed Webhosting; Outsourcing; Risks Management*

1. INTRODUCTION

Outsourcing webhosting is purchasing webhosting services from other provider where consumer can put their contents to provider's server to serve their visitor or clients. This is called outsource because in fact, internally, the consumer can provide this kind services [1], but for one or more reasons, company decide to use other provider to host their website. NIST SP800-145 defines webhosting as Software as a Service (SaaS) where consumer can use provider's application to run their website and display to visitor. However, the consumer does not have control to hardware, operating system, server's configuration, and network [2]. The consumer can use storage, power of server and bandwidth as much as their subscribe to the provider. Furthermore, managed webhosting means the consumer can ask provider's assistance to help and fix any issues related to their services in webhosting. Scope of managed webhosting depends of agreement between provider and consumer. For example, the provider may provide basic managed webhosting for optimizing performance of consumer's website, or provide gold managed webhosting which include managing backup, monitoring performance, and other services. Basically, webhosting provider without managed services only provide space or capacity, power of computing, control panel to manage webhosting, and basic access such as FTP access to the server where consumer's website allocated. Based on the way managing resources, webhosting service usually has two models, shared hosting and dedicated hosting [3] with managed services as add-ons for both models. This paper discuss about managing risk in webhosting outsourcing based on NIST SP800-30 and how an organization or business consider to use webhosting outsourcing.

2. RELATED WORK

Some researchers have been discuss about risk in webhosting and related to cloud hosting with different approach. Currie. L. Wendy [4] discuss about outsourcing of web application, where consumer can use it with model pay-as-you-go, but the research does not discuss about security in webhosting environment. Charles Kubicek [5] studied about QoS (Quality of Service) for webhosting environment. His research focus about performance of webhosting based on response time. Performance is one of important point for webhosting services, but this paper will focus about risks and how to manage it. Ioan Petri et all [6] discussing about risk assessment in service provider and propose SLA (Service Level Agreement) and trust mechanism as risk mitigation for services. In delivering SLA, provider provide server farm to reduce unavailability, but they studied from provider's point of view. In this paper, we are discussing about risk in using outsource webhosting with literature review methodology.

3. FLOW PURCHASING WEBHOSTING

Usually, consumer decide to purchase webhosting from advertising of provider in other websites, and search from search engine without deep analyze about provider. Later, consumer also search about review from other people about provider. For example, if a consumer has 3 candidate of webhosting provider, they can search about review good or bad in internet. Unfortunately, this is sometime bias. Some provider can also send their sales or people to write false good review and spread it to internet. For managed hosting, since consumer will have intensive communication, consumer need to know deeply about their potential webhosting provider, so they usually invite them to meet and present their product to consumer. The consumer, if they need a specific needs, they can ask potential provider if they can provide it. In this case, provider needs to bring a product expert, like *presales* person to discuss about consumer's need and how it works with their product, and consumer can ask detail about their Term of Services (TOS) and Acceptable Use Policy (AUP) because this is related to legal [7]. Also, consumer can ask about provider's SLA [6][7] and compliance if needed. Compliance needed by consumer if regulator enforces them to comply, for example, consumer who runs e-commerce may enforced by local regulator to meet some requirements, even if it is not core's web application (for example, blog website, news website, etc but related to their business). In general, purchasing webhosting service can shown like picture below:

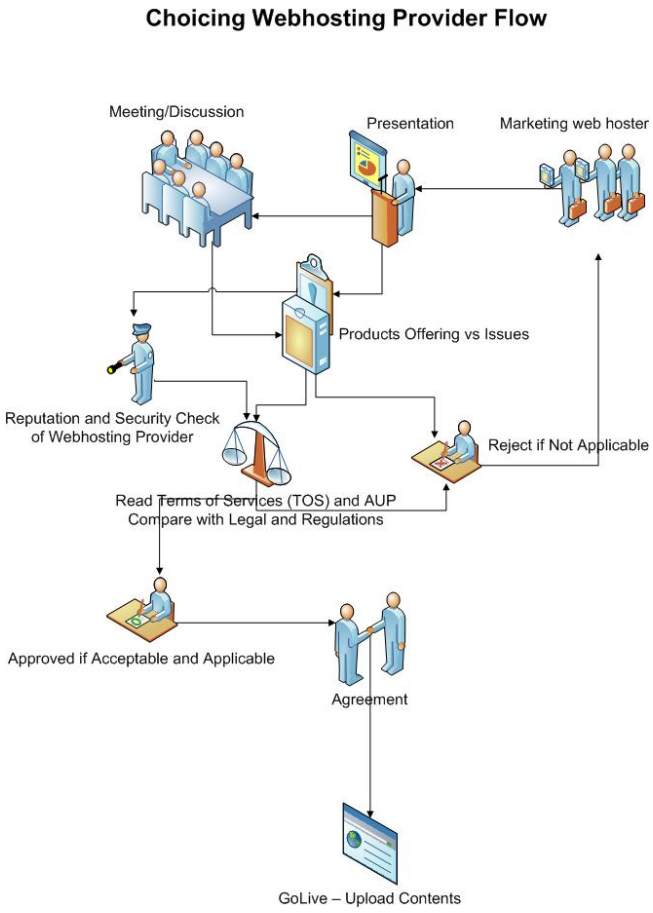


Figure 1. Flow Purchasing Webhosting [7]

The figure above shown that consumer and potential provider (term before agreement) need create good communication and understanding. Potential provider must show their honest and consumer also must tell them what they need, what they expect from webhosting provider.

4. BENEFITS OF OUTSOURCING WEBHOSTING

4.1. Cost Savings

Company who decides to in-house their webhosting should provide man power to manage their infrastructure, including servers, rack, space, power of electric, HVAC (Heating, Ventilating, and Air Conditioning) which is need more resources to manage all of them. Also, they have to ready provide

helpdesk, support, system expert for 24 hours a day. This situation can increase operational cost significantly. In other side, company who decides to outsource their webhosting to other party, not only can save big cost, but also they can focus with their core business. Talking about infrastructures such as servers, router, switch, and other device also concerns about TCO (Total Cost of Ownership) [1] which is difficult to manage, especially if company is not IT related business and does not have experience about managing IT project. With outsourcing webhosting, company just pay small amount to provider and they can start put their content to the server and publish it to internet or for their own usage. But company also must aware about what contents they can put to outsourcing webhosting to avoid any risks in case there is security breach or regulation rules. Of course, if there is critical information or valuable information, company does not have reason to pay only $5 a month to host them to outsource webhosting. Those issues will discuss in next risk management.

4.2. Availability

In-house webhosting for some company with good support also has some problem, availability [8]. In security, availability is one of triad CIA (Confidential, Integrity, Availability) [9] which is include in risk assessment. More questions about availability in-house webhosting are:

- Does company provide redundant power?
- Does company provide redundant internet link?
- How fast company can replace any fault hardware?
- Does company environments support for good connectivity, electric, flood, and other threats?

For internal web application, such as internal portal and any internal consumes website, there is no problem for in-house hosted them internally as long as they do not have any branch or partner at other location which need to access them. Usually webhosting company has datacenter or at least they have space in datacenter with good inter-connection with redundant link to internet (for good webhosting provider who cares about their quality link and provide good SLA). Datacenter also provide redundant power electric and provide 24 hours support and with additional managed services, they can also provide on-hands support (for example, replace hardware in covered SLA, monitoring, and other administration support). Some provider can also provide multiple locations based on their promise SLA to their client.

In other words, company has good reasons to use outsource webhosting, saving cost and good availability. But still they need to know about security aspect, any risk may impact to their business and how to mitigate them.

4.3 Scalability

Advanced webhosting technology especially if they are true cloud, provider can provide an interface where consumer can upgrade or downgrade their resources based on their needs. Nowadays, more provider already have this feature, consumer subscribe to basic resources and with click and go, they can resize their subscribed resources without losing their data. This make consumer has ability to reduce cost which is already low.

5. RISK OF OUTSOURCING WEBHOSTING

NIST SP800-30 defines risk is a probability of an event from threat with negative impact to objectives because of existences of vulnerability. Risk management is a process to assess, identify risk and take necessary steps to mitigate them to the acceptable level [8]. Webhosting in general has some types of risks such as hacking (deface, information leakage, etc), data loss, disruptive event [10] (denial of services, distributed denial of services, power fault). Azeem Aleem et. al [7] find that data leakage is in position 1 for top cloud threat, and insider threats in position 3 which maybe involve provider. For outsourcing webhosting, there are some risks such as legal or regulation which may not allow company to outsource their webhosting to other party, or at maybe regulator requires that provider also must provide standard as requirements. In this case, company need to work together to provider to solve this kind issue. In outsourcing webhosting, trust mechanism, transparency, good communication also need to establish between consumer and provider. In shared environment, there is a possibility of abusive resources which impact to performance of other tenants or user, so provider need to implement some technology to manage those resources [11][12].

6. RISK MANAGEMENT

6.1 RISK ASSESSMENT and ANALYSIS

Risk assessment is a method to help company define any risk which maybe occurred. The output of risk assessment will become input for risk analysis. Risk analysis provides company about comparisons between cost and benefit for any applied protection to mitigate risks. Risk assessment methodology has nine primary steps [8] with associated between input and output as shown in Figure 2.

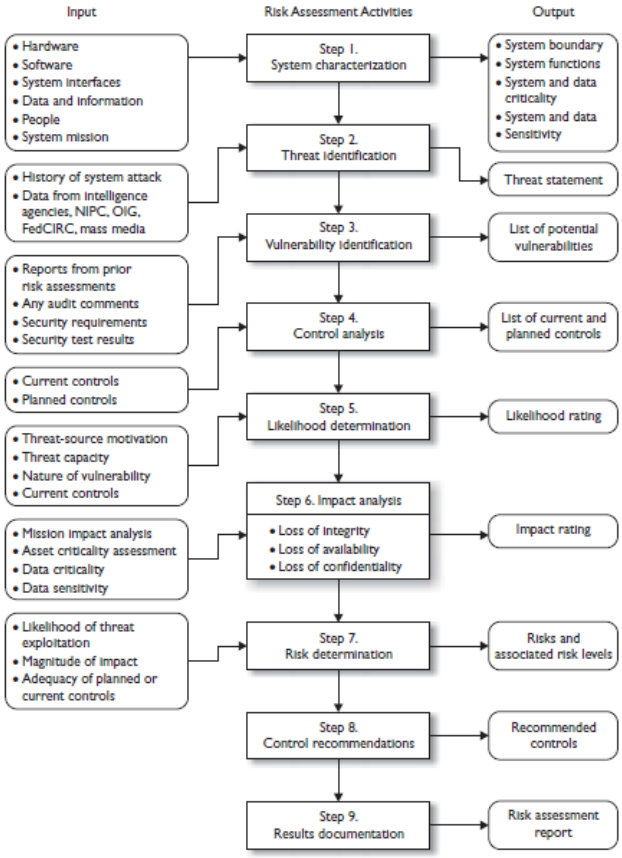


Figure 2. Risk Assessment Methodology in NIST SP800-30 [8]

6.1.1 System Characterization

In this initial step, company can ask provider any details about their system before they decide if their system is acceptable to their business. Later, company can cross check this information from other trusted sources to see if provider is honest. An example form of system assessment for outsourcing webhosting can see as table 1 below:

Assessment Point	Physical	Administrative	Technical
System Characterization	Where is provider's server located?	Who has access to the server?	What is the operating system?
	Is provider's hardware already support trusted computing base?	Does provider has Information Risk Management?	Is it virtualized?
	Is provider's datacenter secured?	Does provider has incident handling procedures?	Is it shared?
	Is provider's rack locked?	What is provider's SLA?	How does provider create

			backup?

Table 1. System Characterization [8]

System assessment also must be done at consumer's side to support and work together with provider's assessment system. For example, collecting data about policy documents, current system including web application which will uploaded to provider's system, system design and how they work, procedure, guidelines, security-related documentations, and soon.

6.1.2 Threat Identification

Threat means a probability of any party exploiting vulnerabilities exist in the system. Threats has three main components, they are threat sources, vulnerabilities, and existing control to mitigate them. Threat source can be intentional, where system already targeted by sources of threat. Threat source also can be situational, like an accident. Bot threat source intentional or an accident can come from human, natural, and environment. For example, in shared webhosting environment, an attacker can obtain access to another user in same system, and then *jump* to other user due to lack of protection per user by system, in this case threat source come from natural and system has vulnerabilities to allow another user *jump* to other users. Usually, threat source from human has motives, therefore company or provider need to assess them and provide necessary protection to mitigate them. Company can use form like table 2 to assess threat identification for outsourcing webhosting:

Assessment Point	Threat Source	Likelihood	Threats Actions
Threat Identification	Human	Hacker/Cracker, Terrorists, Insider Attacker, SysAdmin, Network Admin, Users	Deface, Data Leakage, Unintentional Data Leakage, DOS/DDoS, Unintentional Misconfiguration, Misbehave policy/procedures
	Natural	Flood, Earthquake, Fire	Fire or flood in datacenter
	Environment	Other tenants, Fiber Optic Overseas, Power Fault	Fiber cut, DDoS unintentional to neighborhood

Table 2. Threat Identification

6.1.3 Vulnerability Identification

In this step, company can ask provider about any past vulnerabilities which successfully exploited by threat sources in place for their system and how they handled it. Although this information is sensitive, but with non disclosure agreement between parties, provider can provide this information. Also, company can search in internet related to provider's incidents. Step one which previously collected can be use as another source to identify vulnerabilities. Vulnerability sources information can be identify with table 3 below:

Assessment Point	Physical	Administrative	Technical
Vulnerability Identification	Datacenter does not use proper water sprinklers	Previous risk assessment	Security advisories
	Datacenter does not screen people accessing rack/server	IT Security Audit	Vendor advisories
	Rack is not locked	Terminating Employees	Penetration Testing
	Improper cabling	Lack of Patching	Misconfiguration system and network
	Improper power planting	Does not have security policies and standard	Vulnerability database list

Table 3. Vulnerability Identification

As mentioned above that threat without vulnerabilities then there is no risk and vice versa. This connection formulas as:

risk = threats x vulnerability
and
total risk = threats x vulnerability x asset value [13]

In table 4, this illustration can help to understand about relation between threats and vulnerabilities

Vulnerability	Threat	Risk
Rack is not locked	Other tenant access their own rack and has interesting with unlock rack	Other tenant can access company's rack
Improper cabling	Mouse	Cable damaged and unplugged

Table 4. Relation Threats and Vulnerabilities

6.1.4 Control Analysis

Next step in risk assessment is control analysis. In this step, company can review existing controls which has been implemented or being planned to minimize of probability of threat source against vulnerability. There are 2 categories based on NIST SP800-30 [8], they are preventive and detective

controls with 2 methods technical and non technical. Furthermore, Shon Harris [13] defines control become 3 types: physical, technical or logical, and administrative control. She is also define 6 categories for control functions: Deterrent, Preventive, Corrective, Recovery, Detective, and Compensating.

Control Categories and Types

	NIST SP800-30	**Shon Harris**
Categories	Preventive	Deterrent
	Detective	Preventive
		Corrective
		Recovery
		Detective
		Compensating
Types	Technical	Physical
	Non technical	Technical/Logical
		Administrative

Table 5. Control Types and Categories Comparison

Implementation control can use a conceptual Defense-in-Depth. More important or critical company's assets, more control to implement to protect them. For example, company who wants use outsourcing webhosting and provider provide good protection with their system (firewall, IDS/IPS, securing their system, etc) but company can add some controls to their content (for example, encrypt their disk or code before send it to provider's system, add tracker to their document).

6.1.5 Likelihood Determination

Likelihood is a potential vulnerability exercised by a threat with or without existing control to mitigate. The output of likelihood is a rating indicate a possibility chance of exploiting target. Likelihood has 3 components, threat-source motivation or capability, nature of vulnerability (general, specific, easy to launch), and existence of current controls. Below is an example comparison with similar vulnerability but different threat-source:

Likelihood Rating

	High	**Medium**	**Low**
Some ports open to internet	Threat-source has high skill and motivated, some ports has common vulnerabilities and unpatch	Threat-source has high skill and motivated, but most of ports already patched	Threat-source does not have sufficient skill, and all ports open already patched

Open port only in internal/vpn	-	Threat-source has high skill and motivated, but ports limited to internal only	Threat-source has high skill and motivated, but ports limited to internal only with additional tokens and other control

Table 6. Likelihood rating

6.1.6 Impact Analysis

Impact analysis is one of important step. In this step, company will review and analyze the impact if threat source success exercised vulnerability. Company need to collect information about their asset's value, how important them to company, what happen and consequences if threat source success attack vulnerability, and soon. The impact of any incident can be measure with triad CIA (confidential, integrity, and availability). For example, if threat source success attack a vulnerability of an application (buffer overflow) then that application maybe down (loss availability) or data corruption (loss integrity).

In webhosting case, if an attacker success gain access to system with privileged user, then defacing website or stealing data could be happen. Impact analysis can measure with qualitative and quantitative. Quantitative means impact can be count with amount of value (money), qualitative means impact cannot count with amount of value, but described in rating high, medium, and low. Quantitative risk analysis can be formulas as [13]:

SLE = Asset Value x Exposure Factor

where:

SLE is single loss expectancy

Exposure Factor is percentage of loss

For example, if a company has 2 servers in a datacenter with each server has value $5000 USD, and one of them stolen (assumes there is not important data, only company profile's website) then:

SLE = (2 x 5000) x (50%) = $5000 USD

The advantage of quantitative analysis is company can know how much (in money) loss if an incident occurs. But the disadvantages are difficult to value all assets, decrement value, and not all components could be count as money (reputation, human, knowledge, etc).

Qualitative risk analysis is a method which not count components or losses as amount money. For example, in above case if one of server is stolen where company's profile website available then reputation of that company may impact. Therefore, qualitative describe losses as magnitude high, medium, and low.

6.1.7 Risk Determination

Risk determination has purposes to assess risk level by multiplying the likelihood and impact [8]. NIST SP800-30 has an example matrix for risk determination:

Threat Likelihood	Impact		
	Low (10)	***Medium*** (50)	***High*** (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

Figure 3. Risk matrix [8]

6.1.8 Control Recommendations

In this step, risk assessment team provide recommendation controls to implement by company to reduce risk level to an acceptable by company. Some considerations for control recommendations are:
- Existing company policy
- Law and Regulation
- Effectiveness of recommendations
- Operational

Also, those recommendation must aware if recommendation is applicable. Some recommendations may implemented, some of them may not implemented and replace with alternative solutions.

6.1.9 Results Documentation

After risk assessment is done, all results must be documented and report to top management. This document is important for next assessment or if company has significant change. This reports contains about threats, vulnerability, risk measurement, and recommendations control to mitigate or reduce risk.

6.2 RISK MITIGATION

Next process in risk management after risk assessment is risk mitigation. Once top management receive documentation from risk assessment, they can start evaluate and prioritize implementation of risk controls. Selection controls must reduce risk to an acceptable level with least cost approach [8]. Risk mitigation has 4 components: Risk Mitigation Options, Strategy, Control Implementation, and Control Categories.

6.2.1 Risk Mitigation Options

NIST SP800-30 defines 6 options for risk mitigation [8], they are:
- Risk Assumption or Acceptance means accept current or potential risk and continue activity. Or implement approved controls to reduce risk to an acceptable level.
- Risk Avoidance, avoid potential risk and discontinue activity since there is no sufficient control to reduce it to an acceptable level.
- Risk Limitation, limiting risk by implement control with minimum impact to business
- Risk Planning, manage control selections and implementation control including monitoring and maintains controls
- Research and Acknowledgment, reduce risk by research and acknowledgment of vulnerability and implement control to remove or correcting vulnerability
- Risk Transference, transferring risk to other party for compensating of loss risk. An example is purchasing insurance.

Company must identified and prioritize risk from highest to lower risk. It is near impossible to identified all risk in company, so the key is prioritize and applicable.

6.2.2 Risk Mitigation Strategy

Strategy is one of important things in risk mitigation. Some questions may rise up at top management while thinking or decide what to do with risk assessment report, what things should they must do or what is prioritize. One way is to creating pair of threat/vulnerability. From formula above about risk, if there is no vulnerability, but threat source already identified, then there is no need mitigate them because risk is zero. Hence, top management can start with pairing threat source and vulnerability and then prioritize them from highest impact to lowest impact.

6.2.3 Control Implementation

Next is control implementation. It is useless if company already done with risk assessment, approved control selection, define strategy to implement them, but still they did not take any action to implement to real world. So this step is about implementation and must follow *de facto rules*: "Define what is the highest risk and then select control to reduce it to an acceptable level of risk with lowest cost". There are some steps already define by [8]:
- Prioritize Actions, sort any risk from highest to lowest
- Evaluate Control which is proposed, controls must be effective and applicable.
- Cost/Benefit Analysis, selected control from previous step must be compare with cost/benefit gains after implementation. For example, it is *overkill* if a company decide put their company's profile website without important data to dedicated server which cost around hundreds thousands dollar a month.

- Select Control, After do some analysis with cost/benefit above, top management must define which control must be implemented.
- Assign Responsibility, management can assign who will implement selected controls, who will supervise, and who will validate implementation.
- Developing a Safeguard Implementation Plan, Company must create plan during implementation safeguard, from selected control which already define before. This plan is like project management which contains about: threat, vulnerability, risks level, recommended controls, prioritize, selected control, resources, list of assigned personal to implement, detail of date time, target of implementation, and maintains of safeguard.
- Implement selected controls, after implementation some risks may successfully reduced to lower level, but not completely eliminate them. This risks called residual risk with formula:

total risk - countermeasure (or safeguard) = residual risk [13]

6.2.4 Control Categories

As discuss above (6.1.4), control has 2 main categories [8] but [13] define them as 3 main categories with additional category is physcal (administrative can be assume as non technical). The most important for control categories is about how company define and implement control in the right place to mitigate risks.

7. CONCLUSION

Outsourcing webhosting still one of the best option for company who does not have sufficient resources to manage it. But company need to assess risk through risk management to mitigate any risks which may arise from outsourcing webhosting. Company and provider must work together, honest and diligent to achieve requirements for both parties. For company, they can use webhosting with minimum cost and risk, and focus with their business. For provider, this can be good practice for providing secure outsource webhosting which already define (and could be validate with some standard) and making new opportunity for next client. NIST SP800-30 is one of standard for risk management guide for information technology systems. Although this standard focused on IT and computer systems security without cover about business risk (or relation between security risks to business risk) but it is already good enough for purpose of this paper.

REFERENCES

[1] Keri E. Pearlson , Carol S. Saunders, Managing and Using Information Systems, Wiley Publishing, 2009.

[2] Peter Mell and Timothy Grance. The NIST Definition of Cloud Computing, September 2011 (http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf).

[3] Chan. K.C. Tony, Leung. Yiu-Wing, Lam. C.M. Ernest, Web hosting with statistical capacity guarantee, Information Sciences 254 (2014) 54-68.

[4] Currie. L. Wendy, A knowledge-based risk assessment framework for evaluating web-enabled application outsourcing projects, Elsevier, 21 (2003) 207–217.

[5] Kubicek. Charles, Applying a Stochastic Model to a Dynamic QoS Enabled Web Services Hosting Environment, Elsevier, 151 (2006) 77–95.

[6] Petri. Ioan, Rana. F. Omer, Silaghi. Cosmin. Gheorghe, Rezgui. Yacine, Risk assessment in service provider communities, Elsevier, 41 (2014) 32–43.

[7] Aleem. Azeem, Sprott. Ryan. Christopher, Let me in the cloud: analysis of the benefit and risk assessment of cloud platform, Journal of Financial Crime, Vol. 20 No.
1 , 2013, Emerald Group Publishing Limited, 1359-0790, DOI 10.1108/13590791311287337.

[8] Stonebumer. Gary, Goguen. Alice and Alexis. Feringa. Risk Management Guide for Information Technology Systems, July 2012
(http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf).

[9] Sendi. Shameli. Alireza, Jabbarifar. Masoume, Shajari. Mahdi, Dagenais. Michel, FEMRA: Fuzzy Expert Model for Risk Assessment, Ecole Polytechnique de Montreal,
Canada.

[10] Horwarth. Crowe, Chan. Warren, Leung. Eugene, Pili. Heidi, Enterprise Risk Management For Cloud Computing, COSO, June 2012.

[11] Hara. Daisuke, Nakayama. Yasuichi, Secure and High-performance web server system for shared hosting Service, The University of Electro-Communications, Tokyo.

[12] Monteiro. Felipe. Andre, Azevedo. Vinicius. Marcus, Sztajnberg. Alexandre, Virtualized Web server cluster self-configuration to optimize resource and power use,
Elsevier, 86 (2013) 2779– 2796, June 2013.

[12] Harris. Shon, CISSP All-In-One Exam Guide, Sixth Edition, Page 97, McGraw-Hill, 2013

The Annual Conference on Management and Information Technology (ACMIT) 2016

Vibration Analysis on Rotating Machines using Fast Fourier Transform (FFT)

Iip Muhlisin , Rusman Rusyadi,

Faculty of Master Mechanical Engineer, Swiss German University (SGU)
Edu Town BSD City, Tangerang 15339, Indonesia

Abstract

The history has record that heavy industries face major problems that causes by variant types of mechanical failures came from rotating machines. The Vibrations in rotating machine almost fond in everywhere, due to unbalances, misalignments and imperfect part, analytical approaches has shown that vibration monitoring has great capability in detecting and addressing the defect particular part in the machine line .The vibration velocities and vibration load will be measured at different speeds using The Time-frequency analysis at initial condition. The result of vibration readings spectrum analysis and phase analysis can be determining the figure of vibrations character, and the causes of height vibration will be found. By reading the spectrum unbalance will be identified. When the unbalanced part was balanced then we found that the vibration was decrease. The Vibration experimental frequency spectrum test will be conduct for both balanced and unbalanced condition and also in different speed conditions. To full fill the vibration analysis test, in this experimental research a prototype of vibration monitoring system was constructed. The vibration can be generated and the system performance can be monitored. In this prototype the signal from load cell and velocity sensor will be processed in microcontroller and send to computer where FFT will processed the signal to create spectrum in the computer display. The actual final result of Vibration analysis test will be provide after finish the vibrations analysis test that will be done latter, therefore the chart result on this paper is based on theoretical only.

Keywords: Vibration Analysis; (Fast Fourier Transform) FFT; Unbalance; Spectrum Analysis

1. INTRODUCTION

The Vibration Monitoring System using Fast Fourier Transform (FFT), is become the objective of this paper. This paper is a literature study and theoretical analysis of a future experiment. There was some Vibration monitoring system bases on Time-frequency analysis that have been develop and applied in Industries, to answer the problems of machinery vibration, each model have some advantages and disadvantages as below is the explanation [10]:

a. Short-Time Fourier Transform

The Short – Time Fourier Transform (STFT) was introduce by Gabor in 1946 it was the first time-frequency method for speech communication, The STFT as a method to break down the non-stationary signal into many small segment. The STFT have Major disadvantage in tradeoff between time and frequency that causes the resolution become poor in time domain but good in the frequency domain with a large window width. Conversely The resolution good in time domain but poor the frequency domain with a small window width [10]

b. Wavelet Transforms

The linear time frequency representation can also built by the wavelet transform, the result more flexibility in time and frequency resolution in similar spectrogram, because the wavelet transform have the variable window length property that give us possibility of having frequency resolutions and time depend on the frequency under consideration.

The Wavelet transform have ability to carry out local analysis and this ability become the important advantage, this ability is used to revealing any small change in the signal.

The disadvantage in wavelet transform is the Octave scale of the frequency axis, this characteristic of the frequency axis makes short-duration events at the high frequencies and long-duration events at the low frequencies. The fine frequency resolution of the high frequencies does not permit in the octave scale of the frequency axis [10]

c. Wigner-Ville Distribution and Cohen's Class Time-Frequency Distributions

The Wigner-Ville distribution (WVD) recently has been applied to the field of mechanical signal analysis, this distribution is a bilinear function. The Fourier transform of the instantaneous auto-correlation of the signal is The Wigner-Ville distribution. Thus, independent of the window function is its time-frequency representation. The WVD has excellent resolution in the time and frequency domains, because the WVD has satisfies a large number of desirable mathematical criteria.

There are two major problems in the WVD. Firstly, it is not always forever non-negative, which, since energy is always positive, makes it very difficult how to interpret the Wigner-Ville representation become the energy distribution of the signal in the time-frequency plane. Secondly, because of it is bilinear in WVD, it produces cross terms for multi-component signals or interference terms [10][11]

All above The Time-frequency analysis monitoring methods can be employed for machine condition monitoring to support maintenance decisions [5] by monitoring of vibration spectrum character performance in online mode, there are much possibilities to do the maintenance that the machine in running conditions or the machine not need to dismantling all unit, because the particular failure part was found, so it can be used for further analysis in the repair of the damage caused. By observing vibration analysis on a regular basis, then something is not normal in a machine can be detected before great damage occur.

There are the some beneficial from Vibration analysis: high revenue, increased production reliability, decrease breakdown time, less maintenance cost. This analysis is closely related to protection. However, its main function is that it leads to early detection of faults unlike protection. This greatly helps to schedule activities conveniently reducing downtime and losses. [2]

The break down maintenance in industry is not popular again, it has evolved from breakdown maintenance to time based preventive and predictive maintenance. As predictive maintenance procedures and as support for making decisions action engine maintenance, vibration analysis has been used for many years [2, 3]. The best of standard operational procedure, machines do not break down or fail without some form early warning, which is indicated by an increased vibration level.

The monitoring in a real time with measuring and analyzing the vibration of a machine, make possibilities to determinant the level of defect or wear and tear. The over all of Vibration signals in the machine was generated from much part and the construction that can be linking each other. However a certain spectrum frequency character can be produce from the specific defect part, that lead to shows specific fault conditions. By monitoring and analyzing the time and frequency spectrums, and using Fast Fourier Transform (FFT), the defect part and natural frequencies of the various structural and link part can be identified [1].

In this paper, vibration analysis using FFT is studied. This is achieved by investigating different speed operating conditions of the rotating electrical machines. The rotating electrical machines are to be run under normal operating conditions as a reference test. A series of tests conducted where a number of different machine defects are intentionally introduced.

2. System Design

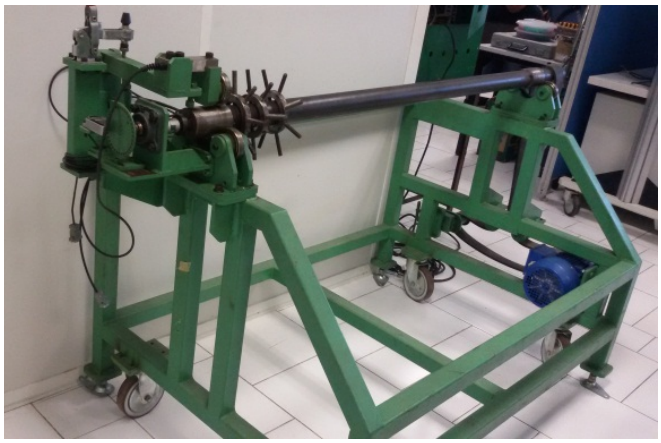


Fig.1. Experimental Test Set-up

An experimental future assembly with controlled operating conditions is set-up to conduct a series of tests using AC Motor 1,5 KW, Siemen Inverter, Arduino Atmega 2560.Flat belt, Rotor shaft, Vishay load cell, Photo Sensor SUB-30. A photograph of the experimental assembly is shown in figure. 1.

The Design of vibration monitoring system consists of a design in hardware and software. The micro controller ARTMEGA 2560 as a Master control provide Analog digital Converter(ADC)and port communication to computer, QT software program application containing the software program that serves to process vibration data collection and data processing vibration that using FFT. The Hardware system design can be described in terms of hardware block diagram as shown in Figure 2. The sensor that used is Vishay loadcell sensor. This sensor measure the Force of vibration direct from rotor shaft and then the force will be conver to voltage in the load cell, The Analog signal will be send to microcontroller to convert from become digital data, the digital data will be proced become spectrum by using Fast Fourier Transport in Computer.

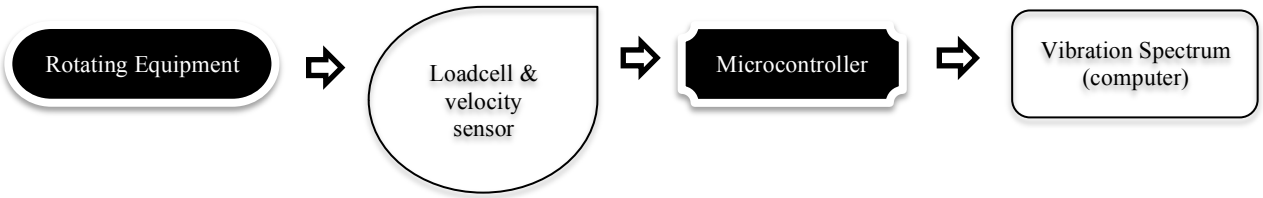


Fig. 2 Analysis hardware diagram block

The rotor Shaft will be drive by Siemen Inverter Micromaster Vector and Motor 1,5 KW, the Siemen Inverter Micromaster Vector can operate to adjust the speeed of the motor. The varaint of speed will be used during test analys. A photo sensor is used togather with a disc encoder to measure the speed of rotor shaft . The Algorithm in pseudocode is shown in Figure 3 and the wiring diagram of the vibration monitoring device is shown in figure 4.

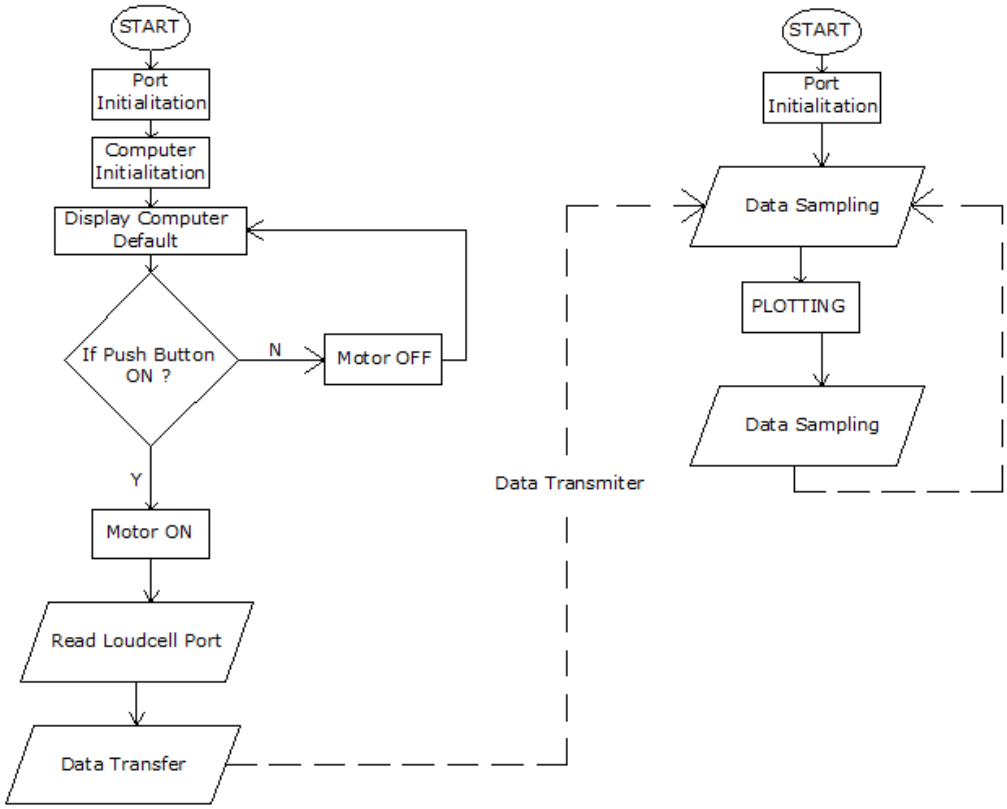


Fig. 3 The Algorithm in pseudocode

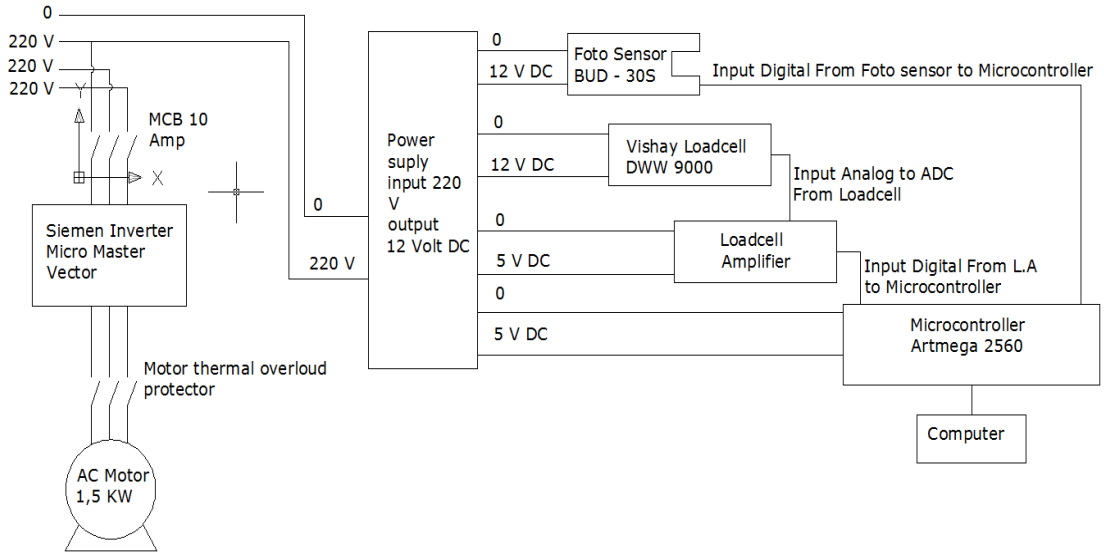


Fig. 4 Wiring diagram of Vibration monitoring

When components of rotating electrical machines operate continuously at high speeds, wear and failure is imminent. The defects can be stated that whenever one or more parts are unbalanced, misaligned, loose, eccentric, damaged or reacting to some external force; they result into higher vibration levels. The vibrations caused by the defects occur at specific vibration frequencies. The vibration amplitudes at particular frequencies are indicative of severity of the defects. The Vibration analysis is use to mapping the vibration response from the component with specific defect that occur in the machine line, although the component is linked in one mechanical structures [4]

On this System Design, a shear beam load cell (figure 5) is used to measure the resultant unbalanced force. The Vishay shear beam load cell used in this experimental is able to measure from 0 to 250 kg.

Fig. 5 Vishay shear beam load cell

The velocity is measure by BUD – 30S photo sensor (figure 6), the photo sensor is applied in this system design due to its have some features, High speed response type, Over current protection built in, reverse power polarity protection built in, selectable Light/Dark On mode by control wire, Water proof structure by IP65 (IEC specification) [8]

Fig. 6 BUD – 30S

The Load cell amplifier module (Figure 7) manage the signal from Load cell therefore the voltage level at 0-5V can be read by the microcontroller and make it easier for data processing, The voltage was create from the load cell in the order of micro-Volt and its cannot be measured by a volt meter. It is need reinforcement for thousands times even hundreds of thousands times therefore its order in volts can be measured with a votlt meter.

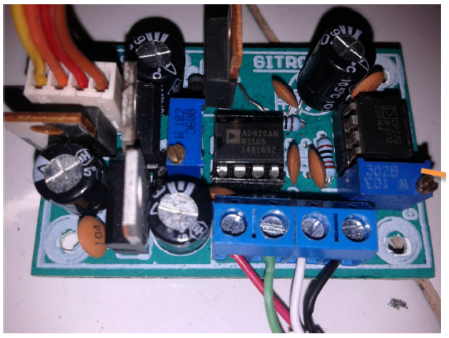


Fig. 7 Loud cell amplifier

The vibration monitoring system in this future experimental is controlled by ATmega2560 microcontroller (Figure8). The ATmega2560 is a microcontroller board based .It has 54 digital input/output pins (of which 14 can be used as PWM outputs), hardware serial ports (4 UARTs),16 analog inputs, a 16 MHz crystal oscillator, a power jack, a USB connection, a reset button and an ICSP header. The features provide everything needed to support vibration monitoring system design.

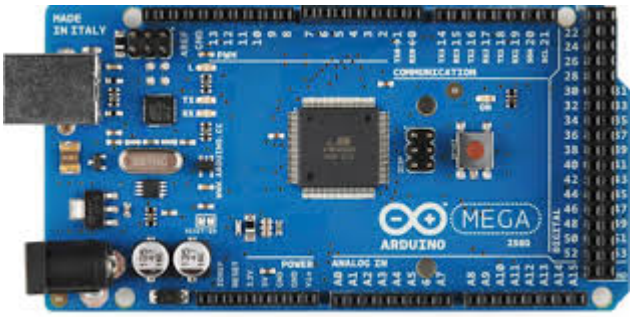


Fig. 8 Atmega 2560 microcontroller

3. VIBRATION ANALYSIS

A sample of FFT spectrum future experimental will be setup at 500, 900 and 1500 RPM for normal working conditions balance condition, and also in unbalance condition. The result of test will be compare with table of ISO 2372 a Guide Line for Machinery Vibration Severity (Figure 10) and also Standard VDI 2056 Table (Figure 11). The Vibration Monitoring System is designed with Power consumptions Bellow 15 KW therefore the device fit in Class 1 in ISO 2372 or Group K in Standard VDI 2056. The Velocity mm/s – rms have range from 0, 28 up to 71.The result of balance and unbalance test will be known whether its Good, Acceptable, Still Acceptable or Not acceptable [6][7].

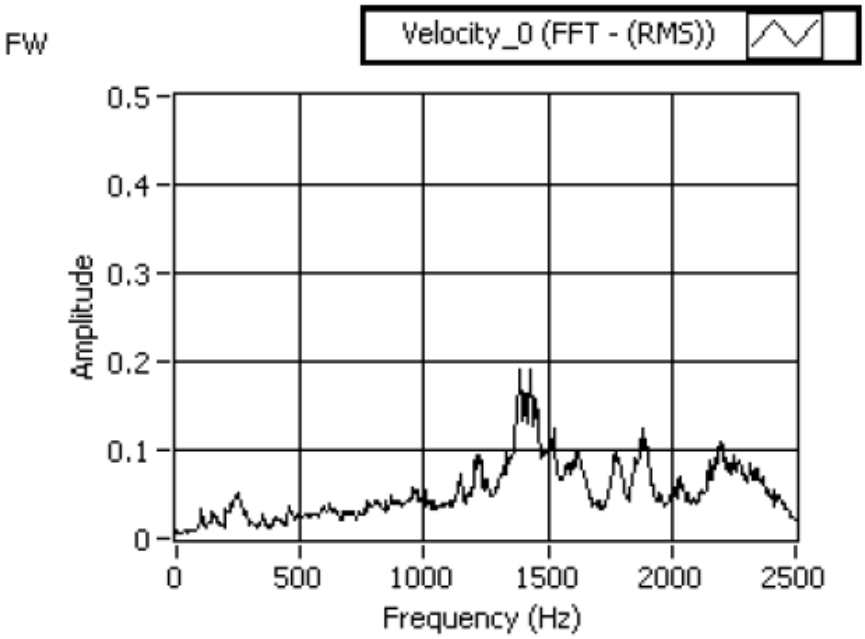


Fig 9.The Spectrum test of vibration analysis sample

The graph (figure 9) is the sample of spectrum analysis result shown that the machine is in Normal Operating condition (balance), according to ISO 2372 the Amplitude of vibration level in range 0,18 – 0,71 mm /s rms interpret the machine in Level A (Good). When the spectrum analysis shown the Amplitude of vibration level in range more than 7.1 mm/s rms its means that the machine is in the bad condition (not acceptable)

ISO 2372 – ISO Guideline for Machinery Vibration Severity					
Ranges of vibration Severity		Examples of quality judgment for separate classes of machines			
Velocity – in/s - Peak	Velocity – mm/s - rms	Class I	Class II	Class III	Class IV
0.015	0.28				
0.025	0.45				
0.039	0.71				
0.062	1.12				
0.099	1.8				
0.154	2.8				
0.248	4.5				
0.392	7.1				
0.617	11.2				
0.993	18				
1.54	28				
2.48	45				
3.94	71				

A – Good
B – Acceptable
C – Still Acceptable
D – Not Acceptable

Class I: Small (up to 15kW) machines and subassemblies of larger machines.

Class II: Medium size (15kW to 75kW) machines without special foundations or machines up to 300kW rigidly mounted on special foundations.

Class III: Large rotating machines rigidly mounted on foundations which are stiff in the direction of vibration measurement

Class IV: Large rotating machines mounted on foundations which are flexible in the direction of vibration measurement.

Figure. 10 ISO 2372 Guideline for Machinery Vibration Severity

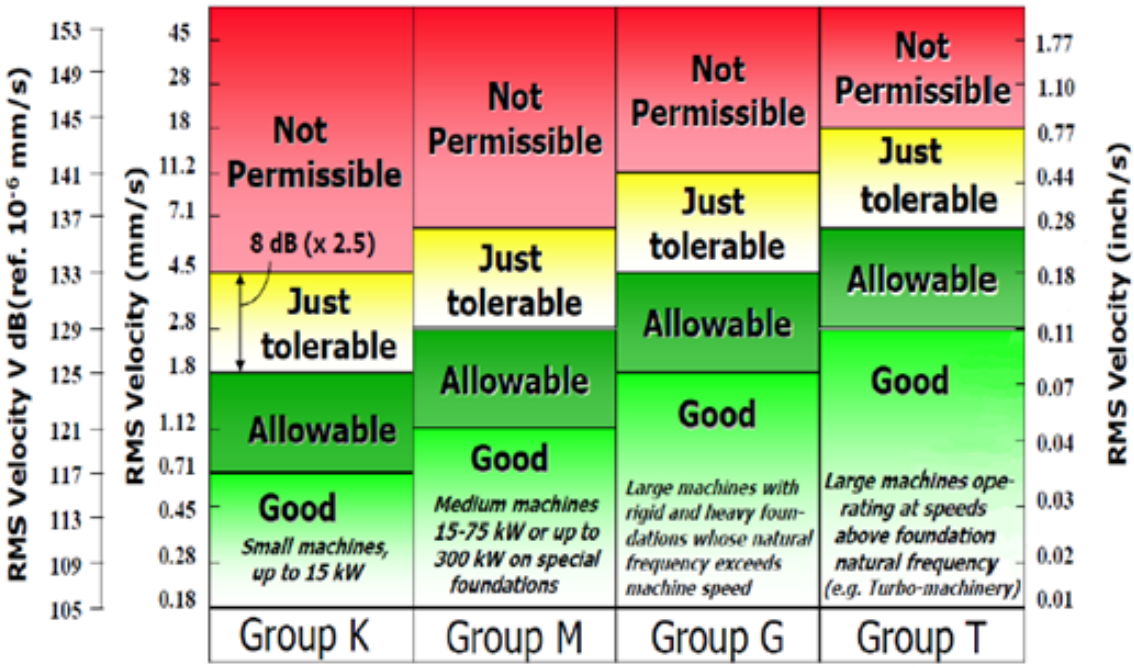


Fig. 11 Standard VDI 2056

4. CONCLUSIONS

1. The Time-frequency analysis has been found to be effective in monitoring the characteristics of machinery vibration signals. The application of time-frequency methods, provide more accurate information about a signal in time and in frequency and gives a better visual representation of the signal rather than the conventional methods in machinery diagnosis
2. There is Vibration monitoring systems based on Time-frequency analysis that have been developed and have been applied in the Industries to answer the problem of vibration. Includes: The Short-Time Fourier Transform, the Wigner-Ville distribution and the Wavelet transforms, each Time-frequency analysis above have some advantages and disadvantages as has been explained in this paper
3. Utilizing The Short-Time Fourier Transform, the Wigner-Ville distribution and the Wavelet transforms vibration monitor online, will have capabilities to monitored the Rotating machine performance condition include : balance and unbalance, transmitting and data signal processing in real time, therefore the component of machine can be detect early to prevent the fault condition before the machine production breakdown
4. The figure of magnitude amplitude in the frequency spectrum can be determined as Standard Normal or abnormal operating conditions of rotating machine.
5. The Models of fault conditions can appear simultaneously in a measurement of the frequency spectrum data

REFERENCES

[1]. S. Ebersbach, Z. Peng and N. J. Kessissoglou, "The investigation of the condition and faults of a spur gearbox using vibration and wear debris analysis techniques," Wear 260 (2006), Page(s): 16-24

[2]. Peter Tavner, Li Ran, Jim Penman and Howard Sedding, Condition Monitoring of Rotating Electrical Machines, IET Power and Energy Series, London, UK, 2008

[3]. C. Scheffer and Paresh Girdhar, Practical Machinery Vibration Analysis and Predictive Maintenance, Newnes-Elsevier, Oxford 2004

[4]. Mok Goh , Yoke SanWong and Geok Soon Hong " Intelligent Prediction Monitoring System for Predictive Maintenance in Manufacturing," Proceedings of the 31st Annual Conference of the IEEE Industrial Electronics Society - IECON'05, North Carolina, USA, 6-10 Nov 2005

[5]. Peng Z., Kessissoglou N., "An integrated approach to fault diagnosis of machinery using wear debris and vibration analysis", Elsevier, Wear 255 (2003), 1221–1232
[6]. International Standard, Mechanical Vibration, ISO 2003.
[7]. VDI 2056: Standards of Evaluation for Mechanical Vibration of machine
[8]. Autonic Product Catalog BUD series data specification
[9]. D. Gabor, "Theory of Communication," J. IEEE (London), Vol. 93, PP. 429-457, 1946
[10]. A.A. Lakis, R Machinery Fault Diagnosis Using Time-Frequency Methods 7th WSEAS International Conference on Electric Power Systems, High Voltages, Electric Machines, Venice, Italy, November 21-23, 2007
[11]. P. Flandrin, "Some features of time-frequency representation of multicomponent Signals," in Proc. IEEE 1984 International Conf. Acoust. Speech, Signal Processing (San Diego, CA), PP. 41.B.4.1- 4, Mar. 1984.

The Annual Conference on Management and Information Technology (ACMIT) 2016

Real-Time Early Detection NTP Amplification Attack

Gede Barkah Widagdo

Swiss German University, EduTown BSD City, Tangerang 15339, Indonesia

Abstract

This paper is the initials of DDoS mitigation, the goal of this research is to detect NTP Amplification as early as possible so that the victim have a data to do further eskalation process. We knows that the goal of the attacker using NTP Amplification Attack is to exhaust the bandwidth of the victim, in this research also simulate an NTP amplification scenario and detection method; the scenario is the attacker sends requests with spoofed IP MONLIST victim to the compromised NTP server NTP server then responds the large volumes of traffic (amplified traffic) towards Victim to consume the bandwidth so as the legitimate user could not access the services. We put DDoS detection device side of the victim, we combine several monitoring tools to detect NTP amplification i.e bandwidth gauge and netflow analyzer. Netflow analyzer (flow analysis) conduct analysis IP packet header that is sent by the router as a flow-exporter. In our experiment, we could perform early detection of the NTP amplification less than 2 minute.

Keyword: *DDoS Detection, NTP Amplification*

1. Introduction

In the beginning of 2014, a largest amount of Distributed Denial of Services (DDoS) occurs against cloudflare, a firm provides acceleration of website. Cloudflare records the attack reach peak 400 Gbps[1] for a couple minutes and then reduced after a few days. In 2013 - 2015 NTP DDoS attack growth significantly, the impact of DDoS resulted in losses and unavailability service of system. By observation of Akamai annual report 2015 on Q1-Q4 record that NTP amplification attack average is about 16% from the peak 180 Gbps, the rank of NTP amplification is 2nd place after SSDP (Simple Service Discovery Protocol) amplification attack, they predicts this type of DDOS still become a popular attack in this year and next year [10]. By using the vulnerability of NTP server and UDP concept, an attacker can easily multiply traffic, it would be a very serious threat. With the combination of various number of client peer and reflector number that the attack has impacted bandwidth usage; the larger number of reflector, the larger the bandwidth being generated, which in turn will lead to more damage to the victim. This research focusing on detection NTP amplification, we hope this research can contribute to subsequent research.

This research organized as follows. Chapter 2 covered is literature review of UDP and related work. Proposed methodology and approach in this research are covered in chapter 3. An experiment setup, attack scenarios and result are covered in chapter 4. Finally, the conclusions appear in chapter 5.

2. Literature Review

2.1 UDP Concept

UDP [2] is connectionless and unreliable protocol with header contains only four parameters (Source port, Destination Port, Length and Checksum) and is 8 bytes in size. UDP is connectionless without reordering of the segmentation of data and does not divide segment into right size for transmission.[3] Application that use UDP are tolerant of the lost data, or they have mechanism to recover lost data. UDP gains some advantages over TCP by not using the sequences and acknowledgement fields.

* Corresponding author. Tel.: +62818788085 ; fax: +62-21-3045-0001

E-mail address: gede.widagdo@student.sgu.ac.id

The most obvious advantage of UDP over TCP is that there are fewer bytes of overhead. UDP does not require waiting on acknowledgements or holding the data in memory until it is acknowledged which make memory is freed more quickly.

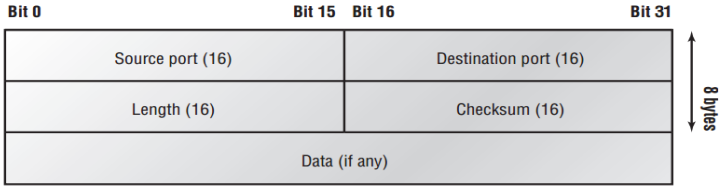


Figure 1. UDP Header [2]

The attacker can take advantage of seeing the UDP header, UDP does not validate the source IP addresses that are very easy forged IP address source by attacker. Attacker can generate a lot datagram packet and forge the source IP datagram packet, attacker spoofed IP address Victim, so as server responds to the Victim. Attacker not only able makes UDP responses linearly on prior request, but with certain instructions, the attacker can multiply respond from the server into hundreds times, it called the reflective DDOS.

2.2 NTP Amplification Attack

The functionality of NTP is to synchronize the clocks of machine (computer, server, mobile phone, etc) over a network, but a miss-configuration in the NTP server could allow request MONLIST from anywhere that can lead misbehave of request-responses. Shown in figure 2, the attacker sends MONLIST request with spoofed IP victim to the compromised NTP server then NTP server responds the amplified traffic towards Victim to consume the bandwidth [5]. Bandwidth consume in the victim divide bandwidth sent from attacker namely BAF (bandwidth amplification factor). The bandwidth amplification factor is determined by the large number of client peer and reflector, the more client-peer and reflector, the greater the bandwidth amplification factor being generated. Bandwidth amplification factor result from the experiment conducted by US-CERT reached 500 [7] and Orlando reached 3000-5500 [8]. The larger number of reflector, the larger the bandwidth is being generated.

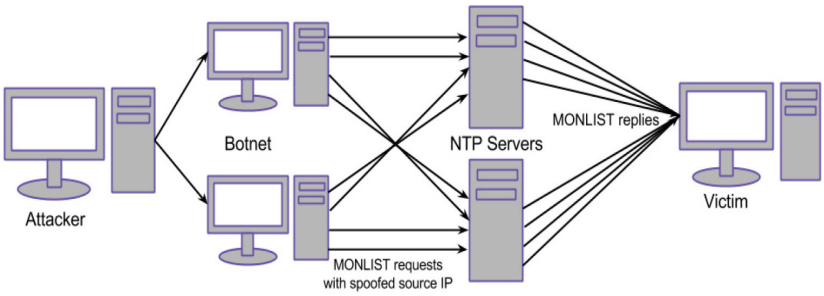


Figure 2. How NTP DDoS works.

2.3 Related Works

Rudman et al [9], his research focusing on analysis and characterization containing packet of NTP Amplification attack. He captured data attack using TCPDUMP from vulnerable NTP server then extract raw data and analysis using custom python algorithm. The data filter criteria are based on packet per hour, unique hosts per hour, IP Address TTL, TTL per hour, IP datagram length. He found that from Time-to-live value he could identify the operation system used to launch DDoS attack, and predict the number of hosts attacker. Need further research i.e real-time NTP amplification detection.

3. Research Method

Our research method follows "Canonical Experimentation Methodology" which include the following process [6] shown in figure 4:

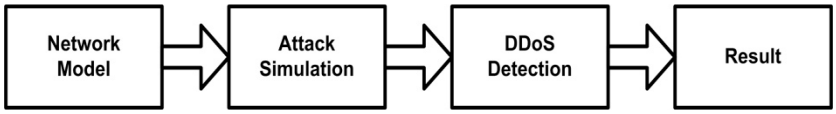


Figure 3. Research Method [8]

In the Network model section describes legitimate traffic flow from client to the victim and attack traffic from attacker to the victim, also responds flow from server to client. In the DDoS detection section describes detection mechanism and the result.

3.1 Network Model

The network model shown in figure 4 has a A is an attacker, V is Vulnerable NTP server, S is a Server, P is a NTP client peer, R is a Victim Router and L is a legitimate user. Legitimate or non-legitimate traffic route to S is through R. R role are route the packet and capture packet then forward to monitoring tools for further analysis.

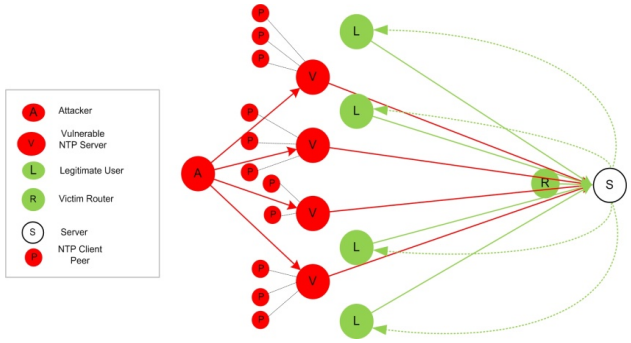


Figure 4. Network Model

3.2 Attack Simulation

In this scenario, Vulnerable NTP server as a reflectors, NTP client peer are routers in the network. The attacker ”get monlist” request to NTP server, then spoofing the request server’s IP address to the IP Victim Server.

3.3 DDoS Detection

Figure 5. Typical Flow Monitoring

Flow exporter and Flow collector is a victim's router. Victim router collect traffic flow then export to analysis application flow or netflow analyzer server. Netflow Analyzer perform filter data based on source IP Address, destination IP Address, protocol, number of packet, bandwidth and port number.

4. Testing and Result

4.1 Experimental Setup

4.1.1 Hardware and Software

The detailed specification of software and tools in the experiment shown on table 1.

Table 1. Hardware and Software

Requirement	Detail
Notebook	Proc i7 (8Core), 32G Ram, Windows 7 Profesional
Simulator	IOS on Unix
Router	IOS Cisco ver 15.2 and 12.4
Routing Protocols-Exchange	Exterior Border Gateway Protocols (eBGP)
Routing Protocols-Internal	Open Short Path First (OSPF)

4.1.2 Virtual Machine Configuration

Simulator contents are compromised servers, web servers, firewalls and IOS on Unix, each emulate on the Virtual Machine, Virtual Machine configuration are shown on table 2.

Table 2. Virtual Machine Configuration

VM	Qty	RAM (kB)	Proc (CORE)	Storage Capacity (GB)
Compromised Server	4	512	1	20
Server	2	512	1	20
IOU	1	10240	6	20

4.1.3 Network Simulation Scenarios

In this research, Tier-1, Tier-2 and Tier-3 of the Service provider network are simulated to equalize Internet Network using External Border Gateway Protocol (eBGP). While Open Short Path First (OSPF) is used in the Internal Tier-3 Network. The simulator contains 13 AS Number as transit point, 32 Routers, 2 Switches, 2 Servers as server farm, 2 servers as compromised server place at ASN2 and ASN3. The detail network topology are shown in figure 6.

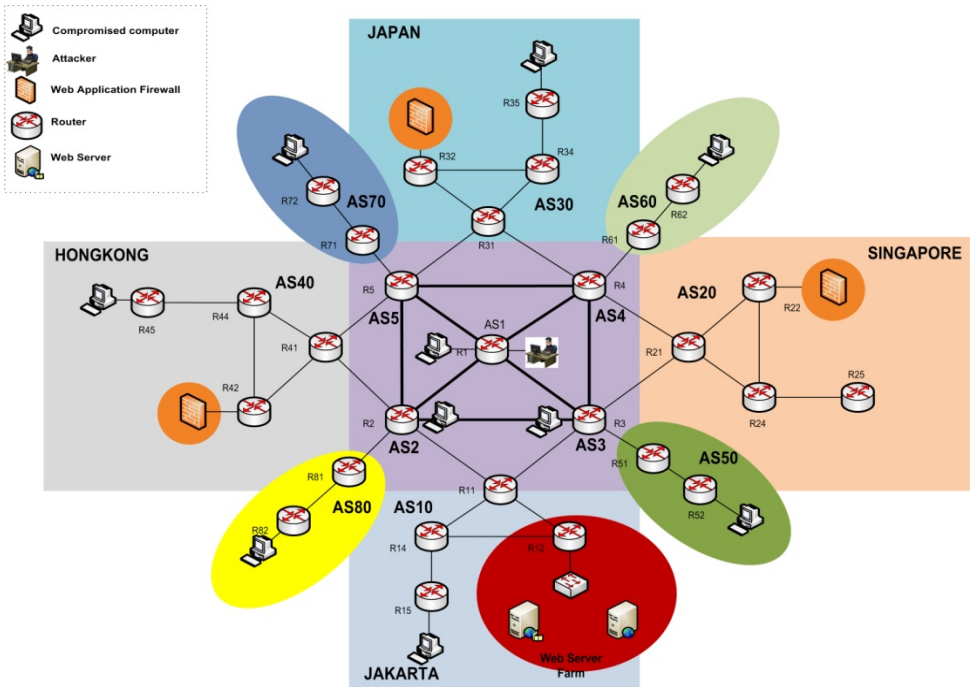


Figure 6. Network Topology Scenario

4.2 Attack Scenario

In this scenario, 2 NTP server as a compromised server become the reflectors, NTP client server are routers in the network. The attacker "get monlist" request to NTP server, then spoofing the request server's IP address to the IP Victim Server. The detail configuration of attack scenarios are shown on table 3.

Table 3. Configuration of attack scenarios

Configuration	
NTP Compromised Server	2 Servers
NTP Client Peer	100 Peer
Target Attack/Victim	1 IP Address
Attacker	1 Server
Duration Test	30 Minutes

4.3 DDoS Detection and Result

Flow exporter and Flow collector is a victim's router. Victim router collect traffic flow then export to analysis application flow or netflow analyzer server. Netflow Analyzer perform filter data based on source IP Address, destination IP Address, protocol, number of packet, bandwidth and port number.

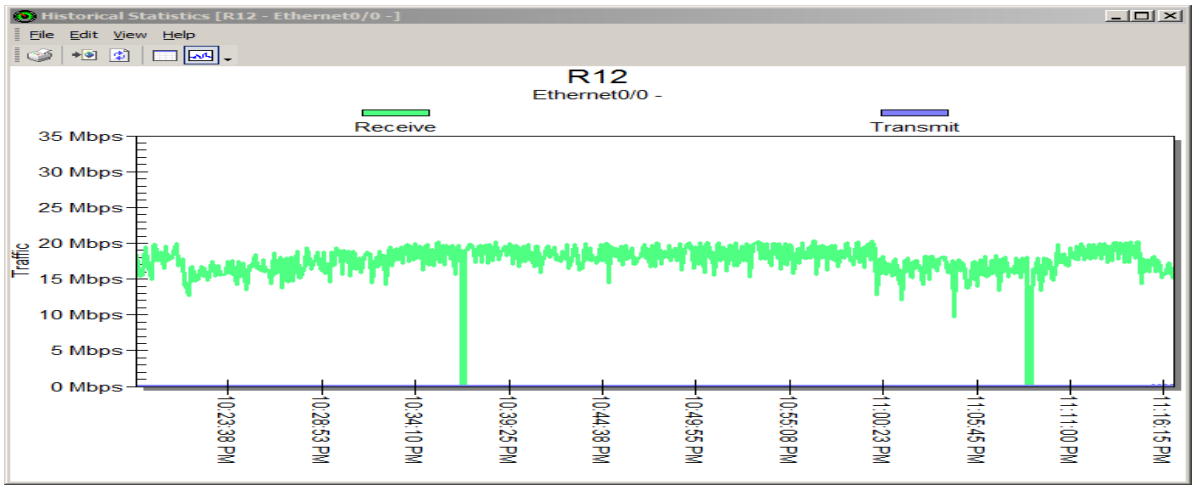


Figure 7. Bandwidth monitoring

Source IP	Destination IP	Application	Port	Protocol	DSCP	Traffic (3.79 GB)	%Traffic
203.2.2.102	203.200.200.200	ntp	123	UDP	CS6	1.9 GB	50%
203.3.3.102	203.200.200.200	ntp	123	UDP	CS6	1.89 GB	50%

Figure 8. Netflow Analyzer Report

Figure 7 shows the capture traffic from the victim router, saturate bandwidth at 20Mbps. From this information we perform further investigation using netflow analyzer. Figure 8 shows the total traffic NTP collected by netflow analyzer is 3.79 GB. Breakdown for the detailed application and are 50% from source IP address 203.2.2.102 and 50% from source IP address 203.3.3.102. 3.79 GB in the second interval 1776 seconds or 30 minutes. This is not normal NTP behavior because normal NTP packet is 50 bytes. For the detail data during attack simulation shown on table 4.

Table 4. Data collected during attack simulation

Traffic Collected (GB)	Interval Collected (Sec)	Bandwidth Average (bps)	Packet/Sec	NTP-Packet-Size/Sec (Amplification) (Byte)	NTP- Packet-Size/Sec (Normal) (Byte)
3.79	1776	17.073.600	4627	461	50

In the other monitoring on victim router during attack simulation, we found that there was an increase in CPU usage on the victim router, this is due to increased packet should be forwarded by the router but this we not happen in on the server at victim side, it's because the victim not listen in TCP/123 so as system not allocate resource to process packet response from reflectors.

5. Conclusion

The goal of this research is to detect NTP Amplification attack in real-time. The goal of the attacker using NTP Amplification Attack is to exhaust the bandwidth of the victim. So the main components to detect NTP Amplification is a bandwidth monitoring; bandwidth monitoring used to record traffic in bits per second, whereas the other components is the network flow analyzer, the output of this analyzer are packet per second, source IP address, destination IP address, protocols, port number and size of packet. In the end we could detected NTP amplification includes source IP address, destination IP address of the target of attack, and application protocols less than 2 minutes.
This research does not aim to mitigate NTP Amplification attack, mitigation of NTP amplification requires further research. But with the early detection results that have been obtained, the victim can perform escalation to Upper-level network or service provider to take further action such as source IP filtering reflector or perform rate-limiting to the NTP protocol to a specific IP destination.

6. Acknowledgment

This work is supported by the Swiss German University, Faculty of Information Technology. In Particular the author thanks to Charles Lim, M.Sc.

References

[1] Surviving a DDoS Attack: What every host needs to know, Cloudflare, 2014.

[2] Postel, J. "Search RFCs." (1980).

[3] Odom, Wendell. *Ccent/ccna icnd1 official exam certification guide (ccent exam 640-822 and ccna exam 640-802)*. Cisco Press, 2007., CCIE No.1624

[4] The Top 10 DDoS Attack Trends, Discover the latest ddos attacks and their implications, Incapsula, 2014.

[5] Rudman, Lauren. "Analysis of NTP Based Amplification DDoS Attacks." (2014).

[6] Schwab, S., Wilson, B., and Thomas, R., "Methodologies and metrics for the testing and analysis of distributed denial of service attacks and defenses," in "Military Communications Conference, 2005. MILCOM 2005. IEEE," pp. 2686–2692, IEEE, 2005.

[7] CERT, U., "UDP-Based Amplification Attacks," CERT, 2016, URL https://www. us-cert.gov/ncas/alerts/TA14-017A.

[8] Orlando, M., "NTP can be abused to amplify denial-of-service attack traffic," CERT, 2014, URL https://www.kb.cert.org/vuls/id/348126.

[9] Rudman, L., and B. Irwin. "Characterization and analysis of NTP amplification based DDoS attacks." Information Security for South Africa (ISSA), 2015. IEEE, 2015.

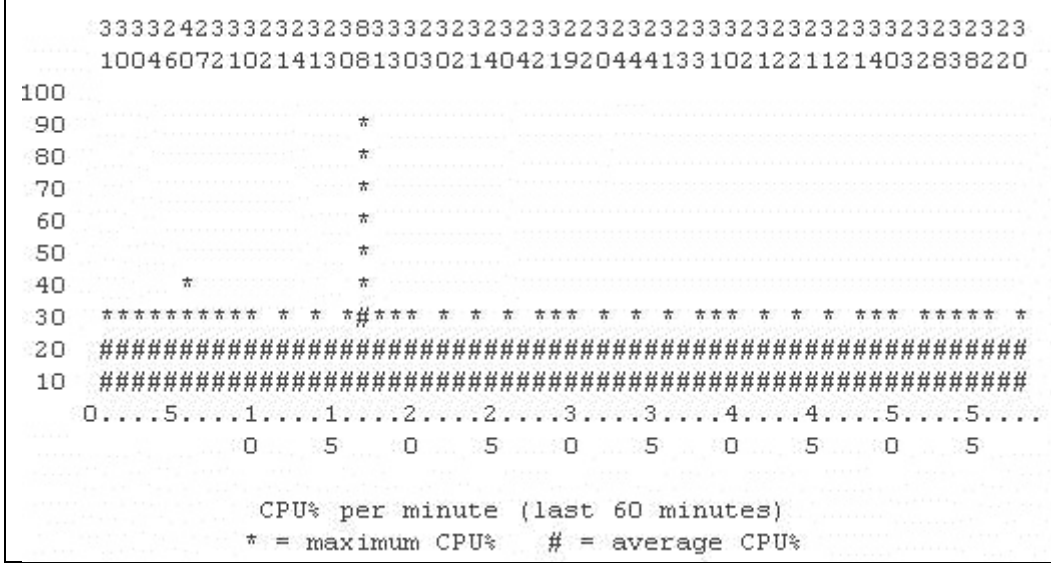
[10] Akamai's state of the internet /security Q1-Q4 2015 report, 2015.

Appendix A

```
/usr/bin/ntpdc  -n -c monlist 203.20.20.102
remote address          port local address      count m ver rstr avgint  lstint
===============================================================================
203.50.50.105          123 203.20.20.102          9 4 4     0    37      0
203.60.60.103          123 203.20.20.102         10 4 4     0    33      0
203.60.60.101          123 203.20.20.102         10 4 4     0    33      0
203.2.2.6             123 203.20.20.102          9 4 4     0    37      1
203.2.2.4             123 203.20.20.102         10 4 4     0    40      1
203.40.40.105          123 203.20.20.102         10 4 4     0    34      2
203.40.40.103          123 203.20.20.102         10 4 4     0    34      3
203.50.50.103          123 203.20.20.102          9 4 4     0    37      3
203.50.50.102          123 203.20.20.102         10 4 4     0    33      3
203.2.2.3             123 203.20.20.102         11 4 4     0    37      3
203.50.50.101          123 203.20.20.102          9 4 4     0    37      4
203.2.2.1             123 203.20.20.102         11 4 4     0    37      4
203.30.30.104          123 203.20.20.102         10 4 4     0    34      5
203.40.40.102          123 203.20.20.102         10 4 4     0    34      6
203.40.40.104          123 203.20.20.102         10 4 4     0    34      6
203.2.2.7             123 203.20.20.102         10 4 4     0    40      7
203.2.2.2             123 203.20.20.102         10 4 4     0    40      7
203.1.1.10            123 203.20.20.102          9 4 4     0    45      9
203.30.30.101          123 203.20.20.102         10 4 4     0    35     10
203.1.1.7             123 203.20.20.102         11 4 4     0    37     10
203.1.1.3             123 203.20.20.102         11 4 4     0    38     10
203.40.40.101          123 203.20.20.102          9 4 4     0    31     11
203.30.30.105          123 203.20.20.102         10 4 4     0    34     11
203.1.1.9             123 203.20.20.102         11 4 4     0    37     11
203.30.30.102          123 203.20.20.102         10 4 4     0    34     14
203.20.20.110          123 203.20.20.102          8 4 4     0    43     14
203.1.1.5             123 203.20.20.102         11 4 4     0    37     15
203.30.30.103          123 203.20.20.102         10 4 4     0    34     16
203.1.1.6             123 203.20.20.102          4 4 4     0    70     16
203.20.20.105          123 203.20.20.102          8 4 4     0    44     17
203.1.1.4             123 203.20.20.102          8 4 4     0    52     18
203.20.20.103          123 203.20.20.102          8 4 4     0    44     19
203.20.20.107          123 203.20.20.102          9 4 4     0    32     20
203.20.20.109          123 203.20.20.102          9 4 4     0    39     21
203.1.1.2             123 203.20.20.102          9 4 4     0    46     22
203.1.1.1             123 203.20.20.102         11 4 4     0    38     22
203.20.20.108          123 203.20.20.102          9 4 4     0    39     23
203.20.20.106          123 203.20.20.102          9 4 4     0    39     23
203.20.20.104          123 203.20.20.102         10 4 4     0    35     23
203.20.20.102          123 203.20.20.102         10 4 4     0    35     23
203.20.20.101          123 203.20.20.102          8 4 4     0    45     23
203.1.1.8             123 203.20.20.102          4 4 4     0    70     23
203.10.10.109          123 203.20.20.102          9 4 4     0    40     25
203.10.10.105          123 203.20.20.102         10 4 4     0    36     28
203.10.10.110          123 203.20.20.102          9 4 4     0    40     29
203.10.10.108          123 203.20.20.102          9 4 4     0    40     29
203.10.10.107          123 203.20.20.102          9 4 4     0    40     30
203.10.10.106          123 203.20.20.102         10 4 4     0    36     30
203.10.10.102          123 203.20.20.102         10 4 4     0    36     30
203.10.10.104          123 203.20.20.102         10 4 4     0    36     32
203.5.5.9             123 203.20.20.102         10 4 4     0    37     34
203.10.10.103          123 203.20.20.102         10 4 4     0    36     35
203.10.10.101          123 203.20.20.102         10 4 4     0    37     36
203.5.5.7             123 203.20.20.102         10 4 4     0    37     36
203.5.5.10            123 203.20.20.102         10 4 4     0    37     38
203.5.5.8             123 203.20.20.102         10 4 4     0    37     41
203.5.5.5             123 203.20.20.102         10 4 4     0    37    103
203.5.5.4             123 203.20.20.102          9 4 4     0    41    106
203.5.5.6             123 203.20.20.102          9 4 4     0    34    109
203.5.5.3             123 203.20.20.102         10 4 4     0    37    109
203.5.5.1             123 203.20.20.102         10 4 4     0    38    110
203.4.4.8             123 203.20.20.102          9 4 4     0    42    110
203.4.4.7             123 203.20.20.102          9 4 4     0    42    111
203.5.5.2             123 203.20.20.102          9 4 4     0    42    111
203.4.4.10            123 203.20.20.102          9 4 4     0    42    112
203.4.4.9             123 203.20.20.102          9 4 4     0    42    112
203.4.4.6             123 203.20.20.102          9 4 4     0    42    112
203.80.80.104          123 203.20.20.102          9 4 4     0    35    116
203.4.4.5             123 203.20.20.102         10 4 4     0    38    116
```

203.4.4.2	123 203.20.20.102	10 4 4	0	38	116
203.3.3.9	123 203.20.20.102	10 4 4	0	39	117
203.4.4.4	123 203.20.20.102	10 4 4	0	38	117
203.80.80.103	123 203.20.20.102	9 4 4	0	35	120
203.80.80.101	123 203.20.20.102	9 4 4	0	36	120
203.3.3.8	123 203.20.20.102	10 4 4	0	39	120
203.4.4.3	123 203.20.20.102	10 4 4	0	38	120
203.70.70.105	123 203.20.20.102	9 4 4	0	36	121
203.3.3.10	123 203.20.20.102	10 4 4	0	39	121
203.4.4.1	123 203.20.20.102	10 4 4	0	39	121
203.80.80.105	123 203.20.20.102	9 4 4	0	35	122
203.80.80.102	123 203.20.20.102	9 4 4	0	36	122
203.70.70.104	123 203.20.20.102	9 4 4	0	36	123
203.3.3.7	123 203.20.20.102	10 4 4	0	39	123
203.3.3.6	123 203.20.20.102	10 4 4	0	39	124
203.70.70.102	123 203.20.20.102	9 4 4	0	36	126
203.3.3.5	123 203.20.20.102	10 4 4	0	39	126
203.60.60.105	123 203.20.20.102	9 4 4	0	36	127
203.70.70.101	123 203.20.20.102	9 4 4	0	36	127
203.3.3.1	123 203.20.20.102	10 4 4	0	40	127
203.60.60.102	123 203.20.20.102	9 4 4	0	37	129
203.70.70.103	123 203.20.20.102	9 4 4	0	36	129
203.2.2.10	123 203.20.20.102	9 4 4	0	44	129
203.3.3.4	123 203.20.20.102	10 4 4	0	39	129
203.3.3.3	123 203.20.20.102	10 4 4	0	39	131
203.60.60.104	123 203.20.20.102	9 4 4	0	36	132
203.2.2.9	123 203.20.20.102	9 4 4	0	44	132
203.50.50.104	123 203.20.20.102	9 4 4	0	37	133
203.2.2.8	123 203.20.20.102	10 4 4	0	40	133
203.3.3.2	123 203.20.20.102	10 4 4	0	39	134
203.2.2.5	123 203.20.20.102	10 4 4	0	40	136
203.1.1.132	45406 203.20.20.102	2 3 4	0	164	329

Router CPU



The Annual Conference on Management and Information Technology (ACMIT) 2016

Strategic Considerations of SaaS Implementation for Retail Banking System

Ageng A. Amukti
Swiss German University
EduTown BSDCity, Kav. II.1BSD City 15339
Indonesia

Ageng31@gmail.com

Abstract

Globalization era has provide us with such benefits with all the technology and business innovations, but with the high pace of competition, the ability to adapt and evolve is increasingly important and demand of creating product with the latest technology became more common, this creates a problem for system provider that offer large Enterprise software as their system, as it is inherently complex and hard to maintain. To deal with this complexity, one of the emerging concept as a solution for this is by converting the enterprise system into SaaS or "software as a service" model, as it enable financial system providers to segregate their banking package into several modules or services with high elasticity and scalability, thus makes it easier to manage. But before adopting the SaaS technology, organizations need to know what kind of changes that need to be expected, as implementing retail banking system with SaaS model can be regarded as a different business model than the traditional in-house retail system, depending of the degree of model adoption, the changes emerged may be significant and if the organization is not ready then it will do more damage than benefits. This paper is trying to provide organization a strategic view for consideration before they can adopt SaaS model for their retail banking applications and highlighting some strategic considerations of SaaS model over traditional in-house applications.

Keywords: Retail banking system; SaaS; strategic view; system adoption.

INTRODUCTION

In this globalization era with ever-changing technology and business landscape, ability to adapt and evolve is more and more needed, at some cases it is even necessary in order to survive in the industry. This is especially true for banking system vendors; if they are incapable of evolving their system then it is very possible to fall behind the other competitors and not getting a market share which needed. One expectation is the innovations of the banking products and services such as 24 hours online banking, internet banking, mobile banking, branchless banking and others which demand the system or platform to be adapted in the newest technologies and concepts existed.

Essentially, the banking system is very important for making transactions of various customers' daily need. While using the banking system, the customers often look for the factors of convenience and ease so that the transactions could be done easily [12]. Another important point is that if the banking system is not flexible and secure, then the clients will not be satisfied with the banking system at all due to which they may even start thinking about changing banks.

Retail banking is the process which is usually known as customer banking since this process could be used for satisfying individual customers as compared to companies or other banking systems [9]. In order to get more customers and to restore their reputation with clients, banks introduced the concept of retail banking so that the individual needs and desires of customer could be satisfied. The only problem which the companies faced due to this system was that the flexibility associated with the traditional banking system.

Unfortunately, understanding an implementation of banking infrastructure and its business information systems are challenging tasks for managers, especially figuring out which IT system or department that can be converted into the cloud service, and whether or not the organization is ready for the adoption. This paper will try to highlight the strategic benefits of SaaS model, to explore

strategical inputs which must be considered before adopting SaaS technology and to provide guidelines for the retail banking organizations in a context of strategic IT management especially in retail banking.

BACKGROUND

Retail banking is basically the backbone of banking systems nowadays and is proving to be the safest source of stability and consistency. Through retail banking, the business of banks is becoming stable and secure. The clients are also more satisfied with the services being provided by the client. They feel that they are listened to and that they are important as customers for banks. The retail banking system provides immense strength to the banking system by providing them an alternative in the form of retail banking system. Fortunately, the new retail banking systems in the form of SaaS through cloud could be a better alternative for this industry because it could save the company significant resources by enabling them to implement new services in a timely manner to the clients and able to upgrade their system capabilities seamlessly as they go to solve problems. In traditional systems, deploying, enhancing and maintaining business information systems are often the hardest part inside the system's lifecycle. Depends on the complexity of the system, SaaS adoption can cost significant amount of time and large sum of money for companies, and even more so if the size of the organization is large. Things like time frame, budget, manpower, and other resources needs to be carefully specified in the requirements to ensure the deployment of business-critical software application is going smoothly, otherwise it may create a significant risk for the organizations.

SaaS could help IT engineers and administrators to manage requirements when deploying patches and updates because of its flexibility, and it could be used as a replacement for traditional delivery model as it is built on a shared infrastructure over the internet backbone and specifically designed for modularity so it's able to handle any complicated databases and management systems. Since the banks usually have very complicated and large database schemes including the names and other details of customers, SAAS technology could prove to be very helpful in this regard [12]. Sharon Mertz, research director at Gartner Inc. stated that after more than a decade of use, the adoption of SaaS growing in a steady pace and evolve regionally within the enterprise application markets. [4]

CONCEPT BEHIND SAAS

The basic concept behind SAAS or "Software as a Service" could be traced back to 1990s where application service providers tried to develop new alternative for selling their program, they develop a new model which enable their customers to rent the software applications instead of the traditional "buy and own" application ownership. After years of attention, there are many definitions of SaaS spread around the community ranging from simple definition such as "*software deployed in a hosted,managed service and accessed through the Internet*" [3], to a bit more specific one such as [5] SaaS as a "*software that is owned, delivered and remotely managed either by one or more providers.*", but in order to understand the term clearly, this paper used the definition presented by U.S National Institute of Standards and Technology (NIST) as the main reference.

"**SaaS or Software as a Service.** Is a capability provided to the consumer by hosting the consumer's applications running through the cloud infrastructures. The applications are accessible from various kinds of client devices either through a thin client interface, such as web browsers, or a program interface. The consumer does not directly manage or control the underlying cloud infrastructure including but not limited to network, servers, operating systems, storage, or individualized application capabilities, with limited exception of user-specific application configuration settings." [14]

SaaS is basically a new distribution model of software where it focuses on separating the possession and ownership of software from its use. The applications are hosted and delivered over the internet through the cloud infrastructure and cloud service providers (cloud vendors), and are available for the customers to access and run for. Because it runs over internet, it is usually accessed through web-based service and users typically access from a "thin client" such as web browser or a graphical user interface (GUI), the client is primarily used only for communication and displaying incoming data, but not doing any calculations or data processing.

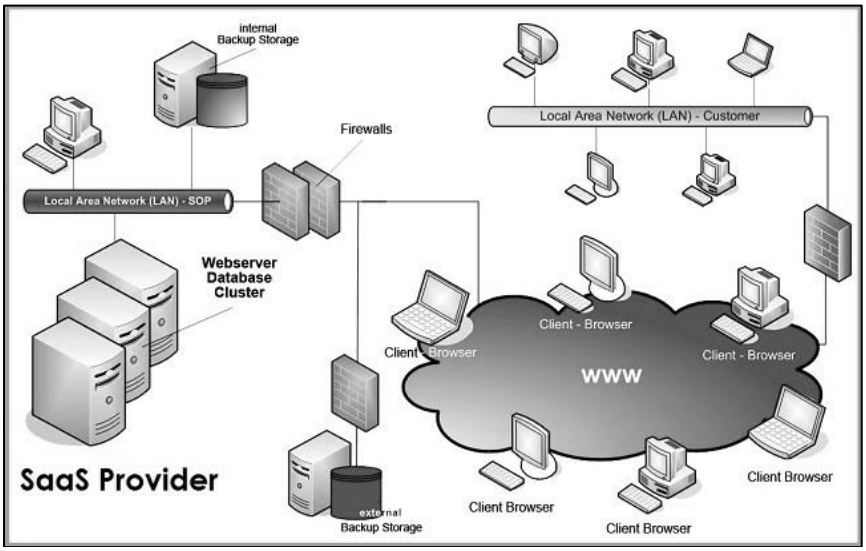


Figure 1. SaaS Model

"*With the SaaS model, all software applications are deployed and hosted inside the vendors' premises after client's adoption. Clients do not purchase software or infrastructure such as hardware and OS upfront, but pay for their access to the services over time."* [18]

Liao and Tao[10] describe that when using SaaS the ownership of software shifts from the customer to SaaS providers and redistributed such as hardware, technology infrastructure and management, and professional services required. They also identify two different forms of SaaS service modes:

- Provide services platform
  Cloud service providers build SaaS platform as a basic interface for the retail applications where third party and independent software vendors (ISVs) can engaged in.

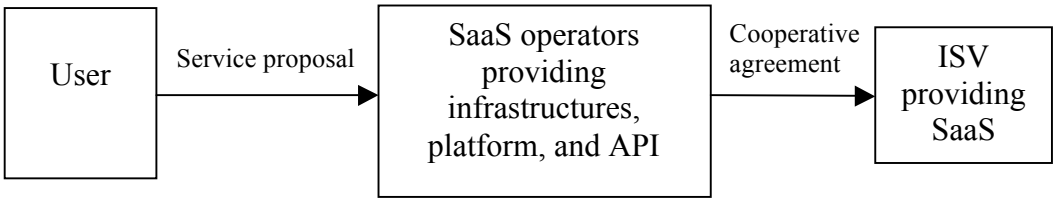


Figure 2. SaaS vendors providing services platform

- Provide full services
  In the second model, SaaS service providers develop their own applications and provide full-range of service such as computing infrastructure, SaaS applications, data storaging and other related services.

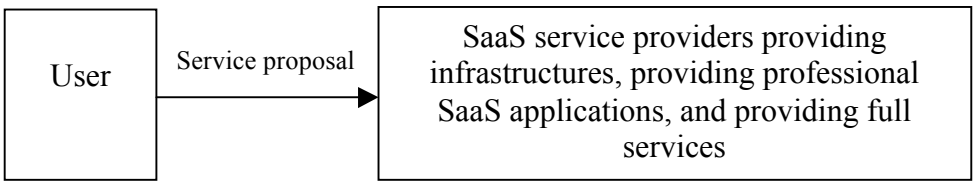


Figure 3. SaaS vendors providing full services

According to Carraro and Chong[3], SaaS can be seen as either "Line-of-business services" or "Consumer-oriented services" . the firs model or the "Line-of-business SaaS services" is named because the service is offered to various size of business organizations and are very often provide large and customizable business information systems supporting the critical business processes such as finances, sales, customer relationship management. "Consumer-oriented services" is the second model where the cloud computing services is offered to the general public. From the customer perspective, there are three major risk identified when adopting SaaS: less application improvement and integration options, risk of losing business-critical data, and the probability performance related problems." [15] And Major challenges for SaaS adoption can be boiled down into several considerations, such as security and privacy considerations [1][16][17], reliability and technical considerations [3][7][10][17], financial considerations [3][10][17], legal considerations [10][17].

The guidelines and considerations offered in this paper about SaaS for banking systems, it is expected to be applied to both SaaS model and could provide valuable input in knowing strategic benefits and limitations of SaaS model around the context of the banking system.

OVERVIEW OF RETAIL BANK BUSINESS MODEL

Retail banking, or also known as Consumer Banking is the provision of services by a bank to individual consumers and small business where the financial institutions are dealing with large number of low value transactions rather than to big entities such as companies, corporations or other banks. This is in contrast to other counterpart such as wholesale or corporate banking where the customers' base are large, often catering multinational companies, local governments and government's enterprise.

The retail concept itself is not new to banks but it is considered as an important and profitable market segment that offers opportunities for growth and profits. Inside retail banking, all the needs of customers are taken care in an integrated manner.

The Retail banking characteristics can be boiled down into three basic element:

- Multiple products (deposits, credit cards, insurance, investments and securities),
- Multiple channels of distribution (call center, branch, and internet) and,
- Multiple customer groups (consumer, small business, and corporate).

One of the most distinguished feature of Retail Banking products is that it is a volume driven business. Further, one of the service such as retail credit ensures that the business is spread widely amongst a large customer base unlike in the case of corporate lending, where the risk may be concentrated on a selected few plans.

STRATEGIC CONSIDERATIONS

Analyzing and evaluating whether a strategy is aligned to our organization is important, even though financial organization such as banks have similar service model to offer, but every organization may have different sales approaches, time to market strategies, competitive differentiation and geographic dispersion. So in terms of decision strategy whether it is good for SaaS adoption, one size does not fit all. However, there are five important key for considerations which every organization faces in determining whether to outsource any IT services: organization culture; core competencies; the impact on people, operations and lastly finances.

1.1. Company Culture

The success or failure of any strategy decision is dependent on the organization's culture, such as its vision, values, norms, assumptions, beliefs and habits. According to a research of cloud computing system adoption, adoption of a new innovation are depends on companies' culture.[2] If your company culture isn't compatible then it can only hinders the process and decision, making the adoption process ineffective or even possibly turning the adoption into a liability. Depending on your current culture inside the company, SaaS technology can be considered as a new innovation and it is important to assess the company's stance for such innovation before adopting. Below are some questions worth considering about organization's culture before making a decision to adopt SaaS for your retail banking:

No.	Questions
1	How amenable to change is the organization culture?
2	Is the philosophy of the organization allows outsourcing such as adopting SaaS?
3	What are our views on job eliminations and layoffs?
4	What is our desired level of control over the bank processes?
5	How well does our organization leverage on the current available technology?
6	What is our position in the SaaS technology adoption comparing to our competitors? (innovators, early adopters, early majority, late majority, or laggards)
7	Is IT viewed as a deciding factor for our organization's success or is it just an expense?

Table 1. Company culture questions

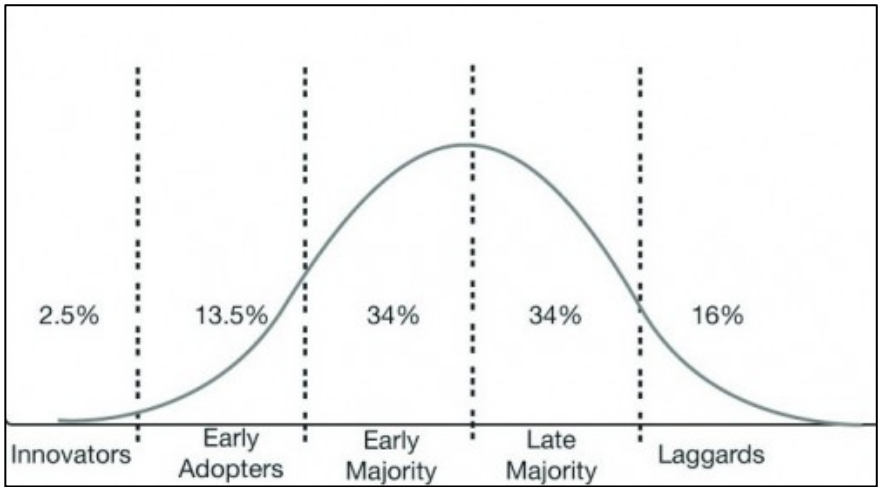


Figure 4. Rogers' Bell Curve of Technology Adoption

1.2. Core competencies

Core competencies basically is an organization's business imperatives, or in other words, the decisive things that the organization good at. Specifically in this case, it's the capability of using certain aspect of information technology to set themselves apart from their competitors. Because applying SaaS for retail banking will need dedication and certain skills either on technical and/or organizational aspects, it is important to know our IT competency before adopting the new technology, because if we adopt the technology without competent enough to utilize it, that IT services may become a burden rather than a capability and the effort will be wasted.

Below is list of examples of IT services financial organization can use to differentiate them from the competition. However, it's important to note that the technology itself is not the one that differentiates the organization from the competition, but it's what the organization does with the technology.

Examples of retail banking services that can be a differentiating force

- Digital channels such as Internet and Mobile
- CRM - Branch Operational
- Customer experience dashboard
- Core banking service – Master Data Management
- General Ledger management
- Loans feature
- Cards
- Current and Saving account customization
- Payment methods
- Term Deposits
- Local clearing feature
- Anti-money laundering and other regulation compliance
- General security aspect for both physical and digital assets, such as storage

Before making a decision to adopt SaaS for the retail system, you can consider these questions to understand the core competencies of the organization:

No.	Question
1	What kind of IT Services that could provide to our organization a strategic advantage over our competitors?
2	Is the SaaS adoption aligned strategically as our competitive advantage to our business?
3	Is the adoption vital to our organization's competitiveness?
4	If we adopt, does it make any difference in our business such as gaining uniqueness, differentiation, or any way that can set us apart?
5	Does the adoption make customers' impression of our organization better against other competitors?
6	Is the SaaS adoption is an added value to our organization and worth our resources, or is it just a waste of time?
7	What IT services that is critical to the organization?
8	What IT application or services that caused us some difficulty?
9	What IT skills and systems do we need, but are not the core of what we do as an organization?

Table 2. Core competencies questions

1.3. People

According to Gartner[6], The main concerns of adopting SaaS in general are keeping up technical requirements, security, ease of integration and functionality. Although after the SaaS adoption the main stakeholder for maintenance and support will be the SaaS providers, organization will still need enough IT staff for general portfolio management in order for the system to work without problem and meet future demands, especially in the technical requirements. Previous research has shown that organizational size has noteworthy implications for IT management[11][13]. But most organization have limited IT staff to do those varied tasks and keeping up the pace, this is why it is important for organization to assess their IT staff's current expertise according to our current technology used as well as the possible technology needs in the future to better anticipate the consequence of the adoption.. Organizations can consider these questions first about your IT staff as an input before deciding whether to adopt SaaS for particular retail services:

No.	Question
1	Are we handling our IT services internally well today?
2	Do we have enough IT staffs / engineers to continue at this pace tomorrow?
3	What technologies are rapidly changing that potentially could give our staff a hard time for staying up-do-date?
4	What is the current condition of the technical IT expertise we need in the organization today?
5	How is the current availability of such expertise in the job market?
6	How are the trends of salary requirements for qualified IT personnel needed?
7	If we adopt SaaS, how would we handle the IT personnel replaced? Is it redeployed, reassigned, etc.?

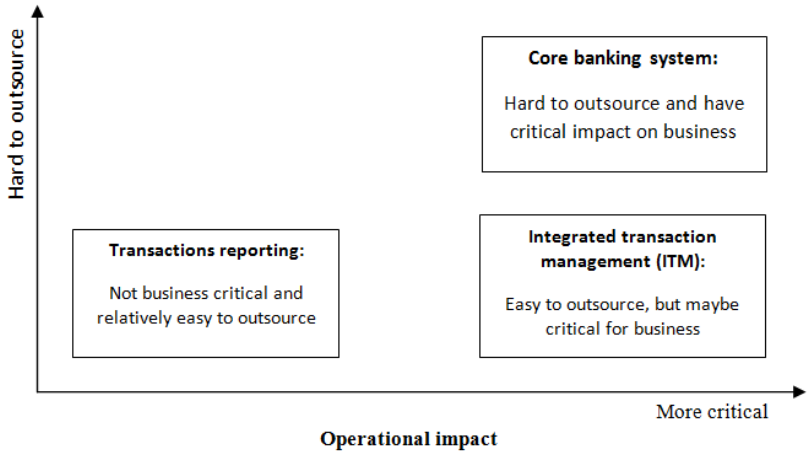
Table 3. Internal resource readiness questions

1.4. Operational impact

The expected benefits from adopting SaaS for retail banking cannot be realized without careful management of the entire adoption process. To build an effective management effort, we need an early understanding of the SaaS impact involved in the retail banking. Important issues could arise during the development of online banking, for example, could include immature technology and shortages of specialists are important to consider[8]. Because the nature of retail banking system can be very complex, different skillsets is required to be able to manage the services well, one rule of thumb is the

harder and more critical a service to adopt, the operational impact will be bigger after the adoption is done.. Below is an illustration of operational impact on some retail banking feature.

Figure 5. Example of operational impact on several retail services



If you feel hard to assess the operational impact of adopting SaaS for certain retail service, some of these questions may help you before considering any decision:

- What is the role of that retail service in our organization?
- Is the retail service requires high availability?
- What is the impact of the retail service on our organization's operational performance?
- Is there a possibility that our operations will suffer noticeably if this retail service is poorly implemented?
- What new technologies, such as hardware or skill expertise do we need in order to maintain and grow our business?
- What is the degree of change in the current technology? Is it occurred frequently?
- Will adopting SaaS for this retail service provide the flexibility to scale up or down?
- What are the risks and disadvantages of adopting SaaS for this service?
- How will the security be maintained?
- What trade-offs are our organization willing to accept:
    - Between High availability of service and cost?
    - Between responsiveness and cost?
    - Disaster recovery and cost?
- Do you think of any other trade-off possible?

1.5. Financial impact

Just like any other investment, any organization will naturally want to know if the adoption is a good investment and how much it will cost. Unfortunately, some advantages of adopting SaaS against traditional system may be hard to quantify, but if we consider the strategic alignment, it may outweigh the cost. For example, converting certain internal assets may add value to core competencies. Of course, we may also need to consider trade-offs between service levels and costs. Organization can consider these questions about the financial impact as part of making a decision to adopt SaaS for certain retail features:

- Can our organization afford the service levels of SaaS we want?
- What service levels is our staff provide in the moment, and at what cost?
- What IT Services can we obtain at the same or higher service levels at a cost savings by adopting SaaS?
- Is it cost-effective to increase our IT staff to meet our IT needs?
- Are we considering adopting the SaaS technology solely to save money?
- If so, what exactly is our target of ROI (Return of Investment)?
- Can SaaS adoption of the service be modified quickly and easily to meet our needs? Or is it too hard and necessary to make the systems or infrastructure in-house?
- What are the economics of traditional in-house system versus SaaS adoption?

- What are the strategic ramifications of SaaS adoption that are not so easily quantified?

1.6. Most Frequently IT service for SaaS adoption

While almost all IT function basically can be converted into SaaS counterparts (including IT management), but in case of retail banking there are some IT functions that especially common and potent for conversion.

No.	Retail IT functions and services
• Application development	
1.	Transactional accounts
2.	Savings accounts
3.	Debit cards
4.	ATM cards
5.	Credit cards
6.	Traveler's cheques
7.	Mortgages
8.	Home equity loans
9.	Personal loans
10.	Certificates of deposit/Term deposits
11.	general reporting
• Application maintenance and updates	
• New features	
• Modification to meet regulation and/or business requirements	
• Application hosting service	
• Database administration	
• Data center operations	
• Customer support	

Table 4. Possible IT functions and services for SaaS adoption

CONCLUSION

The purpose of this study is to provide a strategic view for organization that considering SaaS adoption for their retail banking applications and highlighting some strategic considerations of SaaS model over traditional in-house applications. The paper explore the strategic values and considerations for adopting SaaS model in business organizations in five aspects; company culture, core ompetencies, people, operational, and financial impact. Software as a Service (SaaS) is in a rising trend and steadily draws interest from the business organizations across the world.

As in any investment decision, business and IT executives need to take a strategic analysis in order to understand and realize the potential of SaaS objectively in the context of their own organization conditions, needs and capabilities. Other than saving costs, SaaS can help business organizations to achieve competitive advantages by improving efficiency and better flexibility in the decision making but only if they understand which of their service that can potentially be converted beneficially. This paper provide some guidance and questions to help organizations to understand their position in SaaS adoption, hopefully it will be apparent whether converting certain retail functions to SaaS or not is a good business proposition for the organization. If the organization decides whether to convert certain retail service into SaaS in a firm vision, you can safely move onto the next step for actually adopting SaaS, such as choosing appropriate SaaS provider. Similar to hiring a new employee, it is necessary to investigate service providers available and determine their suitability as the business partner, and this paper can help you to reach the decision.

References

[1] Avram, M, 2013. Advantages and challenges of adopting cloud computing from an enterprise perspective. Proceedings of the 7th International Conference Interdisciplinarity in Engineering (INTER-ENG 2013), pp. 529-534. Elsevier.

[2] Bayrak, E., Conley, J.P. and Wilkie, S., 2011. The economics of cloud computing. The Korean Economic Review, 27(2), pp.203-230.

[3] Carraro G. and Chong F., 2006. Software as a Service (SaaS): An Enterprise Perspective [online]. Microsoft Corporation.

[4] Gartner, 2012. Forecast: Software as a Service, All Regions, 2010-2015, 1H12 Update. Stamford: Gartner.

[5] Gartner, 2013. IT Glossary: Software as a Service (SaaS) [online]. Available from : http://www.gartner.com/it-glossary/software-as-a-service-saas/ [Accessed 02 April 2014].
Gartner Inc.

[6] Gartner.com. (2016). Gartner Survey Shows Many Users are Underwhelmed by Their Experiences of SaaS. [online] Available at: http://www.gartner.com/it/page.jsp?id=1062512 [Accessed 29 Mar. 2016].

[7] Godse, M. and Mulik, S., 2009. An approach for selecting software-as-a-service (SaaS) product, Proceedings of the IEEE International Conference on Cloud Computing. IEEE Computer Society.

[8] Gupta, U., 1999. Information systems: Success in the 21st century. Prentice Hall PTR.

[9] Liao, H., 2009, June. Design of SaaS-based software architecture. In *New Trends in Information and Service Science, 2009. NISS'09. International Conference on* (pp. 277-281). IEEE.

[10] Liao H. and Tao C., 2008. An Anatomy to SaaS Business Mode Based on Internet. ICMECG '08 Proceedings of the 2008 International Conference on Management of e-Commerce and e-Government, 215-220, Washington, D.C.: IEEE Computer Society.

[11] Liberatore, M.J. and Breem, D., 1997. Adoption and implementation of digital-imaging technology in the banking and insurance industries. Engineering Management, IEEE Transactions on, 44(4), pp.367-377.

[12] Ma, D., 2007, July. The business model of" software-as-a-service". In*Services Computing, 2007. SCC 2007. IEEE International Conference on*(pp. 701-702). IEEE.

[13] McGowan, M.K. and Madey, G.R., 1998. The influence of organization structure and organizational learning factors on the extent of EDI implementation in US firms. Information Resources Management Journal (IRMJ), 11(3), pp.17-27.

[14] Mell, P. and Grance, T., 2011. The NIST Definition of Cloud Computing. Gaithersburg: U.S. Department of Commerce.

[15] Sääksjärvi, M., Aki L., and Henry N., 2005. Evaluating the software as a service business model: From CPU time-sharing to online innovation sharing. IADIS international conference e-society. Qawra, Malta

[16] Subashini, S. and Kavitha, V., 2010. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34 (1), 1-11. Elsevier Ltd.

[17] Verma, G., 2011. Software as a Service. Pragyaan: Journal of Information Technology, 9 (1), pp. 32-37. Dehradun: Institute of Management Studies.

[18] Xin, M. and Levina N., 2008. Software-as-a-Service Model: Elaborating Client-side Adoption Factors. Proceedings of the 29th International Conference on Information Systems, Paris, France, December 14-17, 2008.

The Annual Conference on Management and Information Technology (ACMIT) 2016

Benefit and Risk Assessment for Having Disaster Recovery in Cloud Computing for Banking Industry: Go/No-Go Decision Making Model

Krisdian Eko Sutedja [3]*
Swiss German University, EduTown BSDCity, Kav. II.1, Bumi Serpong Damai, Banten 15339, Indonesia

Abstract

Over the past year, we all have been showed many cloud-based solutions for so many purposes, starting from the public storage facilities to the disaster recovery solutions. We have learned that enterprises need to pay more attention to the cybersecurity, especially for the banking industry. The bank needs to encompass all that protects the bank from the attacks, breaches, disruptions, and incidents and also the consequences, but still need to reduce costs. So as the result, the solutions need to be aligned with all of the other aspects within the bank, which include the governance, management and risk assurance. The idea of having the disaster recovery in the cloud have to also consider the information security aspects, as the bank is trying to get the maximum benefit that the bank can get from the cloud like to minimize the cost needed by the bank's activities, but still need to consider the results of the risk assessment as one of the requirement in implementing the cloud solutions. The other thing that the bank has to consider is the compliance aspect.

Keywords: Disaster Recovery; Cloud Computing; Risk Assessment

1. Introduction

Currently the Bank is facing tough economic times. Depreciation of Rupiah, Indonesian stocks continue to fall, and other economic problems that we currently have right now. In the very competitive business environment, The Bank is forced to increase efficiency but still need to improve flexibility and scalability, and the arising ideas are like how to cut costs, keep the trust from the clients by giving reliable services, and help the clients to maintain their good and even make closer relationship with their customers by maintaining the service level as agreed.

One of the things that can be improved to be more efficient is the resource usage. The cloud computing is claimed to be able to reduce recovery time and provide multi-site availability at a fraction of the conventional disaster recovery solutions cost.

* Corresponding author. Tel.: +62-21-3045-0045; fax: +62-21-3045-0001 .
E-mail address: krisdian.sutedja(at)sgu.ac.id .

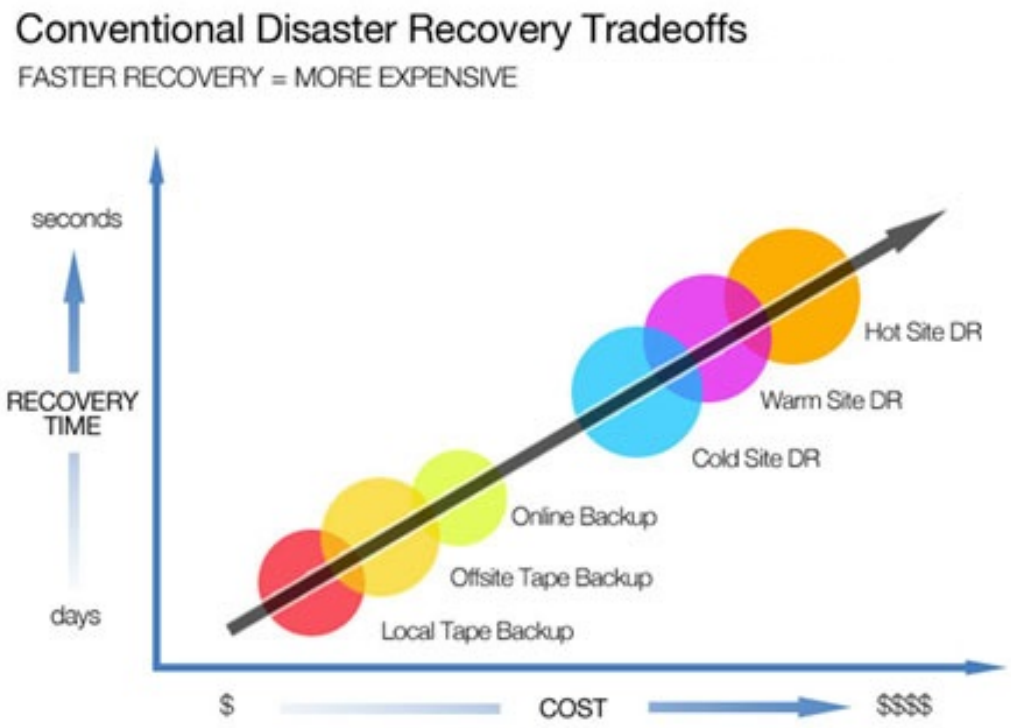


Fig. 1. The conventional disaster recovery tradeoffs [1]

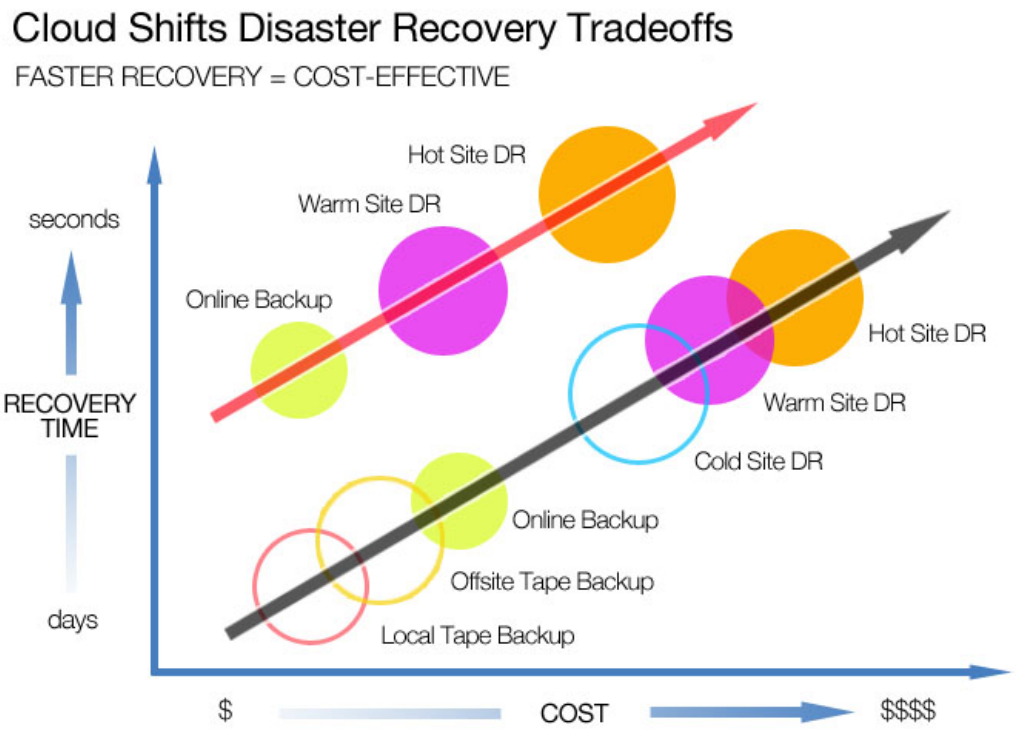


Fig. 2. The cloud shifts the disaster recovery tradeoff curve to the left [1]

As the bank industry is always required to meet the operational and regulatory requirements set by the regulator, in this case Otoritas Jasa Keuangan (OJK), the banks need to design and implement the cloud computing solution very carefully to make sure that it meets the requirements, or else, the project

will be failed to be delivered. We can learn from the cases like what happened in the Bank of Queensland case, where they were unable to meet the operational and regulatory requirements [2]. So, the implementation in banking industry is even trickier because of the regulatory requirements.

This research proposes a comprehensive benefit and risk assessment framework in which the objective hierarchy is constructed and the appropriate measurements are defined to provide the guidance for the assessment. Thus, the research is driven by this research question: *How to decide whether the bank should go with the disaster recovery in the cloud project plan from the perspective of benefit and risk analysis?*

2. Cloud-based Disaster Recovery Solutions: An Overview

Cloud-based disaster recovery solutions can be an attractive alternative for the companies, especially the small and medium-sized business (SMB), where the secondary infrastructure is only idling most of the times. It can reduce the need for spaces, and the resources that may lead to a significant cost reduction [3]. So it may enable the SMBs to have the disaster recovery solution options that were only available for the large enterprises because of the high cost. The cloud-based solution has another benefit that it make the disaster recovery process to become less complicated. But there are challenges in providing cloud-based disaster recovery solutions, that security is usually the top concern. The usual questions regarding the cloud-based solutions are like is the data stored and transferred securely in the cloud, how the user sessions are being authenticated, and as for the banks, they have the additional regulatory requirement considerations. The table below shows the three disaster recovery categories in term of the feature differences.

Table 1. Disaster recovery models [4]

DR model	Data synchronization	Independency	Initial Cost	Ongoing cost	Cost of potential disasters
Dedicated	High	Low	High	Depends	High
Distributed	Medium	High	Medium	Depends	High
Cloud	Low	High	Low	Depends	Low

There are several different types of the cloud-based disaster recovery solutions that are available and can be used by the bank, as follow [5] [6]:

a. Both of the managed application and also managed disaster recovery solutions are in the cloud. By doing this, the bank can have the full benefits of the cloud computing, that are from having the cost based on usage, and further more in eliminating the needs of on-premise infrastructures. In this scenario, the most important thing to be addressed is the Service Level Agreement (SLA) with the vendor.
b. Backup in the cloud as the substitute for tape based off-site backup. In this scenario, the application and database are still remain on-premise, and the data is being backup into the cloud, in case when system failures/disasters occur, the on-premise systems are restored from the data taken from the cloud.
c. Backup to the cloud, and when needed, the restore is also done to the cloud. So in this scenario, when system failure/disaster is happened, the data that was backed up to the cloud, is restored to the virtual machine (VM) in the cloud.
d. Replication to the backup virtual machines in the cloud. In this scenario where the RPO (Recovery Point Objective) is the main objective, the data is replicated to the virtual machine in the cloud. This scenario can be used to replicate and protect both of the on-premise and backup system in the cloud.

3. The Benefits, Risks, and Costs of Cloud-based Disaster Recovery Solutions

The considerations in implementing the cloud-based disaster recovery solutions are basically the same as in the traditional disaster recovery solutions, that are about how long the systems can be down, how much data loss that is acceptable, what business parts that have to be up and when, and also about less downtime of the systems versus the greater disaster recovery solution costs. Or they can be defined as [7]:

- RTO (Recovery Time Objective) : The time between the declaration and the service availability, it's related to the time needed to restore the services to usable state.

- RPO (Recovery Point Objective) : The data in the system that is lost during the disaster time, it's related to the amount of data that is entered into the system since the last backup of the system.
- TTO (Test Time Objective) : The time required in testing the recovery plans, it's related to the resources that are used for the testing.

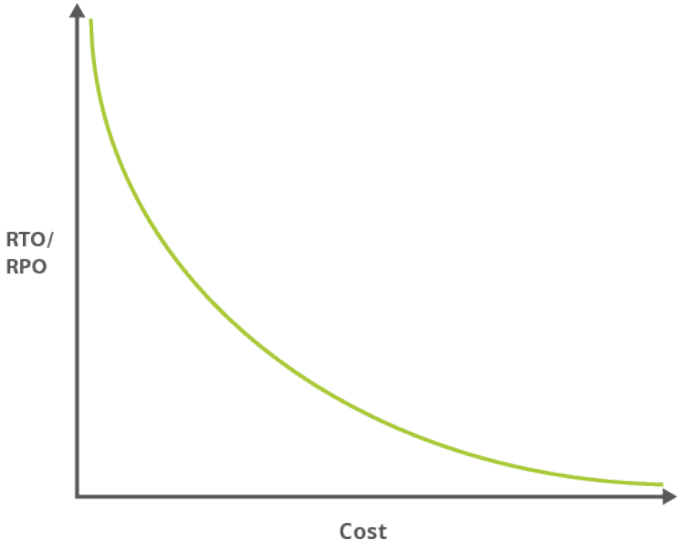


Fig. 3. The ratio of cost to RTO/RPO [7]

The RPO needs to be considered in choosing the disaster recovery solutions. Generally, the necessary RPO of a disaster recovery system is a business decision [7].

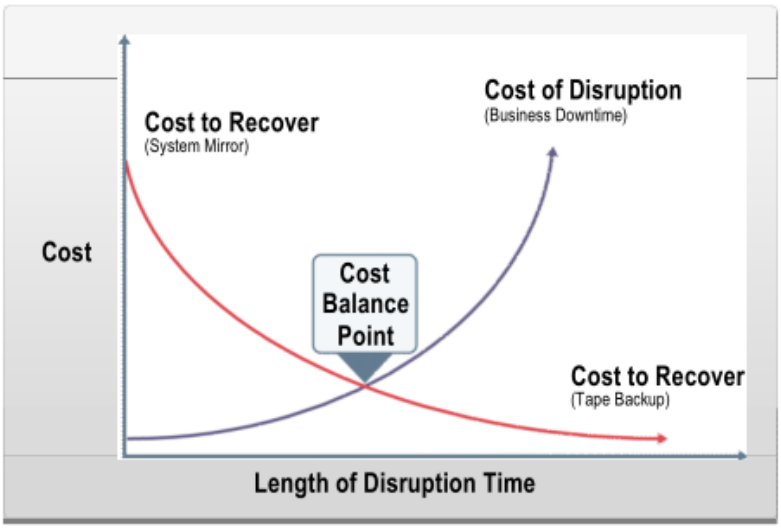


Fig. 4. Cost balancing diagram [8]

What we can see from the above diagram is that the longer the disruption is happening, more costly it will become for the company and the operation. The shorter the RTO, the recovery solution costs to implement will become more expensive [8].

In the disaster recovery system planning, after we've done the business impact analysis (BIA), the next step is to perform the risk assessment. What BIA can help is that the BIA helps in identifying the business processes that are the most critical and describes about the potential impact of the disruption to the processes, and then the risk assessment can identify both the internal and external situations that

may impact the critical processes negatively. The bank should have the Risk Management Policy, as a statement of the overall intentions and the direction of an organization which is related to risk management, including the risks related to the disaster recovery plans [9]. Moreover it can quantify the potential severity of the events like that and the likelihood of them to be occurred [10] [11].

4. Regulatory Challenges

For the banking industry in Indonesia, the regulators require the data to be located in local data centers, to be kept secure and integrity and confidentiality maintained. Failing to conform to the regulation may cause the bank to be penalized by the regulator. The impact may even include the loss of reputation, which may be then reflected in the market shares. So the increasing dependency on the external cloud-based disaster recovery solution can increase the non-compliance probability. That's the reason of why compliance is also an important area of the cloud risk.

The current regulation, legislation, and standards that exist nationally and internationally that are related to the business continuity management and disaster recovery plan need to be checked against the plan that's going to be defined by the company. One of the checklist of the regulation, legislation, and standards is published by Business Continuity Institute (BCI), that lists the legislations, regulations, standards, and good practices from many countries in the world. The example of the regulation from Indonesia is as follows:

Table 2. The business continuity related regulation in Indonesia [12]

INDONESIA

TITLE		AUTHORITY	SUMMARY	LINK
Regulation No 9/15/PBI/2007	Regulation	Bank Indonesia (Central Bank)	Implementation of Risk Management in the use of information technology by commercial banks. ✓ ☐ ☐ ☐ ☐ ☐ ☐ ☐	
Regulation no. 6/8/PBI/2004	Regulation	Bank Indonesia (Central Bank)	The Bank Indonesia real time gross settlement system (unofficial translation). ✓ ☐ ☐ ☐ ☐ ☐ ☐ ☐	
Circular Letter No. 9/30/DPNP - Risk Management in the Use of Information Technology by Commercial Banks (March 31st, 2008)	Regulation	Bank Indonesia (Central Bank)	Requires BCP documentation and at least annual testing with focus on Bank Indonesia RTGS system. Requires internal audit to conduct an audit at least annually and provide report to Bank Indonesia. ✓ ☐ ☐ ☐ ☐ ☐ ☐ ☐	http://www.bi.go.id/web/en/Peraturan/Perbankan/se_093007.htm

5. Evaluating Cloud-Based Disaster Recovery Solutions For Banking: A Case Study

The virtualization technology, the cloud computing and cloud storage of data are among the top main concerns for the companies regarding the required knowledge. The companies need the knowledge about cloud computing in order to explore the more possibilities in deploying the cloud computing and getting more benefits from it [13]. According to the Forrester/DRJ study, 42% of the companies are using some sort of outsourced disaster recovery services [14], and 78% of enterprises have stated that the disaster recovery capabilities improvement is their high priority, in order to be better in identifying and quantifying the risks, in understanding the economic impact, and having less tolerance for the downtime and the data loss [15]. The CEOs (Chief Executive Officers) and business owners are already realized that they can get more of the money with outsourcing. In line with the global IT transformation focus and survey, the bank tries to find the disaster recovery solution that's more cost effective compared to continuing the current conventional way in doing the disaster recovery plan, that's by adding new servers and network devices into the available space at the disaster recovery site. The cost to rent the private space for the servers and network devices is another big issue for the bank, and the needed space is even growing, in line with the growing of the on-premise/production data center site. In doing so, the bank is developing the model about how to decide if the bank should go with the cloud-based disaster recovery solution for each of the systems. So the cloud-based disaster recovery solution can be used for a new banking system, or for the old systems that need to be moved to the cloud, due to

the high maintenance costs, for example. The move to the cloud for the old systems' disaster recovery plan is also to improve the RTO and RPO.

First the bank needs to set the BIA. The bank defines the critical level of the business processes in the BIA into four tiers as follows [16]:

a. Tier 1: Mission-Critical

Mission-critical business processes/activities are those that have the greatest impact on company's operations and potential for recovery. Tolerable downtime for mission-critical process is 0 to 6 hours top. Process must be maintained in top priority under any circumstances.

b. Tier 2: Vital

Vital business processes/activities are deemed very important and should be addressed immediately after the mission-critical processes. Tolerable downtime for vital process is 7-24 hours top.

c. Tier 3: Important

Important business processes/activities will not stop the business from operating in the near-term but they usually have a longer-term impact if they were missing or disabled. Tolerable downtime for important process is more than 1 day.

d. Tier 4: Minor

Minor business processes/activities do not need to wait for any system/facility to recover. They are going to not to be missed in the near-term and that certainly not while business operations are being recovered. They may resume business with workaround that requires minimal effort.

Based on the critical level, the BIA form was then distributed to the each of the business units in the bank, the example of the result is as follows:

Table 3. The example of the BIA results

No.	Critical Business Process	Critical Level				Dependencies on IT Group Software/Hardware	Dependencies on other BU/SU/Vendor	Min. Resource Required	Potential Financial Impact	Legal / Compliance Impact
		Tier 1	Tier 2	Tier 3	Tier 4					
CORPORATE BANKING GROUP										
1	RM and TL as window person for customers, internal department and decision maker	X	-	-	-	N/A	Loan Ops and IRMD	2	N/A	N/A
2	Credit Proposal preparation until obtain final approval - server folder - Core Banking System - counter party related	-	X	-	-	Yes	CRMG	3	N/A	N/A
3	Loan documentation process - Agreement signing - Drawdown process - Repayment schedule	-	X	-	-	N/A	Legal, Loan Ops, IRMD	2	N/A	N/A
4	Cash Management - FBS system - Internet Banking	-	X	-	-	Yes	Operation Group and IT	2	Low	Low

From the BIA results, the requirements from people, process, and technology aspects in order to support the critical business functions can be defined. Like for example, how can the available people related resources owned by the bank support the disaster recovery plan, such as the skills and knowledge needed, the amount of staff, etc.

The metrics like the RTO and RPO can then be obtained and the most critical systems and data can be mapped, which areas of the business that can be down for a longer period without causing the adverse effects. The tiered services can be customized with the availability of the cloud computing, making the disaster solutions to become more flexible, as the bank can get more options for the solutions.

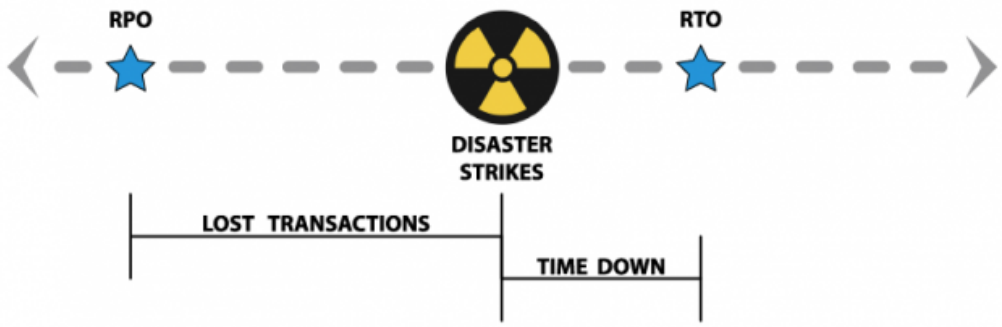


Fig. 5. The RPO versus RTO in disaster recovery planning [17]

In the above diagram, the gap between the disaster and the RPO is the data/transactions of the bank that will be lost as the result of the disaster/system failure. The RTO required can then be mapped to the cloud-based disaster recovery service level that's provided by the vendor. The example of the cloud based disaster recovery packages can be seen as follows:

Table 4. Disaster recovery service level differences from IBM [18]

IBM SmartCloud recovery service level	Recovery time	Description
Gold	1 minute	For mission-critical applications
Silver	30 minutes	For rapid recovery
Bronze	6 to 24 hours	Assisted failover and failback

The return on investment (ROI) of the disaster recovery solutions can be calculated to see the value of the disaster recovery options. The example about how to calculate the ROI is as follows: If the bank had been shutdown for the few days because of disaster, they might lose $900,000 in revenue, for example. Let's say that the bank has an annual cloud-based disaster recovery solution from a vendor that costs about $50,000 per year in order to protect all of the bank's tier 1 and 2 servers. And then, when a disaster hits the bank's business, the bank then fail over to the cloud-based disaster recovery solution and the process takes about three hours total. Because of the successful fail over process, the bank does not suffer any significant productivity lost, that the bank still can serve their customers and continue to earn the revenues. Which means, the ROI can be counted as ($900,000 - $50,000) / $50,000 which equals to 1,700% [19].

The cost of investment and savings comparison from having the legacy disaster recovery solution with the cloud-based disaster recovery solution can be projected as follows:

Table 5. The example of the bank's cumulative investment and savings data

PT. Bank XYZ	
Cumulative Investment and Savings	
Legacy Environment	$ 518,593
Year 1	**$ 377,352**
Year 2	**$ 447,973**
Year 3	**$ 518,593**
Cloud Environment	$ 56,698
Year 1	**$ 25,053**

Year 2	$	40,876
Year 3	$	56,698
Savings	$	461,895
Year 1	$	352,299
Year 2	$	407,097
Year 3	$	461,895

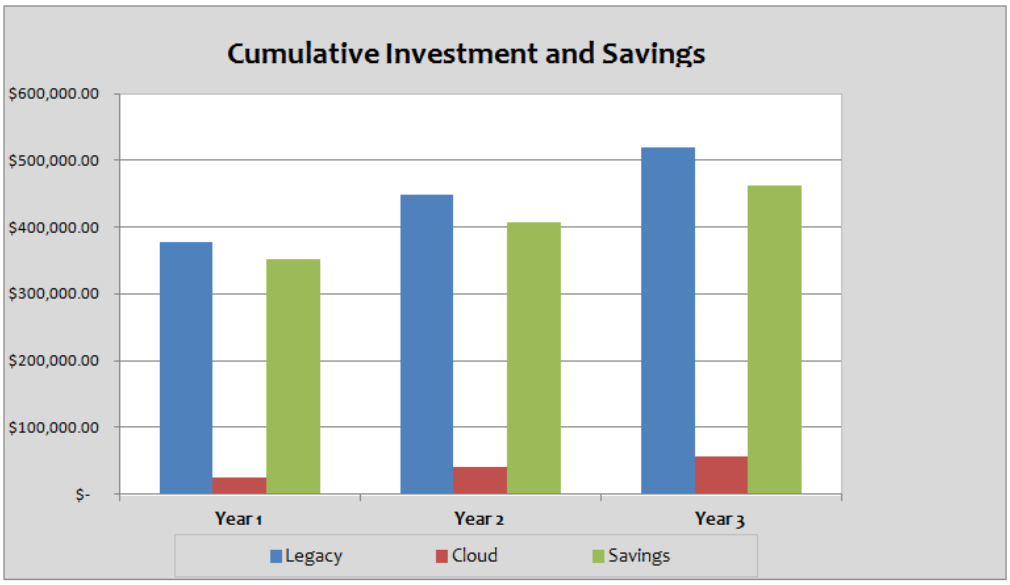


Fig. 6. The example of the bank's cumulative investment and savings graphics

The next step when considering the cloud-based disaster recovery solutions is to do the risk assessment. There are three main things that need to be considered for the cloud-based disaster recovery solutions [20]:

a. Data security. When the data of the company is starting to enter the cloud computing providers, there are always concerns regarding the security aspects. How the cloud computing service providers manage the security aspects of the systems needs to also be monitored, and the bank should have the visibility and certainty into the security elements that are used by the providers of the cloud computing.
b. Service reliability. The network connectivity from the bank to the cloud computing provider and vice versa may have problems and the cloud computing service provider systems may be down sometimes that affects the reliability of the bank's services, so the network dependency and reliability have to be addressed carefully.
c. Software management. The fact that the bank may not have the full control over the software management and development, that causes the editing and updating of the softwares and the bug fixing processes to become more complex compared to if the softwares are hosted in the bank's own premises.

Everytime the bank tries to consider the cloud-based solution for their disaster recovery plan based on the BIA and tiering, the above risks need to be assessed [21]. Like for example, when the bank is thinking about choosing the cloud-based solution for one of their application, the data confidentiality contained in the application needs to be assessed first, and the risks need to be accepted before the bank can then move the disaster recovery plan for the application into the cloud, and the controls need to be defined and implemented to secure the data. Regarding the service reliability, for example for the network connectivity issues that need to be considered in choosing the right cloud-based disaster recovery solution. If the bank's connectivity to the cloud computing vendor is not reliable or the

bandwidth is too small, the bank should consider the other options, or to choose the cloud-based disaster recovery solution that does not require very big network connection bandwidth. The solution that requires the data transfer from the vendor site to bank's site, may depends on how big is the data. For the situation that the network bandwidth is very limited, the option to put both of the production and disaster recovery systems at the cloud that's managed by the same vendor can be choosen.

And finally, before running the implementation of the cloud-based disaster recovery solution, the bank will need to check against the regulation. Regulators may not that keen on the cloud computing, fearing that any data breach may have devastating consequences for the bank customers, so the effect is not only for the bank themselves. Regulators don't allow the bank to use the third-party vendors from outside of the country to store the bank customer data abroad, again for the security concerns. And the cloud computing vendor may not support the actually needed national, international, or industry standards and regulations in providing the cloud-based solutions for banking industry.

Considering the benefit and cost of the cloud-based disaster recovery solution for one of the bank's application, in this case the bank chose to put both the primary server and disaster recovery system server into the cloud-computing vendor sites. In the case like this, the bank needs to make sure about the SLA since the process of activating the disaster recovery system will be much depending on the vendor's SLA.

Regarding the vendor selection, there are several things need to be checked, like the support from vendor (Specialized knowledge & skills), how the disaster recovery (DR) drilling will be done including to state it in the contract, how is the vendor's ability in supporting multiple customers when disaster happens, make sure that the vendor separate the location for the DR from the production servers location, make sure that remote access is provided to the DR servers, the SLA is agreed, and review the certifications that the vendor have, for example the certification from International Organization for Standardization (ISO).

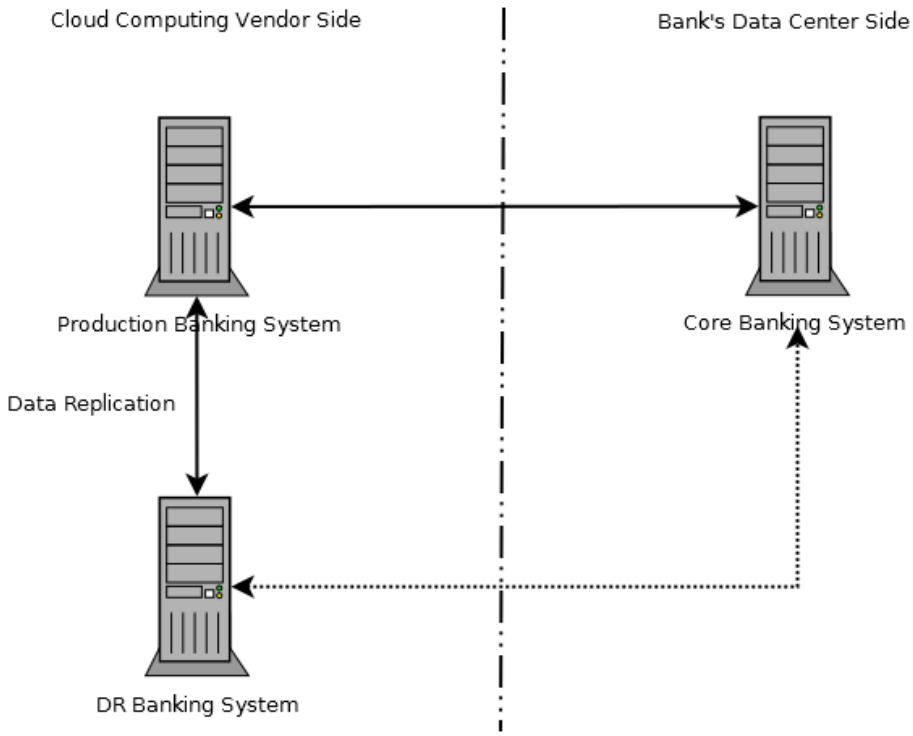


Fig. 7. The network diagram of the bank's cloud-based disaster recovery system

6. Conclusion

While a cloud-based disaster recovery solution is often favourable because of the cost consideration, and especially to the smaller banks, there may still be significant benefits in maintaining the separate data centers, that the larger banks can't also ignore. The banks may explore all of the options, while

still considering the risks caused. Nevertheless, the risks may do change over the project lifetimes, which may be caused by the system modification and operation changes, and the advancement in technology.

The main challenges are like the security and compliance, where SLAs are a must, and the banks need to demand the safety measures from the service providers, and to ensure that the applications meet the latest and most rigorous standards of security. And then about the reliability, in ensuring that the application and data are always be available in the natural disaster or unpredictable events. The management of the cloud-based solution is one of the challenges, where achieving visibility and performance measurement are harder to be done in the cloud-based environment, especially when the bank use the cloud services for both internal and external services, that require the bank to handle multiple security systems. The interoperability is also a challenge as the bank need to ensure that the data and application can be moved as needed acroos the cloud environments from the different service providers, that a single interface and layer management need to be developed, internally and externally. The regulation needs to be understood clearly on where the data is kept. In order to guarantee the successful of the DR in the cloud plan, several things need to be checked, like the use of multiple ISPs (Internet Service Providers) in order to avoid single point of failure, evaluate the list of the applications with their specific requirements, understand about the capability of the vendor, make sure to test everything with the vendor especially for the critical applications, plan for the geographical locations, make sure about the access to the DR servers, and of course to make sure to get the main benefits from the cloud-based disaster recovery plans.

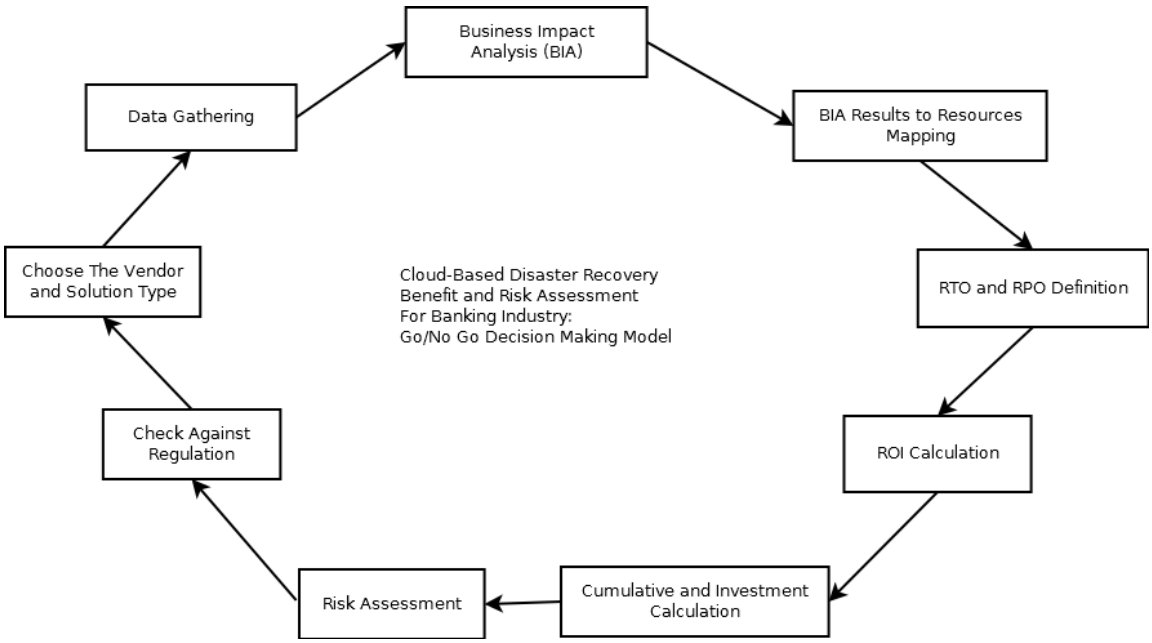


Fig. 8. The cloud-based disaster recovery benefit and risk assessment for banking industry: Go/No go decision making model

7. Future Works

Cloud-based disaster recovery may help in ensuring the high reliability of the data, low cost of backup, and short recovery time, but it still depends on the strategies that are proposed, and suitable for the bank's different kinds of disaster recovery scenarios. So the bank needs to study further about the implementation in the bank, and do risks assessment based on the solution that's chosen by the bank. The adoption rate is increasing continously though, and that now the cloud-based disaster recovery solution is a more viable option for the bank, just need more studies in the future regarding the options and the risks.

References

[1] Online Tech, "Benefits of Disaster Recovery in Cloud Computing," *Online Tech*. [Online]. Available: http://www.onlinetech.com/resources/references/benefits-of-disaster-recovery-in-cloud-computing. [Accessed: 28-Feb-2016]

[2] Financial Review, "BoQ takes $7m hit to earnings after CRM write-off," *Financial Review*. [Online]. Available: http://www.afr.com/markets/equity-markets/boq-takes-7m-hit-to-earnings-after-crm-writeoff-20150225-13p84r#. [Accessed: 28-Feb-2016]

[3] R. Harms and M. Yamartino, "The economics of the cloud," *Microsoft Whitepaper Microsoft Corp.*, 2010.

[4] O. H. Alhazmi and Y. K. Malaiya, "Evaluating disaster recovery plans using the cloud," in *Reliability and Maintainability Symposium (RAMS), 2013 Proceedings-Annual*, 2013, pp. 1–6.

[5] J. Gsoedl, "Disaster recovery in the cloud explained," *TechTarget*. [Online]. Available: http://searchdisasterrecovery.techtarget.com/feature/Disaster-recovery-in-the-cloud-explained. [Accessed: 04-Mar-2016]

[6] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "NIST cloud computing reference architecture," *NIST Spec. Publ.*, vol. 500, no. 2011, p. 292, 2011.

[7] Google, "How to Design a Disaster Recovery Plan," *Google Cloud Platform*. [Online]. Available: https://cloud.google.com/solutions/designing-a-disaster-recovery-plan. [Accessed: 04-Mar-2016]

[8] M. Swanson, *Contingency planning guide for federal information systems*. DIANE Publishing, 2011.

[9] The Association of Insurance and Risk Managers, "A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000." The Public Risk Management Association [Online]. Available: https://www.theirm.org/media/886062/ISO3100_doc.pdf. [Accessed: 28-Feb-2016]

[10] R. Ross, "Guide for Conducting Risk Assessments." NIST, 17-Sep-2012 [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf. [Accessed: 28-Feb-2016]

[11] I. ISO and I. Std, "ISO 27005: 2011," *Inf. Technol. Tech. Secur. Risk Manag. ISO*, 2011.

[12] D. Higgins, P. Alcantara, and G. Riglietti, "BCM Legislations, Regulations, Standards, and Good Practice," *Bus. Contin. Inst.*, vol. February 2016.

[13] K. Underwood, "Protiviti 2015 IT Priorities Survey," *EDPACS*, vol. 52, no. 1, pp. 14–16, 2015.

[14] R. Dines, "Disaster Recovery Service Providers Demystified," *Rachel Dines' Blog*, 17-Jan-2014. [Online]. Available: http://blogs.forrester.com/rachel_dines/14-01-17-disaster_recovery_service_providers_demystified. [Accessed: 04-Mar-2016]

[15] A. Amayri, "Rethink Your Disaster Recovery," 2011 [Online]. Available: http://www.infrastructurestrategiesme.com/2012/docs/NetIQ-Ahmed.pdf. [Accessed: 04-Mar-2016]

[16] S. Snedaker, *Business continuity and disaster recovery planning for IT professionals*. Newnes, 2013.

[17] D. Nolting, "RPO, RTO, PTO and DRaaS: Disaster recovery explained," *Blueblock*, 01-Mar-2013. [Online]. Available: https://www.bluelock.com/blog/rpo-rto-pto-and-raas-disaster-recovery-explained/. [Accessed: 04-Mar-2016]

[18] M. A. Khoshkholghi, A. Abdullah, R. Latip, S. Subramaniam, and M. Othman, "Disaster recovery in cloud computing: A survey," *Comput. Inf. Sci.*, vol. 7, no. 4, p. 39, 2014.

[19] A. Lochart, "Investment Advice: The High ROI of Disaster Recovery," *nscaled*, 11-Nov-2011. [Online]. Available: http://nscaled.com/investment-advice-the-high-roi-of-disaster-recovery/. [Accessed: 04-Mar-2016]

[20] P. Pant, "How to assess risk when considering cloud computing," *NetworkWorld*, 21-Oct-2013. [Online]. Available: http://www.networkworld.com/article/2171040/tech-primers/how-to-assess-risk-when-considering-cloud-computing.html. [Accessed: 04-Mar-2016]

[21] D. Vohradsky, "Cloud Risk—10 Principles and a Framework for Assessment," *ISACA J.*, vol. 5, pp. 31–41, 2012.

The Annual Conference on Management and Information Technology (ACMIT) 2016

The Implementation IT Risk Management of Hardware and Software Obsolescence by using ISO27001/ISO 27002 in Pharmaceutical Industry

Heri Rukmana
rukmah@gmail.com

EduTown, BSD City, Tangerang, Indonesia

Abstract

Risk Management is a discipline that exists to deal with non-speculative risks – those risks from which only a loss can occur. Hardware and software obsolescence which are used in pharmaceutical industry equipment are the subject of Risk Management since these obsolescence may cause either a profit or loss and impact to the business strategy, which can reduce the value of the assets with which the organization undertakes its speculative activity.

Keywords : Risk Management, Hardware and Software Obsolescence..

1. Introduction

The electronic industries are one of the very dynamic sectors of the world economy. In the developed country such as United States, these industries have grown three times greater than the overall economy in the last ten years. The semiconductor industry is now the first value-added to the U.S. economy, and the computer and consumer industry segments stunt almost any other market segments. For instances, Intel's market capitalization was higher than the three largest market capitalization of three combination U.S automakers.

Beginning on April 8th, 2014, Microsoft and all other hardware and software companies will discontinue and stop their support of the Windows XP operating system. When it happens, Windows XP will become vulnerable for viruses because antivirus programs will be outdated and stop not updated. New peripheral devices such as a printer, keyboard, or mouse will be unable to connect to the computer since the system does not meet the minimum requirements to run them. HP has already shut off support for Windows XP, and other big brands will follow suit over the course of the year. If you call a retailer or other company for direct support and say you are still running XP, they will be unable to assist you

With Rapid growth of Technology, rate of obsolescence of hardware and software which are used as components in equipment for pharmaceutical industry has increased.

Factor which have impacted obsolescence of hardware and software of electronics components are:

- Advancement in Microcontroller chips
- Number of generic parts with shorter obsolescence cycles
- Rapid evolution of 64 bit computing hardware
- Microsoft's decision to prepone discontinuation of support for all 32 bit OS

Most of manufacturing systems in pharmaceutical are still in either old PLC/microcontrollers or Windows XP which are no longer available for sale and have limited to no serviceability remaining and support from PLC maker or Microsoft. Hence, pharmaceutical industry has to manage risks which occur due to this obsolescence. The question is "**How do we mitigate business loss due to hardware and software obsolescence of manufacturing system in Pharmaceutical Industry?**"

2. Methodology

This paper will focus on Obsolescence Management Strategy to mitigate business loss due to hardware and software obsolescence.

The methodology will be used for this paper are as follows:

1. Technology life cycle to identified hardware and software obsolescence.
2. Risk identification, mitigation plan and prioritization matrix of hardware and software obsolescence.
3. Field studies by looking the company's preparedness of any hardware and software obsolescence.

2.1 Hardware and Software (H&S) Obsolescence Risk Management Process

There are six steps for Hardware and Software (H&S) Obsolescence Risk Management Process as folows (see Picture 1):

2.1.1 Hardware and Software (H&S) identification
2.1.2 Determine H&S Life Cycle
2.1.3 Determine H&S vulnerabilities and threats
2.1.4 Determine H&S criticality
2.1.5 Risk Assessment
2.1.6 Risk Mitigation Strategy

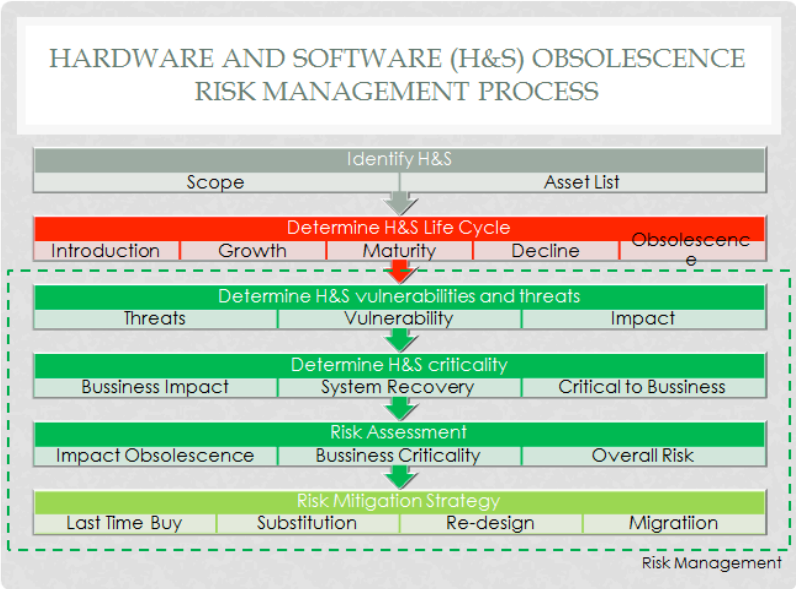


Figure 1. Hardware and Software (H&S) Obsolescenc Risk Management Process

2.2 Life Cycle Stage

Most software and hardware pass through several life cycle stages corresponding to change which is embedded in electronic component. Fig. 1 is a representative life cycle curve and risk of units shipped per time, which depicts the six common life cycle part phases: Introduction, Growth, Maturity, Decline, Phase-out, and Obsolescence. Table I and the proceeding discussion summarizes the characteristics of the phases of the part life cycle.

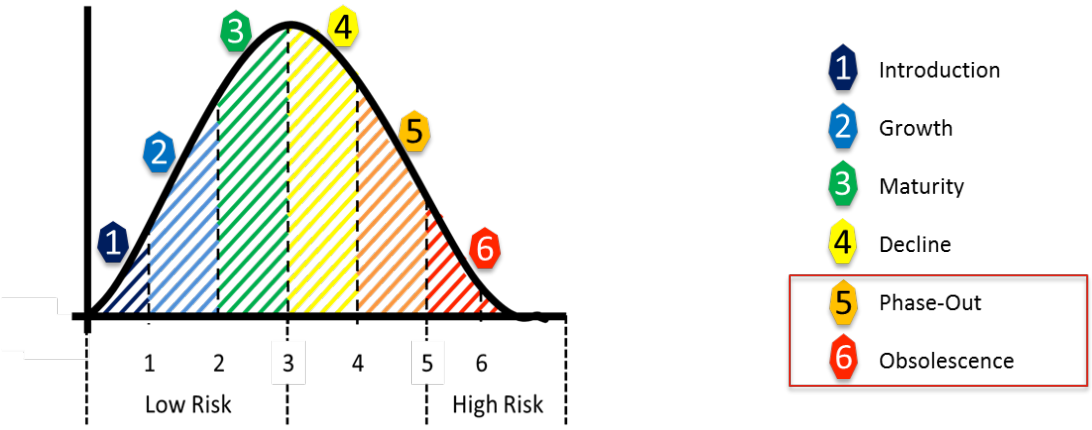


Figure 2. Life Cycle and Risk Curve

Characteristic	Introduction	Growth	Maturity	Decline	Phase-out	Obsolescence
Application	Slow but increasing	Increasing rapidly	High	Decreasing	Upgrades may be offered	Application only from aftermarket sources
Price	Highest	Declining	Low	Lowest	Low	Not applicable or very high if available from aftermarket sources
Usage	Low	Increasing	High	Decreasing	Decreasing	Low
Hardware and software patch or modification	Periodic software patch or modification	Periodic software patch shrinks	Periodic software patch shrinks	Few or none	None	None
Competitors	Few	High	High	Declining	Declining	Few
Manufacturer profits	Low	Increasing	High	Decreasing	Decreasing	Decreasing

Table 1. Typical life cycle characteristics for the six generic stages of a part life cycle

A. Introduction Stage

The introduction stage in the hardware or software life cycle is usually characterized by high development costs driven by recently incurred design costs and low in embedded electronic application, frequent patches or modifications, low or unpredictable software/hardware behavior to meet electronic application requirements, and customization for suitable application. Marketing costs, at this stage, may also be high. Early OEM who use this hardware and software its introduction stage tend to value performance over price.

B. Growth Stage

The growth stage is characterized by hardware and software fulfills electronic application requirements. Increased electronic application during this stage may justify the development and use of patches or modification for better performance, which in turn improves economies of scale of performance. Mass production, mass distribution, and mass marketing often bring about price reductions. There are so many competitors in this stage since as opportunity seeking firms are attracted by the huge potential profit and strategic acquisitions; hence mergers have not yet taken place.

C. Maturity Stage

The maturity stage of the hardware and software life cycle is characterized by high-volume application which is embedded to the electronic components. Competitors with lower cost of production may enter the market, or domestic competitors may shift production facilities to cheaper locations for enabling them to the lower manufacturing costs. The inspection electronic system is an example of a mature hardware and software electronic application.

D. Decline Stage

The decline stage is indicated by decreasing demand and generally decreasing profit margin.

Towards the end of the decline stage, only a few specialized industries remain in the market. The un-expandable PLC or microcontrollers are examples of hardware and software electronic application that have been available very late due to continued electronic application in the legacy pharmaceutical equipment.

E. Phase out and Obsolescence Stage
The phase out and obsolescence stage are the final stage of life cycle whereas hardware and software which is used in electronic application has been replaced by the new hardware and software. Hardware and software use to maintain operations of legacy pharmaceutical equipment due to low utilization or complex system that impact to the business which more challenges to be upgraded or replaced. This is the stage whereas the risks have to be managed to mitigate and prevent loss that will impact to the business continuity.

2.3 Risk Management

Risk management is systematically to identify, evaluate and control potential losses to the organization that may result from things that have not happened yet.

There are four linked objectives in risk management, as follows:

2.3.1 Eliminate the risk
2.3.2 Reduce to 'acceptable' levels those that cannot be eliminated
2.3.3 Controls that keep them in acceptable condition
2.3.4 Transfer to some other organization.

There are two fundamental components on effective management to handle risk management process in information and information technology. An organization's strategic deployment is the first relation of information technology in order to achieve its business goals. Information Technology (IT) projects often represent significant investments of financial and managerial resources. Shareholders' interest in the effectiveness of such deployment should be reflected in the transparency according to the planning, management and measurement, and the way in which risks are assessed and controlled. The second component is the way in managing the risks incorporated with information assets themselves.

The complexity of the risk assessment will depend on the complexity of the organization and of the risks under review. The techniques employed to carry it out should be consistent with this complexity and the level of assurance required by the board. One of the primary functions of security risk analysis is to put this process to be more objective basis and conducted by a qualified and experienced person.

Risk management strategies are usually therefore based on an assessment of the economic benefits that the organization can derive from an investment in a particular control; in other words, for every control that the organization might implement, the calculation would be that the cost of implementation would be outweighed, preferably significantly, by the economic values that derive from, or economic losses that are avoided as a result of, its implementation. The organization should define its criteria for accepting risks (for example, it might say that it will accept any risk whose economic impact is less than the cost of controlling it) and for controlling risks (for example, it might say that any risk that has both a high likelihood and a high impact must be controlled to an identified level, or threshold).

3. Qualitative Risk Analysis

3.1 Assets within the scope

The first step is to identify all the information assets (and 'assets' includes information systems – refer to the information security policy for this definition) within the scope (4.2.1.a) of the ISMS and, at the same time, to document which individual and/or department 'owns' the asset.

3.1.1 Scope

a. Electronics Based control systems and Components
b. PLC & SCADA Software
c. Windows based line control systems

3.1.2 Asset list

Table 2. List of identified asset information corresponding to scope which is software and hardware embedded in electronic component are being used for pharmaceutical equipment.

System Description	Owner	Function
Computerized Maintenance Management System	Engineering	Manage equipment maintenance program and spare part inventory and control
Windows Operating System	All	OS for computerized system
Programmable Logic Control	Manufacturing	Control manufacturing process
Building Automation System	Engineering	Control, monitor and records utility operations
Supervisory, Control and Data Acquisition (SCADA) System	Manufacturing	Control, monitor and records manufacturing operations
Electronic Library Management System (ELiMS)	Laboratory	Control, monitor and records laboratory operations
Human Machine Interface (HMI)	Manufacturing	Interface between operator and machine to opearate manufacuring equipment

Table 2. Hardware and Software List

3.1.3 Hardware and Software Vulnerabilities and Threats

Determine hardware and software vulnerabilities and threats to eliminate or minimized risk and keep them in acceptable condition. Threats is defined as support and substitution capabilities of hardware and software, whereas vulnerability is environment that may cause hardware and software malfunction. It will determine as an impact of hardware and software obsolescence.
Table 3 is the threats and vulnerability level to determine impact obsolescence of each system.

Impact = Threats X Vulnerability

System Description	Threats	Vulnerability	Impact Obsolescence
Computerized Maintenance Management System	Low	Low	Low
Windows XP Operating System	High	Low	Medium
Programmable Logic Control	High	Medium	High
Building Automation System	Low	High	Medium
Supervisory, Control and Data Acquisition (SCADA) System	High	Low	Medium
Electronic Library Management System (ELiMS)	Low	Low	Low
Human Machine Interface (HMI)	High	Low	Medium

Table 3. Hardware and Software Vulnerabilities and Threats

3.1.4 Hardware and Software Business Impacts

Identify hardware and software impact to business and cost for system recovery to determine the criticality to business (table 4).

System Description	Business Impact	System Recovery	Critical to business
Computerized Maintenance Management System	Low	Low	Low
Windows XP Operating System	High	Medium	High
Programmable Logic Control	High	Medium	High
Building Automation System	Medium	Medium	Medium
Supervisory, Control and Data Acquisition (SCADA) System	Medium	Medium	Medium
Electronic Library Management System (ELiMS)	Low	Low	Low
Human Machine Interface (HMI)	High	Medium	High

Table 4. Hardware and Software Business Impact

3.1.5 Risk assessment

Asses the risk to have risk prioritization and mitigation plan (table 5)

System Description	Impact Obsolescence	Critical to Business	Overall Risk
Computerized Maintenance Management System	Low	Low	Low
Windows XP Operating System	Medium	High	High
Programmable Logic Control	High	High	High
Building Automation System	Medium	Medium	Medium
Supervisory, Control and Data Acquisition (SCADA) System	Medium	Medium	Medium

Electronic Library Management System (ELiMS)	Low	Low	Low
Human Machine Interface (HMI)	Medium	High	High

Table 5. Risk Assessment Result

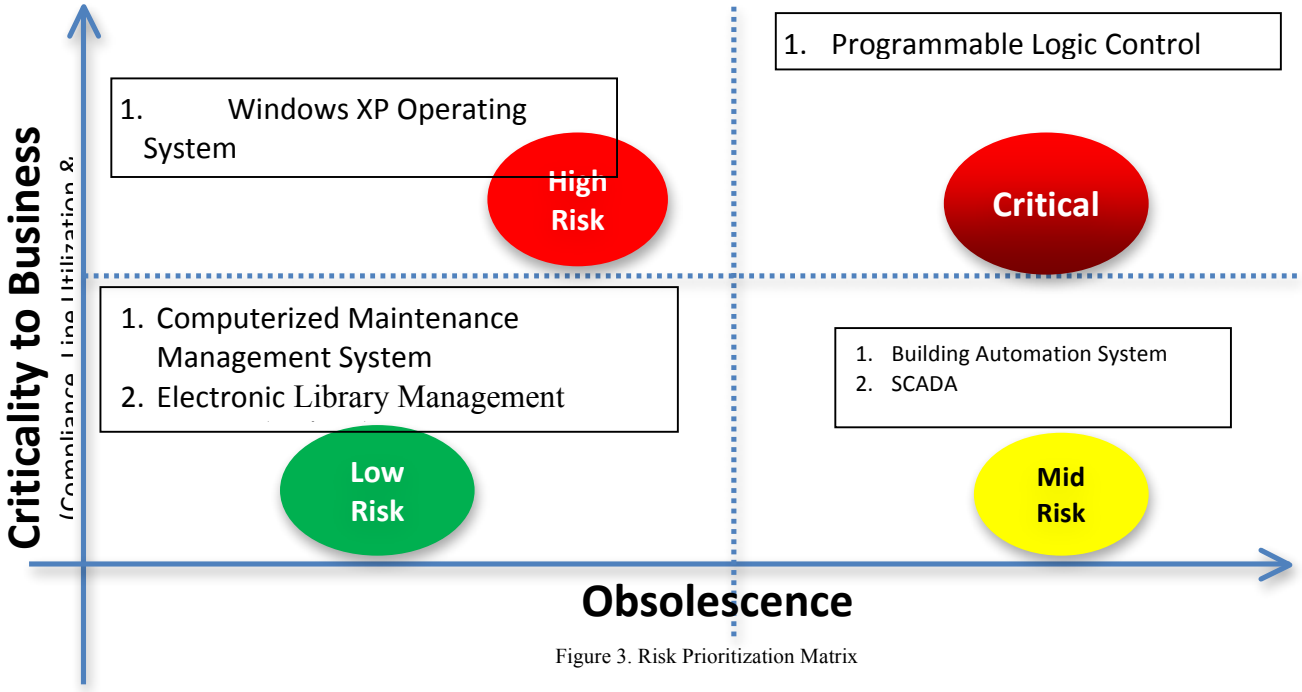


Figure 3. Risk Prioritization Matrix

3.1.6 Risk mitigation strategy

There are four strategies to mitigate the risks which are related to compatibility, reaction time, sustainability, effort and innovation are as follows:

3.1.6.1 Last time buy

Backup software or stock obsolescence hardware. It provides less effort and time, more compatibility. It will be used as short term solution.

3.1.6.2 Substitution

Substitute with new hardware and software if applicable. It provides compatibility but need more time and effort. It will be used as short to medium term solution.

3.1.6.3 Re-design

Redesign new software and hardware as per intended use. Time consuming since it develops the software and hardware form beginning. More effort and current process knowledge and experience in translating the hardware and software obsolescence to the new one. Innovation supposed to be applied to execute this solution. It will be used as medium to long solution.

3.1.6.4 Migration

Time consuming since it has to learn old software and hardware system prior to develop the new software and hardware. More effort and current process knowledge and experience are mandatory requirement in migrating the hardware and software obsolescence. Innovation must be applied to execute this solution. It will be used as long solution.

Benefits Relationship	Compatibility	Reaction Time	Sustainability	Effort	Innovation
Last Time Buy	✓✓✓	✓✓✓	✓	✓	✓
Substitution	✓✓✓	✓✓	✓✓	✓✓	✓
Redesign	✓✓	✓	✓✓	✓✓	✓✓
Migration	✓	✓	✓✓✓	✓✓✓	✓✓✓

S.No	Strategy	Remarks
1	Last Time Buy	Backup software or stock obsolescence hardware
2	Substitution	Substitute with new hardware and software if applicable
3	Re- Design	Redesign new software and hardware as per intended use
4	Migration	Migration software and hardware if applicable

Figure 4. Solution Benefits Relationship.

4. Discussion

Every factory has to submit the asset list of the manufacturing system and apply mitigation strategy as per required. Risk assessment should be applied into all assets that within the scope of hardware and software obsolescence. Determine the risk prioritization base on risk assessment to mitigate the risks and apply appropriate strategy according to business and obsolescence impact. Hence, electronic components which are used for equipment can be operated as per intended use. Apply mitigation strategy as per risk prioritization matrix as shown in table 6 below:

Risk Prioritization	Strategies			
	1=Last Time Buy	2=Substitution	3=Re-design	4=Migration
Low	🙂🙂🙂	🙂🙂🙂	🙂🙂🙂	🙂🙂
Medium	🙂🙂🙂	🙂🙂🙂	🙂🙂	🙂
High	🙂🙂🙂	🙂🙂	🙂	😐
Critical	🙂🙂	🙂	😐	☹

Table 6. Mitigation strategy base on overall risk result

5. Conclusion

Pharmaceutical industries face challenges in hardware and software obsolescence since most of these industries have been built for many years and use old technology in running their factory. The IT Risk Management is a methodology which can be used to identify, eliminate, reduce and control their hardware and software obsolescence in acceptable condition.
There are some steps in conduction the Risk Assessment of hardware and software obsolescence:

1. Identify assets within the scope
2. Determine Life Cycle
3. Identify Hardware and Software Vulnerabilities and Threats as obsolescence impact
4. Hardware and Software Business Impacts to find out the software and hardware criticality to the business.
5. Risk Assessment to assess and prioritization the risk according to the obsolescence and business impact.
6. Risk Mitigation Strategy as a mitigation plan to eliminate, reduce or maintain the hardware and software in acceptable condition.
7. Apply risk mitigation strategy based on risk prioritization.

IT Risk management of manufacturing system in pharmaceutical industry result for this paper can be found in table below:

System Description	Overall Risk	Mitigation Strategy No	
		Primary	Secondary
Computerized Maintenance Management System	Low	1, 2, or 3	4
Windows XP Operating System	High	1	2 or 3
Programmable Logic Control	High	1	2 or 3
Building Automation System	Medium	1 and 2	3 or 4
Supervisory, Control and Data Acquisition (SCADA) System	Medium	1 and 2	3 or 4
Electronic Library Management System (ELiMS)	Low	1, 2, or 3	4
Human Machine Interface (HMI)	High	1	2 or 3

1 = Last Time Buy 2 = Substitution 3 = Re-design 4 = Migration

Table 7. Risk assessment result and mitigation strategy

References:

[1] Managing Control System Obsolescence - Understand your Risk and Options, Lonnie Morris, 2012

[2] IT Governance, Manager's Guide to Data Security and ISO27001/ISO 27002, Alan Calder & Steve Watkins, 4th Edition.

[3] Electronic Part Life Cycle Concepts and Obsolescence Forecasting, Rajeev Solomon, Peter Sandborn, and Michael Pecht, Dec. 2000

[4] Information Security Harmonisation—Classification of Global Guidance, Information Systems Audit and Control Association (ISACA®) (www.isaca.org)

[5] Risk Management Guide for Information Technology Systems, NIST, 2002

[6] http://www.pcninja.us/countdown-to-windows-xp-obsolescence/

The Annual Conference on Management and Information Technology (ACMIT) 2016

Analysis of Data Center Risk Management in Indonesia National Traffic Police Corps

Wita Susilowaty

Swiss German Uniersity, Indonesia

Abstract

Topic about Data Center crisis highlighted that significant risk failures persist despite the investments in the disciplines of risk assessment and risk management. Although isolated incidents of one-time governance failure are reduced, the systemic ruin are more than just a stray differensiation. Various experts and professional institutions dealing with risk management have come to the judgement that the failures may be caused by a confusion in the risk information due to diverse risk assessments from different point of view [3][6]. The Data Center crisis and the resulting regulatory pressure forced the chief data center officers and high ranked management of Indonesia Traffic Police Corps to focus more on assessment, mitigation and reporting of risk. The process of organizing these risk assessments to provide the Indonesia Traffic Police Corps with a more holistic view of the enterprise risk is fundamental to mastering risk assessment.

Keywords: Data Center; Risk Management.

Introduction

Indonesia National Traffic Police Corps is one of the institutions in charge of traffic and road transport. To support the tasks and responsibilities, they built traffic and road application and systems that is placed in the Data Center, called NTMC Data Center. The NTMC Data Center has almost close to the standard Tier 3.

The terms availability, reliability, mean time between failure (MTBF), and the others are often used interchangeably to describe data center performance [1]. However, the management of NTMC Data Center not currently applied risk management and failure, so vulnerable a system failure occurred due to the absence of prevention.

Risk assessment is a part of the overall discipline of risk management. Risk is defined as the suspicion of an event appear that could have an effect on the achievement of objectives. The definition of risk assessment then follows as the identification, estimation and evaluation of the levels of risks involved in a situation, their comparison with benchmarks or standards, and determination of an acceptable level of risk. Risk assessment should answer the following questions: what can go wrong, how can it go wrong, what is the potential harm, and what can be done about it.

1. Data Center Risk Management

1.1. Challenges in the Datacenter

Every institutions face the challenges about how to manage datacenter, like delivery of reliable services, operational efficiency, and improved business responsiveness [8].

a. Delivery of Reliable Services.
   Data center must provide high avaliabe services and full uptime in a reliable and predictable situation. IT manager must have a holistic and operational view with their datacenter environments [8].

b. Improved Business Responsiveness.
There is a high expectation on IT to be agile and responsive with business needs. Because of that, institutions have started to investigate cloud solutions. Nonetheless, many are unsure about how and where to begin making a transition [8].

1.2. Risk Identification

The basic step of risk management is risk identification. This step determines the highly occurring potential risks, and other events which occur very frequently [7]. Risk is investigated by looking at the institutions activity in all directions and attempting to introduce the new exposure which will arise in the future from changing the internal and external environment. Correct risk identification guarantees risk management effectiveness [9], and will helps the management to identify the forthcoming risk from any direction at the initial stages in order to avoid overlapping of the process in the future outcomes.

1.3. Risk Evaluation

Risk evaluation is very important in specific situations and provides adequate material for make decisions [11]. This step will show whether risks are acceptable or need treatment. Evaluation means whether to accept the risk or not. If it is accepted, the management should decide at which position they could handle the situation, and if they cannot handle, what is the further process to be undertaken. Thus evaluation plays a vital role in the risk management to consider the tolerance of risk, which depends on the voluntary association.

1.4. Risk-based approaches

Many groups within an institution risk assessment are increasingly conducted by to fulfil a variety of business and regulatory requirements. Various groups in the same institutions often depend on guidance from different professional institutions to provide a framework for directing the risk assessment. As these professional institutions offer disparate approaches to risk assessment, they contribute to a huge of risk information. In this context, information systems and/or information technology (IS/IT) of risk assessment take parts in an entirely exceptional role in each institution. There are two reasons for that statement [10]. The first: IS/IT integrates all different functional domain within an institution and it has a prospect to combine the risk assessment activities as well; the second: IS/IT deals with data or information processing and by organizing it risk will reduce unvaluable information. In the same time, we enhance the quality of business processes, as information is the important pieces of each business process. According on the hypothesis, we can conclude that there is no use to create a dissimilarity between business risk and IS/IT risk. IT risk is specifically business risk, the business risk related with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise [4].
The business value and Information Technology risk are two sides and risk is inherent to all enterprises. At the same time, to eliminate all the risks, we can jeopardize the profit driving opportunities.
In practice, there is no single unified solution to the complex situation mentioned. Therefore, there are many various risk assessment frameworks aiming at different purpose and different tools.

1.5. The Risk IT

The scope of the Risk IT framework is also covered with the scope of the COBIT 5 framework [4]. To implement Risk IT framework, we need to review the COBIT 5 framework first, if it need more guidance on risk, reference the Risk IT publications for more detail. While COBIT provides a set of controls to mitigate IT risk, Risk IT present a framework as a tool to identify, govern and manage IT risk. Simply put, COBIT presents the means of risk management; Risk IT provides the ends. Enterprises who have use (or are planning to use) COBIT as their IT governance framework can adopt Risk IT to enhance risk management.

2. Methodology

Before integrate existing framework in analysis, first thing to do is understand how the frameworks work individually and then conduct a detailed study about how the frameworks can be integrated.
The methodology used consists of the following steps:

a. Review and study of existing literature.
b. Analysis data using COBIT frameworks.
c. Mitigation of gaps based on previous study and research and current analysis result.

The purpose of this analysis is to get clear traceability with integrated framework using a top down approach. To achieve this, it is critical to ensure that the output of one framework is aligned perfectly with the input of the other framework, thereby establishing a robust input-process-output methodology.

3. Data Analysis

In order to do an assessment of IT Risk Management in NTMC Data Center, COBIT framework is used to determine the risk level of the data center.

3.1. Process AI3: Acquire and Maintain Technology Infrastructure

3.1.1. Control Objective AI3.1– Technological Infrastructure Acquisition Plan

Prepare and produce a plan or strategy for the acquisition, implementation and maintenance of the technology infrastructure that can established functional of business and technical requirements and is in accord with the institution's technology policy.

Conclusion: Objective Not Met

Observations: The NTMC Data Center has compiled a formal set of information technology standards. However, this document did not include standards for the technological infrastructure.

Risks: If the Indonesia Traffic Police Corps does not establish technological infrastructure standards, then the impact:

1) May acquire and install hardware and/or software that are not compatible with the Indonesia Traffic Police Corps technology and Infrastructure.
2) May acquire and install hardware and/or software that are not consistent with the Indonesia Traffic Police intended technology direction.

3.1.2. Control Objective AI3.2–Infrastructure Resource Protection and Availability

With the implementation of internal control, security and auditability, and then measures them during configuration, integration and maintenance of device or hardware and infrastructural software to guard resources and assure availability and integrity. Responsibilities for implement sensitive and crusial infrastructure components should be defined very clear and can be understood by developer and integrator infrastructure components. Usage of infrastructure components should be monitored and evaluated.

Conclusion: Objective Not Met

Observations: The Indonesia Traffic Police Corps' IT control environment has a lacks critical policy, procedure and guideline documentation.

The Indonesia Traffic Police Corps relies heavily on the knowledge and dedication of an experienced IT staff. The Indonesia Traffic Police Corps division does control changes to the infrastructure by change management process. However, the Information Technology Departement of The Indonesia Traffic Police Corps does not have policies, procedures or guidelines that documented for capacity management and monitoring.

Risks: Capacity Management / monitoring practices may not be effective in determining the need to increase bandwidth, address root-causes, or report on usage presenting potential risks to network and system availability.

3.1.3. Control Objective AI3.3–Infrastructure Maintenance

Prepare and build a strategy and plan for infrastructure maintenance, and ensure that changes are according to the institution's change management procedure. The procedure might include periodic reviews against institution needs, patch management, and upgrade strategies, risks, susceptibility assessment and security requirements.

Conclusion: Objective Met

Observations: Based upon work performed, it feels this objective is being satisfactorily met due to infrastructure changes being subject to the Indonesia Traffic Police Corps' IT Change Management Process Policy. The policy requires review of change requests by the Change Advisory Board, which consists of the Indonesia Traffic Police Corps IT Department's Senior Management team. The Change Advisory Board meets on a weekly basis.

3.1.4. Control Objective AI3.4– Feasibility Test Environment

Establish development and examinate the environments to support effective and efficient practicability and integration testing of infrastructure components.

Conclusion: Objective Not Met

Observations: The Indonesia Traffic Police Corps does not have development and examinate the environments to support effective and efficient practicability and integration testing of infrastructure components.

Risks: Changes to the production environment may present security, integrity and availability risks to the computing environment.

3.2. Process DS12: Manage the Physical Environment

3.2.1. Control Objective DS12.1– Site Selection and Layout

Define and select the physical location for IT devices to support the technology strategy linked to the business strategy. The selection and layout of a location should take into account the risk associated with natural and man-made disasters. Beside that, it should considering relevant laws and regulations, such as regulations of occupational health and safety.

Conclusion: Objective Met

Observation: Based upon work performed, it feels this objective is being satisfactorily met due to the location and layout of the Indonesia Traffic Police Corps data center appears to support the business needs of the Indonesia Traffic Police Corps and appears to take into account risks associated with natural and man-made disasters.

3.2.2. Control Objective DS12.2– Physical Security Measures

The definition and implementation of physical security scope with business needed to secure the site and assets. Result of meauses physiscal security must be effective and capable of preventing, detecting and mitigating risks relating to theft, temperature, air flow, fire, smoke, vibration, water, humidity, terror, power outages, chemicals, disasters or explosives.

Conclusion: Objective Met

Observations: Based upon work performed, it feels this objective is being satisfactorily met due to the following physical security controls being in place at the Indonesia Traffic Police Corps Data Center:

1) Data center housed in a secure facility
2) Camera with video feed for remote viewing
3) Card key required to access Data center
4) Alarm system for the data center
5) Server enclosures restrict access to authorized IT personnel.

3.2.3. Control Objective DS12.3– Physical Access

Define, describe and implement procedures to grant, limit and revoke access to sites, buildings and location based on business needs, including emergencies. Access to sites, buildings and areas should be justified, authorized, logged and supervised. This should apply to all those who entered the site, including staff, members, temporary staff, employees, clients, vendors, contractors, visitors or any other third party.

Conclusion: Objective Met

Observations: Based upon work performed, it feels this objective is being satisfactorily met due to data center personnel access the data center via card key and all other Indonesia Traffic Police Corps employees, contractors, vendors, visitors and other third parties are required to sign in prior to entering the data center.

3.2.4. Control Objective DS12.4– Protection against Environmental Factors

Design, define and implement measures for protection against environmental factors. Also install specialized equipment and devices to monitor and control the environment.

Conclusion: Objective Met

Observations: Based upon work performed, it feels this objective is being satisfactorily met due to the following Environmental Controls existing at the NTMC data center:

1) Fire / Heat / Smoke / Humidity Monitoring
2) Dry pipe sprinklers.
3) Raised Floor

3.2.5. Control Objective DS12.5–Physical Facilities Management

Manage and control facilities, including power, network, communications equipment, in line with laws and regulations, technical and organization or business requirements, vendor specifications, and health and safety regulations / guidelines.

Conclusion: Objective Met

Observations: Based upon work performed, it feels this objective is being satisfactorily met due to the following physical facility controls existing at the NTMC Data Center: UPS Battery (60 min capacity) and Backup Generator, Two separate electrical feeds from power company (AEP), Raised Floor.

4. Future works

This research present a comprehensive framework and subject to any number of limitations in analyzing by just using COBIT 5 framework. In future work, the limitations of this research might be explored and combine with other framework like IT Risk in analysis to get more comprehensive analysis and results.

5. Conclusion

This research presents a comprehensive framework and analyze the NTMC Data Center Risk using COBIT 5 framework. Result of the analyze are that The NTMC Data Center doesn't establish technological infrastructure standards and may affect incompatible technology and infrastructure that acquire and install and inconsistent hardware and software that acquire and install in data center; the IT department does not documented policies, procedures or guidelines for capacity management and monitoring. Capacity Management / monitoring practices may not be effective in determining the need to increase bandwidth, address root-causes, or report on usage presenting potential risks to network and system availability; and they don't have development and test environments to support effective, efficient, and competent feasibility and integration testing of infrastructure components, it may present security, integrity and availability risks to the computing environment.

According to the analyze result, to reduce the risk in NTMC Data Center needs to take the following steps:

a. Indonesia Traffic Police Corps must prepare and establish a formal set of information standards. With this standards, will reduce incompatible hardware and/or software that implement in NTMC Data Center.
b. Indonesia Traffic Police Corps must formulate critical policy, procedure and guideline documentation to control, security and auditability implementation hardware, software, and infrastructure in data center.
c. Indonesia Traffic Police Corps should have development and test environment that different with production environment. This will support effective, efficient, and competent feasibility and integration testing of infrastructure components.

References

[1] Avelar, Victor. Guidelines for Specifying Data Center Criticality/Tier Levels. American Power Conversion, USA, 2007.

[2] Cobit 4.1 Framework, Control Objectives, Management Guidelines, Maturity Models. (ISACA). 2007

[3] Ernst &Young. 2009. Risk Convergence: The Future State of Governance, Risk, and Control.

[4] Isaca, COBIT 5 Framework, The Risk IT Practitioner Guide, USA,2009

[5] Isaca, The Risk IT Framework, USA, 2009.

[6] Mc Cuaig, B. 2008. Fundamentals of GRC: Mastering Risk Assessment [White Paper]. Thomson Reuters, 2008.

[7] Meenakshi, RK and Arivazhagan, D. Risk Management in IT Sector: Opportunities and Challenges. IUP Journal of Computer Sciences. 9, 2, 31-45, Apr. 2015. ISSN: 09739904.

[8] Microsoft Corporation, Data Center Management and Virtualisation, One Microsoft Way, USA, 2010.

[9] Tcankova L. Risk Identification: Basic Stage of Risk Management. Environmental Management and Health, Vol. 13, No. 3; 2002, p. 290-297.

[10] Vlasva Svata, Martin Fleischmann. IS/IT Risk Management Banking.

[11] Vrijling J K, Hengel W V and Houben R J. A Framework for Risk Evaluation, Journal of Hazardous Materials, Vol. 43, No. 3; 1995, p. 245-261.

The Annual Conference on Management and Information Technology (ACMIT) 2016

Implementation of Fuzzy Logic Control on Battery Charging System

Prihangkasa Yudhiyantoro[a] 4*
[a]*Master's student of Mechanical Engineering in Mechatronic at Swiss German University, Faculty of Mechanical and Information Technology (2016)*

Abstract

This paper presents the implementation fuzzy logic control on the battery charging system. To control the charging process is a complex system due to the exponential relationship between the charging voltage, charging current and the charging time. The effective of charging process controller is needed to maintain the charging process. Because if the charging process cannot under control, it can reduce the cycle life of the battery and it can damage the battery as well. In order to get charging control effectively, the Fuzzy Logic Control (FLC) for a Valve Regulated Lead-Acid Battery (VRLA) Charger is being embedded in the charging system unit.
One of the advantages of using FLC beside the PID controller is the fact that, we don't need a mathematical model and several parameters of coefficient charge and discharge to software implementation in this complex system.

The research is started by the hardware development where the charging method and the combination of the battery charging system itself to prepare, then the study of the fuzzy logic controller in the relation of the charging control, and the determination of the parameter for the charging unit will be carefully investigated. Through the experimental result and from the expert knowledge, that is very helpful for tuning of the membership function and the rule base of the fuzzy controller.

Keywords: fuzzy logic, battery charger, microcontroller, Pulse Width Modulation, VRLA battery.

1. Introduction

When a Valve Regulated Lead Acid Battery (VRLA Battery) is charged by using constant voltage method, at the earlier stage of charging process the voltage will rise slowly. After receiving a certain amount of charge, the voltage will rise quickly and the current limit will be reached almost immediately. The charging process will stay in current limit until the battery charge voltage reaches the predetermined charging voltage. When the battery voltage equals the charger voltage setting, the charging current will begin to fall. The current will decrease exponentially and at some point will achieve a steady-state value — a so called 'float' voltage value [1].

The stage which the voltage sharp rise, is indicates that the battery is entering the gassing state. Gassing occurs due to the electrolysis of the water content of the electrolyte. It generates O_2 gas at the positive plate and H_2 gas at the negative plate. The batteries charged at low rates experience less gassing and have a superior charging efficiency than those operated at high rates. At low overcharge rates, both processes are in balance and the battery's temperature and pressure are maintained within comfortable ranges. When a battery is charged under a high gassing condition, the recombination process cannot maintained very well, and it will provide higher temperature and the pressure as well. The efficiency of the charge recovery will be very low which may shorten the battery's lifecycle and create an explosion hazard. The level of gassing voltage, which is the terminal voltage while gassing, varies according to

* Corresponding author. Tel.: +62-21-3045 0045; fax: +62-21-3045 0001.
E-mail address: prihangkasa.yudhiyantoro@student.sgu.ac.id

battery types and charging conditions [2]. There are several parameters which normally need to be identified for an effective charging process (or control). They are: the types of batteries, the rated capacity, the maximum allowable charging current, the gassing voltage, the battery's charge retention, temperature, manufacturing tolerances, the dynamic 'time-constant' of the battery, the age of the battery and other such parameters which affect the occurrence of gassing. Unfortunately, most of these parameters cannot easily be accessed by users and some of them may also depend on other parameters. Besides that, the common problem of using conventional charger are that the battery will be charged with either too small a current, which result in a long charging time, or too large a current which causes gassing water los, grid corrosion and heat build-up.

In this study, a fuzzy logic controller is designed to provide a suitable level of charging current without needing to identify the battery parameters. The designed system also offers to perform a safety charging process with several protections by monitoring of temperature and current.

Fuzzy Logic Control (FLC) has several advantages, namely [5]:

- Fuzzy logic does not require a nonlinear mathematical model functions, that are very complex.
- Fuzzy logic is extremely flexible
- Fuzzy logic can tolerate data that is not appropriate
- Fuzzy logic can develop and apply the experiences of experts directly without having to go through the training process.
- Fuzzy logic can work with conventional control techniques.

Fuzzy logic control will change and adjust control parameters automatically in accordance with the desired system behavior through a set of rules drawn from the experience of experts in the system.

Nomenclature

°C	degree Celcius
Ah	ampere hour (=3600 coulombs)
AGM	Absorbed Glass Mat
FLC	*Fuzzy Logic Control*
I	Current (Amp)
LCD	Liquid Crystal Display
MCU	Microcontroller Unit
MOSFET	Metal Oxide Semiconductor Field Effect Transistor
PWM	Pulse Width Modulation
V	Voltage (V)
VRLA	Valve Regulated Lead Acid

4.1.17 Design consideration

3.1 Design of Battery Charger

VRLA battery is a type of lead acid rechargeable battery that commonly known as sealed battery. The construction of VRLA is different than flooded lead-acid battery. VRLA battery construction does not require regular addition of water to cells and it vents less gas than flooded lead acid battery. VRLA battery can be used in confine space or poor ventilated spaces because of the venting advantage that result in less gas produce [3]. VRLA batteries are commonly classified as AGM battery and gel battery (gel cell). When the battery is recharged at high voltage, typically greater than 2.30 volts per cell, it wills active the pressure relief valve. By releasing the some gas on the battery, it decreased the overall capacity of the battery. They are not permanently sealed, but are maintenance free. Unlike lead acid batteries that must be placed in an upright position to prevent acid spills and to maintain the fixed plate vertically oriented, VRLA Battery can be stored at any position.

This charger method provides a dual level charging process which has three charging states as shown in figure 1.

In the three charging state, a charging cycle normally starts with the bulk charge state. The charger produces a constant charge rate by supply a constant current source to the battery. In this state, the maximum current of the charger flows in to the battery. After the battery voltage reaches a threshold value V_H the charger enters the over-charge state. The threshold value V_H is a preset voltage limit that already set up in the overcharge region that will not damage the battery. In the over-charge state, the charging current drops exponentially to the certain value I_H and at this value the charger achieves a

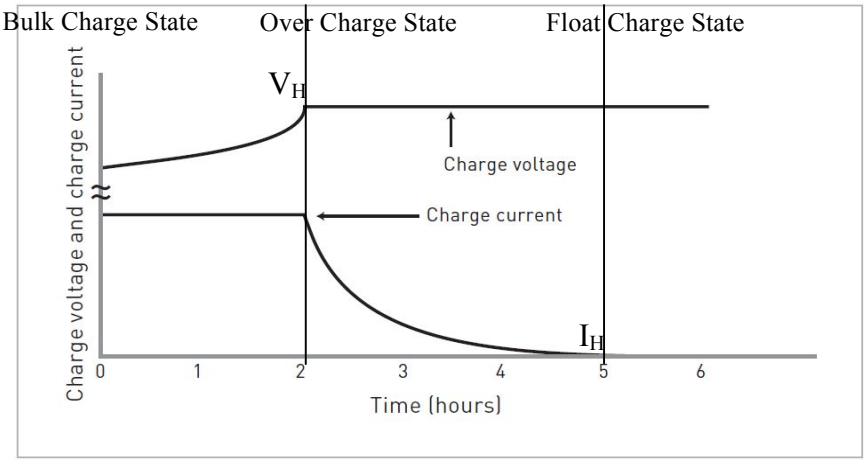


Figure 7 Constant Voltage Charging Method [4]

steady state value before the charger enters the final state, called the float charge state. In this states, the maximum energy has been transferred into the battery

The hardware implementation photograph is shown in figure 2.

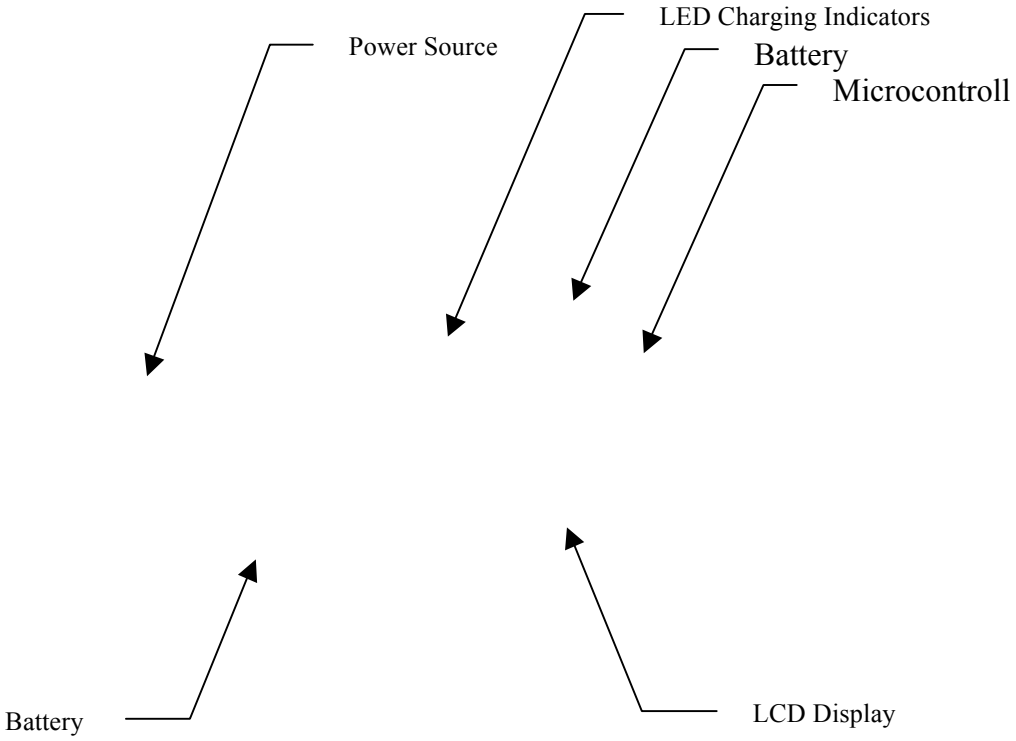
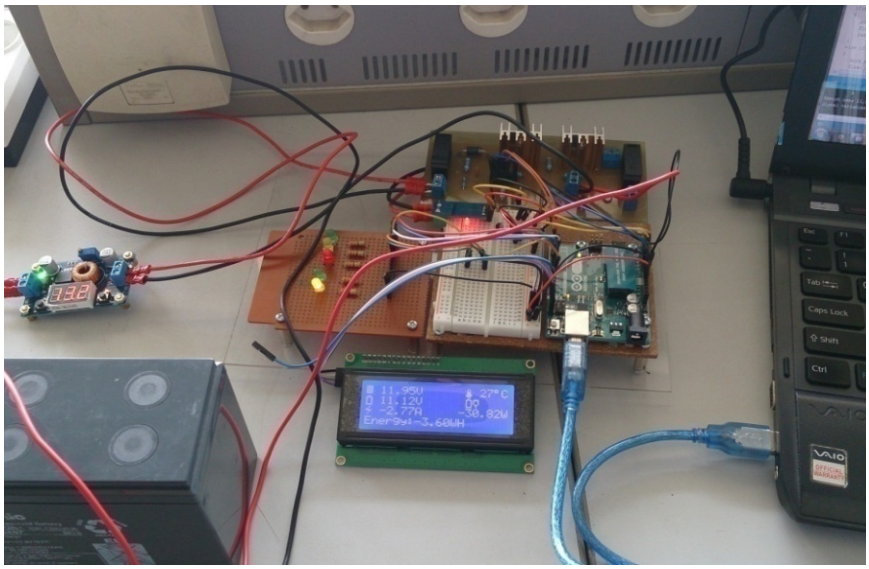


Figure 8 Hardware Implementation



The circuit diagram implementation is shown in figure 3. The microcontroller unit programmed applies the fuzzy rules according to the battery conditions and generates the required PWM duty cycle pulse that appears at A_0 pin of microcontroller and goes to the gate of MOSFET Driver. The power is given to battery through buck converter. The charging rate of the battery will be controlled by the Fuzzy PWM of the controller. The LCD 20x4 display unit displays the present current, voltage of the battery, environment temperature and the charging state. The real time voltage and current signal are given to Fuzzy controller by voltage and current sensor.
There are three sensors that developed and implemented on the interface circuits. These sensors are used to lead the signals to the microcontroller.

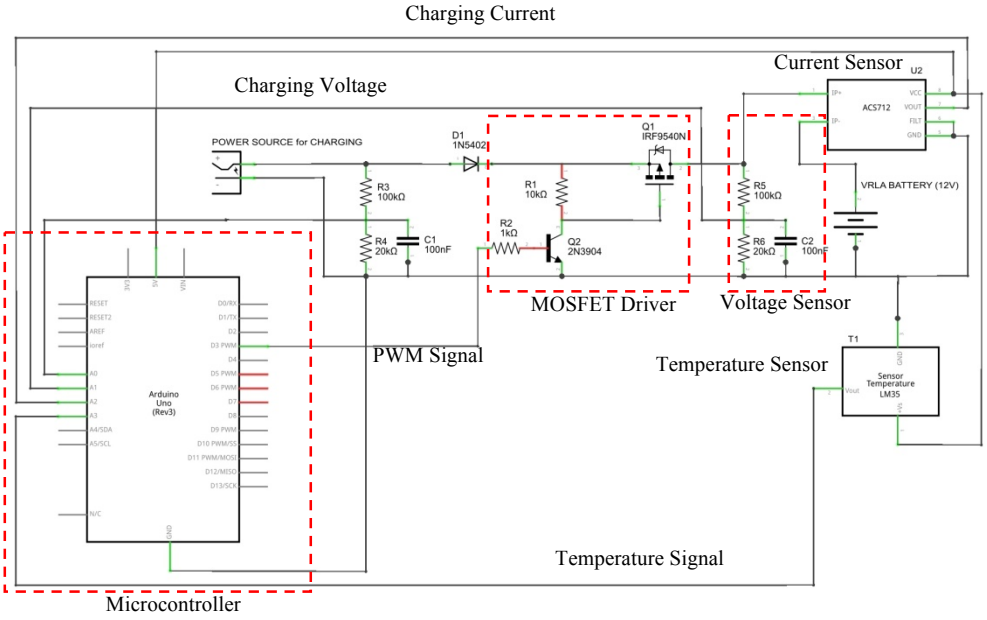


Figure 9 Circuit Diagram Implementation

A. MOSFET Driver

In the charge controller circuit, we use MOSFET Driver to control the power flow to the battery. A gate driver is a power amplifier that accepts a low-power input from a microcontroller and will produces a high-current drive input for the gate of the MOSFET. According to the battery charging voltage, the controller generates a duty cycle given by the MCU PWM pin. The PWM signal is applied to the MOSFET through gate terminal and it will vary the power that flow through the source terminal of the MOSFET P-channel IRF9540N which can hold a maximum drain to source voltage of 100V and can pass a maximum current of 19A.

B. Sensor

The voltage sensor can easily implemented by using a voltage divider circuit. The microcontroller analog pin input voltage is restricted to 5V, and then we have to design that the output voltage from the voltage divider should be less than 5V. To step down the voltage to lower than 5V, it used R_5=100kΩ and R_6 =20kΩ in sensing the battery voltage. So by this voltage divider circuit, we can measure the charging voltage directly.

The capacitor used parallel with R_6 is used as filter which removes any unwanted ripple/noise signal.

The charger equipped with current sensor by using Hall Effect sensor ACS 712. The current sensor is used for measuring the charging current.

The third sensor is a temperature sensor. The temperature sensor is used to sense the environment temperature and include the battery temperature as well. We used LM35 temperature sensor which is rated for −55°C to +150°C Range. The battery's chemical reactions change with temperature. As the battery gets warmer, the gassing increases. As the battery gets colder, it becomes more resistant to charging. Depending on how much the battery temperature varies, it is important to adjust the charging process for temperature changes. The temperature sensor will measure the battery temperature, and the controller uses this input to adjust the charge set point as required. The compensation value is – 5mv /°C/cell for lead acid type batteries (–30mV/ºC for 12V and –15mV/ºC for 6V battery). The negative sign of temperature compensation indicates, increases in temperature require a reduction in charge set point.

3.2 Fuzzy Logic Control Implementation

To design a fuzzy logic controller for a battery charging system, an input membership function relating to battery voltage, a input membership function relating to the battery current, an output membership function of a value relating to PWM duty cycle are constructed in the way that, they in trapezoidal and triangle shape. Figure 4 and figure 5 shows input membership functions for this application [6]. The *Fuzzy Logic Controller* goes through three steps: Fuzzification, Fuzzy Inference and Defuzzification.

A. **Fuzzification:** Here in the fuzzification, actual measured input (voltage) values and voltage difference values also the cycle value as output are mapped into fuzzy membership function.

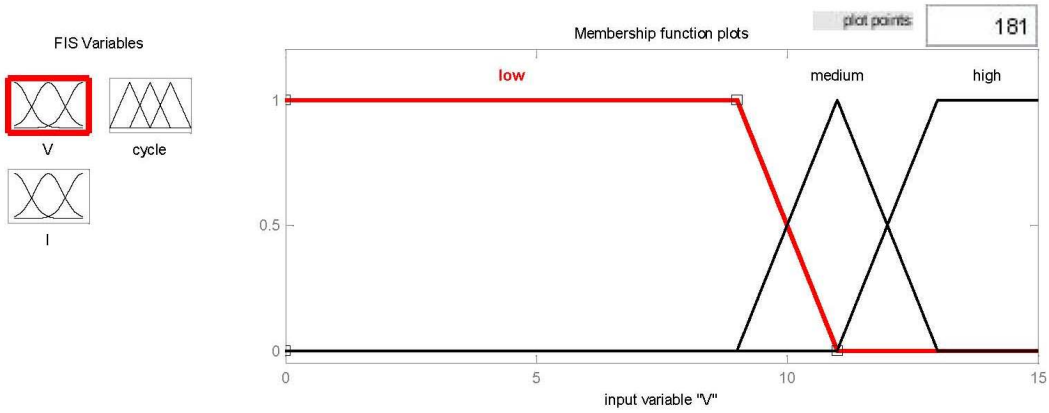


Figure 10 Input membership function (Voltage)

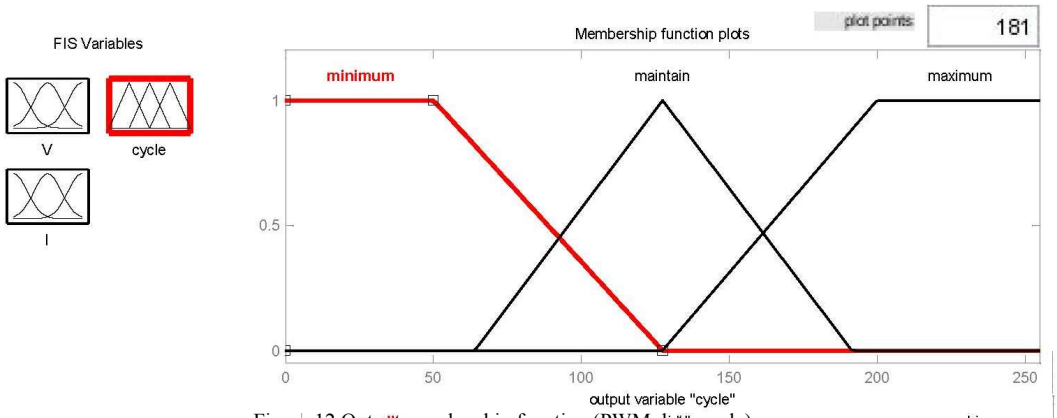


Figure 12 Output membership function (PWM duty cycle)

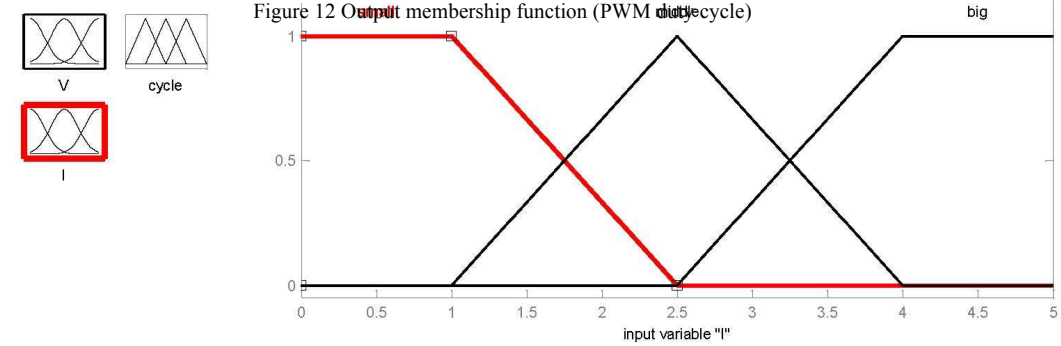


Figure 11 Input membership function (Current)

B. **Fuzzy Inference**. The Fuzzy Inference forms a key part of *Fuzzy Logic Control*. The Fuzzy IF-THEN rule base matrix is in Table 1.

Table 1 Rule Base Matrix

V \ I	**small**	**middle**	**big**
low	maintain	maximum	maximum
medium	maintain	maintain	maximum
high	minimum	maintain	maintain

These rules are expressed as IF – THEN statements and the syntax is as follows:
"IF {voltage (V) is low AND current (I) is big THEN {cycle = maximum}"

C. **Defuzzification**

As the final step in the fuzzy logic controller is to combine the fuzzy output into a crisp system output. Output of the battery charger is duty cycle, to drive the MOSFET in the circuit of the charger. The value is 0 – 255, in accordance with the microcontroller PWM signal output. The Fuzzy Inference based on Mandeni's scheme is shown in figure 11 for present voltage of 7.5V, current of 2.5A thereby suggesting a PWM of 82% or 208 cycle.

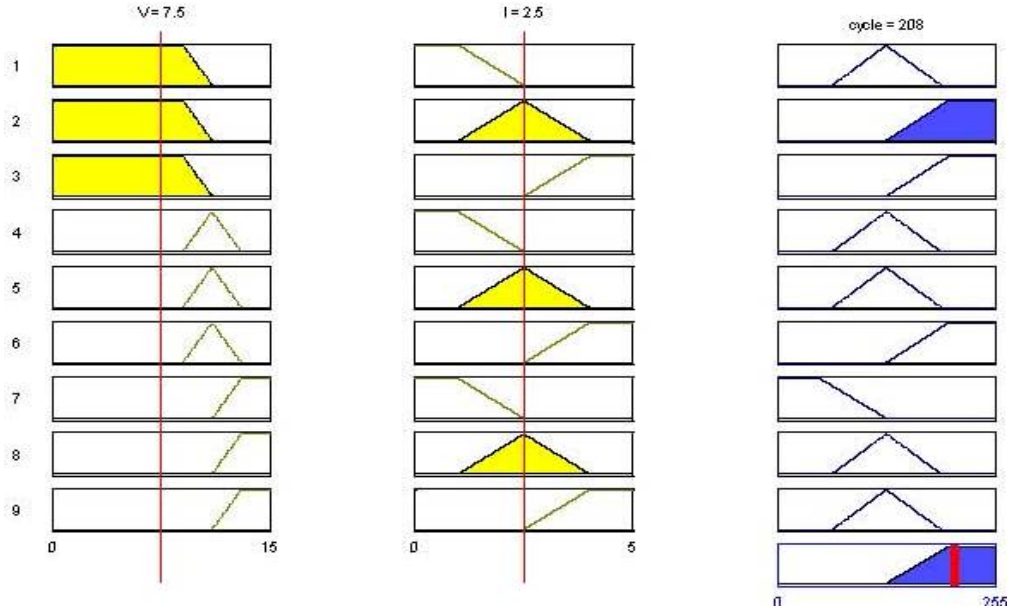
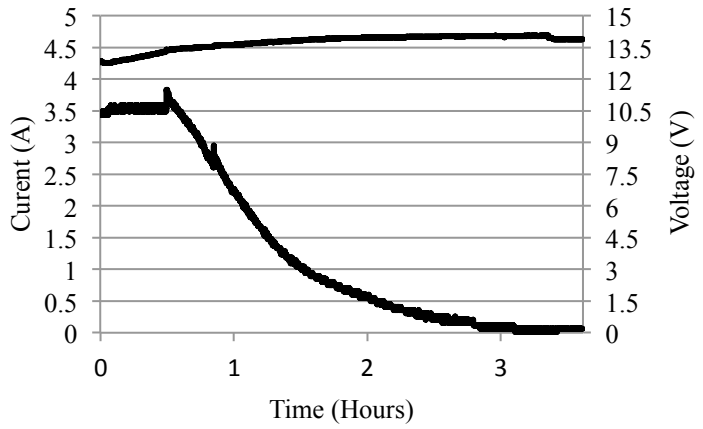


Figure 13 Rule Viewer

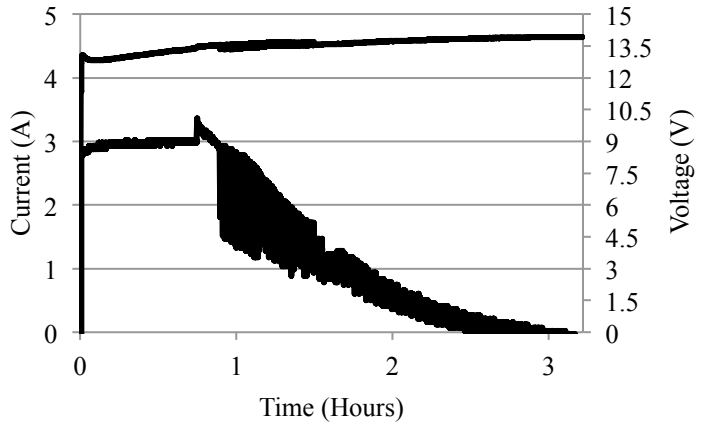
4.1.18 Result and Conclusion

After several experiments is done by optimization of the fuzzy logic member function and also by analyses the rule base and then redesign the rules, we are success to implemented fuzzy logic in the battery charging as shown in figure 8.



$V_{(chg.)}$: 14.2V
$I_{(chg.)}$: 3.5Amp
Temp : 27°C
Battery charging process
Start : 11.13V
Finish : 14.1 V
Chg. Time : 3.5 h

Charge method: Constant Voltage



$V_{(chg.)}$: 14.0V
$I_{(chg.)}$: 3.0Amp
Temp : 27°C
Battery charging process
Start : 11.35V
Finish : 14 V
Chg. Time : 3 h

Charge method: Constant Voltage with FLC.

Figure 14 Battery Charging Comparison (CV compare to CV with FLC)

The proposed system has good performance characteristics such as proper charging rates and insignificant gassing occurrence. The fuzzy logic has successfully controlled the current charging (PWM signal), it produces lower charging current but the charging process is faster. The algorithm that developed has the capability to detect the temperature change of the battery, in order to protect the battery from gassing. So if the temperature rises, it will adjust the charging voltage with temperature rise by reduce the charging voltage. Then through this way, the charging process will reduce the amount of hydrogen produced which will prevent the battery from explosion hazard and also it can improve the life cycle of the battery.
With the implementation of fuzzy logic technique on the system charging, we can avoid the battery from overcharged and the battery temperature stay controlled which will leads to the life span of the battery.

Acknowledgements

The authors would like to express their appreciation to Bapak Dedy Loebis ST, MBA, M.Sc., Ph.D, Bapak Dr. Ir. Gembong Baskoro, M.Sc. and Bapak Dena Hendriana, B.Sc., S.M., Sc.D., for their valuable advises and support effort.

References

[1] LIANG, Y. C. NG, T. K. - Design of battery charging system with fuzzy logic controller, INT. I. ELECTRONICS, 1993, VOL. 75, NO. I, 75-86
[2] Patrick T. Moseley, Jurgen Garche, C.D. Parker, D.A.J. Rand. Valve-Regulated Lead-Acid Batteries, Elsevier Science, 2004.
[3] David Linden, Thomas B. Reddy. Handbook of Batteries, McGraw-Hill, 2002.
[4] VRLA Handbook Industrial Batteries Panasonic, https://eu.industrial.panasonic.com/sites/default/pidseu/files/downloads/files/id_vrla_handbook_e.pdf.
[5] Roland S. Burns. Advanced Control Engineering, Butterworth-Heinemann, Oxford, 2001.
[6] Yu Qin, Shanshan Du - A Practical and Low Cost PWM Battery Charger Using Fuzzy Logic Control for UPS Application

The Annual Conference on Management and Information Technology (ACMIT) 2016

Optimized Process Control for Operation, Energy, Management, and Maintenance in Boiler Plant Using SCADA

Kenny Jesse Hartanto*

Faculty of Engineering and Information Technology, Swiss German University, BSD – City, Tangerang 15339, Indonesia

Abstract

The purpose of this study is to design the SCADA to monitor and control the boiler operation using PLC, and to analyze the efficiency of the boiler. This paper outlines the various stages in the operation of the boiler conversions manually operated, towards the boiler operates in full. Boiler is very important part in industry and it require inspection and monitoring process continuously with a specific time interval. Earlier days this inspection and monitoring process is done with human workers. By done with human workers, there are possibilities of errors with human workers while measuring parameter values in boiler operation process. So it is needed a reliable monitoring system is required to avoid these errors and maximize profit. The automation can be easily done by using Programmable Logic Controller (PLC) and SCADA, by constant monitoring using SCADA that already connected to the PLC using communication cable. In this paper the design and automated development of some techniques used for boiler automation. Boiler automation includes the monitoring of water level, pressure and temperature using different sensors.

Keywords: Automation; Programmable Logic Controller (PLC); Supervisory Control and Data Acquisition system (SCADA); Boiler.

Introduction

Over the years for high quality, greater efficiency and automated machines has increased in the industrial. Plants require continuous monitoring and inspection at specific time intervals. There are number of possibilities of errors at measuring parameters and various stages involved with human workers and also the lack of few features of microcontrollers. This paper attempt to explain the advantages the companies will face by implementing automation into them. The boiler control which is the most important part of any plant, and its automation is the precise effort of this paper. In order to automate and minimize human intervention, there is a need to develop a Supervisory Control and Data Acquisition (SCADA) system that used to monitors the plant cand helps to reduce the errors caused by humans. While the SCADA is used to monitor all parameter system in plant, Programmable Logic Controller (PLC) is also used for the internal storage of instruction for the implementing function such as programming, sequencing, logic, counting, timing and arithmetic to control through digital or analog I/O modules.

Nomenclature

Level	Amount level of boiler in (% / Percent)
Pressure	Amount pressure of boiler in (Bar)
Temperature	Amount temperature of boiler in (°C)

Literature Study

Shital S. Chopade [5] et al describes the purpose of this paper is to present a programmable logic controller (PLC) system that is applied to the water tube boiler which will increase high quality and greater efficiency. This system monitors boiler temperature and pressure and volume via different sensors which provide input to PLC. The output of PLC is to controls the boiler temperature and pressure and gives out the user required volume of steam. All pressure and temperature log are shown on SCADA screen and are controlled through SCADA.

Present System and Proposed System

Present System

Previous days, boiler parameters such as water level, pressure, temperature is monitored by human work. These parameters are controlled by manual only. The data are maintained only in log book so there is no an effective data analysis for taking a preventive action leading to production loss.

Proposed System

The proposed system of this paper is to monitor and control the boiler parameters by using SCADA-PLC. Now the process control in boiler is fully automatic and analysis data of status obtained in SCADA, and boiler operation controlled by PLC.

Boiler

Boiler is defined as a closed vessel in which steam is produced from water by the combustion of fuel. Generally in boiler, steam is produced by the interaction of hot flue gases with water pipes which is coming out from the fuel. In boilers, chemical energy of stored fuel is converted into the heat energy and this heat energy is absorb by water which convert them into a steam [4].

There are many different types of boiler, they are:

Fire-tube Boiler
Water-tube Boiler
Superheated Steam Boiler
Hydronic Boiler
Haycock or Pot Boiler

Fire-tube Boiler

Fire-tube boiler is the most basic types of boiler and the design is also very old. In **fire-tube boiler**, the gases is burnt inside a furnace. Hot gases produced in the furnace then passes through the fire tubes. As the hot gases are passed through these tubes. The heat energy of the gases is transferred to the water surrounds them. As a result steam is generated in the water, steam naturally comes up and stored upon the water in the same vessel of **fire-tube boiler**. This steam is taken out from the steam outlet for production. The water is fed into the boiler through the feed water inlet.

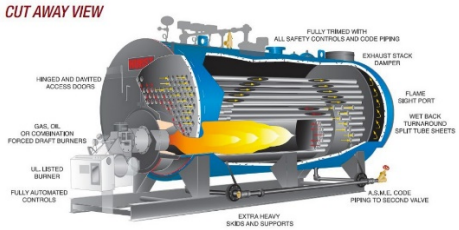


Fig. 1 Cut Away View of Fire Tube Boiler

Water-tube Boiler

A **Water-tube boiler** is a boiler where the water is heated inside tubes and the hot gas surround them. This is a basic definition of water tube boiler. Actually this water-tube boiler is just the opposite of fire-tube boiler where hot gases are passed through tubes which are surrounded by water.

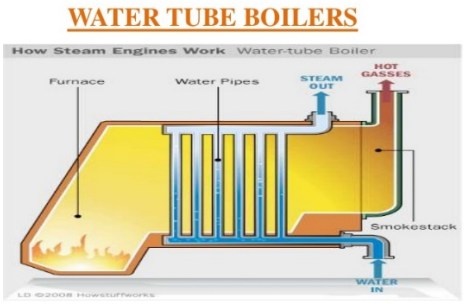


Fig. 2 Water Tube Boiler [8]

Superheated Steam Boiler

Superheated Steam Boiler, is a process of reheating a steam which has been produced in the boiler become superheated steam. This superheated steam is different from the steam before reheating. Superheated steam has condense less rapidly and less water vapor condense less rapidly compare to saturated steam.

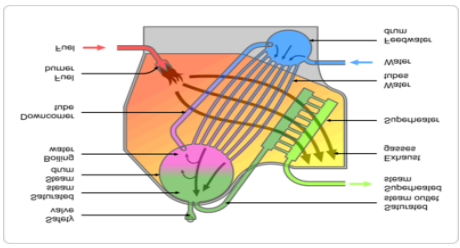


Fig. 3 Superheated Steam Boiler

1.1 Critical Control Parameter in Boiler

- Level Control
  Level of steam in the drum High and Low level
- Level Pressure Control
  Level of Steam Pressure in the drum
- Flow Control
  Flow water, Flow gas, Flow steam
- Temperature Control
  Temperature of boiler

1.2 Boiler Operation

Boiler is a water containing vessel which transfer heat from a fuel source into steam which is piped to a point where it can be used to run production. Water plays as a main part in the generation of steam. Feed water pump's will switched ON by using feed water pump switch. In this water should be maintained at least at 50%. The level of water connected to the PLC, PLC controller senses the change of the level and sends an appropriate control signal to the feed water pump valve to be switch ON or

OFF. The heat quantities and temperature relationships need to be taken into consideration. Temperature and pressure are continuously monitored through signals and sensors that fed into PLC, and for the controlling action will be take as pre-desired objective

SCADA

Supervisory Control and Data Acquisition or SCADA is an application program for monitoring process control in plant. SCADA gather all of the data in real time from PLC. SCADA is used in power plant such as telecomunications, oil and gas, food and beverage, transportation, manufacturing, and etc. SCADA systems include hardware and software components. The hardware give data into a computer SCADA, and the computer process the data and present it. SCADA systems used to monitor the plant and helps reduce the errors that caused by humans, it also records and log all events into a file that stored on hard disk / database to be print by operator. SCADA also give warns when condition in the field become Hazardous/dangerous by sounding alarms.

SCADA control system offers:

- Vizualization Process (HMI)
- Supervisory Control and Data Acqusition (SCADA)
- Local or remote operating mode
- Historical trending
- Alarming, alarm management and printing
- High performance networking
- Development softwares allows continued development on site

PLC

Programmable Logic Controller or PLC is a digital computer used for automation in industrial. PLC are used in many machines, in many industries. PLC are designed for multiple arrangements of Digital Input, Digital Output, Analag Input, Analog Output, and more programming elements.

PLC Working

After PLC is initialised, CPU brings all the field input signals from the module to be reads and store into the internal memory as process of input signal. PII (Process Input Image) is the internal memory of CPU. The application / user program will be stored in CPU. CPU will processes the program that already stored in the internal memory, it consist of a list of logic functions, instructions, after success processed, the input information will be ready to access before read in PII and the results are written into PIQ(Process Image Output), also other storage for counter, timer, bit memory will be accessed during the program process by the CPU. After the process of application, the status from the piq will transfer the output and then switch it to on / off, and it will execute the next cycle from the PLC initialized

Ladder Logic

Ladder logic diagram is a visual and logical method of displauing the control logic which, based on the inputs determine the outputs of the program. Ladder logic is made up of series logical expression expressed graphically as series and parallel. The circuits of logic elemests such as contacts, timer, counter, I/O, etc.

Timer

Timer in PLC represent a time delay relay in ladder logic. Timer function are a fixed component of the central process unit. It is possible to achieve time delays in the range of few milliseconds to few hours

Counter
Counter is a counting fucntions to operate same as hardaware counters. It is possible to count up and count down as well. The counting range start from 0 until 999. The count is either dual or BCD coded for further processing

Addressing

Addressing is refered to the designation of an input or output in the program. The input and output of PLC are mostly defined in groups of eight on DI/DO. The eight unit is called byte.The address can start from 1 to 8 or 0 to 7

I/O

The operands in PLC program can be classifed as Inputs, and Outputs. The input operands reger to external signasl of the controlled system. The operating system of PLC assigns the signal status of the input

Research Methodology

All the values can be filled up by the introduction of the automation technique. The automatic control of all the process in plant which includes the monitoring process and inspection needs provides for a very efficient system. The automation process helps the company to reduce the amount of errors that occur, increased efficiency, reduction in the human resources, and most importantly very cost effective.

1.3 System definition

System Definition describes the scope and boundaries of the application system and the major user views. A user view defines what is required of the application system from the perspective of user role.

1.4 Requirement Collection and Analysis

Requirment collection and analysis is the process of collecting and analyzing the information about the real condition, problem that occur, and habit that is supported by the system, and using this information to identify the requirements for the new system. Visit site needed to know the process of the machine/system in the site, and to get information what that want to be monitored, control. When visit site user will explain all of the process, and we need to make the SCADA system according to the process it will help user to monitored the process in the SCADA system. Collecting Data and Information, after visit the site the important thing is data in the site, such as address, name of address, min/max value, and the type of data (bool, word, int, float, and char).

1.5 Design Application

Design the application for the User Interface SCADA, and system process.

1.6 Design SCADA

Design the monitoring SCADA system from the infromation and requirement that collected to

make a HMI for monitoring and control porcess.

1.7 Data Conversion and Loading

Data that already collect from PLC in real time will be drawn into the SCADA system to be displayed according to the address thats given.

1.8 Testing

Testing the application to check the error and adapting the user need. When testing, user need to develop by himself to know how the program work. There are two basic types of testing, black box testing and white box testing. Black box testing is a testing that ignores internal mechanism of a system or component and focuses to the output generated in response to selected inputs and execution. White box testing is a process of testing that takes into account the internal mechanism of a system or component.

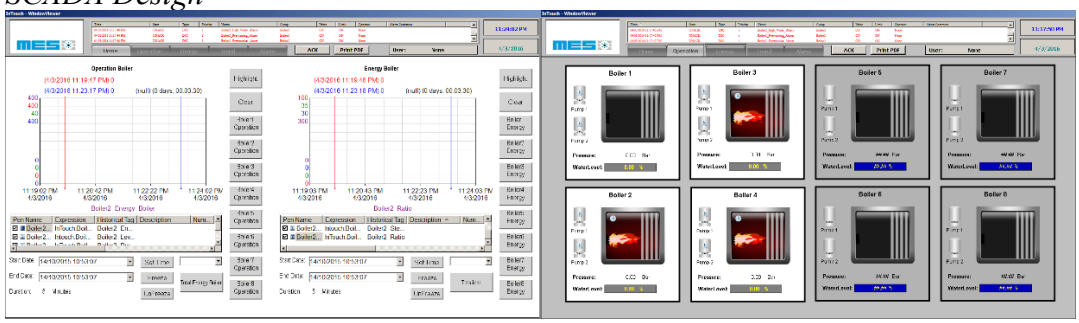
1.9 Operational Maintenance

Operational maintenance is the process to monitoring and maintaining the SCADA system following installation

Result

In this section, the result obtained is discussed in details. SCADA system used to monitor a plant or equipment in industries. And for PLC, PLC used to run the program to control the boiler so it will run auto.

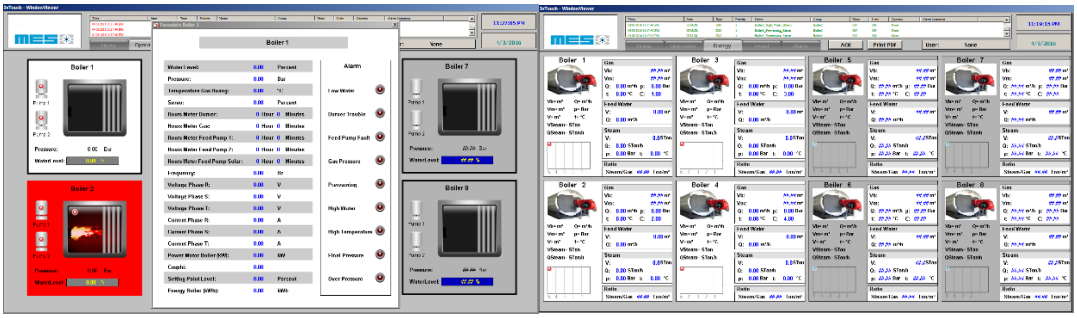
SCADA Design



(a) (b)

Fig. 4 (a) Boiler SCADA design for Home Menu and (b) Boiler SCADA design for Operation Menu

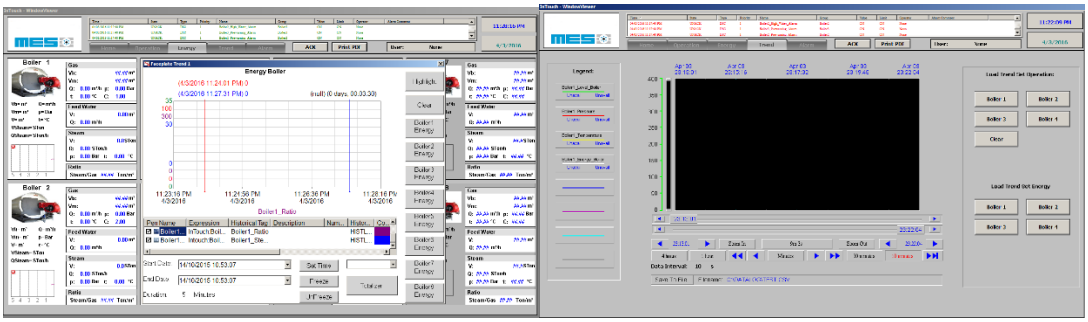
In this Home Menu user can choose the Boiler from 1-8, then the parameter for Operational trend and Energy trend will be different, and for the Operation Menu user can see the boiler is active or not by seeing the burner and pump, and also if there is an alarm the boiler will blinking into red.



(a) (b)

Fig. 6 (a) Boiler SCADA design for Operation Menu when user click on "Boiler 1" and (b) Boiler SCADA design for Energy Menu

If user click on the Boiler 1, it will pop up and give all the detail of the boiler parameter that already connected to the PLC. In this energy menu the parameter is come from meter device in the field, it gives information about the totalizer, flowrate, pressure, temperature of gas, water, and steam.



(a) (b)

Fig. 8 (a) Boiler SCADA design for Energy Menu when user click on "Boiler 1" and (b) Boiler SCADA design for Trend Menu

Trend menu show the historical trend that different from the home menu, in this menu the parameter that already log will be saved and will send to database of SCADA.

Beckhoff TwinCAT PLC Control

Programmable logic controller is an intelligent system of modules which has introduced in the control instruments in industry for replacing manual system. TwinCAT PLC Control is a complete development environment for PLC. The PLC program can be written in one or more of the language provided for in the IEC 61131-3 Standard there are IL (Instruction List), LD (Ladder Diagram), FBD/CFC (Function Block Diagram), SFC (Sequential Function Chart), ST (Structure Text).

Automated Boiler Proposed:

Table 1. Automated Boiler Proposed

	Percent
High Level	85 %
Spoint level	77 %

Pump On	67 %
Pre warning	50 %
Low Level	45 % - 40 %

Algorithm for Control Level and Burner Boiler

Table 2. Algorithm for Control Level and Burner Boiler

	Then	Else
Level		
Adjust SetPoint Level		
Adjust PumpOn Level		
If Level < PumpOn	Pump Running	Pump Stopped
If Level > SetPoint	Pump Off	Pump On
If Level > Set High	Alarm High Level On	Pump Off
If Level < Prewarning	Alarm Prewarning On	Pump On
If Level < Low Water	Alarm Low Water On	Pump On and Burner
Burner		
Check Low water alarm		
Check over pressure		
Check final pressure		
Check low gas pressure		
Check Burner trouble		
If low water alarm on	Burner Off	Burner On
If over pressure alarm on	Burner Off	Burner On
If final pressure alarm	Burner Off	Burner On
If low gas pressure	Burner Off	Burner On
If burner trouble	Burner Off	Burner On

The number of I/O for conventional Boiler (LGK):

Table 3. Conventional Boiler (LGK) I/O

	I/O
DI (Digital Input)	15
DO (Digital Output)	13
AI (Analog Input)	4
AO (Analog Output)	1
Analog Input Metering	6
V (Voltage)	3
I (Ampere)	3

The number of I/O for Programmable Boiler (WFM):

Table 4. Conventional Boiler (WFM) I/O

	I/O
DI (Digital Input)	13
DO (Digital Output)	11
AI (Analog Input)	3
AO (Analog Output)	1
Analog Input Metering Power	6
V (Voltage)	3
I (Ampere)	3

Conclusion

In this paper various Boiler control and Automation techniques has been discussed from which we can conclude that the technique of PLC and SCADA based boiler automation is an effective system which overcome the present system of other control methods. The future work deals with continuous monitoring and inspection process of boiler parameters can also be done using internet and can be access anywhere.

References

[1] Van der Geer J, Hanraads JAJ, Lupton RA. The art of writing a scientific article. *J Sci Commun* 2000;**163**:51–9.

[2] Strunk Jr W, White EB. *The elements of style*. 3rd ed. New York: Macmillan; 1979.

[3] Boyer, Stuart, A. *SCADA: Supervisory Control and Data Acquisition*, Instrument Society of America, Research Triangle, NC. 1993

[4] Hjalti Kristinsson and Sofie Lang, "*Boiler Control*", Springer, Berlin, 2010.

[5] Shital S. Chopade, Pradhuman Verma, Prashant Verma, "*Simulation of Boiler Control using PLC & SCADA,*" (IJEAT) ISSN: 2249 – 8958, Vol. 3, Issue-3, December 2013

[6] Anabik Shome, Dr. S.Denis Ashok , "Fuzzy Logic Approach for Boiler Temperature & Water Level Control," International Journal of Scientific & Engineering Research, Volume 3, Issue 6, 2012.

[7] K. Gowri Shankar, International Multi Conference of Engineers and Computer Scientists 2008 Vol II IMECS 2008, 19-21 March, 2008, Hong Kong

[8] Sanjoy Kumar Chakraborty, Nilotpal Manna and Surodh Dey" Importance of three-elements boiler drum level control and it installation in power plant" International Journal of Instrumentation and Control Systems (IJICS),2014.

[9] Shneiderman, B., & Plaisant, C. (2010). *Designing the User Interface: Strategies for Effective Human-Computer Interaction, Fifth Edition.* Pearson Education, Inc., Boston, MA 02116.

[10] Whitten, J. L., & Bentley, L. D. (2007). *System Analysis and Design Methods.* New York: McGraw-Hill/Irwin.

[11] William G. Zikmund, B.J. (2013). *Business Research Methods*. South Western

[12] Williams, L. (2006). A (Partial) *Introduction to Software Engineering Practices and Methods.* Testing Overview and Black-Box Testing Techniques (Seventh) Edition from https://online.ist.psu.edu/sites/ist412/files/williamstext.pdf

[13] Mane S. Ratnakar (2013). Energy Management in a Diary Industry Edition from http://iraj.in/up_proc/pdf/5-137666433405-10.pdf

[14] Yang Chia-han, and Vyatkin Valeriy (2008). Design and Validation Distributed Control with Decentralized Intelligence in Process Industries: A Survey. Edition from http://homepages.engineering.auckland.ac.nz/~vyatkin/publ/YangVyatkin_INDIN.pdf

The Annual Conference on Management and Information Technology (ACMIT) 2016

Simulation Study for Optimization Design on Vertical Axis Wind Turbine blades

Arie S. Pangemanan[a], Houtman P. Siregar. [β], and Maman Suryaman[a,b,]5*

[a]*Swiss-German University, EduTown BSDCity, Tangerang 15339, Indonesia*
[a]*Indonesian Institute of Indonesia,Muncul Serpong, Tangsel 15320, Indonesia*

Abstract

In this article is conducted research to harness wind energy which is firstly generated by vehicle / truck that is runing on the public road highway. To take advantage of wind energy of the moving truck is designed, otherwise advisor had some ideas during the proposal defense change into fixed vertical axis wind turbine. The purpose of this evaluation study is to get optimization for the design blades of the vertical axis fixed wind turbine and finding the best blades installed and angle of attack will result in highest lift/drag ratio. While other test parameters such as air pressure, wind speed and others are held constant. In this evaluation study the angle of attack are used ranging begin from 45 and until 90 degrees. Evaluation result showed that the best blades install and angle of attack that gives the best lift/drag ratio is 5 blades at AoA ninety degree. Blades diameter of the designed wind turbine are 0.35 m and the number of blades which is the best in analytical of CFD techniques in the designed wind turbine are five pieces. The speed of the wind which is used to test the blades is 8 m/s on turbine rotation 80 rpm. The evaluation study has suceeded to do parametric optimization of the turbine blades. The optimised blades have been ready to re-designed assamble with another componens of the wind turbine to construct the prototype but there some problems / handicaps during the changes the prootype of turbine from movable to fixed wind turbine. The assambled vertical axial wind turbine postponed to further be tested in order to know its performance.
CFD simulation has been performed with ten different VAWT designed models. Moving mesh and fluid flow simulation have been developed in CFD software FLUENT. The findings of these numerical simulations provided pressure contour, velocity contour, C_D or $C_{L.}$.

Keywords : Design, vertical axial wind turbine, Ansys R15-CFD simulation, wind energy, integrated turbine blades

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address: author@institute.xxx .

1. Introduction

Wind energy by the time the wind was blowing, wind produce kinetic energy (force movements) which can perform work. The demand for energy is creeping highly due to increased of population, industries, agricultures advancement and if we still used traditional handling of the energy sources are limited and will became empty. Therefore, renewable energy is the only answer in finding a replacement for the old energy indispensable / 'non'renewable such as petroleum, coal, uranium etcetera are parts of all of that is not replaceable and will be used up. [1] Wind energy is one of the renewable energy potential that can make a significant contribution to the energy needs of domestic electricity, especially remote areas. Wind energy plants is free of pollution and wind energy resources are available everywhere, so this plant can answer environmental concerns and the availability of energy sources for Indonesia which are islands country in the equator with the very rapid population. Indonesia need to find alternative energy to anticipate the energy crisis in the future.

In this journal we conduct evaluation study to get the best optimization design of integrated vertical axis wind turbine at the satelite/urban city of Jakarta is Tangerang Selatan city.
The purpose of this evaluation study by computational CFD software is to do parametric optimisation of the wind turbine blades and find the best angle of attack will result in highest lift/drag ratio for the integrated blades of the design wind turbine.

4.1.19 Evaluation of the Rotor Aerodyamic Forces acting on the Wind Turbine

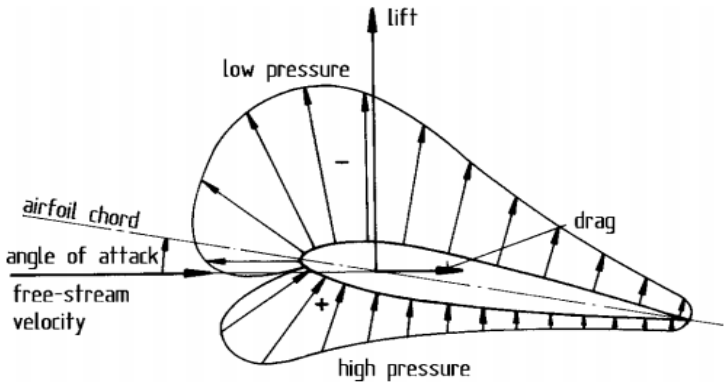


Fig. 1

From the figure 1: there are two forces type acting on the wind turbine rotor: ***lift*** force and ***drag*** force.

Lift is the force which perpendicular to the fluid flow stream. If the air swept airfoil cross-section with a certain speed, then air pressure at the top of the wings will be smaller than in the bottom of the wing, this causes the lifting force on the wing called the ***lift force***. While the ***drag force*** is drag while the opposite direction of blade rotor motion. [12]

`

$$L = C_L \frac{\rho}{2} A v^2 \qquad [1]$$

And

$$D = C_P \frac{\rho}{2} A v^2 \qquad [2]$$

Where: L=Lift force (N), D=Drag force (N), ρ = Air density ($\frac{kg}{m3}$);
A=Rotor cross-section area (m^2);
$v = velocity\ of\ the\ airflow\ through\ rotor$ ($\frac{m}{s}$)

In general, there are four types of the blade form i.e. rectangular form, linear taper form, reverse linear taper form and parabolic taper form. In this reserach is used linear taper blade form and its geometric form.

Pitch angle is ones of the control mechanism for wind turbine by controling the aerodynamic of the blade by means of the slope angle of toward direction wind blow or angle of attact

The shape of the blade is the function of tip speed ratio,rotore diameter of the rotor, and the number of blades. Forces been in designing the shape of the blade is plan form blade, blade width (chord) c, the radius, we know the resultant forces results of the base (root radius), thick blade, and pitch angle. Hugh piggots provide formulations to determine the width of the blade as a function of distance from the centre of rotation by using the approach Betz: [14]

$$C = \frac{16\pi.R(\frac{R}{r})}{9.\lambda^2 B} \qquad [3]$$

where:
C = width of the blade (chord) (m)
R = radius of rotor (m);
r = distance from the centre of rotation (m)

To determine the pitch angle β can use the equation:

$$\beta = acrtan\left(\frac{2R}{3r\lambda}\right) - \alpha$$

with:
α = angle of attack (degrees)
R = radius of rotor (m)
r = distance from the centre of rotation (m)
λ = tip speed ratio
Velocity elements acting on the blade are shown in the fig.2

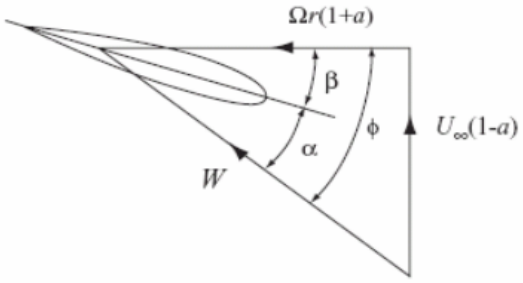


Fig. 2.

Apparent wind w_r the resultant of the free air stream and tangential velocity which can be computed by :

$$w_r = v.\sqrt{1 + \left(\frac{r}{R}\lambda\right)^2} \qquad [5]$$

where:
w_r = resultant wind velocity (m / s)
v = wind speed free (m / s)
λ = tip speed ratio
r = distance from the centre of rotation element (m)
R = radius of rotor (m)
And the apparent wind ϕ direction is calculated by the equation:

$$\phi = arctan\frac{R}{r\lambda} \qquad [6]$$

Where : φ = apparent wind angle (degrees)
R = radius (m)
r = distance from the centre of rotation element (m)
λ = tip speed ratio

Forces act on the blade is shown in figure 3.

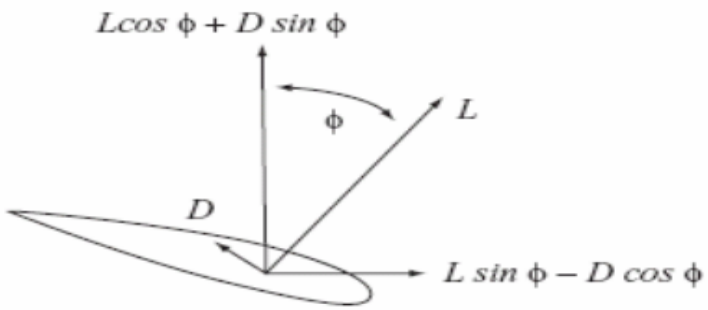


Fig. 3

the force on the rotor is tangential force and axial force. Style tangential and axial force is obtained by the equation:

$$F_t = L\cos\phi + D\sin\phi \quad [7]$$
$$F_a = L\cos\phi - D\sin\phi \quad [8]$$

Where,

F_t = tangential force (N)
F_a = axial force (N)
L = lift force (N)
D = drag force (N)
ϕ = apparent wind angle (degrees)

Axial force that occurs at each station is represented in the form of moment to center of rotation by the equation:

$$\sigma = F_t . r \quad [9]$$

where:
σ = moment of force (Nm)
R = distance element against rotation center (m)

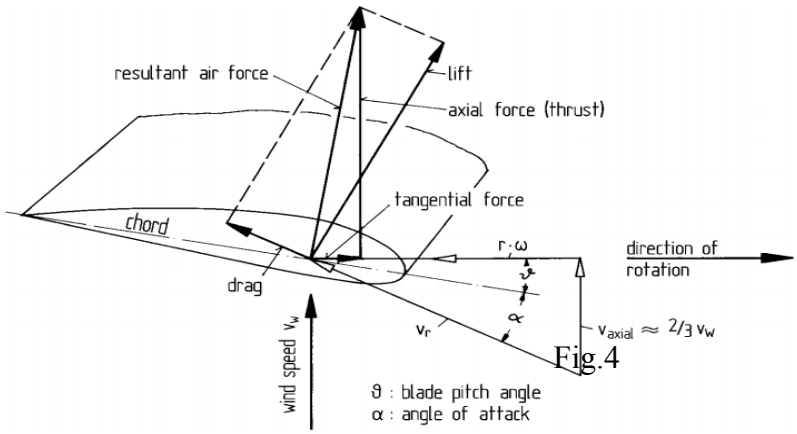


Fig.4

4.1.20 Aerodynamic forces Evaluation on VAWT (CFD Analysis)

For the realization of wind turbine that we propose in the article, we compose the flowchart of research as shown in figure 5. First of all, it is determined the specification of the turbine that will be designed. Through the prescribed specification then it is selected the type of the turbine blades which will be used in the wind turbine. Furthermore, based on those blades that have been mentioned, its

dimensions are optimized through simulations with the help of Computational Fluid Dynamics "FLUENT" release 15 package program.

From the simulation results, it is obtained the best dimensions of blades for wind turbine which is designed. Furthermore, it is determined the sized of the wind turbine components. Such as shafts, gears, casing and other components. With the completion determination of the size of the turbine components, then the proceed with the assembly of these components into a wind turbine and ready to be tested. Wind turbine that have been completed assembling, furthermore it is tested to obtaine the performance of the wind turbine. Blades of the movable wind turbine are maid of wood and the number of the blades are six pieces. The blades are shrauded by alumunium sheet metal. Diameter of the blade is 0.34 m. Types of the fix turbine which is constructed in this

4.1.21 Result of Evaluation Study and Discussion

For optimizing the turbine blades in this research, the variables used are 2 angles of attact and optimal blades used from 2 until 5 blades which will affected to get the highest power and efficiency. In this study there are 2 options angles of attact are used ranging (45 and 90) degrees. To obtain the optimum blades used blade is used package program Computational Fluid Dynamic "FLUENT" R15. With the fix wind velocity condition 8 m/s simulate

The data of the tested result are shown in the figure 5 to figure xx

Contour of pressure magnitude for 2 different angle of attact 45^0 and $90^{0\backslash}$of variations turbine rotor baldes from 2 through 5 blades.

The angle of attact which give optimum performance on integrated fan blades turbine is ninety degrees. Consideration of the best angle of attact on the maximum cross sectional area covered to accelerate rotor and get maximum pressure.

In inspecting the images which are shown as CFD result in figure 9 to figure 20, we observed that the best contours of of velocity and pressure magnitude is figure xx with maximum 5 blades and the angle of attack equal to ninety degrees.

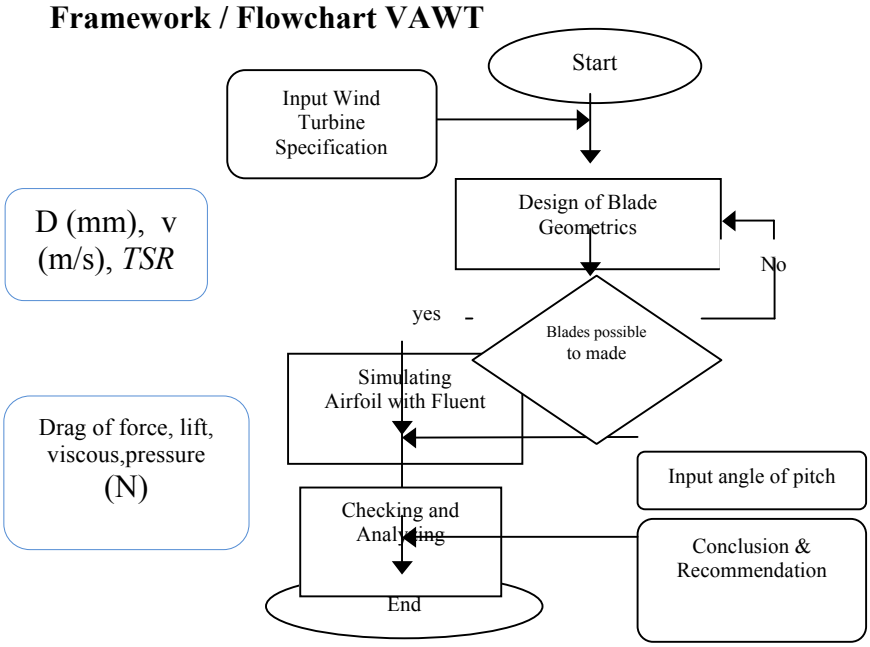


Fig. 5 Flowchart of vertical axis wind turbine design

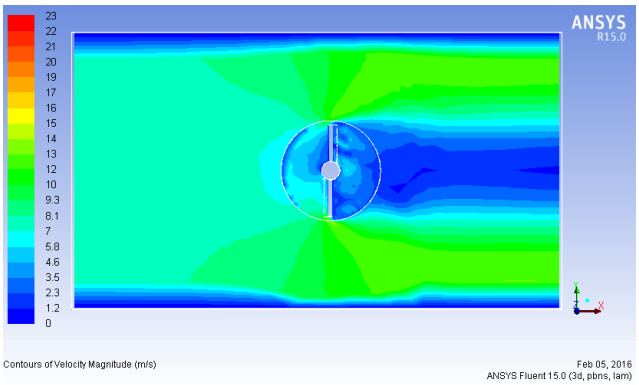


Fig. 6 Contour of velocity magnitude for 2 turbine blades and 45^0 AoA

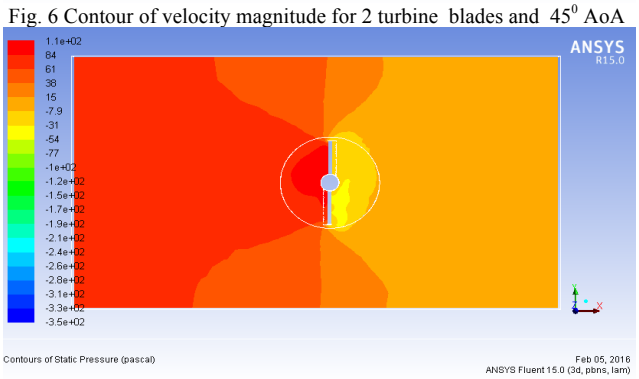


Fig. 7 Contour of Pressure magnitude for 2 turbine blades and 45^0 AoA

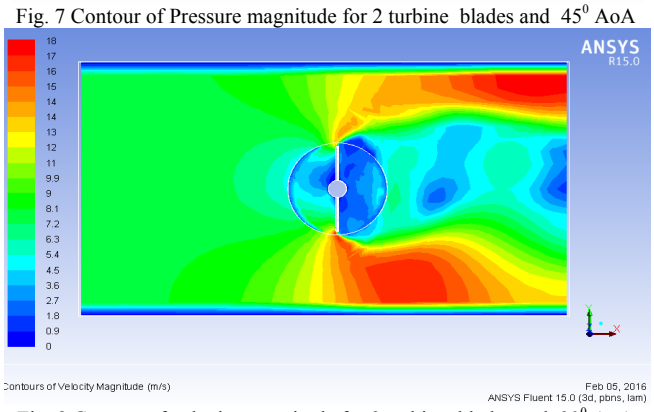


Fig. 8 Contour of velocity magnitude for 2 turbine blades and 90^0 AoA

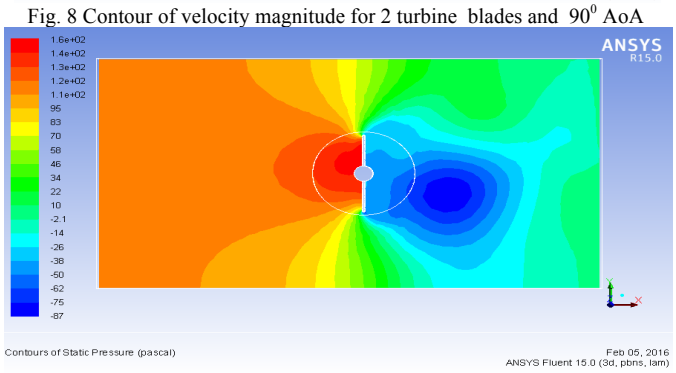


Fig. 9 Contour of Pressure magnitude for 2 turbine blades and 90^0 AoA

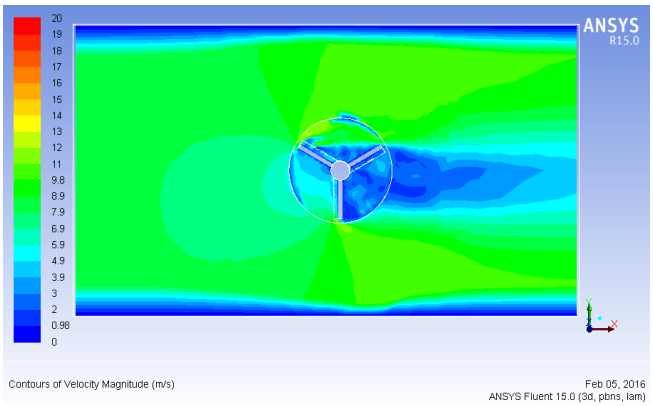


Fig. 10 Contour of velocity magnitude for 3 turbine blades and 45^0 AoA

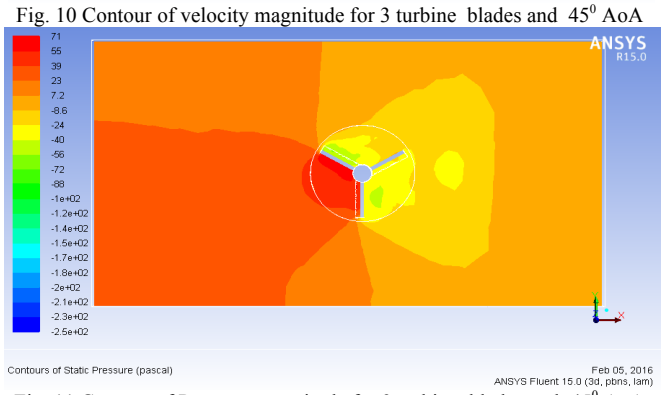


Fig. 11 Contour of Pressure magnitude for 3 turbine blades and 45^0 AoA

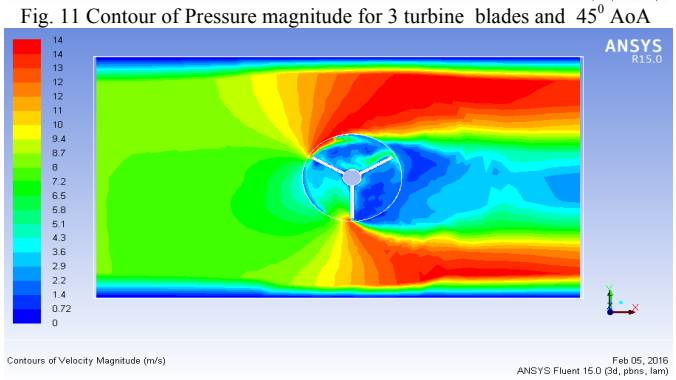


Fig. 12 Contour of velocity magnitude for 2 turbine blades and 90^0 AoA

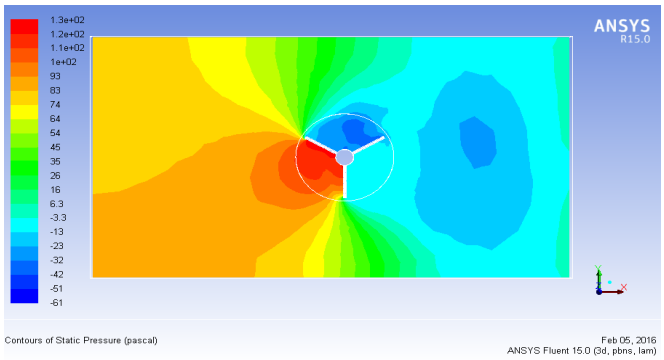


Fig. 13 Contour of Pressure magnitude for 3 turbine blades and 90^0 AoA

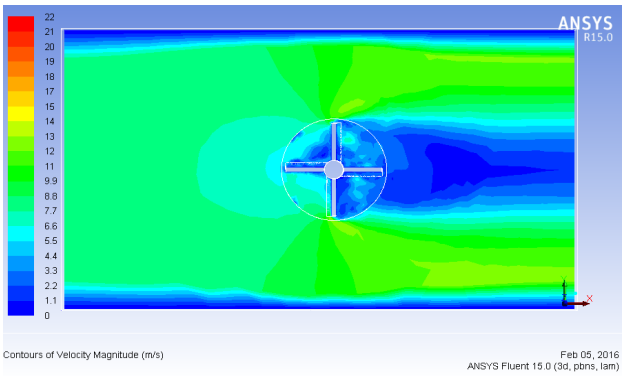


Fig. 14 Contour of velocity magnitude for 4 turbine blades and 45^0 AoA

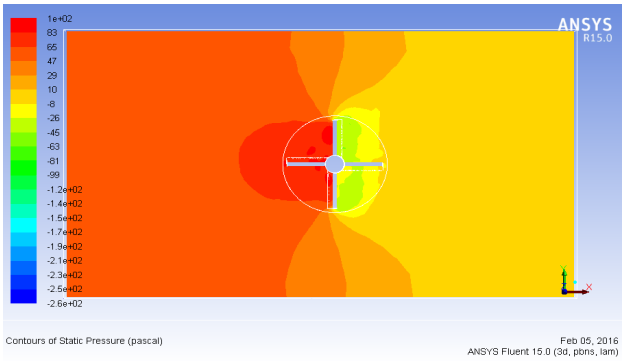


Fig. 15 Contour of Pressure magnitude for 4 turbine blades and 45^0 AoA

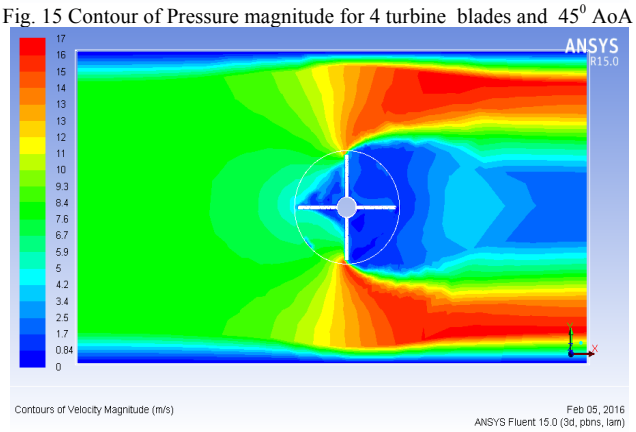


Fig. 16 Contour of velocity magnitude for 4 turbine blades and 90^0 AoA

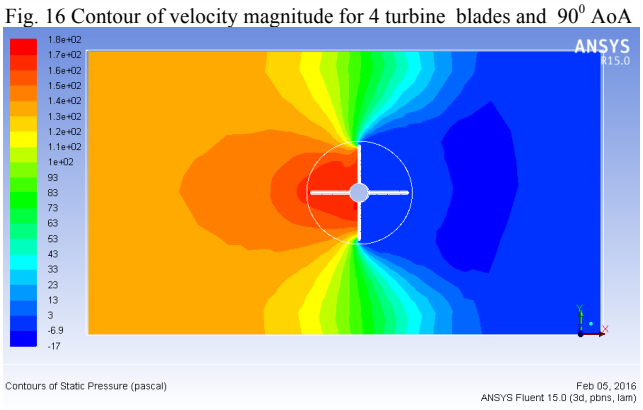


Fig. 17 Contour of Pressure magnitude for 4 turbine blades and 90^0 AoA

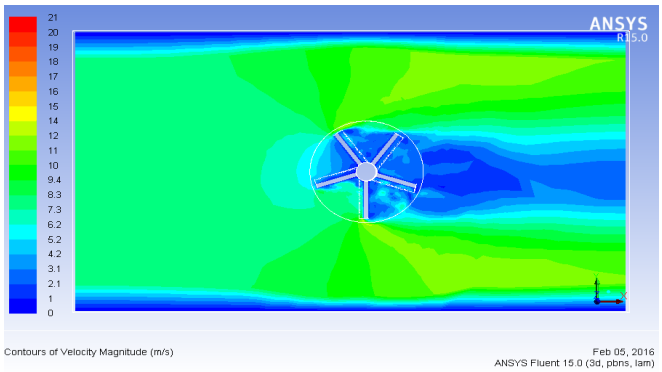


Fig. 18 Contour of velocity magnitude for 5 turbine blades and 45^0 AoA

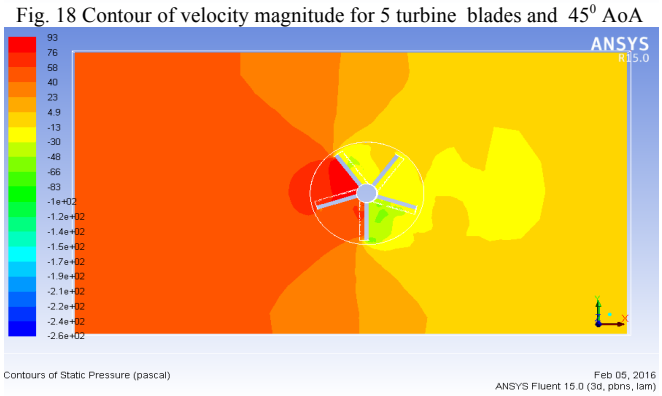


Fig. 19 Contour of Pressure magnitude for 5 turbine blades and 45^0 AoA

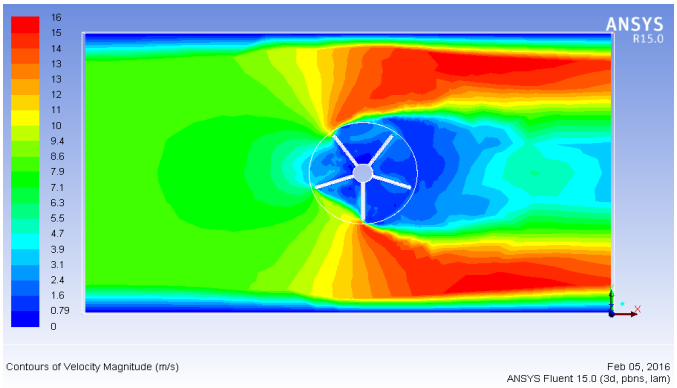


Fig. 20 Contour of velocity magnitude for 5 turbine blades and 90^0 AoA

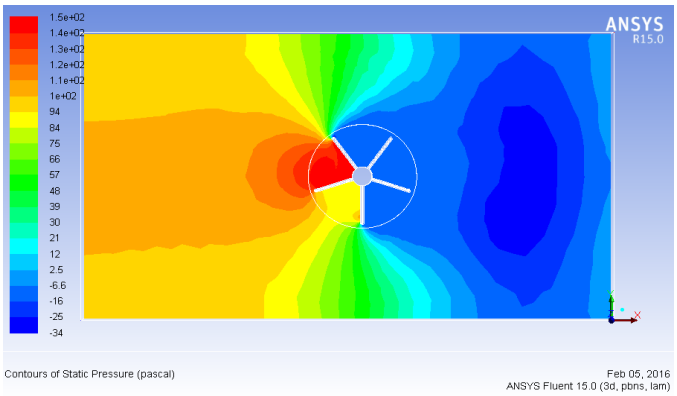


Fig. 21 Contour of Pressure magnitude for 5 turbine blades and 90^0 AoA

5. Conclusion

1. This computational study has achieved to evaluate optimization design for integrated VAWT blades rotor for axial movable wind turbine by changing some angle of attact and total number of blades and the resulted optimum angle of attact is ninety degrees with five turbin blades.
2. The optimum total number of blades are continue to be used to buid up / made the prototype.

References

[1] Contained Energy, Hanraads *A Guidebook to Renewable Energy.* : http://www.containedenergy.com, 2010

[2] Hau Eric. Wind Turbines: fundamentals, technologies, application, economics. 2 nd ed. Berlin : Heidelberg; 2006.

[3] Wirachai Roynarin. *Optimation of Vertical Axis Wind Turbine*. In: Jones BS, Smith RZ, editors.

[4] Hugg Piggots. *How to Build Wind Turbine: The Axial flux Windmill,* 2005

[5] Suryaman Maman. *Pembuatan dan Pengujian Turbin Angin dengan memanfaatkan kecepatan angin truk yang berjalan*", ITI Serpong, 2013

The Annual Conference on Management and Information Technology (ACMIT) 2016

Study of PET Spectral Absorbance in Designing Infrared Heating Control of Vacuum Forming Machine

Elizabeth Steffina Grafita*
Faculty of Engineering and Information Technology, Swiss German University, BSD – City, Tangerang 15339, Indonesia

Abstract

Heating process is the first step in vacuum forming that transforms the plastic sheet from its glassy state to rubbery state, pliable enough to be formed to mold's shape. Infrared ceramic heaters with zoning control are commonly used in thermoforming industry, in which temperature distribution and its consistency throughout processing time become very important in determining the thickness and properties of manufactured parts. Compared to other thermoplastics, Polyethylene Terephthalate (PET) with its crystallization characteristics is known to have narrower process window. Slight uneven temperature distribution and overheating will degrade PET as well as cause visible defects in final product. In order to obtain proper parameter setting of infrared ceramic heater in PET vacuum forming, a numerical approach that considers PET spectral absorbance was deployed and two methods to control temperature were compared. The experiment resulted in a reliable temperature distribution by means of voltage potentiometer control for pre-heating and implanted thermocouple inside ceramic emitter for main heating in PET vacuum forming machine.

Keywords:PET spectral absorbance; infrared heating control; vacuum forming

1. Introduction

PET (Polyethylene terephthalate) is a semi-crystalline thermoplastic made by combining either terephthalic acid or dimethyl terephthalate acid with ethylene glycol [1]. Due to its favorable properties (clarity, toughness, and recyclability), PET has dominated packaging industry for the last decade, especially for beverage bottles, food and fresh products' trays, blister packs, etc [2]. All of these products are manufactured by thermoforming process that involves heating a plastic sheet heated above the softening point or glass transition temperature (T_g) but below its melting point (T_m), then stretching the heated sheet over or inside a mold cavity by rapid application of force [3].

Heating is the most important process for PET thermoformers, for it determines the quality of final product. Under-heating will result in failing to forming to the contours of the mold, while overheating leads to numerous problems including poor quality, visible haze, and brittle products [4]. For PET, T_g is between 67-80 °C and Tm range is between 248-267 °C, while the rate of crystallization (T_c) starts from 149-180 °C [5,6] up to high crystallization at 220-230 °C [7]. Therefore, it is crucial to maintain PET's proper forming temperatures at 140-149°C [3,4].

Non-contact heating oven with infrared ceramic heaters is commonly used for vacuum forming due to its highest radiant efficiency (96%) compared to quartz tube, quartz lamp, and flat faced panels [8]. Ceramic infrared heats objects not the air, so energy is not wasted on trying to heat the air in an open conveyor type oven, as would convection style heating elements. Another benefit is that in an enclosed heating application, objects is heated faster because heat absorbed on the object's surface by radiation will further be reinforced by convection [9]. This can only be achieved if infrared radiation is fully absorbed, instead of reflected or transmitted. It is important therefore to first consider infrared spectral absorbance of PET and then to match it with suitable control of emitter source.

Simulation and modeling of infrared heating for thermoplastics had been the subjects of many research with the objective to control product's wall thickness, either for deep draw thermoforming of

polystyrene [10] or blow molding of PET bottles [11]. A thorough study by Cosson [12], Champin [13], and Bordival [14] explored and elaborated ray tracing method, 3D modeling, as well as numerical optimization to simulate temperature distribution and solve heat balance equation in heating process. This further supported the importance to understand object's spectral absorbance in designing effective and efficient infrared heating system for industry use.

Nomenclature

ρ	amount of infrared energy reflected from a surface
α	amount of infrared energy absorbed by a surface
τ	amount of infrared energy transmitted from a surface
e	emissivity value of infrared source
W_s	total radiant energy emitted from a source at temperature T_1
W_{bb}	total radiant energy from a blackbody at temperature T_1
λ	wavelength of electromagnetic energy
$R(\lambda)$	radiation from a blackbody source given at a certain wavelength
σ	Stefan-Boltzmann constant (36.58072×10^{-12} W/in^2.°K
T	surface temperature of the source in K (Kelvin)
T_g	glass transition temperature
T_m	melting temperature
T_c	crystallization temperature
λ_m	peak wavelength in meters, T_k is temperature in Kelvin

4.1.22 Literature Study

Infrared (IR) is invisible radiant energy, part of electromagnetic spectrum with longer wavelengths than those of visible light, extending from the nominal red edge of the visible spectrum at 700 nm to 1 mm [15]. When infrared energy strikes a non-opaque (transparent) object it may be absorbed, transmitted, or reflected from the surface. The sum of the amount of energy that is absorbed, transmitted, and reflected must equal 100% of the total incident energy [8, 16], as denoted by equation (1).

$$\rho+\alpha+\tau = 1 \tag{1}$$

Emissivity value governs the efficiency of a radiant heater, since it specifies how well a certain real body radiates energy as compared with a blackbody [16]. It is defined as the ratio of the radiant energy emitted by an object at a given temperature and the radiant energy emitted by a blackbody at the same temperature [8]. Emissivity value can be obtained through equation (2). For non-metals like plastic, normal emissivity value is about 0.90 - 0.95 depending on color [8, 17].

$$e = \frac{W_s}{W_{bb}} \tag{2}$$

Planck's Law gives us the spectral distribution of radiation from a blackbody source as denoted in equation (3), i.e. a source that emits 100% infrared radiation at a given single temperature. In practice however, infrared sources are made up of thousands of so-called point sources that are all at different temperatures, with each of them has different spectral distribution. The combination of these point sources will make up the entire spectral distribution which can only be estimated using an average surface temperature and emissivity value [8].

$$R(\lambda) = \frac{e\times 2.416069\times 10^{-25}\ Watts}{\lambda^5\left[exp^{\frac{.014408}{\lambda T}}-1\right] in^2.\mu m} \tag{3}$$

By integrating/summing over frequencies in Planck's radiation law (3), one obtains Stefan-Boltzmann's Law, that states the total radiated energy R(T) per unit surface area, emitted by a blackbody is proportional to T^4 [18].

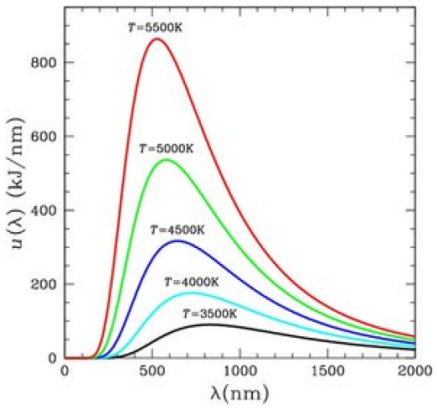


Fig. 1 Spectral distribution of a blackbody at various temperatures [13]

In other words, Stefan-Boltzmann Law gives the total power radiated at a specific temperature from an infrared source at all associated wavelengths (4).

$$R = e\times\sigma\times T^4 \tag{4}$$

Fig.1 shows that as the temperature of the source increases, then the peak wavelength of the source becomes shorter. When the temperature of the source becomes very high, a significant amount of

energy is emitted from the source as light. Wien's Law (5) gives the wavelength at which the spectral distribution (given by Planck's Law) of the radiation emitted by a blackbody is at a maximum point or simply, the peak wavelength [8].

$$\lambda_m = \frac{2.898 \times 10^{-3}}{T_k} \ (mK) \tag{5}$$

Research that had been dedicated to the searching of optimum control of infrared heating oven for thermoforming includes the deployment of commercial, numerical software package and fault tolerance technology [19, 20]. The common ground of those studies is based on the advantage of zoning control, wherein a specific, different temperature zone is imposed on the plastic sheet with the intention of affecting a more uniform stretch in the final part. Individually controlled element and careful control of zone's thermal gradients allows for smooth thickness variations from point to point in the final formed part, because lower temperature will be applied on mold location that requires less stretch and vice versa [21].

Similar concept was become the basis for use in this research, by taking PET blister vacuum forming as a case study.

4.1.23 Research Methodology

The research focus is aimed at obtaining optimum design and control of ceramic heating oven for PET vacuum forming. Ceramic heaters are made with a resistance wire trapped within a ceramic shell. When a current is sent through the wire, the wire heats up and subsequently also heats up the ceramic body and gives off both convection and radiant heat [17].

3.1 Setup of heater array panel

In setting up heating oven with ceramic emitters, the choice of emitter face styles depends on the application. Since a uniform pattern for even heating is desired and the distance between emitter and the target is at close proximity, flat surface emitter with radiant emission pattern as in Fig. 2 was selected [8].

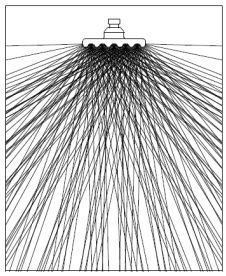


Fig. 2 Uniform radiant pattern of flat face ceramic emitter [8]

It was also highly recommended that to achieve an even heat pattern, the emitters are spaced so that their radiant emission patterns overlap when reaching the target. The more pattern overlap that occurs, the more even the heat will be across the face of the product being heated [8]. As Fig.3 illustrate with 50mm-wide emitter, the area of highest radiant emission intensity for a single emitter is shown within the two dark crossed lines on the grid. However in this particular study, by taking sheet size consideration into account, there were 3 sizes of emitters used, i.e. 60 mm x 120 mm, 60 mm x 245 mm, and 120 mm x 120 mm, arranged in 25mm spacing (Fig.4). By using similar concept, element emissions would be maximized at a distance of 100 mm (4 inch) from targeted object (PET sheet).

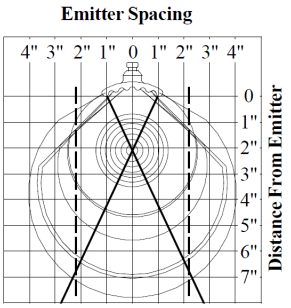


Fig. 3 Relationship between emitter spacing and emission patterns [8]

Considering crystallization behavior of PET [5,6,7], the heating process were divided into two stages which were pre-heating and main heating. Pre-heating panel positioned on the top of plastic sheet would warm PET from ambient temperature of 25°C to 80°C. Main heating was comprised of two panels on top and bottom of PET sheet to ensure radiation overlap and even distribution of forming temperature. Both panels were set up to heat PET from 80°C to 140°C.

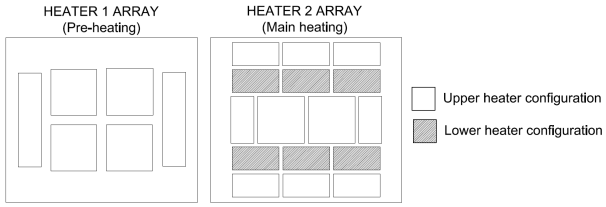


Fig. 4 Array of ceramic emitter configuration in heating panel

3.2 Estimating required power density of emitter source

Although in a given heating system any or all of the three modes of heat transfer (convection, conduction, radiation) should be taken into account, the calculation was done under the assumption that 100% of the heat transfer is by infrared radiation and any heat losses are considered to be negligible. The energy required to heat the PET sheet is given by Eq. (6).

$$\text{Energy density}\left(\frac{\text{Watt.Hour}}{\text{in.}^2}\right) = \frac{(\text{Material weight})(\text{Specific heat})(T_2 - T_1)}{3.412 \text{ BTU per Watt.Hour}} \tag{6}$$

In addition, since the ceramic emitters are known to be relatively slow responding, a warm up time also needs to be included in the equation.

$$\text{Power density}\left(\frac{\text{Watt}}{\text{in.}^2}\right) = \frac{\text{Power density}\left(\frac{\text{Watt.Hour}}{\text{in.}^2}\right) \times 3600 \text{ sec/hr}}{\text{Warm-up Time}} \tag{7}$$

By superimposing Planck's Law curve on spectral absorption curve for PET, the power radiated and absorbed equals to the total area under the curves at which the two curves intersect. The calculation can be extremely time consuming and requires that accurate curves is made available. A much simplified method is provided to estimate the power radiated and absorbed, that is the effective emissivity between two parallel plates (8).

$$e = \frac{1}{(1/e_1 + 1/e_2 - 1)} \tag{8}$$

In the case where two panels are used on top and bottom of the sheet, the power required per panel will be halved. This two-side heating is advantageous since it will minimize the temperature gradient within the sheet which could cause deformation in finished blister [8].

From Stefan-Boltzmann Law, one can then calculate the minimum surface temperature required for the emitter to heat up the plastic within desired cycle time (9).

$$T_2 = \sqrt[4]{\frac{R/_2}{e \times \sigma} + \left(T_1{}^4\right)} \tag{9}$$

3.3 Control of ceramic emitters

The methods to control ceramic emitters can be categorized as either non-feedback or feedback control. In non-feedback, the temperature can be controlled by: (1) a percentage-on/percentage-off duty cycle with timer; or (2) through voltage potentiometer control that regulates the amount of voltage the emitters are receiving. With feedback control, a thermocouple is used to measure the temperature of the element's coil or, more accurately, the surface temperature of the element. A type K thermocouple is most commonly used because of its 0-2000° F temperature range and because it is able to be casted into the emitter where it measures the actual internal element temperature [9].
Both feedback and non-feedback control are implemented in the study with wiring diagram as shown in Fig.5 below.

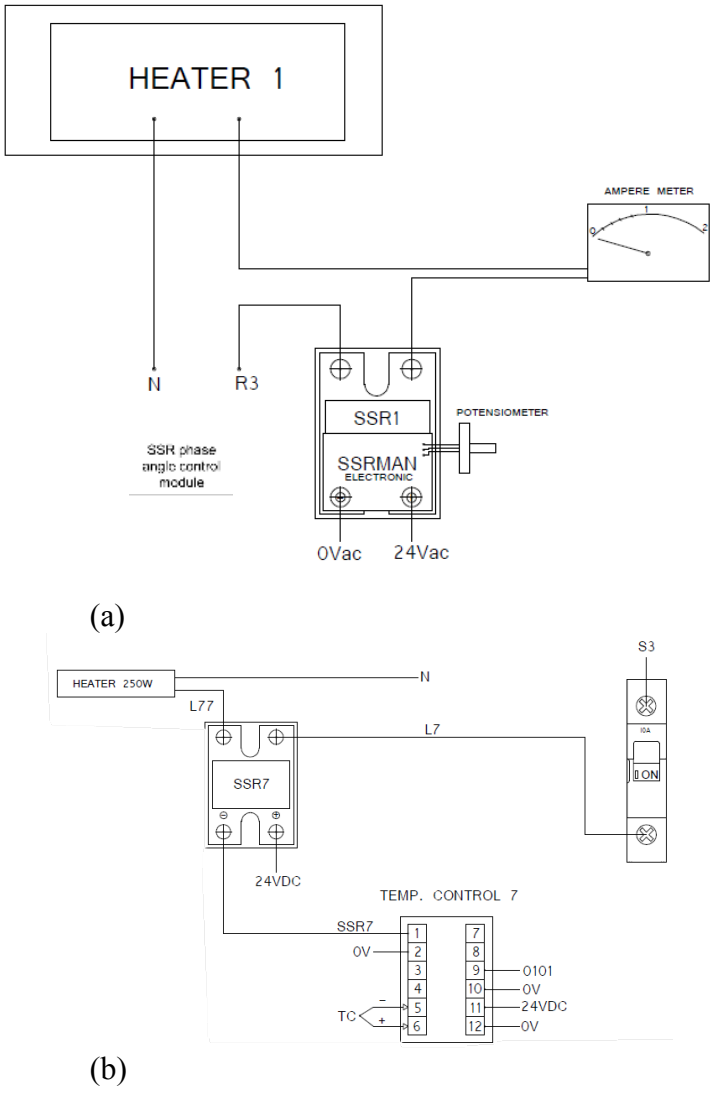


Fig. 5 Ceramic heater wiring diagram: (a) Non-feedback control with voltage potentiometer and (b) Feedback control with implanted thermocouple inside ceramic element.

4.1.24 **Discussion and Analysis**

In plastics processing, main point of interest is in the portion of the infrared spectrum from about 0.1 - 100 µm as this is the region in which most of radiated energy be used to heat up the plastic. Referring to spectral absorption of PET [14], the greatest absorption is between six and ten microns with a notable, narrow absorption point at about 3.7 microns.

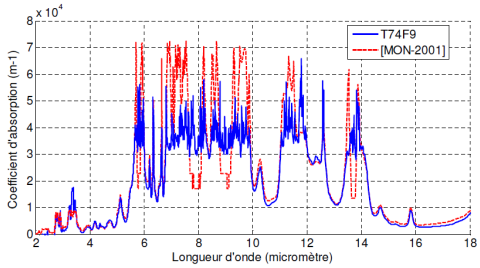


Fig. 6 Bordival's spectral absorption curve for PET [14]

The amount of energy radiated by a heater and the wavelength of this energy is determined by a heater's temperature and the surface area exposed [12]. This is where Stefan-Boltzmann and Planck's radiation law comes into play, in determining both required surface temperature of infrared source to emit the desired wavelength and power density absorbed by target object. Since only energy that is absorbed will be useful in heating up the plastic, the more area we can get under the plastic absorption curve, the more efficient a heater is [12].
As Fig.7 shows, when Planck's spectral radiancy curve is superimposed on PET's spectral absorption, the plastic is either efficient or inefficient at absorbing this energy. It is worth noting that increasing emitter's surface temperature does not necessarily relate in proportion with radiant absorption since the peak wavelength given by Wien's Law will shift to the left side of the curve, without any increase in absorption at all. The observed phenomenon was that the emitter might be so hot that it glowed and emitted visible light, but the radiation was not absorbed by the target. Furthermore, the convection heat would be so high and the plastic was scorched to the point of melting.

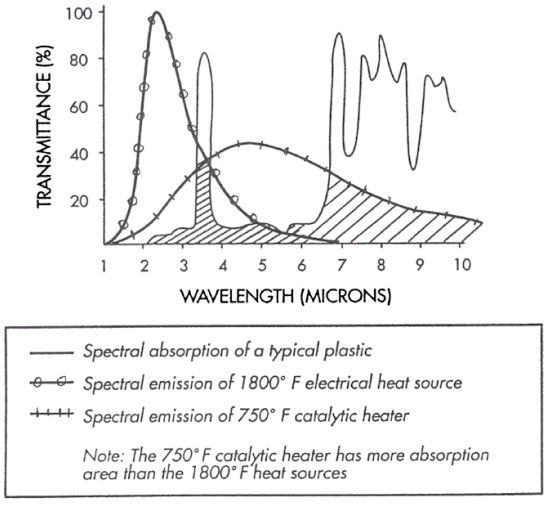


Fig. 7 Energy absorbed by a typical plastics at various wavelengths [17].

Back to the case at hand, the application required that a 0.5mm thick PET sheet be heated to 140°C in cycles of 10 seconds. Using Eq. (6) to (9) gave results as in Table 1.

Table 1. Calculated emitter surface temperature and required power	Emitter surface temperature (°C)	Ceramic heater size L x W (mm)	Power required (Watt)	Power of available standard emitter (Watt)
Pre-heating	338.61	120 x 120	86.05	150
		245 x 60	87.85	150
Main heating	384.13	120 x 120	109.52	150
		120 x 60	54.76	125

Considering that heat loss was inevitable in actual practice and there would be high probability that the vacuum forming module will process PET materials with different thicknesses ranging from 0.4 to 0.6 mm, the preference was to use ceramic emitter with the next closest, higher power specification available in industry standard. To compensate the higher power of emitter's maximum radiancy, both non-feedback and feedback control was deployed.
Ceramic heater with embedded thermocouple was used for the main heating that operates near crystallization temperature of PET, where any temperature shift was critical and needed more accurate control. On the other hand, with less number of emitters whose function is more to warming up PET to its glassy temperature, pre-heating will use voltage control with adjustable potentiometer.

4.1.25 Conclusion

Through the understanding of PET spectral absorbance and its thermal properties, the suitable infrared emitter for blister forming application is flat-faced ceramic heater whose emitted infrared radiation covers the medium and long-wave infrared range of 2 - 10 µm. Method to calculate required power density and surface temperature of emitter were presented. SSR phase angle control module is used as non-feedback control for pre-heating, while feedback control embedded inside ceramic emitter is utilized for main heating. Zoning control further ensured PET was heated within its forming temperature as well as prevented crystallization to occur. Individually controlled emitter also allowed flexibility for various PET sheet thickness and width size. Fig.8 gives the optimum temperature setting for PET sheet 0.4mm thickness.

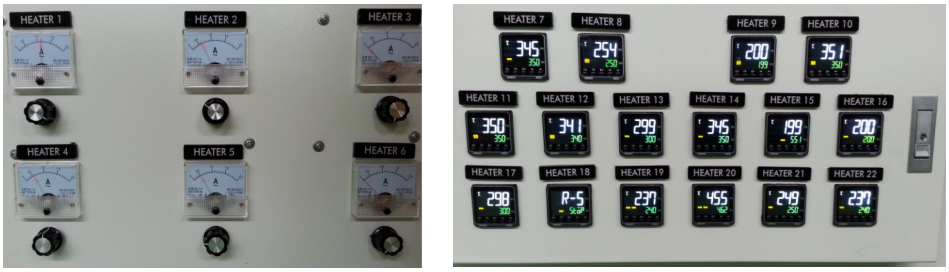


Fig. 8 Non-feedback and feedback control for ceramic heaters in PET vacuum forming application.

References

[1] D. Parthasarathy Pattabiraman, I. Sbarski, and T. Spurling, "Thermal and Mechanical properties of recycled PET and its blends," ANTEC 2005.

[2] NAPCOR White Paper. PET Features, Benefits & Information Resources. Retrieved from http://www.napcor.com on March 6, 2016.

[3] James. L. Throne, Technology of Thermoforming. Hanser/Gradner Publications, (1990).

[4] Koester, Larry, Sheila Nemeth, and Mark Koester. (2003). Thermoforming & Die Cutting of Recycled/Virgin PET Sheet (PETCO of Lavergne Group). Quebec, Canada: PET Article of Lavergne Group.

[5] Bila Demirel, Ali Yaras, Huseyin Elclick. Crystalization Behaviour of PET, Bau Fe. Bil. Enst. Dergisi Cilt 13(1) 26-35 (2011)

[6] Amit Dharia. Thermoformability Analysis of PET sheets Using Novel Test Equipment. Transmit Technology Group, LLC, Irving, TX

[7] L. Baldenegro-Perez, D. Navarro-Rodriguez, F. Medellin-Rodriguez, B. Hsiao, C. Avila-Orta, and I. Sics, "Molecular Weight and Crystallization Temperature Effects on Poly(ethylene terephthalate) (PET) Homopolymers, an Isothermal Crystallization Analysis," Polymers, vol. 6, no. 2, pp. 583–600, Feb. 2014.

[8] Mor Electric Heating Association, Inc. Salamander Ceramic Infrared Emitters Technical Manual.

[9] https://www.infraredheaters.com/frequent.html. Retrieved on March 6, 2016.

[10] F.M. Schmidt, Y. Le Maoult, and S. Monteix, "Modelling of infrared heating of thermoplastic sheet used in thermoforming process," Journal of Materials Processing Technology, vol. 2003, no. 143–144, pp. 225–231.

[11] S. Monteix, F. Schmidt, Y. Le Maoult, R. Ben Yedder, R. W. Diraddo, and D. Laroche, "Experimental study and numerical simulation of preform or sheet exposed to infrared radiative heating," Journal of Materials Processing Technology, no. 119 (2001), pp. 90–97.

[12] Benoit Cosson, Fabrice Schmidt, Yannick le maoult, and Maxime Bordival, "Infrared heating stage simulation of semi-transparent media (PET) using ray tracing method," International Journal of Material Forming, no. March 2011.

[13] C. Champin, "Modélisation 3D du chauffage par rayonnement infrarouge et de l'étirage soufflage de corps creux en PET," École Nationale Supérieure des Mines de Paris, 2007.

[14] M. Bordival, "Modelisation et optimisation numerique de l'etape de chauffage infrarouge pour la fabrication de bouteilles en PET par injection-soufflage," École Nationale Supérieure des Mines de Paris, 2009.

[15] Liew, S. C. "Electromagnetic Waves". Centre for Remote Imaging, Sensing and Processing. Retrieved from www.wikipedia.com on 03/06/2016.

[16] Robert Siegel and John R. Howell, Thermal Radiation Heat Transfer, 3rd. Edition. Taylor & Francis, 1992.

[17] Boser, Leroy M. (2012). Thermoforming Manual and Troubleshooting Guide. Spartech Plastics.

[18] Claes Johnson, "Mathematical Physics of BlackBody Radiation." Icarus iDucation 2012, Nov-2011.

[19] Khoo Guan Soon, "An investigation of temperature control issues related to intelligent thermoforming," Lehigh University, Jan-2001.

[20] Zhen-Zhe Li, Tai-Hong Cheng, Yun-De Shen, and Dong-Ji Xuan, "Optimal Heater Control with Technology of Fault Tolerance for Compensating Thermoforming Preheating System," Advances in Material Science and Engineering, Hindawi Publishing Corporation, vol. 2015, no. Article ID 403730.

[21] Chao-Hsin Wang and Herman F. Nied, "Temperature Optimization for Improved Thickness Control in Thermoforming," Journal of Materials Processing and Manufacturing Science, no. October 1999.

The Annual Conference on Management and Information Technology (ACMIT) 2016

Small Indonesian Holding Company Of SME's : Study on The Value on IT Investment : PT.XYZ Core

Dodik. Novianto
Swiss German University
GSB Arcadia G17 Tangerang 15322
Indonesia
Doni_divayoga@yahoo.com

Abstract

This paper explains that in PT.XYZ as SMEs do not have the IT integrated . IT managers perform checks on the company and find the condition that it is true in the enterprise IT integrated yet. In this paper further research requires a comparison with conducting surveys and studies in several large holding company. This is what causes the difficulty to estimate the cost and benefits of information technology investment Compared to investment value. (Money et al., 1995) share the benefits the use of information technology into two kinds, tangible and intangible . This has the caused many organization have difficulty how to calculate the cost and benefit of the investment associated with the resulting benefits and using Val IT one of the solution to study on the value on IT investments in SMEs at PT.XYZ . Val IT is now, the realization of business value of a clear investment, measured monitoring, to provide a means to optimize, and add the best practices for the end.

Keywords: *SMEs; Value IT Framework.*

INTRODUCTION

Companies in this case an n SMEs which has multiple business. PT.XYZ IT managers get information from some of the staff in the company, that the company was in the running of the business transaction for the information technology sector is still not optimal Furthermore, IT managers follow up to check and found that the current conditions at XYZ Company is not optimal for the information technology sector, and for it takes the IT investment plans are uniform and can provide value to business development and other strategic matters. In this case the information technology has become the backbone of the company to achieve a competitive advantage. Therefore, many companies are having trouble estimating the benefits of information technology investment than investment value. This resulted in the importance of estimating how big the benefits derived from the information technology sector as compared to the investment. The benefits of information technology there is a measurable or not measurable, there are perceived benefits quickly, and after a certain period of time. This is what causes the difficulty to estimate the benefits of information technology investment compared to investment value. (Money et al., 1995) share the benefits the use of information technology into two kinds, tangible and intangible. The real benefits is that will directly affect the profitability of the company, either reduction or cost savings (cost) and increase revenue (income). Intangible benefit is defined as the positive benefits acquired by the company use of information technology, but have no correlation directly to profitability company. This has caused many organizations have difficulty how to calculate the cost and benefit of the investment associated with the resulting benefits and Val IT one of the solution for estimating the value of IT investments. Val IT provides a means to now clear , add the last of the best practices for the end, it provides a means for accurately measuring, monitoring and optimize the realization of business value from investment in IT(ITGI, 2006). In this research paper will be study on the value on IT investment at SMEs (PT.XYZ core)

CHALLENGES

In this study concentrates on the challenges facing the company or organization that does not have an integrated IT, particularly in IT in the company or organization to make changes that will occur when using IT investment plans. The purpose of this paper is the company will be relevant to use IT investment plan. When designing the research methodology, one important thing to decide is determining the appropriate framework. in this case the selected Val IT framework to study IT investment planning in SMEs. In this research question will be discussed on Value: Viewed from business goals to reach the target company becomes more optimal, how IT investment opportunities in order to see the needs of SMEs can still exist and see the challenges ahead ?

LITERATURE REVIEW

3.1 SME's Indonesian

Currently , the evolution of many small and medium sized enterprises (SMEs) business environment that is complex and also starts with globalization, the internationalization of markets, then innovation and based on the knowledge , greater efficiency , the need for effectiveness and competitive and knowledge. It has put an increase in the pressure on these companies management especially the manufacturing SMEs that must now compete globally (Cagliano and Spina, 2002).

3.2 SME's Challenges

SMEs wish to establish a corporate culture of sustainability, but face organizational realities such as a high turnover and disparities in employee awareness levels or willingness to act. The challenge for SMEs is to remain focused on sustainability within a dynamic context. Creating a sustainability policy is not enough; objectives must be clear, employees and management must show commitment through consistent actions and, little by little, a set of values and habits transcending the individuals of the organization can emerge. This is even more critical for SMEs, since time dedicated to the education of sustainability is limited. To optimize their activities, SMEs seek to establish a culture of sustainability that creates a cycle, strengthening the customs and sustainable value in the workplace. This promotion of sustainability involves all employees in the organization – not just a few (France, 2013).

1.3 IT adoption by SMEs

(Adeosun et al., 2008) found that the use of IT value positive for management strategies related to aspects of communication, access information, decision-making, data management and knowledge management in an organization . IT can be a force strategies and tools for organization that provide benefits to the promotional aspects and competitiveness forces (Buhalis, 2004).(Den Hengst and Sol, 2001) argues that IT provide benefits to business organizations to reduce costs and improve business organizations in coordination with outsiders. However, some researches the research that has been conducted reveal the fact that the adoption of IT in SMEs is still lower than expected (Chung et al., 2007).

3.4 *VAL IT*

Interest Val IT initiative includes research, publications and support services to help management understand the value of IT investments and ensure that the organization can obtain optimal value on IT investments in the context of the costs and the risks are acceptable. Val IT consists of guidelines, processes and some practical suggestions to help the parties management and executives to understand and fulfill their role in IT investment (INVESTMENTS, 2008).

Some of the benefits that can be gained from the implementation of Val IT are as follows:

1. Increase the understanding and on the basis of sufficient information, it costs due to management decisions, transparency of risks and benefits.

2. Increase the ability to select investments that have the greatest potential economic returns.
3. Increasing tendency of success in running the selected investments so that these investments can generate the intended benefits.
4. Stop the investment that does not generate the potential benefits to reduce the cost to do what needs to be done simply, immediately take the deal, or is expected. Reduce the risk of failure, especially high risk of failure.
5. Reduce the 'shock' associated with IT cost and delivery, thus increasing business value, reduce unnecessary costs and increase overall confidence in IT.

3.5 The VAL IT Initiative

Initiative is based on the experts and scholars, collective experience of existing practices and methodologies, and emerging team the research to develop the Val IT framework. Work of the team, including the selected organization to support the work of more initiative, are reviewed by a broader group of global advisors, it has been extended. Val IT is now obvious, the measurement and monitoring, to provide a means to optimize the realization of business value of IT investments, and add the best practices for the end. Val IT complements COBIT from a view of the business and finance, it will help all of the people who are interested in providing the value of IT (ITGI, 2006). As the initiatives evolves, it will include a number of types of research activities, Publications and grouped support services around the IT framework described in the text document, as illustrated in figure 1

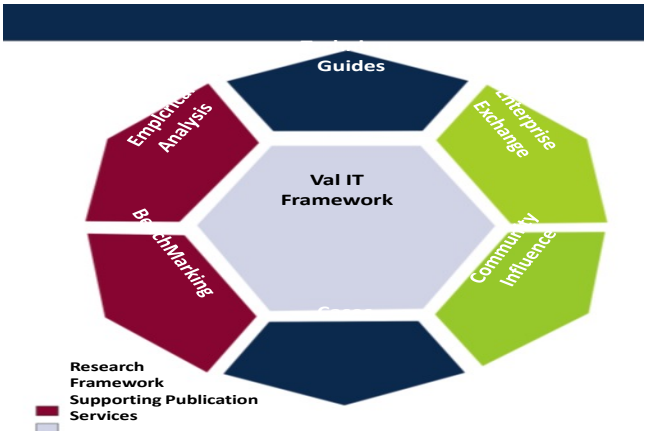


Figure 1: Val IT Initiative

3.6 Strategic Alignment of Business and IT

Strategic business alignment and IT IT strategic objectives of the investment company is defined as consistent with the (intended, the current strategy and business goals), and therefore to build the capacity necessary in order to provide "case" commercial value(ITGI, 2003, p. 22)

3.7 Delivery of Value from IT Systems

Delivery of value from IT systems has been defined as" the on-time and of appropriate quality budget delivery, the inner throat achieves the benefits that were promised"(ITGI, 2003, p. 24). This important component of ITG process, aims to make sure that the IT resources to provide maximum business value. Since the organization is investing in large-scale IT systems in the past 10 years, this issue has become more important. Board and other stakeholders, as part of their governance process, trying to determine the value escape from these large-scale investment.

3.8 Val IT Framework

Over the years the management team has struggled to achieve both short-term profits and long-term survival and growth of the company for that company needs a mature IT investment planning. To calculate the estimated value of the investment, there are several models and one that can be used include one Val IT Framework. The Val IT Framework is a comprehensive framework and pragmatic that enables the creation of business value from IT-enabled investment possibilities. Designed to align with and complement COBIT, Val principle and integrates a series of processes that are proven to support guidelines help practice IT governance, the practices and board, Management team of executives and other business leaders, optimize the realization of value from IT investments.(IT Governance, 2008)

3.9 IT/Enterprise Alignment(Davis, 2008)

Board, must be driven by the integrity of the business:

- Ensure that is aligned with the business strategy of the IT strategy.
- Measure and determine the delivery of its IT to the strategy through a clear understanding.
- Directing IT strategy in order to take the balance of investment between the support and the growth of the company.
- We examined a decision about where to concentrate the making IT resources.

4.0 Val IT Processes

For investment income, Val IT principles, should be applied by the effective interest groups IT investment in the following process(ITGI, 2006) :

- Value Governance
- Portfolio Management
- Investment Management

RESEARCH METHODOLOGY

This study uses qualitative research using a case study approach, in which researchers carefully an activity, process or group of individuals. This is consistent with the qualitative method according to Bogdan & Taylor (Lexy, 2002) Definition of qualitative methods, such as a research procedure that produces descriptive data in the observed writing and speech in the form of actions and people. This research aims of this study How IT investment in SMEs is getting the benefits and optimal results in tune with the company's business goals and targets.

The subject of this research is to conduct research in SMEs (PT.XYZ), which in Companies included in the SME, there are several subsidiary companies with several different characteristics. Characteristic in this company is different, because there are several different forms of business among existing hospitality, suppliers of medical equipment, IT maintenance and partners with the government, which is still a lack of facilities at the company's IT infrastructure.

3.1 Data Collection

The data source here, namely SMEs in the parent company with subsidiaries, which are both unsupported and supported with IT infrastructure data retrieval are good sign .The place in scattered locations in Jakarta and the SME Solo. For this study requires Study on The Value at IT Investment.

3.2 Data analysis

Data analysis by organizing the data, synthesize, choose what is important and make conclusions.

RESULTS AND DISCUSSION

This section describes the SMEs that are the focus of this study. SMEs which is the object of this study is SMEs engaged in Several business units. Data was obtained through interviews with

management and executive ranks XYZ core. Each of Different divisions of the company are given some questions questionaire prepared by the researchers by giving some question questionnaire prepared by the researchers outline consists of 10 questions. This research was conducted area in Jakarta and Solo. Result from discussion with management that SMEs at PT.XYZ inadequate and support , but SMEs are aware of the role and benefits of information technology to support the business of the company.

CONCLUSION

Based on the analysis and discussion of the results, the conclusions of this study can be expressed as follows:

1. SME IT adoption in PT.XYZ inadequate and support, for it to support the performance of the business is run currently required IT investment.

2. Although SMEs in PT XYZ is still inadequate, but SMEs are aware of the role and benefits of information technology to support the business or the business of the company.

3. Use of Information Technology by SMEs in PT.XYZ still not optimized to deliver more strategic value to the development effort.

4. Utilization of Information Technology by SMEs in PT.XYZ is very much needed. This shows that in fact, businesses already have a strategic view in an effort to maintain good relations with customers, informing business or business to another party to seek information.

REFERENCES

Adeosun, O., Adeosun, H., Adetunde, A., Adagunodo, R., 2008. Strategic application of information and communication technology for effective service delivery in banking industry, in: Computer and Electrical Engineering, 2008. ICCEE 2008. International Conference on. IEEE, pp. 135–140.

Buhalis, D., 2004. eAirlines: strategic and tactical use of ICTs in the airline industry. Inf. Manage. 41, 805–825.

Cagliano, R., Spina, G., 2002. A comparison of practice-performance models between small manufacturers and subcontractors. Int. J. Oper. Prod. Manag. 22, 1367–1388.

Chung, W.W., Hua Tan, K., Lenny Koh, S., Pavic, S., Koh, S., Simpson, M., Padmore, J., 2007. Could e-business create a competitive advantage in UK SMEs? Benchmarking Int. J. 14, 320–351.

Davis, P.T., 2008. Understanding Val IT.

Den Hengst, M., Sol, H.G., 2001. The impact of information and communication technology on interorganizational coordination, in: System Sciences, 2001. Proceedings of the 34th Annual Hawaii International Conference on. IEEE, p. 10–pp.

France, M., 2013. SME sustainability challenges.

INVESTMENTS, O., 2008. ENTERPRISEVALUE: GOVERNANCE OF IT INVESTMENTS.

ITGI, P. 22, 2003. Strategic Alignment of Business and IT.

ITGI, R.M., IL 60008 USA, 2006. Enterprise Value :Governance of IT Investments,The Business Case.

IT Governance, I., 2008. Enterprise Value: Governance of IT Investments, the Val IT Framework, Version 2. 0. ISACA.

Lexy, J.M., 2002. Metode Penelitian Kualitatif. Bdg. PT Remaja Rosdakarya.

Money, A.H., Twite, A., Remenyi, D., 1995. Effective Measurement and Management of IT Costs and Benefits.

The Annual Conference on Management and Information Technology (ACMIT) 2016

Simulation and Analysis of Two-Mass Suspension Modification Using MATLAB Programming

Hendry D. Chahyadi
Swiss German University, EduTown BSD City, Tangerang 15339, Indonesia

Abstract

The designs of automotive suspension system are aiming to avoid vibration generated by road condition interference to the driver. This final project is about a quarter car modeling with simulation modeling and analysis of Two-Mass modeling. Both existing and new modeling are being compared with additional spring in the sprung mass system. MATLAB program is developed to analyze using a state space model. The program developed here can be used for analyzing models of cars and vehicles with 2DOF.

The quarter car modelling is basically a mass spring damping system with the car serving as the mass, the suspension coil as the spring, and the shock absorber as the damper. The existing modeling is well-known model for simulating vehicle suspension performance. The spring performs the role of supporting the static weight of the vehicle while the damper helps in dissipating the vibrational energy and limiting the input from the road that is transmitted to the vehicle. The performance of modified modelling by adding extra spring in the sprung mass system provides more comfort to the driver. Later on this project there will be comparison graphic which the output is resulting on the higher level of damping system efficiency that leads to the riding quality.

Keywords: Suspension; Overshoot; Settling Time; DOF, MATLAB

1. Introduction

This paper describes some principles on how car suspension system as a mechanism physically separates the body from the car wheels. The suspension purpose is to enhance driving comfort, road handling and vehicle stability. Apple Yard and Well Stead (1995) have proposed some performance characteristics that should be considered in order to achieve a good suspension system. [1].

Suspension consists of a system of springs, shock absorbers and connection from vehicle to wheels. In another definition, the suspension system is a mechanism that physically separates the underbody of the car wheels, with its main function to minimize the vertical acceleration transmitted to the passenger who directly provided with comfort road. Automobile suspension systems while using passive components can only offer a compromise between these two contradictory criteria by providing spring and damping coefficients at fixed rates [1].

Shock absorption in automobile is an important area of concern for the design engineers. Suspension system prevents shocks in automobiles which may be caused by irregular road profile, drag forces, drivetrain or engine vibrations, and wheel/tire non uniformity. Speed bumps and pot holes are most responsible for the vehicle body vibration through wheel/tire assembly and suspension system. Passenger comfort will be affected by overshoot and settling time of vehicle under vibration. MATLAB program has been developed to analyze the overshoot and settling time of a 2-DOF quarter car model. The analysis has used a current passive suspension system state space and new design model. This dynamic quarter car model can be utilized as the basis of analyzing the full car model response to speed bump [2].

Nomenclature

A	2-DOF quarter car model
B	suspension system
C	overshoot
D	settling time

4.1.26 Mathematical Model

Modelling in automotive suspension is an important part for automotive and vibration engineers, since vehicles ride quality is the most concern for the engineers when a vehicle passes over the speed bump. The analysis of this 2-DOF quarter car model (Figure 1) has been developed based on the following assumptions [1]:

- Vehicle is rigid body with the suspension
- Suspension consists suspension spring, absorber, sprung, un-sprung mass of the body
- Tire stiffness and tire absorptivity is considered separately

Parameters used for mathematical modelling are as follow:

m_1 = sprung mass or body mass (250 kg)
m_2 = un-sprung mass (40 kg)
c_1 = suspension damper damping coefficient (1,917 N.m/s)
k_1, k_2 = suspension spring stiffness (1.5 x 10^4 N/m)
k_3 = tire stiffness (1.5 x 10^5 N/m)
x_1 = sprung mass vertical movement
x_2 = un-sprung mass vertical movement
y = Road input (height of speed bump)

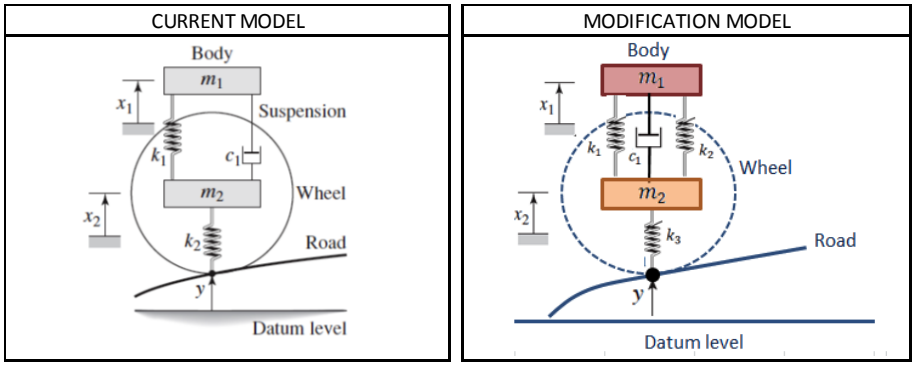


Figure 15. Two-Mass Suspension on Current and Modified Models

The equations of motion of two-mass suspension models are as shown below:

$$m_1\ddot{x}_1 = k_1(x_2 - x_1) + k_2(x_2 - x_1) + c_1(\dot{x}_2 - \dot{x}_1) \quad (1)$$

$$m_2\ddot{x}_2 = -k_1(x_2 - x_1) - k_2(x_2 - x_1) - c_1(\dot{x}_2 - \dot{x}_1) + k_3(y - x_2) \quad (2)$$

Equations of the motions can be expressed in state-variable form by determining that:

$z_1 = x_1$
$z_2 = \dot{x}_1$
$z_3 = x_2$
$z_4 = \dot{x}_2$

Furthermore, equations of motion are defined as follow:

$$\dot{z}_1 = \dot{x}_1 = z_2 \quad (3)$$

$$\dot{z}_2 = \ddot{x}_1 = \frac{1}{m_1}\left(k_1(x_2 - x_1) + k_2(x_2 - x_1) + c_1(\dot{x}_2 - \dot{x}_1)\right)$$
$$= \frac{1}{m_1}\left(k_1(z_3 - z_1) + k_2(z_3 - z_1) + c_1(z_4 - z_2)\right)$$
$$= \frac{1}{m_1}\left((k_1 + k_2)z_3 - (k_1 + k_2)z_1 + c_1(z_4 - z_2)\right)$$
$$= \tfrac{1}{m_1}(-(k_1 + k_2)z_1 - c_1z_2 + (k_1 + k_2)z_3 + c_1z_4) \quad (4)$$

$$\dot{z}_3 = \dot{x}_2 = z_4 \quad (5)$$

$$\begin{aligned}\dot{z}_4 = \ddot{x}_2 &= \frac{1}{m_2}\left(-k_1(x_2 - x_1) - k_2(x_2 - x_1) - c_1(\dot{x}_2 - \dot{x}_1) + k_3(y - x_2)\right)\\ &= \frac{1}{m_2}\left(k_1(x_1 - x_2) + k_2(x_1 - x_2) + c_1(\dot{x}_1 - \dot{x}_2) + k_3(y - x_2)\right)\\ &= \frac{1}{m_2}\left((k_1 + k_2)x_1 - (k_1 + k_2)x_2 + c_1(\dot{x}_1 - \dot{x}_2) + k_3(y - x_2)\right)\\ &= \frac{1}{m_2}\left((k_1 + k_2)z_1 - (k_1 + k_2)z_3 + c_1(z_2 - z_4) + k_3(y - z_3)\right)\\ &= \tfrac{1}{m_2}\left((k_1 + k_2)z_1 + c_1 z_2 - (k_1 + k_2 + k_3)z_3 - c_1 z_4 + k_3 y\right)\end{aligned} \quad (6)$$

Above equations are expressed in vector-matrix form by $\dot{z} = Az + By(t)$, where:

$$\dot{z} = \begin{bmatrix}\dot{z}_1\\ \dot{z}_2\\ \dot{z}_3\\ \dot{z}_4\end{bmatrix}$$

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ \frac{-(k_1 + k_2)}{m_1} & \frac{-c_1}{m_1} & \frac{(k_1 + k_2)}{m_1} & \frac{c_1}{m_1} \\ 0 & 0 & 0 & 1 \\ \frac{(k_1 + k_2)}{m_2} & \frac{c_1}{m_2} & \frac{-(k_1 + k_2 + k_3)}{m_2} & \frac{-c_1}{m_2} \end{bmatrix}$$

$$B = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \frac{k_3}{m_2} \end{bmatrix}$$

$$z = \begin{bmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{bmatrix} = \begin{bmatrix} x_1 \\ \dot{x}_1 \\ x_2 \\ \dot{x}_2 \end{bmatrix}$$

By simplifying the notation, the equations defined as:

$$a_1 = \frac{(k_1 + k_2)}{m_1}$$
$$a_2 = \frac{c_1}{m_1}$$
$$a_3 = \frac{(k_1 + k_2)}{m_2}$$
$$a_4 = \frac{c_1}{m_2}$$
$$a_5 = \frac{k_3}{m_2}$$
$$a_6 = a_3 + a_5 = \frac{(k_1 + k_2 + k_3)}{m_2}$$

Therefore, matrices A and B are becoming:

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -a_1 & -a_2 & a_1 & a_2 \\ 0 & 0 & 0 & 1 \\ a_3 & a_4 & -a_6 & -a_4 \end{bmatrix} \quad B = \begin{bmatrix} 0 \\ 0 \\ 0 \\ a_5 \end{bmatrix}$$

The next step is selecting appropriate values for the matrices in the output equation for $y = Cz + Dy(t)$. The displacement or vertical movement of system suspension is executed by plotting x_1 and x_2, of which for the area z_1 and z_3, we determine the following matrices for C and D below:

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad D = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

In regard to the velocity of system suspension, for plotting $\dot{x}_1$ and $\dot{x}_2$, of which area z_2 and z_4, we are using the following matrices for C and D as shown below:

$$C = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad D = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

4.1.27 Program Development (MATLAB)

MATLAB can be utilized to solve the ordinary differential equations of linear and nonlinear type. The 2-DOF quarter car model MATLAB programs in this paper are developed to analyze sprung and un-sprung mass displacement and velocity also for the suspension travel responses in suspension system when the vehicle passes over a speed bump [1]. Input parameters to be analyzed are as shown in Table 1.

Table 1. Input Parameters to Analyze Sprung and Un-sprung Mass Displacement and Velocity

Input Parameters	Symbol	Value
1. Sprung mass or body mass	m_1	250 Kg
2. Un-sprung mass	m_2	40 Kg
3. Suspension damper damping coefficient	c_1	1,917 N.m/s
4. Suspension spring stiffness	k_1, k_2	1.5 x 10^4 N/m
5. Tire stiffness	k_3	1.5 x 10^5 N/m

3.1 MATLAB Simulation by Simulink

By using Simulink at MATLAB, the system model can be described as shown in figure below:

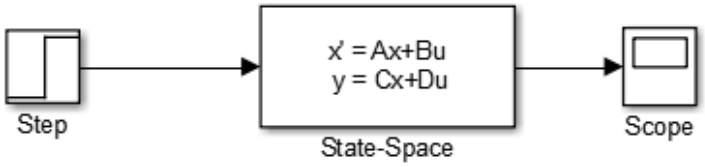


Figure 16. Simulation Two-Mas Suspension Models

```
%Journal Project for Simulation and Modelling for Current Suspension
m1=250; m2=40; %kg
k1=1.5e+4; k2=1.5e+5; %N/m
c1=1917; %N.m/s
a1=k1/m1; a2=c1/m1; a3=k1/m2;
a4=c1/m2; a5=(k2/m2)*0.1; a6=a3+a5;
A=[0, 1, 0, 0; -a1, -a2, a1, a2; 0, 0, 0, 1; a3, a4, -a6, -a4];
B=[0; 0; 0; a5];
C=[0, 1, 0, 0; 0, 0, 0, 1];
D=[0; 0];
t=0:0.01:3;
u=0.1*ones(size(t));
[y,x]=lsim(A,B,C,D,u,t)
plot(t,y);
legend('sprung mass vertical movement','un-sprung mass vertical movement');
title('Current Suspension Model k1=1.5x104')
xlabel(' Time(s)');
ylabel(' Displacement(x)');

%Journal Project for Simulation and Modelling of Modification Model
m1=250; m2=40; %kg
k1=1.5e+4; k2=1.5e+4; k3=1.5e+5; %N/m
c1=1917; %N.m/s
a1=(k1+k2)/m1; a2=c1/m1; a3=(k1+k2)/m2;
a4=c1/m2; a5=(k3/m2)*0.7; a6=a3+a5;
A=[0, 1, 0, 0; -a1, -a2, a1, a2; 0, 0, 0, 1; a3, a4, -a6, -a4];
B=[0; 0; 0; a5];
C=[1, 0, 0, 0; 0, 0, 1, 0];
D=[0; 0];
t=0:0.01:3;
u=0.1*ones(size(t));
[y,x]=lsim(A,B,C,D,u,t)
```

4.1.28 Result and Analysis

In this paper, the simulation based upon mathematical model for a quarter car using MATLAB/Simulink software is presented. Performance of the suspension system in term of ride quality and car handling is observed, by assuming the road disturbance as the input for the system. Parameters to be observed are the suspension travel, wheel deflection and the car body acceleration for a quarter car. The goal is achieving small amplitude value for suspension travel, wheel deflection and car body acceleration. The steady state for each part also should be fast.

Based on MATLAB programming, response output of displacement or vertical movement can be seen on Figure 3. Analysis results of suspension system for a quarter car model for speed bump with 0.1 m height (step input) shows that vehicle sprung mass displacement for current model has the overshoot of 90.5% and amplitude 0.125 m (left figure). This condition is undesirable from comfort point of view. High overshoot is the most undesirable for suspension better performance and longer durability. Comparing with the additional spring, Modification model has lower overshoot than the current one. There is a frequency graphic displaying on the right figure (Figure 3), which shows the reduction of damping process frequency. The graphic on the right figure shows the comfortable area of this function part.

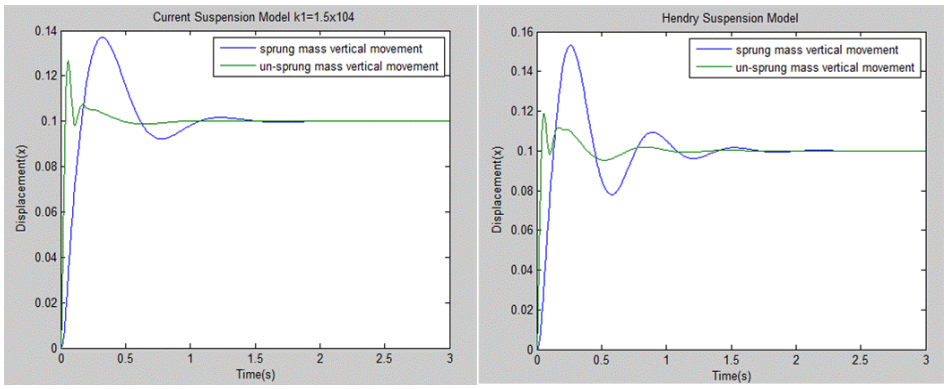


Figure 17. Vertical Movement Suspension Comparison

In term of velocity, as seen in Figure 4, the velocity level between sprung and un-sprung mass has the similar graphics and condition. This means that the velocity of vibration is almost at the same level.

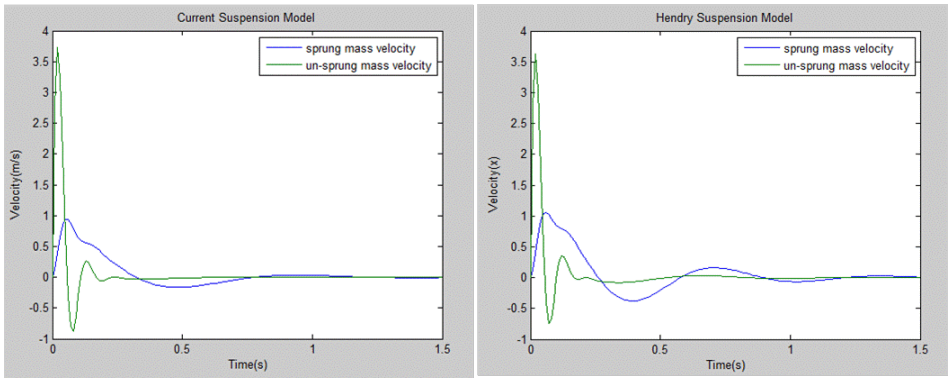


Figure 18. Velocity Suspension Comparison

4.1.29 Conclusion and Further Works

From the simulation of two different kinds of modelling systems, it can be determined that the modified system of two-mass suspension results in a better vibration performance. Further work will be on incorporating the damping effect into the system.

References

[1] Abdolvahab Agharkakli, Chavan U. S. Dr. Phvithran S., "Simulation and Analysis of Passive and Active Suspension System Using Quarter Car Model for Non Uniform road Profile", 2012, International Journal of Engineering Research and Application (IJERA), ISSN:2248-9622, Department of Mechanical engineering, University of Pune (Vishwakarma Institute of Technology), Pune, Maharashtra, INDIA.

[2] Pankaj Sharma, Nittin Saluja, Dimple Saini and Parveen SainiAbdolvahab**,** "Analysis of Automotive Passive Suspension System with Matlab Program Generation, 2013, Mechanical Engg., JMIT, Radau (Yamunanagar), 135133, INDIA

[3] William J. Palm III: *System Dynamic*, McGraw-Hill Inc., Third Edition, 2010, 1221 Avenue of the Americas, New York, NY 10020, USA.

[4] William J. Palm III: *Introduction to MATLAB for Engineers*, McGraw-Hill Inc., Third Edition, 2005, 1221 Avenue of the Americas, New York, NY 10020, USA.

The Annual Conference on Management and Information Technology (ACMIT) 2016

Influence of Process Parameters on HVOF Coating Quality: A Review

Aluisius Ganang Yunanto[6]
[a]*Master Candidate, Swiss German University, Edu Town BSD City, Tangerang 15399, Indonesia*

Abstract

The application as well as study of HVOF (High-Velocity Oxy-Fuel) coating has been grown recently by many researchers. There have been several researchers approaching the HVOF parameters such as, temperature, oxygen and fuel flow, oxygen and fuel ratio, powder flow rate etc. The more researchers found the relationship between the process parameters to the quality response such as porosity, adhesive strength and oxide content. The understanding of the process parameter to quality improves the qualification process in the more efficient way and lead to the opportunity to explore the dynamic control design during the coating process. While the qualification process that involving the more robust process parameter references improve the quality assurance of the process. This paper summarises the earlier finding in order to identify the relationship of the process parameters to the output quality. It describes the important of maintaining the process parameters as part of the quality assurance. The author are now assisting the qualification process of HVOF coating and the study of the process parameters is aimed to improve the qualification process in the sense of effectively and efficiently.

Keyword: HVOF coating Parameters; Stastical Design; Quality Assurance

1. Introduction

The HVOF (High Velocity Oxy-Fuel) is one of the thermal spray process which works on the principle of using thermal and kinetic energy for melting and accelerating powder particles to deposit desired coatings. This process utilizes only powder as the coating material rather than wire and rod. The fuel gases used in the HVOF process can be: propane, propylene, acetylene or even pure hydrogen. The gas temperature depends on two parameters, the ratio of oxygen and fuel gas flow rate and the choice of fuel gas [1]. The application of HVOF for repair services has been widely developed. The typical proposes to improve the wear-resistance, surface hardness and re-build the surface are some of the desirable application purposes. On the service center of rotary equipment such as compressor, turbine pump etc., the HVOF coating is aimed for repairing the damage surface area such as journal bearing, carbon seal ring of turbine and compressor. On the final product, there is limitation of quality testing, as most of the testing is destructive test which could not be applied on the final product. The best approach is to maintain the process qualification on each type of HVOF coating.

4.1.30 HVOF Process and Design

Processing of coatings may involve several steps. Each step represents an essential part of the planning process that must be considered before and during the coating process. Thermal spray begins with surface preparation, including cleaning, roughing, and deburring, chamfering, or radiusing and so on. Repairing worn shaft will require undercutting to remove damaged surface. After cleaning, masking protects selected component areas from unwanted abrasive and/or spray particle impact. There are several applications to protect the areas such as metal shadow plates, high-temperature tapes, and paint-on compounds. Preheating, the next step before spraying is used to remove moisture and present a warm, dry surface to the first impacting particles. During spraying process, temperature needs to be

* Corresponding author. Tel.: +62 8111 244 18; fax: +62 254 310903.
E-mail address: aluisius.yunanto@sgu.ac.id

controlled. The present of heat in the base material may introduce the substrate degradation, oxidation, shrinkage or expansion. Post coating treatment will be required to produce the clean and good roughness surface by using the grinding machine [2].

As the process coating spans from preparation to the finishing with multiple process, it is significant to have the quality process controlled in place. This is to avoid the poor quality which cause so much time and cost to redo the process. In some coating case the thickness of the coating shouldn't be excessive. The more thickness will introduce the low adhesive strength, hence the coating must be kept as minimum. In case of repair coating has failed and need to be redone, the base material will be required to be re-contoured or re-machined and will lead to thicker coating layer. If the thickness limit has been passed, so there is potentially the part will be scrapped or repaired with welding which is costly.

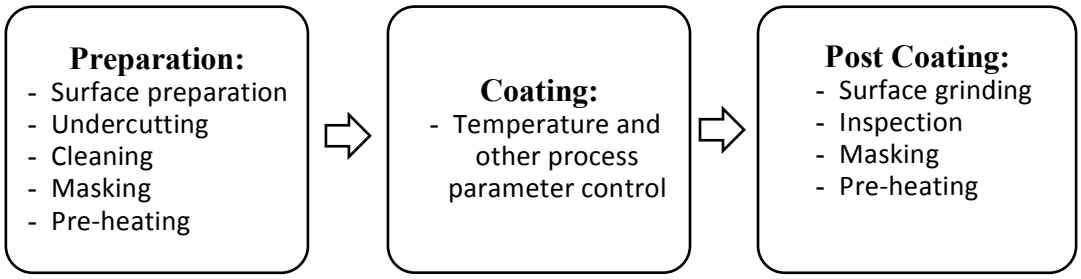


Figure.1: HVOF Coating Process

4.1.31 Relationship HVOF Process Parameters to the Coating Results

During the preparation on the HVOF coating process, there are phase to set up the machine in accordance to the reference from the manufacturer. The set up parameters will be clustered based on the certain application of the coating material which is in this case coating powder. Refer to Figure.2, there are many parameters coming into the HVOF spray gun. All of the inputs parameters will determine the coating process such as the temperature, melting phase, particle velocity which will influence the coating result.

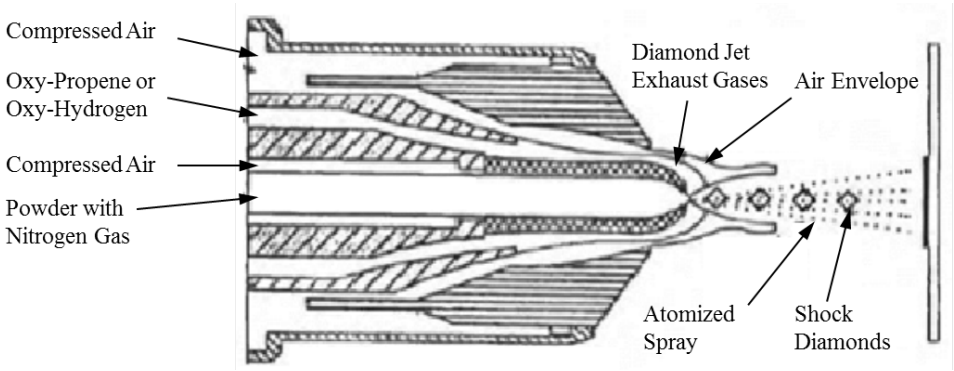


Figure.2: HVOF Spray Gun

The adhesive strength and microstructure of the coating is influenced by the in-flight particle properties such as temperature and velocity. The combination between temperature and velocity has clearly increased or decreased the adhesive strength. Also a clear relationship between particle in-flight properties as well as coating microstructure was derived: the higher the particle velocity, the lower the porosity level and higher the oxides content [3]. Similar result also obtained by Bobzin, etc. who verified that the higher particle velocity on the 316L as well as Fe-based powder has reduced the porosity [4].

On the NiCoCrAlY coating experiments, it was found a correlation between the fuel/oxygen ratio to the porosity and oxide content on the coatings based on the reaction between particle and the fuel flame (its power and chemistry). It is found that using fuel-rich ratio affect in coatings with low porosity and

oxidation, low residual stresses as well as high deposition efficiency as a result of the high velocity and low temperature attained by the particles [5]. In the same experiment, it was found the spray distance has significant influence on the residual stresses and deposition efficiency, while the porosity and oxide content is dependent on spray distance but also on oxygen and fuel flows. On the specific spray distances between 250 to 300mm, it produced coatings that are homogeneous, dense high intersplat cohesion coatings. The particles spread at their optimal velocity and temperature which has influencing in a balance of spreading, flattening, as well as solidification [5].

Based on Saaedietc [6] the fuel flow, spraying distance, and oxygen flow were the significant process parameters influencing the in-flight particle temperature and velocity. While feed rate and air flow were found as insignificant effects over the range examined. It was found that the spraying distance found as insignificant variable on the oxygen content of the coatings, but a correlation between fuel-to-oxygen ratio and oxygen content was observed. It is found that the higher fuel/oxygen ratio and less powder rate has produced high in-flight particle temperatures and dense coatings with relatively high oxide content. The micro-hardness of these coatings was higher than that of the feedstock powder due to the presence higher of oxygen in the coatings. A much higher F/O ratio reduced the in-flight particle temperature and the amount of oxygen in the flame. This was beneficial for minimizing the oxide content, as return the coatings contained a fairly large amount of retained un-melted particles [6].

On the other research by M. Hasan, Stokes, Looney and Hashmi, found that the spray distance had greater effect on residual stress in the coatings compared to the flow rate ratio of oxygen to propylene and flow rate of the compressed air [7]. Same concentration on the spray distance research done by Hong, etc, which found the spray distance is the significant factor for affecting the porosity and, in turn the corrosion resistance of the coatings [8].

Settles and Bekofske [9] found Coatings at the highest particle temperatures are undesirable due to a high melted phase with a high oxide content. While intermediate in-flight particle velocity and temperature (TP 1900-2000 K, VP 275-325 m/s) produce excellent dense coatings with plastic deformation of particles and very low oxide content. Coatings with high particle velocity and low particle temperature produce undesirable coatings containing a high melted phase with high oxide content [9].

Stand-off distance is the most important factor to impact the compressive residual stress in the coating. At a low level stand-off distance, higher velocity of in-flight particle and higher substrate temperature post spraying contribute more peening and cooling stresses, resulting in greater compressive residual stress in the coating. Higher temperature of in-flight particle in flame at high level oxygen flow results in more pore/oxide in microstructure it also which relaxes tensile quenching stress in the splat, and lowers elastic modulus of coating material due to less WC in the coating which reduces quenching stress. Hydrogen flow at high level significantly increases velocity of in-flight particle in flame, enhancing peening stress, thus increasing the compressive residual stress in the coating [10].

With the reference to the previous researchers, there are definitely relationship between the process parameters and the quality results. These are the basis of the quality improvements for the future application to maintain the quality assurance of the product. Figure.3 describes the quality responses that we are interested to know.

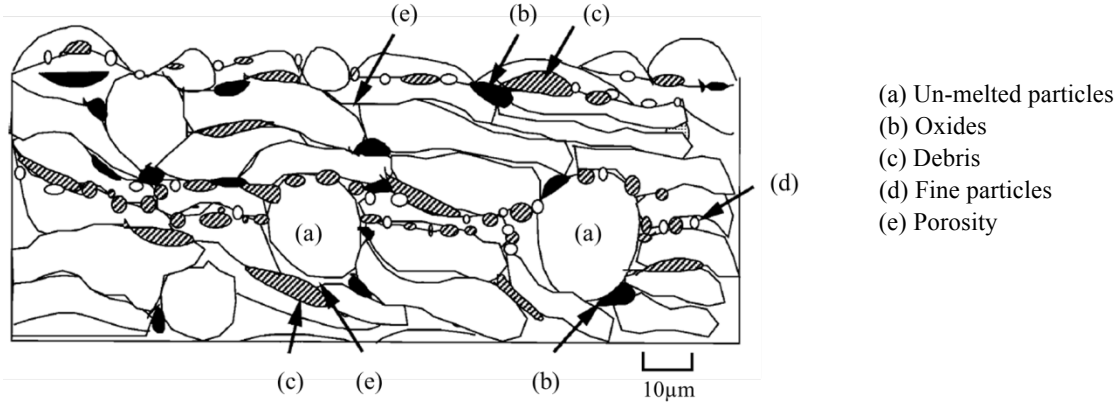


Figure.3: Quality Responses: a typical coating microstructure, containing un-melted particles, oxides, porosity, and debris [2].

4.1.32 Statistic Design Techniques & Quality Assurance

As noted earlier in this article, many variables or parameters require study before a coating can be optimized. Statistical design techniques reduce the number of experimental runs or parameter iterations needed for coating. The results obtained are often unambiguous and at a minimum cost. Statistical design methods encourage the systematic study of the many variables that confront coatings engineers. Furthermore, these studies provide data on how variables interact and how they influence coating properties, as well as a plan for constructively changing input parameters to affect the most desirable properties**.** Designs of experiments and Taguchi factorial experiments are two commonly used statistical techniques. The fundamental approach for each is the same: A matrix of selected variables versus a series of experimental runs is established [2]. Tabel.1 gives the example of typical needed parameters and constants to observe the coating experiments. There is no need to have all variant of the parameters applied on experiment. The main goal is to obtain the optimized process parameters to result the best quality result. Typically, a fractional factorial matrix is constructed with variables deemed most likely to influence coating results, rather than a complete factorial of all variables.
Then to understand the significant of the process variable, the analysis of variant (ANOVA) shall be performed. An ANOVA is a Taguchi analysis of results showing how each variable, both high and low, influences results [2]. The following Table.1 is an example of Taguchi process parameters matrix and the hardware information. The test specimens then will be investigated on the laboratory to obtain the quality response of each run.

Tabel.1: Example of Taguchi matrix variables and constants [2].

Experiment	Spray distance, mm	Spray rate, g/min	Carrier flow, scfh	Application temperature, °C	Particle size, µm	Power, kW
1	76	30	12	177	-100	40
2	76	30	15	343	-53	50
3	76	76	12	177	-53	50
4	76	76	15	343	-100	40
5	152	30	12	343	-100	50
6	152	30	15	177	-53	40
7	152	76	12	343	-53	40
8	152	76	15	177	-100	50

	Constant	Variable	Level	
			Low(1)	High(2)
Gun	Metco 3 APG	Spray distance, mm	76	152
Nozzle	Metco 315	Spray rate, g/min	30	76
Powder	No. 2	Carrier flow, scfh	12	15
Plasma	Argon	Application temperature, °C	177	343
Pressure	75 psi	Particle size, µm	-100	-53
Flows	60 scfh	Power, kW	40	50

scfh, surface cubic feet per hour

The result of the experimental runs, the proper documentation and record will be required to the specific coating application. The parameters will be the base line of next application on the final product. This will assure the quality of the coated product in the best prediction of quality responses. This quality assurance is critical due to the actual finish product cannot be tested directly to understand the coating quality properties.

4.1.33 Conclusion

The study on the HVOF coating parameters has significant purposes to maintain the quality of the product. The study will give a quality assurance to the coating providers so that the final product will suffice the design and avoid the coating providers from the multiple rework due to the coating poor quality.
From the previous researches there is a definite understanding that there is a relationship between the processing parameters to the quality response. It is found the repeatable relationship between process

parameters and quality responses such as the higher temperature introduces more porosity due to the inclusion of oxygen.
A good understanding of the process parameter provides better approach on the quality improvement. The best process parameter is needed for further development of the mechatronic application on the close loop HVOF coating process.

References

[1] Handbook of Thermal Spray Technology (#06994G): Introduction to Thermal Spray Processing, ASM International, 2004.

[2]R.C. Tucker, Jr.. Introduction to CoatingDesign and Processing. Handbook of Thermal Spray Technology (#06994G). ASM International, 2013.

[3] Christophe Lyphout, Per Nylen, and Lars Ostergren. Relationships Between Process Parameters, Microstructure, and Adhesion Strengthof HVOF Sprayed IN718 Coatings, Journal of Thermal Spray Technology; 2011, Vol. 20(1-2),

[4] Kirsten Bobzin, Nils Kopp, Thomas Warda, Ivica Petkovic, Marcel Schaefer, Klaus Dieter Landes, Guenter Forster, Stephan Zimmermann, Jose-Luis Marques, Stefan Kirner, Marina Kauffeldt, and Jochen Schein. Particle In-Flight and Coating Properties of Fe-Based Feedstock Materials Sprayed with Modern Thermal Spray Systems, Journal of Thermal Spray Technology; 2013, Vol. 22(2-3)

[5] H. Ruiz-Luna, D. Lozano-Mandujano, J.M. Alvarado-Orozco, A. Valarezo, C.A. Poblano-Salas, L.G. Trapaga-Martınez,F.J. Espinoza-Beltran, and J. Munoz-Saldana. Effect of HVOF Processing Parameterson the Properties of NiCoCrAlY Coatings by Design of Experiments, Journal of Thermal Spray Technology; August 2014, Vol. 23(6)

[6] J. Saaedi, T.W. Coyle, H. Arabi, S. Mirdamadi, and J. Mostaghimi. Effects of HVOF Process Parameters on the Properties of Ni-Cr Coatings, Journal of Thermal Spray Technology; 2010, Vol. 19(3)

[7] M. Hasan, J. Stokes, L. Looney, M.S.J. Hashmi. Effect of Spray Parameters on Residual Stress Build-up of HVOF Sprayed Aluminium/tool-steel Functionally Graded Coatings. Surface & Coatings Technology; 2008

[8] Sheng Hong, Yuping Wu, Yugui Zheng, Bo Wang, Wenwen Gao, Gaiye Li, Guobing Ying, and Jinran Lin; Effect of Spray Parameters on the Corrosion Behavior of HVOF Sprayed WC-Co-Cr Coatings; Journal of Materials Engineering and Performance; 2014, Vol. 23(4)

[9] Gary S. Settles and Sarah R. Bekofske. HVOF Thermal Spray Velocity, Temperature, and Stainless Steel Coating Properties. Gas Dynamics Laboratory, Mechanical Engineering Dept., Penn State University

[10] M. Gui, R. Eybel, B. Asselin, S. Radhakrishnan, and J. Cerps. Influence of Processing Parameters on Residual Stress of High Velocity Oxy-Fuel Thermally Sprayed WC-Co-Cr Coating. Journal of Materials Engineering and Performance; 2012, Vol. 21(10)

The Annual Conference on Management and Information Technology (ACMIT) 2016

A Study Case in NTMC POLRI: Reducing Data Breach Risk from Insider Threats by Using Risk IT Framework

Musdi Muhammad Soleh
Swiss German University, EduTown BSD City, Tangeramg - Indonesia

Abstract

Risks is not only merely comes from external threats, it is also comes from inside - internal actor. Vormetric Insider Threat mentioned that in 800 surveyed enterprise companies, 89% vulnerable to insider attacks [1]. It mentioned that Data Breach issue the highest risk happened to the company caused by insider threats. This paper will analyse the insider attacks, Risk IT framework will be used to reduce to reduce and prevent these vulnerabilities in valuable assets.

Keywords: Risk IT Framework ; Insider Threats ; Mitigation ; Asset

1. Introduction

1.1 Background

Risks is not only merely comes from external threats, it is also comes from inside - internal actor. Vormetric Insider Threat mentioned that in 800 surveyed enterprise companies, 89% vulnerable to insider attacks. It mentioned that Data Breach issue the highest risk happened to the company caused by insider threats. The highest the value of the data the highest the Data Breach risk. This paper will analyse the insider attacks, Risk IT framework will be used to reduce to reduce and prevent these vulnerabilities in valuable assets.

1.2 Overview

The threat of internal (insider threat) is usually more damaging than external, because the parties have access to know exactly what they are looking for. The threat to enterprise security is dynamic then static security tool is not enough. There are many novel ways to protect themselves against various kinds of cyber-attacks and infiltration, including hiring an expert on cyber security in particular, but one method of prevention is the most effective way is to focus more on providing training to their employees and to improve their internal processes as most problems cyber security comes from the gap in procedures or human error. To improve the perimeter defence, the company should also invest in a system that can detect attackers in a network and also provides the ability to monitor and understand the behaviour of the employees, so they can recognize unethical behaviour before it becomes a more serious problem.

1.2.1 Insider Threats

Enterprise data security has become a major issue over the years, but the act of hacking that recently happened it as a thing that needs to get more serious attention, not only for the company's enterprise-class, but also to small and medium enterprises.

It only takes one small hack, then all information stored by companies - ranging from employee passwords to sensitive information about clients - could be in the hands of hackers.
Then there is the possibility that the company will be forced to pay a large ransom, pay leading security experts to resolve the problem, or bite the bullet and make an apology to the public that can destroy a company's reputation.
An insider may cause threars when There is an try to steal property or information for personal gain that cause Data Breach, or to benefit purposes[2]

1.2.2 Asset

Property can't be stated to be dependable within the company network can occur because of negligence, and ignorance of the importance of supervision required for a specific asset.

1.2.3 Risk

Understanding the risks can be explained as follows. The first notion is: the uncertainty (uncertainty) that may give rise to loss events (loss). Understanding risk is the uncertainty over the second occurrence of an event[3]. Risk is the potential danger that may arise from some of the current process or from some future events. From the perspective of information systems, risk management is to understand and respond tors factors that could cause failures in integration, confidentiality and security of information systems. This risk would harm the process or information generated from several events, either intentional or unintentional. This risk can also come from ourselves internal or external parties that are trying to steal our data[4]

According to G. Stoneburner 2002, IT risk management involves three processes:

1. Risk Assessment
Risk assessment (risk assessment) is an early stage in risk control. Manager uses a risk assessment to determine the level of potential threats and risks associated with the whole process of information systems.
The results of this process, it is expected all the potential threats can be assessed according to its category. Who have the highest risk level will be given priority in terms of prevention, which will help managers in controlling risks.

2. Risk Mitigation
Risk Mitigation is the process or steps to control, evaluate, re prevention and control of the risk incurred. With proper control, can reduce the level of risk that occurred to most minimal level so as not to affect the resources and the business running, so the risks that is occurred will not be repeated.

3. Evaluation and assessment
Evaluation of the risk management should continue to be made and updated. Rapid technological developments allow attacks (risks) that may threaten the resources previously did not have this level of risk.
Generally what happens is after a Risk Assessment and Risk Mitigation done, evaluate the results of these activities is rarely done, so that the level of risk remains high. For example, there is no annual evaluation of the risks that have been predetermined.

1.2.4 Risk IT

IT risk is a factor of the total risk universe of the enterprise, as shown in figure 1. Different risks an enterprise faces include strategic chance, environmental danger, market hazard, credit hazard, operational hazard and compliance threat. In lots of businesses, IT-related threat is regarded to be a factor of operational risk, e.g., within the financial enterprise within the Basel II framework[5]. Nonetheless, even strategic chance can have an IT aspect to it, mainly the place it's the key enabler of recent industry initiatives. The same applies for credit score danger, where terrible IT (security) can lead to minimize credit scores. For this reason it's better not to depict IT risk with a hierarchic

dependency on probably the most other threat classes, however probably as proven within the (economic industry-oriented) instance given in figure 1.0 [5]

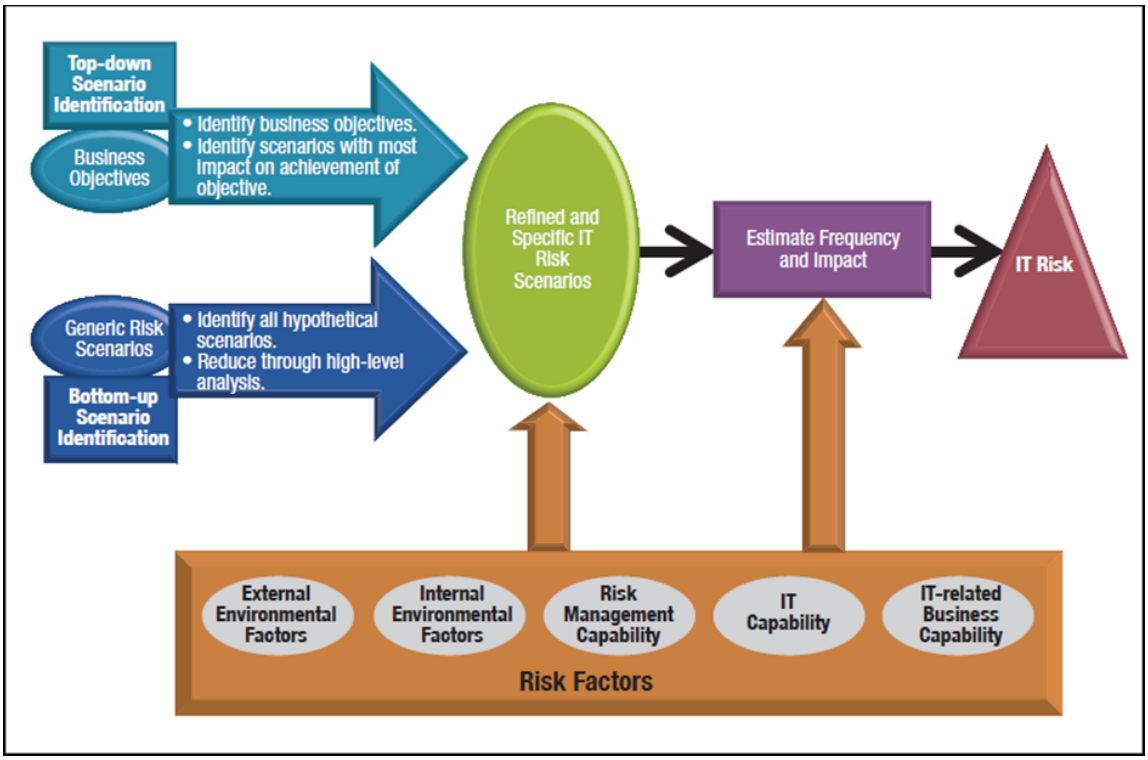


Figure 1.0 IT Risk Scenario development

Shows that risk of affairs with two specific mechanism:

1. Prime-down strategy, start from the overall industry objective and perform
2. Backside-down technique, list of regular situation is used to define a set more concrete and customised the scenario

The procedures square measure complementary and should be used at the same time, risk should be relevant and joined to actual business hazard. However, utilizing a collection of illustration generic risk eventualities helps to make sure that no risks square measure un-noted and provides an additional complete and full read over IT threat. In the figure 1.1 we can find that Internal actor (staff and contractor) has a role play in causing insider threats.

Figure 1.1 IT Risk scenario component

An IT Risk state of affairs may be a description of associate degree IT-related occasion which will result in a business impact, once and if it ought to occur. For risk eventualities to be whole and usable for risk analysis functions, they must contain the subsequent elements

- Internal actor who generates the threat is actors can be internal or external and they can be human or non-human
- External actor include outsider, competitors, regulators and the market

IT risk continually exists, whether or not or not it's detected or recognised by Associate in Nursing enterprise. during this context, it's necessary to spot and manage probably important IT risk problems, as opposition each risk issue, because the latter might not be value effective[5]

1.3 Problem Statement

There are two main threats based on the actor views, outside and inside. Insider threats cannot be ignored anymore due to the threat report is increase by the year. These insider threats should be prevented and reduced in proper way to avoid any impact to the company. The highest risks and the most happened due to insider threat is Data Breach that will raise an impact to company asset.

1.4 Expected Outcome

The result of this analysis is expected to be used and re-developed in the future to achieve and meet security goal in reducing insider threats and risks.

2. Theoretical Framework

To Analyze the insider these insider threats, the writer will use Risk IT especially Risk Avoidance module [6] to prevent Data Breach in company assets. The Risk IT Practitioner Guide will be also used in solving this problem [7]. Avoidance means prevent any activity or conditions that cause rise to risk [6]. Risk avoidance is delivered when no other risk response is provided. This issue can raise when:

- There is no alternative efficient response which will reach reducing the frequency and magnitude below the outlined thresholds for risk appetence.
- The risk cannot be shared or transferred.
- The risk is deemed unacceptable by management.

Some IT-related samples of risk turning away might embrace relocating a knowledge centre far from an area with important natural hazards, or declining to have interaction terribly} very massive project once the business case shows a notable risk of failure.
Based on the security issues from insider threats published by Vormetric [8] below, Data Breach is the highest issue that happened in 2015 to enterprise company:

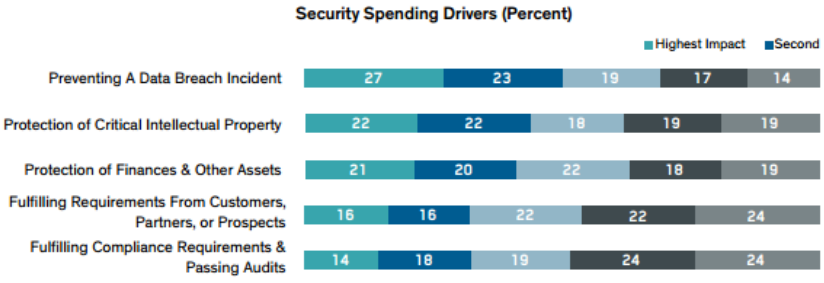


Image 1.0 Insider Threats and Risk

Vormetric also mentioned that Data Breach is happened caused by the lack of these factors as listed in the table 1.0 below:

Data Breach could be happened due to lack of these factors below
Database/File Encryption
Data Access Monitoring
Data Loss Prevention (DLP)
Privileged User Access Management
Application Layer Encryption
SIEM and Other Log Analysis and Analytical Tools
Multi-factor Authentication
Data Masking
Single Sign On
Federated Identity Management
Tokenization

Table 1.0 Data breach Risk Avoidance

3. Result

Below will be described the analysis result of Data Breach caused by insider threats.

3.1 Risk Causes

The writer found these below risks could raise Data Breached caused by insider threat:

- Most insider has accessed, even privilege access to the system
- Risk could be growth by time

The risk cause above will be avoid by using Risk IT in the next session.

3.2 Risk Avoidance

By using Risk IT (COBIT and Val IT) framework, the writer create risk avoidance solutions as described in this table 1.1 below:

CobiT Controls and Val IT Key Management Practices for Data Breach Risk Avoidance						
Essential Control	**Control Reference**		**Control Title**	**Risk Avoidance**	**Effect on Frequency**	**Effect on Impact**
1. Infrastructure theft						
Yes	AI3	AI3.2	Infrastructure Resource Protection and Availability	Solution to Data Breach : Database/File Encryption Data Access Monitoring Data Loss Prevention (DLP) Privileged User Access Management Application Layer Encryption SIEM and Other Log Analysis and Analytical Tools Multi-factor Authentication Data Masking Federated Identity Management Tokenization		High
	DS12	DS12.3	Physical Access	Solution to data breach : Privileged User Access Management Federated Identity Management		Medium
2. Logical attacks						

Yes	DS5	DS5.5	Security Testing, Surveillance and Monitoring	Solution to data breach : Database/File Encryption Data Access Monitoring Data Loss Prevention (DLP) Privileged User Access Management Application Layer Encryption SIEM and Other Log Analysis and Analytical Tools Multi-factor Authentication Data Masking Federated Identity Management Tokenization	High	
Yes	DS5	DS5.9	Malicious Software Prevention, Detection and Correction	Solution to data breach : Database/File Encryption Data Access Monitoring Data Loss Prevention (DLP) Privileged User Access Management Application Layer Encryption SIEM and Other Log Analysis and Analytical Tools Multi-factor Authentication Data Masking Federated Identity Management Tokenization	High	
Yes	DS5	DS5.10	NETWORK Security	Solution to data breach : Data Access Monitoring Data Loss Prevention (DLP) Privileged User Access Management Application Layer Encryption SIEM and Other Log Analysis and Analytical Tools Multi-factor Authentication Data Masking Federated Identity Management Tokenization	High	Medium
	PO4	PO4.9	Data and System Ownership	Solution to data breach : Privileged User Access Management Multi-factor Authentication Federated Identity Management	Medium	
	AI2	AI2.4	Application Security and Availability	Solution to data breach : Database/File Encryption Data Access Monitoring Application Layer Encryption SIEM and Other Log Analysis and Analytical Tools Data Masking		
	DS5	DS5.1	Management of IT Security	Solution to data breach : Data Access Monitoring Data Loss Prevention (DLP) Privileged User Access Management Multi-factor Authentication Federated Identity Management	Medium	Medium
	DS5	DS5.3	Identity Management	Solution to data breach : Data Access Monitoring Privileged User Access Management SIEM and Other Log Analysis and Analytical Tools Multi-factor Authentication Federated Identity Management Tokenization	Medium	
	DS5	DS5.7	Protection of Security Technology	Solution to data breach : Database/File Encryption Data Access Monitoring Data Loss Prevention (DLP)	Medium	

				Privileged User Access Management Application Layer Encryption SIEM and Other Log Analysis and Analytical Tools Multi-factor Authentication Data Masking Federated Identity Management Tokenization		
	AC1	AC1	Source Data Preparation and Authorisation	Solution to data breach : Data Access Monitoring Data Loss Prevention (DLP) Privileged User Access Management SIEM and Other Log Analysis and Analytical Tools Multi-factor Authentication Federated Identity Management	Medium	
3. Logical attacks *(cont.)*						
	AC3	AC3	Accuracy, Completeness and Authenticity Checks	Solution to data breach : Data Access Monitoring Privileged User Access Management SIEM and Other Log Analysis and Analytical Tools Multi-factor Authentication Federated Identity Management Tokenization	Medium	
	AC4	AC4	Processing Integrity and Validity	Solution to data breach : Privileged User Access Management Multi-factor Authentication Federated Identity Management Tokenization	Medium	
	AC5	AC5	Output Review, Reconciliation and Error Handling	Solution to data breach : Data Access Monitoring Data Loss Prevention (DLP) Privileged User Access Management SIEM and Other Log Analysis and Analytical Tools Multi-factor Authentication Federated Identity Management	Medium	
	AC6	AC6	Transaction Authentication and Integrity	Solution to data breach : Data Access Monitoring Privileged User Access Management Multi-factor Authentication Federated Identity Management Tokenization	Medium	
4. Information media						
Yes	DS11	DS11.2	Storage and Retention Arrangements	Solution to data breach : Database/File Encryption Data Access Monitoring Data Loss Prevention (DLP) Privileged User Access Management Application Layer Encryption SIEM and Other Log Analysis and Analytical Tools Multi-factor Authentication Data Masking Federated Identity Management Tokenization	High	Medium
Yes	DS11	DS11.5	Backup and Restoration	Solution to data breach : Data Access Monitoring Data Loss Prevention (DLP)		High

				SIEM and Other Log Analysis and Analytical Tools		
	DS5	DS5.11	Exchange of Sensitive Data	Solution to data breach : Database/File Encryption Data Access Monitoring Data Loss Prevention (DLP) Privileged User Access Management Application Layer Encryption SIEM and Other Log Analysis and Analytical Tools Data Masking Federated Identity Management Tokenization	Medium	
	DS11	DS11.6	Security Requirements for Data Management	Solution to data breach : Database/File Encryption Data Access Monitoring Data Loss Prevention (DLP) Privileged User Access Management Application Layer Encryption SIEM and Other Log Analysis and Analytical Tools Multi-factor Authentication Data Masking Federated Identity Management Tokenization	Medium	
	DS12	DS12.3	Physical Access	Solution to Data Breach : Data Access Monitoring Data Loss Prevention (DLP) Privileged User Access Management SIEM and Other Log Analysis and Analytical Tools Federated Identity Management	Medium	
	DS13	DS13.4	Sensitive Documents and Output Devices	Solution to Data Breach : Database/File Encryption Data Access Monitoring Data Loss Prevention (DLP) Privileged User Access Management Data Masking Federated Identity Management	Medium	

Table 1.1 COBIT Controls and Val IT Key Management Practices for Data Breach Risk Avoidance

4. Conclusion

A Data Breach is the highest risk caused by insider threat due to they have privilege access to the system which sensitive, Companies must provide a balance between investment in prevention is balanced, so that it can detect and perform a reasonable reaction to data breaches or cyber attacks. By the Data Breach report keep growing by years, it should be Minimizing attacks on one side and deal damage but can not be avoided on the other side. The main consideration should be made a reasonable plan including measures and tools around the disposition of business risks

References:

[1] *Insider threat report*. Vormetric, 2015.

[2] FBI, "The Insider Threat An introduction to detecting and deterring an insider spy." [Online]. Available: https://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat.

[3] M. L. S. C. Arthur C Williams Jr, Peter C Young, "Risk Management & Insurance," in *Risk Management & Insurance 8th Edition*, 2009, p. 1.

[4] C. Alberts, S. Behrens, R. Pethia, and W. Wilson, "Operationally critical threat, asset, and vulnerability evaluation

(OCTAVE) framework, Version 1.0," 1999.
[5] ISACA, *The Risk IT Framework*. USA.
[6] *The Risk IT Framework*. Information System Audit and Control Association (ISACA) IL, 2009.
[7] *The Risk IT Practitioner Guide*. 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA, 2009.
[8] A. Kellett, "Insider threat report," *Vormetric*, p. 10, 2015.

The Annual Conference on Management and Information Technology (ACMIT) 2016

Optimization Fuzzy Controller Parameters for Soot Blower in Power Plant

By
Chandra Thomas, Jemmy Septiawan, SauwAlbertusFajar, Dr. Ir. Hanny J. Berchmans, M.T.,M.Sc., Dena Hendriana B.Sc., S.M.,Sc.D.,

SWISS GERMAN UNIVERISTY

ABSTRACT
In power plant, soot blower operation plays important role in efficiency. Most soot blowing process on the power plants is using fixed schedule of time. In many instances, certain boiler stages are blown unnecessarily, resulting in efficiency loss. The Target of this research is to optimize the control of soot blowing fuzzy logic techniques.

Keywords: Fuzzy, soot blower, power plant, efficiency

1. Background

Today the demand for power increasing significantly makes our government planning to build many power plants. There will be many power plants need to be controlled in order to make efficient and it will be very high cost to control the power plants.
In power plant, slagging usually occurs in the furnace and on the screen tubes and upper heater sections of the boiler, whereas fouling usually occurs at the back end of the boiler in areas like the economizer region. Both slagging and fouling create significant problems. In particular heat transfer is reduced [2] and the necessary operator compensation action, (likely to include adjustments to burner tilt, water flow, firing rates, etc) inevitably leads to a loss of efficiency, and a subsequent increase in operational costs. Other problems include loss in load capacity, physical damage due to heavy slag falls, departure from optimal turbine conditions, and increased maintenance [3].

2. Research Problem

In power plant, soot blower operation play important role in efficiency. As we know that most of the power plants, the soot blowing is using fixed schedule of time. In many instances, certain boiler stages are blown unnecessarily, resulting in efficiency loss. Some others using sensors such as camera and temperature sensor which is not too effective due to estimating the cleanliness factor.
By introducing the notion of degree in the verification of a condition, thus enabling a condition to be in a state other than true or false, fuzzy logic provides a very valuable flexibility for reasoning, which makes it possible to take into account inaccuracies and uncertainties. One advantage of fuzzy logic in order to formalize human reasoning is that the rules are set in natural language [12]. Therefore a fuzzy based system is applied which shall indicate individual section cleanliness to determine correct soot blowing scheme. Practical soot blowing optimization improves boiler performance, reduces NOx emissions and minimizes disturbances caused by soot blower activation.

3. Research Objectives

The target of this research is to optimize the control of soot blowing using fuzzy techniques in order to increase the efficiency.

4. LITERATURE REVIEW

4.1 Soot Blower

A soot blower is used for removing the soot that is deposited on the furnace tubes of a boiler during combustion.

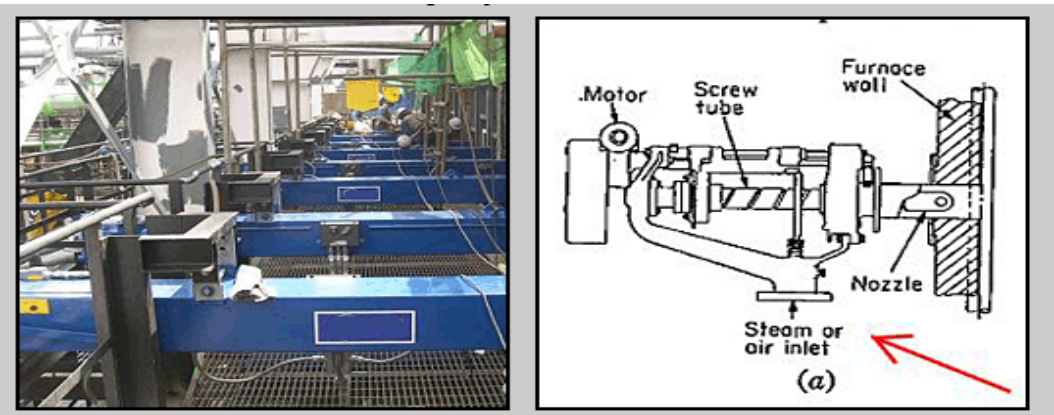


Figure 1. Soot blower

Problems caused by soot:

- Reduced efficiency

Soot will acts as a heat insulator when deposited on the heating surfaces of a boiler. The result is that less heat is transferred to the water to raise steam and more heat is wasted up the chimney. This leads to higher fuel consumption and/or poor steaming.

- Soot fires

A soot fire can be damaging to a boiler because it can cause localized hotspots to occur in the tubes. These hotspots may reach temperatures that weaken the materials of the tubes. Soot blowers reduce the risk of soot fires and their resulting damage [9]

Figure 2.Boiler damage due to soot

4.2. Cleanliness Factor

The cleanliness factor, CF, of a boiler is defined as

$$\text{CF} = \frac{Q_i}{Q_i^*} * 100\%$$

Where:

Q_i =the actual heat transfer rate ith section , Btu/hr

Q_i^* =the clean heat transfer rate of ith section , Btu/hr

A cleanliness factor of 100 percent means the boiler is free of fouling, and cleanliness factors less than this value mean that the heat exchanger has some fouling that is reducing the heat transfer of the network.

The most difficult part in calculating the cleanliness factor, CF, is estimating the heat transfer rate for the clean condition. This quantity,Q_i^*depends on current values of temperatures, pressures and flow rates of the two fluids. The issue is how to model Q_i^*as a function of these variables. [7]

4.3 Ash Content in coal

High ash contain in coal will leads boilers to an increase in the erosion of pressure parts, slagging and fouling of pressure parts, poor electrostatic precipitator (ESP) performance and overloading of draft fans.
ESP design parameters are dependent on coal characteristics, therefore the ESP size, performance, and cost vary with a change in coal composition and ash characteristics [11].

5. Simulation

Kariangau Power Plant soot blower optimization simulate using Matlab: Load of Power Plant operation (MW) - 2x15MW, SH metal temperature (Celcius) - 485 ℃, Total spray flow (times/hour) ,Burner Tilt (degree)- 45deg, Elapsed Time since last soot blowing - 12hrs. Coal Quality (Ash %).

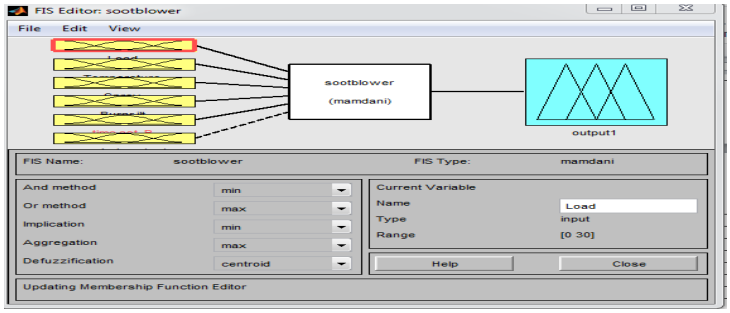


Figure3. FIS Editor display for soot blower

Figure 3 shows 6 input parameter (Load, SH metal temperature, total spray, burner tilt, elapsed time since last soot blowing, and coal quality) the rules set to predict the output (cleanliness factor). The rule in fuzzy create with the input parameter already define above.

Table 1. Define soot blower parameter

Linguistic Value	Notation	Unit	Range		Reason
			Min	Max	
Gauss MF	LOAD				In power plant the output load can be achieved only 80% so 80% of the power plant capacity load is high, 70% is medium , and 60% is low.
Low	L	MW	15	20	
Average	A	MW	18	23	
High	H	MW	21	26	
Bell MF	LTSH Temperature				The LTSH temperature is 485 degCelcius while the LTSH temperature changing should be not lower or higher than 10 degCelcius[Kakac, 1991]
Low	L	℃	475	485	
Normal	N	℃	480	490	
High	H	℃	485	495	
Gauss MF	Spray				According to T.K.Say, spray is low : 20-40 times/hour, normal: 25-45 times/hour, high: 30-50 times/hour
Low	L	times/hour	20	40	
Normal	N	times/hour	25	45	
High	H	times/hour	30	50	
Gauss MF	Burner Tilt				According to T.K.Say, Burner

Down	D	degree	-30	0	tilt down :-30 until 0 degree, normal :-20 until 20 degree, up: 0 until 30 degree
Normal	N	degree	-20	20	
Up	U	degree	0	30	
Bell MF	Time since last SB				According to T.K.Say, time since last soot blowing categorized short: 0-8 hour, average: 6-14 hours, and long 10-24 hours
Short	S	hour	0	8	
Average	A	hour	6	14	
Long	L	hour	10	24	
Bell MF	Cleanliness Factor				According to SadikKakac the CF design is from 75%-85%
Dirty	D	%	0	75	
Clean	C	%	75	100	
Coal Quality	Ash (%)				According to Circular volumes 889-894, high ash content if above 15%, and low ash content if below 8%
Gauss MF					
High Ash	H	%	12	30	
Avg Ash	A	%	8	12	
Low Ash	L	%	5	9	

Table 2. Rule for soot blower in fuzzy

Rule	Load	Temp	Spray (No)	Tilt	Time (No)	Coal	Output	Com
1	Low	Low	Low	Normal	Long	Low Ash	Clean	0
2	Low	High	High	Down	Short	High Ash	Dirty	1
3	Avg	Normal	Normal	Normal	Avg	Avg Ash	Clean	0
4	Avg	High	High	Down	Short	Avg Ash	Dirty	1
5	High	Low	Low	Normal	Avg	Avg Ash	Clean	0
6	High	High	High	Down	Short	High Ash	Dirty	1
7	High	High	Normal	Normal	Avg	High Ash	Dirty	1
8	Avg	High	High	Down	Avg	High Ash	Dirty	1
9	Low	Normal	Normal	Up	Avg	High Ash	Clean	0
10	High	Normal	High	Down	Short	High Ash	Dirty	1
11	High	High	High	Down	Short	Avg Ash	Dirty	1
12	Avg	High	High	Down	Long	Avg Ash	Dirty	1
13	Avg	Low	Low	Normal	Long	Low Ash	Clean	0
14	Avg	Low	High	Normal	Long	Avg Ash	Clean	0
15	Low	Normal	Low	Up	Avg	Low Ash	Clean	0
16	Low	Normal	Normal	Up	Short	High Ash	Clean	0
17	High	Low	High	Down	Avg	Low Ash	Clean	0
18	Low	High	Normal	Up	Short	High Ash	Dirty	1
19	Avg	Normal	Normal	Down	Avg	Avg Ash	Clean	0
20	Low	Normal	Low	Up	Long	Low Ash	Clean	0

6. Data Analysis

If the data input is load, SH Temp, spray, burner tilt, time, and coal ash than it can get CF(%) as below :

Table3. Estimating cleanliness factor with input the parameter data

Load (MW)	SH Temp (°C)	Spray	Burner Tilt	Time (Hour)	Coal Ash (%)	CF (%)
18	475	35	20	12.5	20	76.4
20	480	35	-20	12.5	5	84.6
26	485	50	10	5	35	50
24	490	20	-10	20	30	50
23	480	25	30	18	5	69.7
22	475	30	-30	5	8	76.3
21	490	40	5	7	10	82.2
20	475	45	-5	3	20	50
19	495	50	0	22	28	50
22	485	35	0	15	12	67.4

By inputting the parameter into the fuzzy we can know the CF%. The CF% can be seen in table 3. The CF is clean when the load is low, when the load is higher the CF will be dirty since there will be more coal to be burned which means more coal ash deposition and the temperature become increasing.

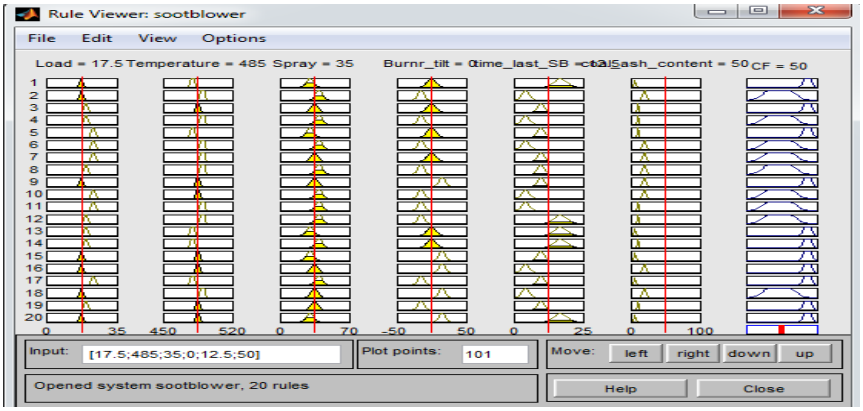


Figure4. Rules viewer of fuzzy soot blower

Figure 4 show the rules viewer of fuzzy soot blower. The CF value which show in table 3 is get after we input the value of the input parameter to this fuzzy rules viewer. Now we can know whether the surface of the boiler is clean or dirty. If dirty, the system will activate the soot blower to blow the soot and if it is clean, the soot blower will not be activated. This method is more efficient than conventional system using fixed time schedule. Compare to sensor based system also it is better since sensor base system only monitor some parameter and cannot combine all the input parameter to define the cleanliness factor. It can use camera but it has limitation, the camera can know the thickness of the soot but to cannot define how clean the surface since it is involving more complex input parameter.

7. CONCLUSIONS AND RECCOMENDATIONS

7.1 Conclusions

Compare to conventional method, fuzzy logic can predict the cleanliness factor so the soot blower can effectively working. The problem in conventional method, soot blowers work based on fixed time schedule, so it is possible the cleanliness factor is dirty but the soot blower still not working, consequently the heat transfer process will not effective and cause losses. Even with sensor based, the technology to directly measure section cleanliness is currently limited. Heat flux sensors and infrared cameras have been used to estimate the fouling of the furnace water walls with limited success. With fuzzy logic, the soot blower will be on when it defines that the cleanliness factor is dirty and if it is consider clean, the soot blower will not working. So soot blowers will work on appropriately.

7.2 Recommendations

The fuzzy rules can be changed based on the Power Plant Capacity and adjusted until get its best performance. It is also suggested to do deeper research of coal quality and ash deposition in power plant which affect the temperature and efficiency of the boiler.

8. REFERENCES

1. T.K. Sai, K.A. Reddy "Fuzzy Application in A Power Station "International Journal on Soft Computing (IJSC) Vol.6, No. 2, May 2015
2. Anderson, D.W., Viskanta,R, and Incopera, F.P., Engineering Gas Turbine and Power, 109, 215-221.1987.
3. Hayman, J.R, Slag Monitoring for Utility Boilers, Electrical Power Research Institute Inc, USA, EPRI Project RP, 1893-1895, 1988.
4. Sanyal, A., and Williamson, J., .Energy, 158, 158-162,1981.
5. Kaya.A.,Process Joint Automatic Control Conference, USA, TA-8D, 1981.
6. Alarick Tavares and Simon Youssef, JuhaMustonen, and Mika Haikola, Retrofitting Soot Blower Systems to Use a Lower Pressure Steam Source.
7. Ramirez, Benjamin A., "Determination of Cleanliness Status of Boiler Heat Transfer Surfaces by Using Artificial Intelligent Techniques"(2000).Theses and Desertation.Paper 671.Lehigh University.
8. ABB Energy Efficiency Handbook.
9. https://en.wikipedia.org/wiki/Soot_blower
10. http://www.ignou.ac.in/upload/Unit-2-58.pdf
11. Saxena, Pratosh, Powerline July 2013, page 56-57
12. Dernoncourt, Franck, "Introduction to Fuzzy Logic" , MIT January 2013
13. https://www.isa.org/standards-publications/isa-publications/intech-magazine/2010/august/special-section-flow-and-level-boiler-drum-control/
14. Begum, K.Ghousiya, et all , "An Inteligent Model Based Level Control of Boiler Drum", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 3, Issue1, January 2013.
15. Kakac, Sadik, "Boilers, Evaporator, and Condensors", John Wiley & Sons, 1991
16. Circular, Volumes 889-894, The Survey , 1984

The Annual Conference on Management and Information Technology (ACMIT) 2016

Application Fuzzy Logic System for Accurate Sheet Trim Shower Position

Yudi Wibawa
Faculty of Engineering and Information Technology,SGU Univerity, Indonesia

Abstract

This paper aims to study for accurate sheet trim shower position for paper making process. An accurate position is required in an automation system. A mathematical model of DC motor is used to obtain a transfer function between shaft position and applied voltage. PID controller with Ziegler-Nichols and Hang-tuning rule and Fuzzy logic controller for controlling position accuracy are required. The result reference explains it that the FLC is better than other methods and performance characteristics also improve the control of DC motor.

Keywords: Fuzzy logic, DC motor position control, fuzzy propotional-derivative controller

1. Introduction

Paper is so much part of our daily lives that we cannot imagine the word without it. For most papermakers the optimal positioning of the edge trim shower nozzle is a subject in its own right. In fact, good runnability of a paper machine depends to a significant extent on the problem free operation of the edge trims. A low break paper level–throughout the whole machine, smooth sheet transfer at the pickup, the prevention both of sheet drop–off and edge trim following the pickup fit together with trouble-free sheet feeding are among other things-the benefits to be obtained of the perfect performance of the trim edges. In practice, sheet breaks in the paper machine can originate from faults in the sheet edge which are caused by the edge trims. Obviously individual constructional and production factors influence the functioning of the edge trims. For the reason the following is limited to comments on basic sources of error, which in many cases significant causes of the faults which occurred such as water quality, sufficiently high water pressure and angles and position of nozzle etc. The angles and position edge shower nozzles should be optimally adjusted both in relation the machine direction and the cross-machine direction. Machine direction (MD) is the direction of paper and board which parallel to the longitudinal direction of the web. Cross-machine direction (CMD) is the direction perpendicular to the machine direction. The angle of the water jet on the sheet becomes very important with the addition of machine speed. With increasing machine speed, the angle of impingement of the water jet on the sheet becomes increasingly important. The water jet of a slightly obliquely positioned nozzle in MD (between 20 and 40 degree from the vertical on the fabric) hits the sheet equally obliquely in the machine direction, see Fig 1.b. Additionally the speed difference between the water jet and the fabric must be taken into account. Inclined position prevents or reduces the effects of the water and bounce back to the mist generation fiber. In this way a clean cut is obtained. At the same time it is a position the nozzle also slightly obliquely in CMD about 6-12mm depending on basis weight, grade and speed, so that the jet is directed towards the edge trim. In this way the cut edge of the edge trim is disrupted securely from the sheet by a light under wash, see Fig 1.c. The function of the passage of high-speed paper machines could be affected by the edge of the paper defects-cracks, creases and tears. Performance operation for the edge trim shower system for reducing sheet break is very importance. Accurate sheet trim position of edge trim shower are very important to get good trimming of the sheet but it is very difficult to set the nozzle position. Whereas, the users often change to correct position of the edge trim shower that it's depending on production planning (grade, basis weight of sheet paper, and speed of the machine). The edge trim shower system usually still using manually for setting the nozzle position, see Fig 1.a. The edge trim shower systems are installed at front and back in CMD. Therefore the system can be changed automatically as a replacement of manually system. The

automatic nozzle position can be adjusted obliquely in MD and CMD. Therefore this project are performed to study the characteristic of DC motor by conducting simulations of a DC motor using PD-Fuzzy Logic controller systems for position control of edge trim shower.

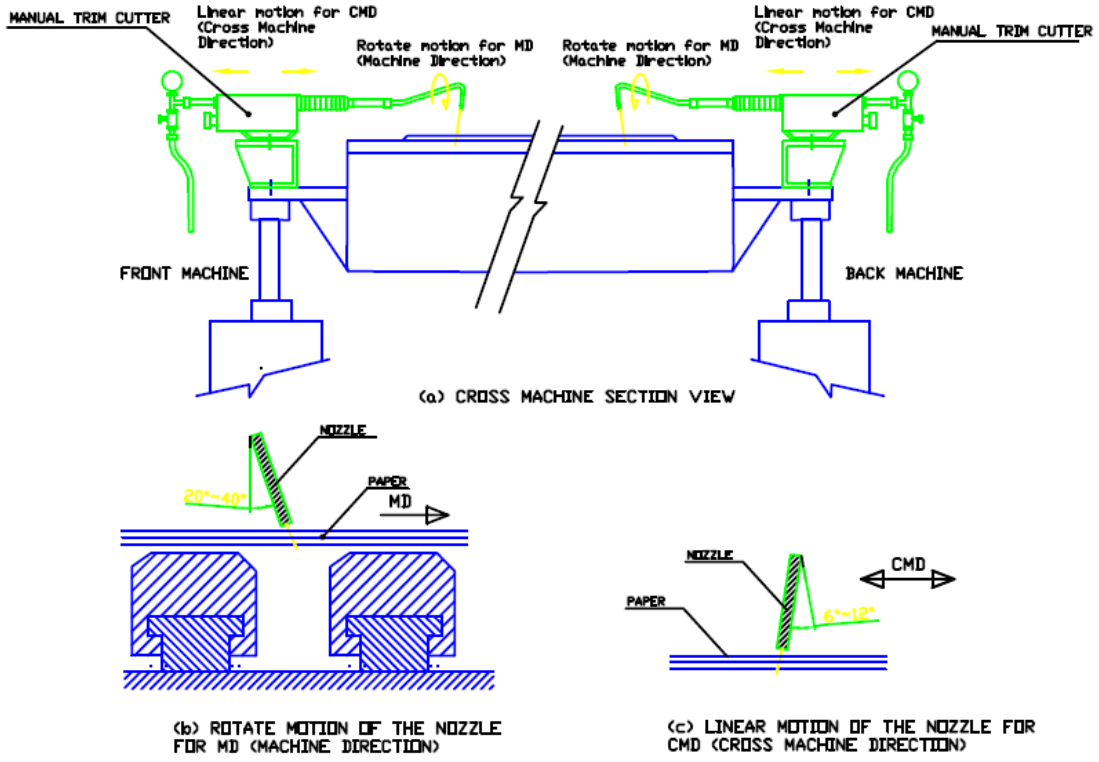


Fig. 1. (a) Cross Machine section view; (b) Rotation motion of the nozzle for MD (Machine Direction); (c) Linear motion of the nozzle for CMD (Cross Machine Direction)

4.1.34 DC motor

An electric motor is an electric machine that can convert electrical energy into mechanical energy that can be tailored to the needs. AC and DC motors are two types of motor drives currently being used in every industry. Although direct current (DC) motors can be considered much better than alternating current (AC) motors especially when considering transportation parts because of their maximum torque producing quality at stalls which is very poor in AC motors. DC motors are powerful words for extensive use in modern technology and in almost every industrial application robot manipulation and appliances where speed and position control of motor is required. DC motor is much better then AC motors for energy recovery mechanism. Moreover DC motors provide a low horsepower rating at a much cheaper rate than AC motor drives. To achieve maximum productivity, everything from the machine must be taken into account and analysed accordingly. In the motor control system, hundreds of problems encountered such as changes in the dynamics of the load. Factors affecting the most important would be the noise parameters are too many different and unexpected that affect the functioning of the machine. Similarly, the other major factor is the speed that must be continuously monitored in accordance with the requirements for the desired output and reliable. Proportional-integral-derivative (PID) controllers are commonly used for controlling speed and position of motors because their simple structures and intuitionally comprehensible control algorithm. Controller parameter is generally set using a hand -tuning or frequency response method Ziegler - Nichols. Both methods have a successful outcome but time and effort required to obtain a satisfactory response system. Two of the major problems encountered in motor control are time-varying nature of motor parameters on the operating conditions and the absence of noise in the system loop. Methods frequency response Ziegler - Nichols typically used to adjust the parameters of the PID controller. However, what

is needed to get the system into oscillation mode for realizing the tuning procedure. But it is not always possible to get most of the plant technology into oscillation. The proposed approach uses both fuzzy controller and response optimization methods to obtain approximate values of controller parameters. Then the parameters can be slightly varied to obtain the specified performance of the real-time control systems. Thus, this is a real problem for designing an adaptive PID controller without the system to oscillation mode.

4.1.35 Mathematical model of DC motor

Consider in DC motor, whose electric circuit of the armature and free-body diagram of the rotor are shown, see Fig. 2.

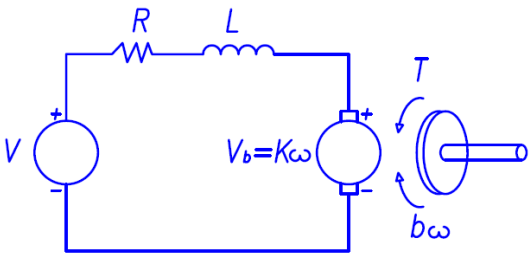


Fig. 2. DC motor model

T (Nm) is the motor torque which is related to the current of phase ***i*** (A) by a constant factor ***K*** (Nm/A):

$$T = Ki \quad (1)$$

Vb is the back electromotive force (emf) which is related to angular velocity ***θ*** by:

$$Vb = K\omega = K\frac{d\theta}{dt} \quad (2)$$

Base on fig. 2 that the Kirchhoff's and Newton's law can be written the equation as follow:

$$J\frac{d^2\theta}{dt^2} + b\frac{d\theta}{dt} = Ki \quad (3)$$

$$L\frac{di}{dt} + Ri = V - K\frac{d\theta}{dt} \quad (4)$$

J (kg.m²) is moment of inertia of the rotor, ***b*** (Nms) is damping of the mechanical system, ***L*** (H) is electric inductance, ***R*** (Ω) is electric resistance.
By using the Laplace transform that the equations (3) and (4) can be described as follow:

$$Js^2\theta(s) + bs\theta(s) = KI(s) \quad (5)$$

$$RI\,(s) + LsI(s) = V(s) - Ks\theta(s) \quad (6)$$

where **s** indicates the Laplace transform, from (6) can be described ***I*** (s):

$$I(s) = \frac{V(s) - Ks\theta(s)}{R + Ls} \quad (7)$$

and combined it with (5) equation to obtain:

$$Js^2\theta(s) + bs\theta(s) = K\frac{V(s) - Ks\theta(s)}{R + Ls} \quad (8)$$

With equations can be show a DC motor block diagram as follow:

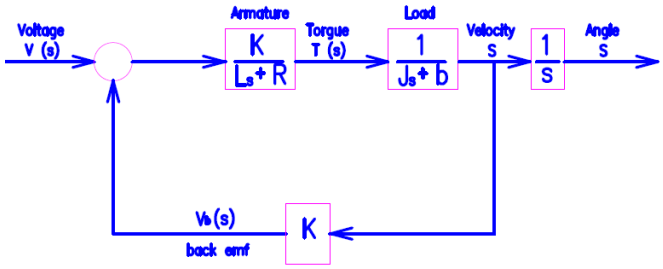


Fig. 3. Block diagram DC motor

From the output angle $\boldsymbol{\theta}$ and the input voltage $\boldsymbol{V}$ (s) can be described as transfer function as follow:

$$Ga\,(s) = \theta(s) \,/\, (V\,(s)\,) = K\,/s[(R + Ls)(Js + b) + K^2] \quad (9)$$

And the angular velocity ω and the input voltage V (s) can be described as transfer function as follow:

$$Gv\,(s) = \omega(s) \,/\, (V\,(s)\,) = K\,/(R + Ls)(Js + b) + K^2 \quad (10)$$

4. PID controller

Proportional-integral-derivative (PID) controller are applied in industry due to their simplicity in structure and their applicability to various processes. Input is an error signal that can be explained by the difference between the reference signal and the output signal. The output of the PID controller is the sum of three terms: proportional term, integral term and derivative term. PID transfer function is represented, see Fig. 4.

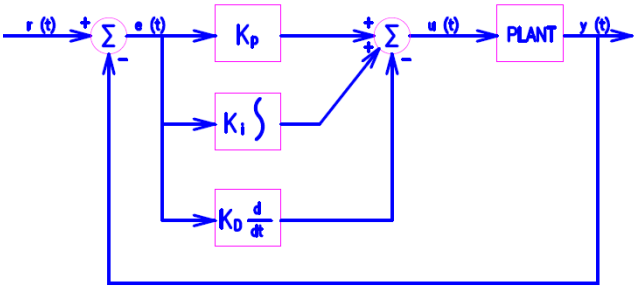


Fig. 4. PID control system

The equation of control signal ***u(t)*** for PID as below:

$$u(t) = Kp\; e(t) + Ki \int e(t)dt + Kd\; (de(t)/dt$$
(11)

$$u(t) = Kp\; e(t) + 1/Ti \int e(t)dt + Td\; (de(t)/dt \quad (12)$$

Proportional gain ***Kp*** , Integral gain ***Ki***, Derivative gain ***Kd***, Integral time ***Ti***, Derivative time ***Td***.

PID controllers can use hand-tuning or Ziegler-Nichols methods. Hand-tuning can be used by experienced control engineers based on the rules, See in Table 1.

Table 1. Hand-tuning rules Operation	Rise time	Overshoot	Stability
Kp (increase)	Faste	Increase	Decrease
Tp (increase)	Slow	Decrease	Increase
1/Ti (increase)	Faste	Increase	Decrease

Ziegler-Nichols method can be used as another method for tuning PID parameters. The rule of procedure is as follows, see in Table 2.

Table 2. Ziegler-Nichols rule Controller	*Kp*	*Ti*	*Td*
P	0.5*Ku*		
PI	0.45*Ku*	*Tu*/1.2	
PID	0.6*Ku*	*Tu*/2	*Tu*/8

5. Fuzzy logic controller

Fuzzy logic expressed using human-language. A fuzzy logic controller is to change the linguistic control strategies into automatic control strategy and fuzzy rules established by the expert experience or knowledge database. FLC (Fuzzy Logic Controller) has four principle units. These are fuzzification, base of knowledge, decision making and defuzzification units. The basic FLC structure is show, see Fig. 5.

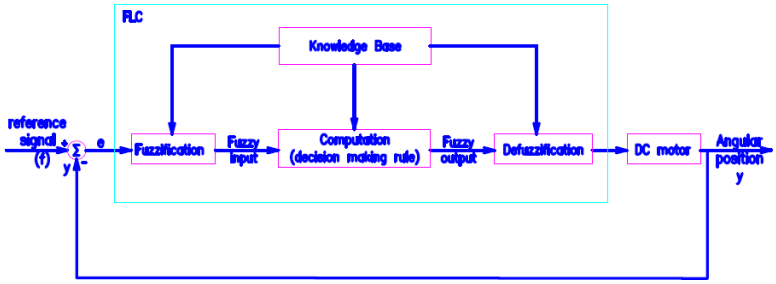


Fig. 5. Basic of FLC

Inputs set the error (e) and set the change of error (ce) where the output variable of the fuzzy logic controller is control voltage. Input and output variables of fuzzy logic controller consist of seven fuzzy sets namely. The input and output names are {NB, NS, Z, PS, PM, PB}, where means NB is negative big, NM is negative medium, NS is negative small, PS is positive small, Z is zero, PM is positive medium and PB is positive big. Fuzzy logic system as shown in Fig 5(a),..and 5(e).

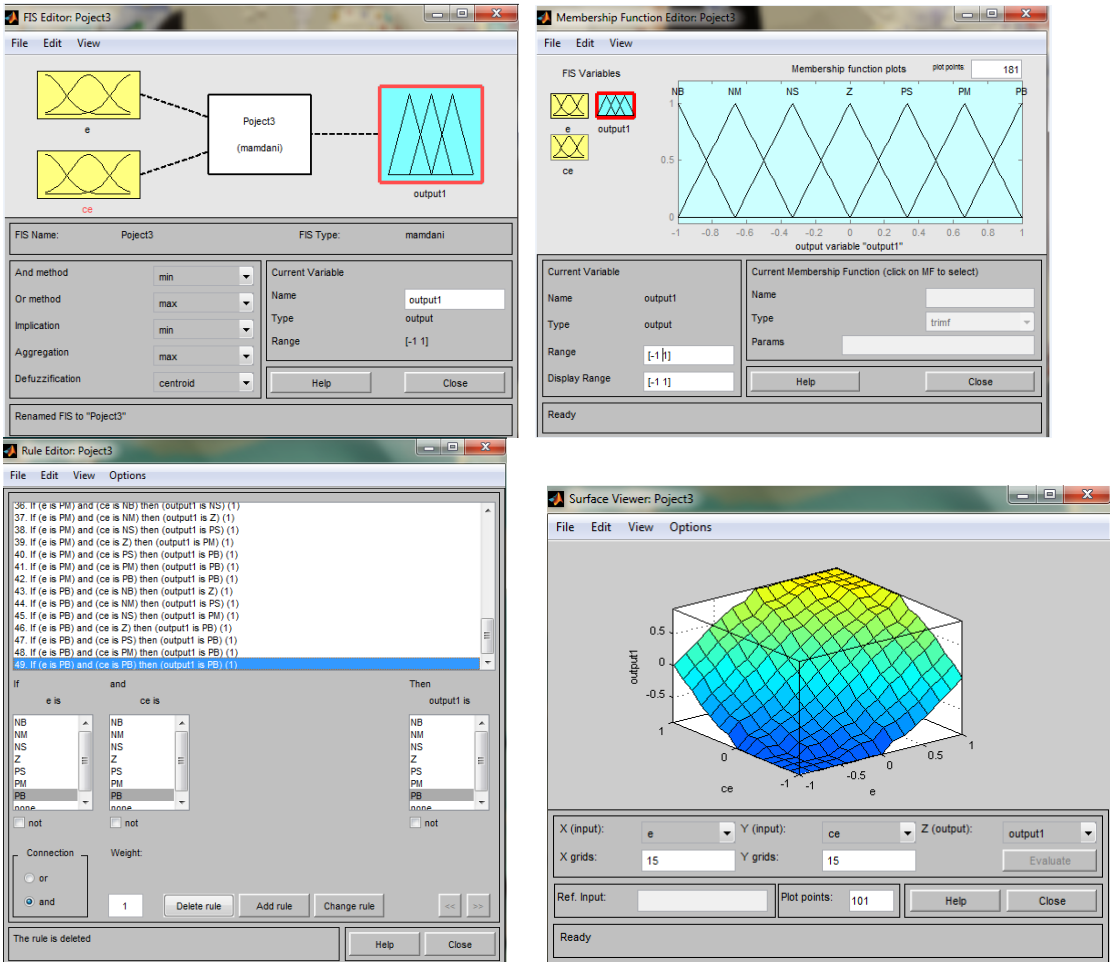


Fig. 5. (a) FIS editor; (b) membership function; (c) rule editor; (d) surface view

6. Conclusion

An accurate position for sheet trim of shower position is required an automation system. DC motor is used as an actuator which can convert electrical energy into mechanical energy. The three control methods can be used for controlling a speed and position of DC motors. The methods are Ziegler-Nichols, Hand- tuning and Fuzzy logic controller. The result table is an example difference tuning methods, Table 5.(8)

Table 5. Methods controller	%Overshoot	Rise time	Setting time	Steady state error
Ziegler-Nichols	70	2	15	0
Hand-tuning	50	1.5	10	0
FLC)	0	1	0	0

Base on the table is found that FLC is better than other methods and performance characteristics also improve the control of DC motor.

References

[1] A. Bellini, C. Concari, G. Franceshini, A. Toscani, "Mixed mode PWM for high performance stepping motors," presented at the 30th Annual conference of IEEE Industrial Electronics Society, IECON November 2004.

[2] Benjamin A. Throp, "Pulp and Paper Manufacturing," Paper Machine Operations,Volume 7

[3] C Kershaw, Hans J. Struck, "Edge Trim Installations in The Forming Section," Heimbach UK Ltd

[4] Fuzzy Logic Toolbox 2, User's Guide (January 10, 2008)

[5] K.P. Ramachandran, G.K. Vijayaraghavan, M.S. Balasundaran, "Mechatronics," Integrated Mechanical Electronic System, ISBN 978-81-265- 1837-1,2008

[6] Curtis D. Johnson,"Process Control Instrumentation Technology," ISBN 0-13-197669-9,1988

[7] Nasser T. and others "Design and Applications of Fuzzy Logic for The Speed Control of a Direct-Drive DC Motor", 4th International Conference, Cattaee, Amman-Jordan 2002.

[8] Ahmed H. Singh G, " controlling of D.C. Motor using Fuzzy Logic Controller," Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013)

The Annual Conference on Management and Information Technology (ACMIT) 2016

Thermal Calculation for Water Cooling Tower To Cool Compressor ATLAS COPCO GA 250 FF

Yudha Khosala
Department Of Mechanical Engineering, Swiss German University, Tangerang INDONESIA

Abstract

The aim of this paper is to choose the correct capacity of Thermal Calculation for Water Cooling Tower to Cool Compressor ATLAS COPCO GA 250 FF since a cooling tower is considered as an essential component for a compressor in an oil and gas pipe manufacture plant. Cooling tower is an equipment device commonly used to dissipate heat from air conditioning, water-cooled refrigeration, power generation units, and industrial process. In this paper, we use a induced draft counter flow tower for the design of cooling tower which based on Merkel's method. The tower characteristic is determined by Merkel's method. A simple algebraic formula is used to calculate the optimum water and air flow rate. This paper calculate the cooling tower characteristic, air flow required, efficiency, effectiveness, and cooling capacity of cooling tower need to cool the compressor compare with the availability cooling tower product in the market. In this paper, we will design based on calculation thermal capacity which lead to decentralizing the cooling tower to reach better energy efficiency of the plant.
Keywords : Cooling Tower, Thermal Design , Merkel's Method;

1.Introduction

The fall of WTI (West Texas Intermediate) crude oil price is affecting oil and gas company around the world. In this condition, oil companies reducing their investments which causing company that supply the goods and service for them also feel the effect. With this condition the company is in efficiency condition and cost reduction is one of the way to be able to survive from the ongoing crisis.

For supplying company that provide pipe for oil and gas, cost reduction means maximizing their production with minimum variable. Since production is low, not all line production is operating at the same time, so centralized cooling tower is over capacity. In this paper, we will design based on calculation thermal capacity which lead to decentralizing the cooling tower to reach better energy efficiency of the plant.

1.1 Theory and Principle

Cooling tower is heat exchanger that work as heat rejection equipment. The main function is to extract waste heat from water to the atmosphere. Heat transfer in a cooling tower is specified as convection between the droplets of water and the air, and also as evaporation which generate a small portion water to evaporate into moving air, the process is involves heat and mass transfer. Cooling tower are used in the power generation unit, refrigeration and air conditioning industries [1].

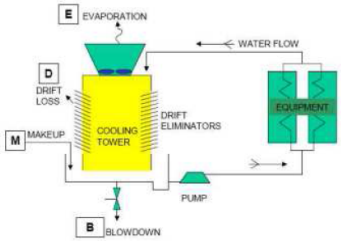


Figure 1. Diagram of Cooling Tower [4]

Water pumped from the tower basin cooling water through the process cooler and condensers in an industrial facility. The water absorb heat from the hot process which need to be cooled or condensed and absorbed heat warms the circulating water. The warm water return to the top of the cooling tower and trickles downward over the fill material inside the tower. Warm water trickles down, it comes in contact with ambient air rising up through the tower either by natural draft or forced draft using large fans in the tower. That contact causes a small amount of the water to be lost as wind age and some of the water to evaporate. The water back to the original basin water temperature and the water is then ready to recirculate [2].

Cooling tower can be classified by the movement of water and air as counter-flow and cross-flow types. Cooling tower can also be classified by air flow into mechanical draft and natural draft types. A cooling tower is a device for evaporative cooling of water using air contact. The main function of cooling tower is to remove waste heat into the atmosphere. Cooling towers are an integral part of much industrial processes such as oil refineries, petrochemical, thermal power plants, and chemical plants and HVAC system for cooling buildings [1], [4].

1.2 Purpose of a Cooling Tower

Cooling Tower is used by industrial applications that produce waste heat as a by-product of their operations. It provides energy efficiency and environmental friendly means of rejecting waste heat, saving our natural bodies of water from receiving quantities of warm water. They allow wind and air circulation to diffuse heat from the factories or manufacturing plants [1].

1.3 Type of a Cooling Tower

Base on the water and air flow arrangements, cooling towers divided into two type:

1. Natural draft
   Natural draft tower use large concrete chimneys to introduce air through the media. These types of tower normally used by utility power stations [4].
2. Mechanical draft
   Mechanical draft towers are available in the following airflow arrangements:
   - Counter flows induced draft.
   - Counter flow forced draft
   - Cross flow induced draft.

In the counter flow induced draft design, hot water enters to the top, while the air is introduced at the bottom and exits at the top of tower . Both forced and induced draft fans are used. For cross flow induced draft towers, the water enters at the top of tower and passes over the fill. An induced draft fan draws the air across the water fill and exit through the top of the structure [4].

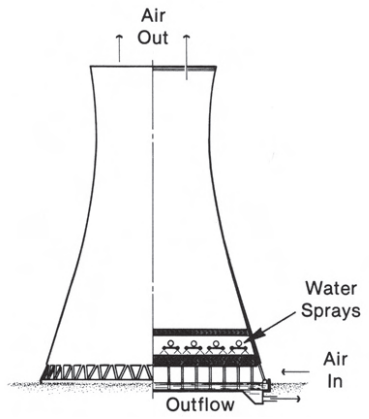


Figure 2.Counter flow Natural draft Tower [4]

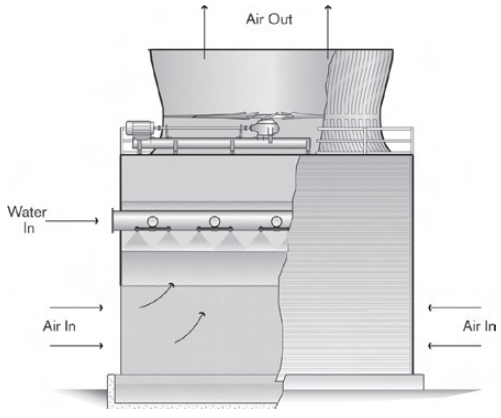


Figure 3.Induced draft counter flow Tower [4]

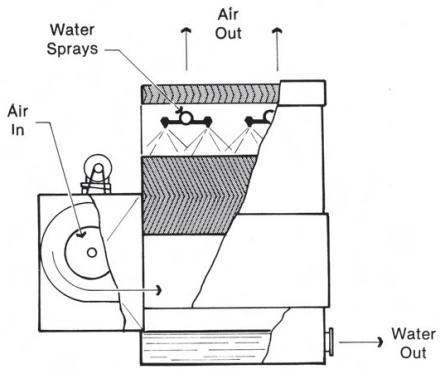


Figure 4.Forced draft counter flow blower fan tower [4]

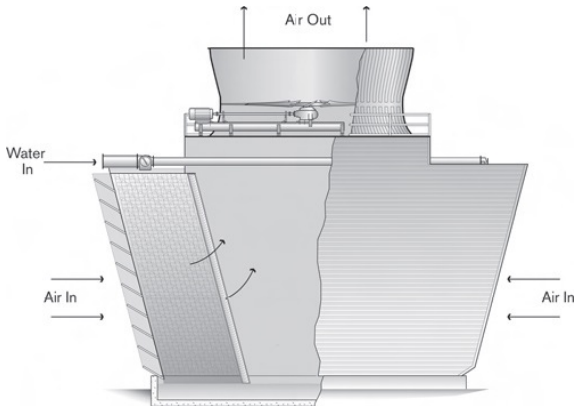


Figure 5.Cross flow Induced draft [4]

Nomenclature

a	surface area per unit volume (m-1)
Cp,	a specific heat of saturated air, (kJ/kg)
Cw	specific heat of water, (kJ/kg K)
G	mass air flow rate (kg/sec)
Hw	enthalpy of saturated air at local water temperature, (kJ/kg)
Ha	enthalpy of local air stream, (kJ/kg)
Ha1	enthalpy of inlet air, (kJ/kg)
Ha2	enthalpy of outlet air, (kJ/kg)
ΔH1	enthalpy difference, (kJ/kg)
ΔH2	enthalpy difference , (kJ/kg)
ΔH3	enthalpy difference , (kJ/kg)
ΔH4	enthalpy difference , (kJ/kg)
K	mass transfer coefficient, (kg/m2 sec)
L	mass water flow rate, (kg/sec)
P	ambient pressure, (kPa)
ΔTw	water temperature different, (^oC) [= (T_1-T_2)]
T_1	inlet water temperature, (^oC)
T_2	outlet water temperature, (^oC)
Ta1	inlet air temperature, (^oC)
T_{wb}	temperature wet bulb, (^oC)
V	volume of packing, (m^3)
Vair	volume Air flow capacity (m^3/minute)

2. Cooling Tower Performance and Characteristic

Before designing a cooling towers, very important to determine the range and approach. Approach varies the entering air wet bulb temperature, flow rate of water and heat load. The first step in design cooling tower is to choose the design condition like inlet water temperature, outlet water temperature, water flow rate and inlet air wet bulb temperature [3].

The parameters from the point of determining the performance of cooling towers, are:

1. Approach
   is the difference between the cooling tower outlet cold water temperature and ambient wet bulb temperature. [1].
2. Range
   is the difference between the cooling tower water inlet and outlet temperature
3. Characteristic of Cooling Tower Heat transfer [5]
   This heat transfer process can generally be modeled using the Merkel Equation :

$$KaV/L = \int_{T_2}^{T_1} dT/(h_w - h_a) \quad (1)$$

where
KaV/L = Cooling tower characteristic;
K = Mass transfer coefficient, lb water/hr ft2;
a = contact area/tower volume, 1/ft;
V = active cooling volume/plan area, ft,
L = water mass flow rate, lb/hr ft2;
T1 = entering (hot)water temperature, ^{o}F;
T2 = leaving (cold) water temperature, F;
T = bulk water temperature, 8F,
hw = enthalpy of air–water vapor mixture at bulk water temperature, Btu/lb of dry air;
ha= enthalpy of air–water vapor mixture at wet bulb temperature, Btu/lb of dry air.

While the tower characteristic can be calculated from eq (1) using numerical method, it can be also be represented graphically as shown in figure below:

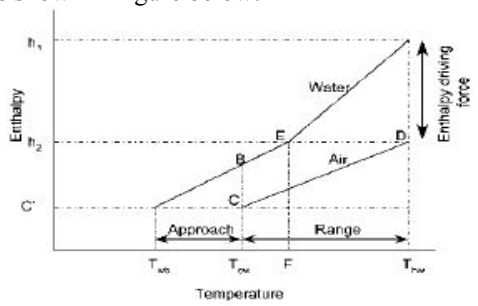


Figure 6. Graphical representation of the cooling tower characteristic [5]

where

C'	entering air enthalpy at entering air wet bulb temperature (T_{wb}),
BC	initial enthalpy driving force
CD	air increasing enthalpy line with slope L/G
DEF	projecting the leaving air point onto the water operating line and then onto the temperature axis yield the outlet wet bulb temperature
ABCD	the area within this region is graphical solution for cooling tower characteristic.

The amount of the heat lost by water is equal to the enthalpy rise is the air [3]. The heat balance equation is written as :

$$C_W \Delta t_w \, L = \Delta H_a \, G \quad (2)$$

Cooling Tower Efficiency
since a cooling tower base on evaporative cooling, the maximum cooling tower efficiency is influenced by the wet bulb temperature (T_{wb}) of the cooling air [1]
The cooling tower efficiency can be expressed as

$$\eta = (T_1 - T_2)100/\ (T_1 - T_{wb}) \quad (3)$$

where η = Cooling tower efficiency, T_1 = inlet temperature of water to the tower,
T_2 = outlet temperature of water from the tower ,
Twb = wet bulb temperature of air

Cooling tower effectiveness
*i*s the ratio of range, to ideal range, difference between cooling water inlet temperature and ambient wet bulb temperature, or in other words is = Range / (Range +Approach) [1],[2].
The effectiveness of cooling tower can be expressed as

$$\varepsilon = (T_1 - T_2)/(T_1 - T_{a1}) \quad (4)$$

Cooling Capacity
Cooling Capacity is the heat rejected given as product of water mass flow rate, water specific heat and temperature difference [1],[2].
The cooling capacity can be expressed as

$$HL(\text{ Heat Loss}) = L \times Cw \times \Delta tw \quad (5)$$

3. Design of Cooling Tower

In company ABCD, the fall of crude oil price effected of productivities in pipe production became 30% of total production capacity. This condition affected of production schedule that not all machine operation every day. Atlas Copco GA 250 FF Rotary Screw Oil Injected Air Compressor. Motor speed 1487 rpm, power 263 kW, 400V, intensity 440. Air flow rate 1236 cubic feet/minute (35 m3/min), maximum working pressure 118 psi (8.2 bar).[6]. Instead of 4 compressor running continues together in normal production, now a day only running 1 until 2 compressor intermittent base availability material to process.

Data Measurement Temperature and Flow Water
The data that collected is the data that come from manual book and also data from measurement temperature of water and air in the utility area where the compressor installed and also the current central cooling tower was installed. in this calculation was limited to 1 time measurement, there is possibilities the variant of temperature change affected by weather when the ambient temperature getting hot or cloudy/rain.

Table 1. Data Measurement Temperature and Water Flow

Water Temperature Outlet Compressor	39.7	°C
Water Temperature inlet compressor	30	°C
Temperature ambient	28	°C
Cooling Water flow	5.6	l/s
Humidity	80	%
Assume temperature Outlet Cooling tower	33	°C
Temperature wet Bulb	25	°C

Psychrometrics of Evaporation
Understanding the evaporation cooling process can be enhanced by tracing on psychometric chart (fig.7) the change in condition of a pound of air as it moves through the tower and contacts a pound of

water (L/G =1), as denoted by solid line. Ambient air , at 78 ^{o}F DB and 50% RH, enters to the tower at point 1 and begin to absorb moist in an effort to gain equilibrium with the water. This process continue until the air exits the tower at point 2 [4],[5].

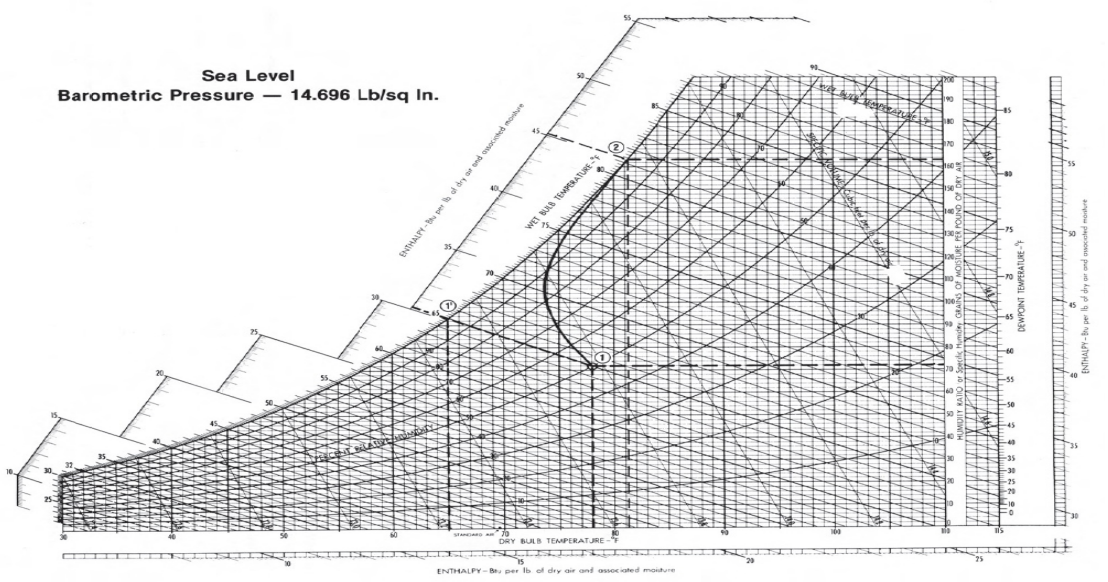


Figure 7. Psychrometric Chart Air - Water temperature curve [4],[5]

4. Conclusion

Base on the Calculation we choose cooling tower type induced draft counter flow cooling tower. In the market we found some cooling tower manufacturing and type of cooling tower, in this design we choose induced draft counter flow cooling tower due to more compact size with capacity same as calculation result : capacity air volume 559 m3/min. and water flow capacity is bigger than calculation 336 l/min. In the ideal condition, the heat loss by water must be equal to heat that absorbed by air, but in the actual practice it is not possible because some type of loses. In order to cover some losses, we have to choose the cooling tower that we need to multiply by 1.25 of calculation capacity as safety factor. The product we choose is a product with one level higher than ideal calculation which is a cooling tower with air volume capacity 700 m3/min to compensate the variation of ambient temperature if the ambient temperature increasing during the day.

References

[1] Balashanmugan P, Balasaubramaian G. Experimantal Study on the Design of Cooling tower for Central Air Conditioning Plant.International Journal of Engineering and Technical Research (IJETR) March 2014.ISSN:2321-0869

[2] Shah Ronak, Rathod Trupti, Thermal Design of Cooling Tower . International Journal of Advanced Engineering Research and Studies(IJAERS) April-June 2012. E-ISSN2249-8974

[3] Shah Parin, Tailor Nishant. Merkel's Methode for Designing Induced Draft Cooling Tower. International Journal of Andvanced Research in Engineering and Technology (IJARET) . Volume 5, issue 2, February 2015,pp63-70. ISSN 0976-6499

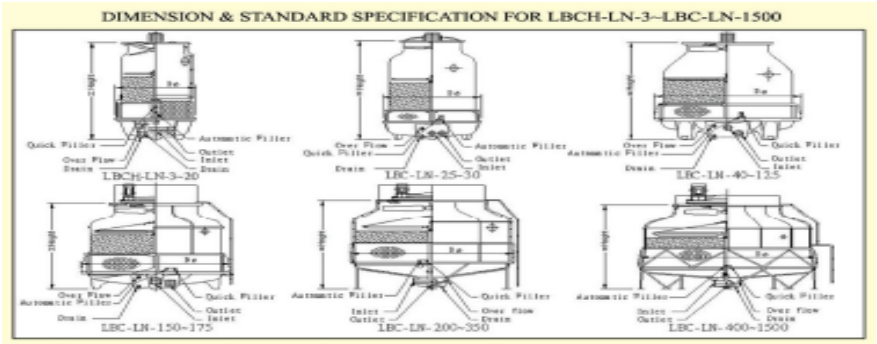
[4] Hensley John C. Cooling tower Fundamentals. SPX Cooling Technologies, INC. Overland park, Kansas USA, 2009 [Section1 p.7-33]

[5] Stanford III, Herbert W. HVAC Water Chiller and Cooling Towers Fundamental Application and Operation. Marcel Dekker, Inc. New york. 2003 [Chapter 9 p. 115-120]

[6] Instuction Book for Compressor GA 250 APF164827. Atlas Copco. August 2011.

Appendix A.

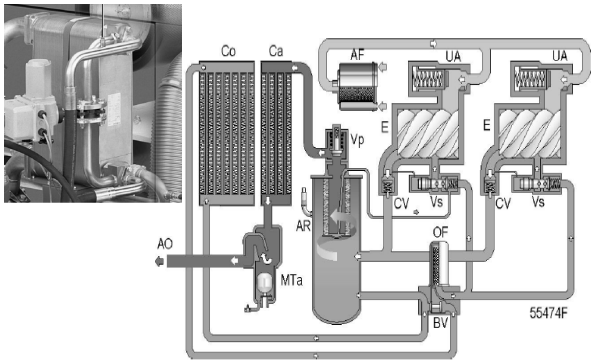
A.1 Specification of Cooling Tower



Tower Model LBC-LN	Cooling Capacity Kcal/Hr *1	Nominal Water Flow L/min	Dimensions mm H Height	Dimensions mm D Dia.	Fan Assembly Motor HP	Fan Assembly Air Volume m3/min	Fan Assembly Fan D ϕ mm	Pipe Connections(A) mm *2 INLET	OUTLET	DRAIN	OVER FLOW	Filter *3 Automatic (Ea)	Filter *3 Quick (Q)
H-3	11700	39	1410	750	1/6	25	500	40	40	20	25	15	15
H-5	19500	65	1410	750	1/6	60	500	40	40	20	25	15	15
H-8	31200	104	1690	860	1/6	75	500	40	40	25	25	15	15
H-10	39000	130	1690	860	1/4	100	500	40	40	25	25	15	15
H-15	58500	195	1940	1170	1/4	135	670	50	50	25	25	15	15
H-20	78000	260	1940	1170	1/2	180	670	50	50	25	25	15	15
25	97500	325	1970	1380	3/4	160	770	65	65	50	25	15	15
30	117000	390	2305	1580	1	200	770	65	65	50	25	15	15
40	156000	520	2340	1820	1	260	970	65	65	50	25	20	20
50	195000	650	2340	2000	1	330	970	80	80	50	25	20	20
60	234000	780	2345	2000	1 1/2	420	1170	80	80	50	25	20	20
70	273000	910	2395	2175	1 1/2	450	1170	100	100	50	25	20	25
80	312000	1040	2395	2175	1 1/2	500	1170	100	100	50	25	20	25
100	390000	1300	2585	2650	2	630	1470	100	100	50	25	25	25
125	487500	1625	2610	3050	2	750	1470	125	125	50	50	25	25
150	585000	1950	2580	3300	5	950	2360	125	125	50	50	25	25
175	682500	2275	2780	3300	5	1150	2360	125	125	50	50	25	25
200	780000	2600	2890	3370	5	1250	2360	150	150	50	50	32	32
225	877500	2925	3054	3370	7 1/2	1750	2970	150	150	50	50	32	32
250	975000	3250	3300	3370	7 1/2	1750	2970	200	200	50	50	32	32
300	1170000	3900	3355	4440	10	2200	2970	200	200	50	50	32	32
350	1365000	4550	3461	4790	10	2200	2970	200	200	50	50	32	32
400	1560000	5200	4000	5180	15	2600	3380	200	200	50	100	50	50
500	1950000	6500	3835	5580	15	2600	3380	250	250	50	100	50	50
600	2340000	7800	4360	6600	20	3750	3580	250	250	50	100	50	50
700	2730000	9100	4605	6600	20	3750	3580	250	250	50	100	50	50
800	3120000	10400	4945	7900	30	5000	4270	300	300	80	100	50	50
1000	3900000	13000	5145	7900	30	5000	4270	300	300	80	100	60	60
1250	4875000	16250	5870	8430	40	6200	4270	300	300	80	100	65	65
1500	5850000	19500	6300	8430	50	7500	4270	350	350	80	100	65	65

A.2 Compressor and Flow Diagram

Compressor GA 250 FF



Flow diagram Compressor GA 250 FF

A.3 Cooling tower calculation

Cooling Tower Approach
CTA = T2 - T_{WB} = 30 - 25 = 5°C

Cooling Tower Range
Range = T1 - T2 = 40 - 30 = 10 °C

Heat Balance Equation
The amount of heat removed from the water must be equal to heat that absorbed as shown by equation below :

Cw x Δtw x L =ΔHa x G
4.186 (40-30)5.6 = (117.46 - 95.36) G

Since we need to find air flow rate of cooling tower, we assume that the air outlet cooling tower is the same value of Cooling tower Approach 5°C, so we can define 28°C + 5°C , using enthalpy air at 33°C we can get air flow rate required to cooling tower is G = 234.42/22.1 = 10.6 kg /s. From the calculation we can found also the water to air mass flow ratio (L/G) from the equation = 5.6 /10.6 = 0.528. To find Volume of air required in the cooling tower can be shown by equation
Vair= G x VS1 ,

where
Vs1 is Specific volume of air inlet temperature 28° C = 0.879 M3/kg.

So Vair= 10.6 x 0.879 =9.317.06 m3/s.≈ 559 m3/min.

Merkel gives the cooling tower characteristic equation as :
$KaV/L = \int_{T_2}^{T_1} dT/(h_w - h_a)$
(KaV/L) = [(T1 - T2)/4] x {(1/Δh1) + (1/Δh2) + (1/Δh3) + (1/Δh4)

now

Δh1 = Value of Hw - Ha at T2 + 0.1(T1 - T2)
Δh2 = Value of Hw - Ha at T2 + 0.4(T1 - T2)
Δh3 = Value of Hw - Ha at T1 - 0.4(T1 - T2)
Δh4 = Value of Hw - Ha at T1 - 0.1(T1 - T2)

Calculation for ΔH1
= T2 + 0.1(T1 - T2)
= 30 + 01(40 - 30)
= 31 °C
Value of Hw at 31°C = 129.23 KJ/Kg
Value of Ha at 31°C = 109.32 KJ/Kg
ΔH1 = Hw - Ha = 19.91 KJ/Kg
Calculation for ΔH2
= T2 + 0.4(T1 - T2)
= 30 + 04(40 - 30)
= 34 °C
Value of Hw at 34°C = 142.47 KJ/Kg
Value of Ha at 34°C = 130.25 KJ/Kg
ΔH2 = Hw - Ha = 12.22 KJ/Kg
Calculation for ΔH3
= T2 - 0.4(T1 - T2)
= 30 - 04(40 - 30)
= 26 °C
Value of Hw at 26°C = 109.04 KJ/Kg
Value of Ha at 26°C = 86.06 KJ/Kg
ΔH3 = Hw - Ha = 22.98 KJ/Kg

Calculation for ΔH4
= T2 - 0.1(T1 - T2)
= 30 - 0.1(40 - 30)
= 29 °C
Value of Hw at 29°C = 121.57 KJ/Kg
Value of Ha at 29°C = 97.69 KJ/Kg
ΔH4 = Hw - Ha = 23.88 KJ/Kg
so (KaV/L) = [(40 - 30)/4] x {(1/19.91) + (1/12.22) + (1/22.98) + (1/23.88) = 0.525
Efficiency of Cooling Tower
η = (T1 - T2)/(T1 - T_{WB})
η = (40 - 30)/(40 - 25) = 66.7 %
Effectiveness of Cooling Tower
ε = (T1 - T2)/(T1 -Ta1)
ε = (40 - 30)/(40 - 28) = 0.833
Cooling Capacity
HL= L x Cw x Δtw
= 4.186 (40-30)5.6
= 324.4 KJ/s ≈ 843 897.6 KJ/hr

The Annual Conference on Management and Information Technology (ACMIT) 2016

How the Role of Risk Tolerance on Manage Satisfaction Level

Sand Frans C. Nainggolan
MIT Student, EduTown BSD City, Tangerang, 15339, Indonesia

Abstract

Many major firms within the world, particularly in Indonesia, they contend to every different to allow best services as the way to achieve the goal of their main business. They need launched several programmes to enhance and commit for higher quality management by approach of listening their customers. In an exceedingly service surroundings, info on client response toward services is one in all the simplest key component of feedback that indicates whether good or not, the services meet into perception or even below expectation. Someday what we would like is simply assembling info from client and re-evaluation to actual system of performance report. Supported analysis and assesment, we would like change some parameters to satisfy into the client expectation that become their satisfaction. Since client satisfaction can bring United States into trust and commitment, that loyalty are going to be the the last word goal and bussiness can continue once more and once more, coincidental.
To adjust some parameters appears straightforward however really all tough. To measure Perception and Expectation become Service Quality is tough, want observation from time to time to induce the best values, particularly to face risk factors like internal and external setting factors, Risk Management capability, IT capability, and IT-related business capability become Risk Response. To achieve the goal to produce Service Quality between Risk Factors and Risk Response, we have got to regulate Risk Tolerance to induce ideal worth and at an equivalent time manage service quality.

"Keywords: Service Management, Risk Management, Tolerance, Satisfaction;"

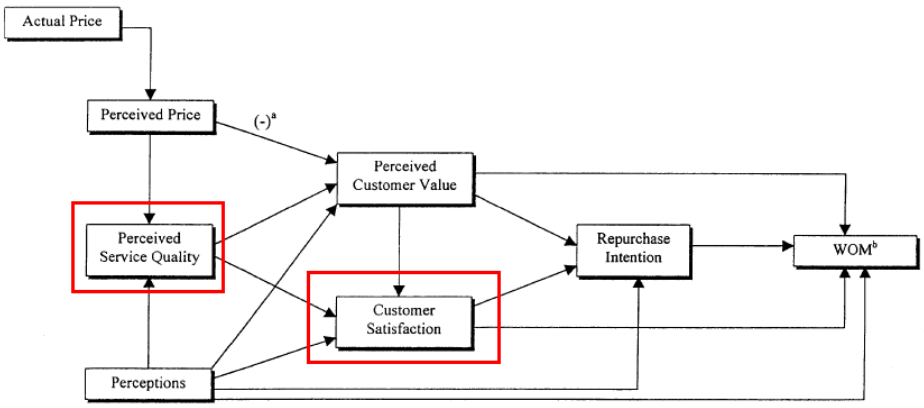
1. Introduction

Loyalty is that the final goal of success of the many corporations to require care of customers which is this most tough challenges because of maintaining of customer's psychological and behavior since these factors are not simple to regulate the changes of them. However, after we produce the standard of service as worth, thus it will conjointly maintain quality of the connection of three main elements (satisfaction, trust and commitment) incessantly then we are able to get their loyalty and generate it mechanically.[1] So, we can see that to maintain the satisfaction the maximum amount as attainable and within the same time will increase trust level continously. In fact, this ideal condition is usually difficult to realize once some Risk Factors happen and the way responsive we have a tendency to area unit to resolve or to mitigate for any risk. within the real state of affairs Risk Factors like internal and external setting factors, risk management capability, IT capability, and IT-related business capability are not continuously will resolve as presently as attainable however we are able to deal to place a threshold as Risk Tolerance as a part of Service Quality in an agreement as Service Level Agreement. That's why inter-correlation between Loyalty and service Quality can become a problem if we have a tendency to cannot define it with agreed value. For that the problematic of our study was as follow: - How role of risk tolerance to manage satisfaction level in Telecommunication Company?

3.1 Service Quality

In International Journal of Hospitality Management, introduced a 22-item scale, called as SERVQUAL, for measuring service quality which is this model already adopted by many across industries. In service quality, customer has measured indirect comparison between expectations (pre sales) and perception (after sales) of company performance. That measure is indicated by, or outlined as, the arithmetic of perceived service quality and customer satisfaction across the 22 measurement items. They are then reduced to fewer factors like dependability, Assurance, Tangibles, Emphaty, and Responsiveness through correlational analysis. The result scores will represent service quality are "indirect" to the researcher(s), not the subjects themselves (customers), performs the comparison between expectations and perceptions. [2], [3]

Figure 1. Model of service quality and satisfaction



Note: Arrows indicate hypothesized causal effects.
[a] The hypothesized relationship is negative; all the other causal paths are hypothesized to be positive.
[b] Word-of-mouth communication intention.

3.2 Customer Satisfaction

Theory posits that customers measure their satisfaction with comparisons between their expectations and perceptions toward target service as a result of subjective (or direct). To provide that comparison value, mostly some customers directly asked as questioner for obtaining some parameter value through "worse than/better" scale. The perceptions and expectations are determined can influence satisfaction of customer and subjective to be confirmation.

Another item to be considered to support Customer Satisfaction is Customer Value itself. We have to examine between price and quality. Mostly, when the price is higher then will indicate higher quality as well, which this will implicate also more higher Customer Value than more higher Customer Satisfaction level since the expectation will be more and more.[3] To accommodate this situation, most of company aware to provide the perception of quality service more precise.

3.3 Risk Tolerance Threshold

Risk tolerance is the level of risk appetite which is value of deviation still can be tolerable and business objectives.[4] Propose Risk Tolerance threshold is creating the boundary to take care of customer satisfaction to meet its objectives and express limitation of perception measurement to the underlying business objectives and impacts (acceptable and unacceptable). Most of the time, Risk Tolerance can inter-related to five factors for SERVQUAL (Reliability, Assurance, Tangibles, Emphaty and Responsiveness).[5]

4.1.36 Methodology and Hypotheses

Sometimes unwanted event is something that unavoidable but how to emphasize impact of customer satisfaction on loyalty, was drafted as following hypothesis:

- Customer loyalty, at Telecommunication Company, impacts positively on trust, and trust will generates commitment to be loyalty to company.
- To get better hypothesis, we have the objective: "To find out customer satisfaction towards telecom service providers in PT. XYZ"

But to create a trust and a commitment, we have to line up some attending to manage the chance, we are going to use the chance IT Framework for reference on Risk Analysis, Risk Response. This framework tells once the matter or the risk came to intercept, that we have to analysis and estimate frequency and also the impact. If the chance exceeding risk tolerance level then consequent step is choose risk response possibility. To measure the risk tolerance level is referring to service level agreement and actual condition from customer side since sometime perhaps the value of threshold already below from the agreement however if actual condition still under-control then it may be compromised as a part of the chance tolerance, further over SERVQUAL.

3.1 Sample data

The data will collect from database outage in one of telecommunication company from W17-W33 2015. Those data will indicate repeatitive complaint toward service level agreement. Repeat complaint state is indicating a trust and within SLA state is indicating a commitment. During that period, we can process and combine data between repeat complaint and within SLA into percentage (%).

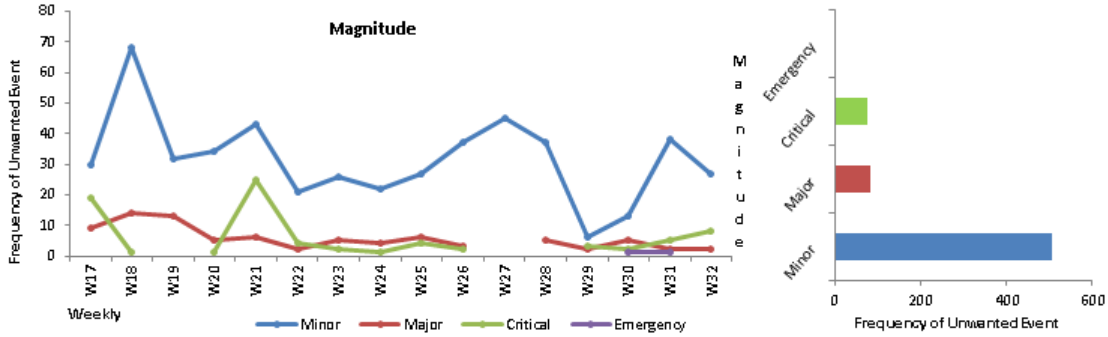


Figure 2. (a) Trend Magnitude of Outage towards Frequency – Weekly; (b) Magnitude vs Frequency

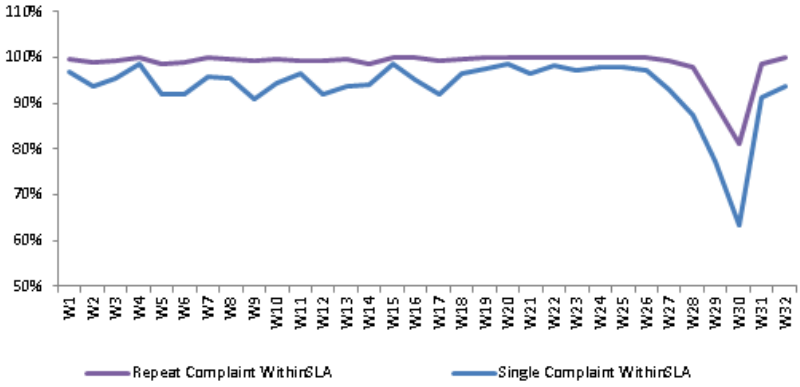


Figure 3. Impact of Unwanted Event (Outage) towards to SLA (Trust & Commitment)

Table 1	Repeat Complaint		Single Complaint	
Period	WithinSLA	OverSLA	WithinSLA	OverSLA
2015-1	99.77%	0.23%	99.77%	0.23%
2015-2	99.46%	0.54%	99.46%	0.54%
2015-3	99.62%	0.38%	99.62%	0.38%
2015-4	99.83%	0.17%	99.83%	0.17%
2015-5	99.19%	0.81%	99.19%	0.81%
2015-6	99.34%	0.66%	99.34%	0.66%
2015-7	99.83%	0.17%	99.83%	0.17%
2015-8	99.67%	0.33%	99.67%	0.33%
2015-9	99.72%	0.28%	99.72%	0.28%
2015-10	99.84%	0.16%	99.84%	0.16%
2015-11	99.68%	0.32%	99.68%	0.32%
2015-12	99.61%	0.39%	99.61%	0.39%
2015-13	99.77%	0.23%	99.77%	0.23%
2015-14	99.38%	0.62%	99.38%	0.62%
2015-15	99.90%	0.10%	99.90%	0.10%
2015-16	99.93%	0.07%	99.93%	0.07%
2015-17	99.63%	0.37%	99.63%	0.37%
2015-18	99.80%	0.20%	99.80%	0.20%
2015-19	99.89%	0.11%	99.89%	0.11%
2015-20	99.90%	0.10%	99.90%	0.10%
2015-21	99.93%	0.07%	99.93%	0.07%
2015-22	99.91%	0.09%	99.91%	0.09%
2015-23	99.79%	0.21%	99.79%	0.21%
2015-24	99.93%	0.07%	99.93%	0.07%
2015-25	99.92%	0.08%	99.92%	0.08%
2015-26	99.78%	0.22%	99.78%	0.22%
2015-27	99.68%	0.32%	99.68%	0.32%
2015-28	98.88%	1.12%	98.88%	1.12%
2015-29	94.33%	5.67%	94.33%	5.67%
2015-30	91.05%	8.95%	91.05%	8.95%
2015-31	99.38%	0.62%	99.38%	0.62%
2015-32	99.90%	0.10%	99.90%	0.10%

Table 1. Impact of Unwanted Event (Outage) towards to SLA (Trust & Commitment); (refer to Figure 2)

3.2 Result and discussion

In IT Risk Framework, Risk appetite can be defined using risk maps which different bands of risk significance can be defined. This map can be indicated by coloured bands on the risk map shown below figure.[4] in that example, there are four bands of significance:

• Red : Indicates really unacceptable risk. It is too far beyond normal condition (service level agreement), and it should be triggering an immediate to fix the situation.

• Yellow : Indicates increasing risk and above acceptable risk appetite. It should be triggering a mitigation or another adequate response to be defined within certain time boundaries to isolated the risk.

• Green : Indicates no special action required or a normal acceptable level of risk

• Blue : Indicates very low risk, where cost-saving opportunities will be found by decreasing the degree of control or for assuming more risk might arise

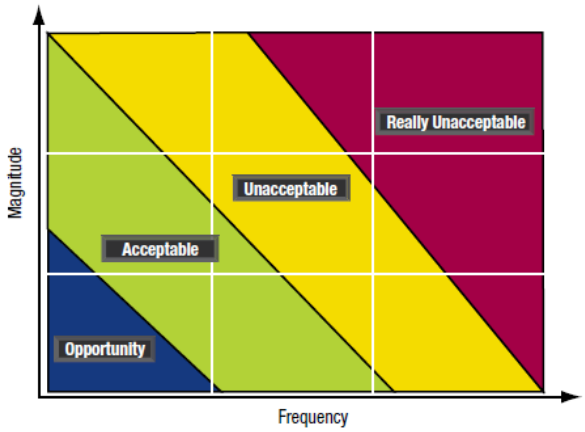


Figure 4. Risk Map Indicating Risk Appetite Bands (The Risk IT Framework)[4]

To adjust Risk Tolerance, should involve parameter of Frequency and Magnitude towards to consider risk as the effect of uncertainty on objectives. Mostly Risk depends on two aspects: the probability of an unwanted event and how it deviate the desired outcomes. Give a time frame can treated as a tolerance, an unwanted event may occur anytime, this may impact or not in the desired outcomes. Thus, unwanted event equal to frequency and impact desired outcomes equal to magnitude. For example, if a single disk fails within a storage system with redundancy, an unwanted event occurred but its impact is low (cost of replacement, but no data has been loss). In business case, the impact of risk will be determined by the penalty which is specified in the SLA.

Thus, based on Risk Map, we can conclude as follow: to keep maintain frequency of unwanted event and magnitude of impact desired outcomes on lower value then it will increasing value of SERVQUAL which is keeping maintain trust and commitment, indirectly. In fact, sometimes, we cannot always reduce unwanted event occur, but good communication to customer for begging tolerance since the impact already below Risk Appetite, is a must even though delta of Risk Tolerance will not bigger than 1-4%. For example, if Risk Appetite in SLA is 95% then risk tolerance might be around 93-94%, depends on particular situation at the time.

We can calculate value of risk tolerance based on experience, culture, magnitude, frequency, duration, asset, services, knowledge, etc. but in this paper we discuss it on magnitude and frequency.

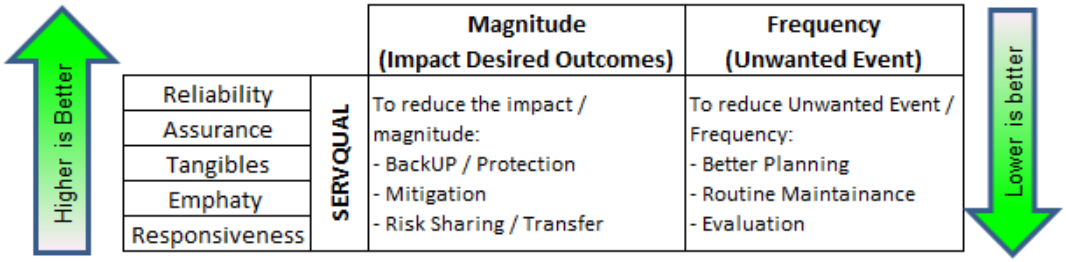


Figure 5. SERVQUAL vs Magnitude&Frequency Model

Customer Service (Weekly Basis)	SERVICE QUALITY	Mean	Standard Deviation
Number of Complaints	Reliability	3.219	1.376
Number of Interruptions	Assurance	3.380	1.737
Outages Clearness	Tangibles	3.676	1.683
Complaint within SLA	Emphaty	3.531	1.379
Hardcomplaint, Priority	Responsiveness	4.435	1.199

Table 2. Mean and Standard Deviation of perception of customers towards Network Condition

The Customer Satisfaction has been computed on some dimensions such as network condition, complaint, SLA, magnitude and those items have been analyzed to measure the opinion of customers using a five point likert scale (Strongly Disagree= 1 and Strongly Agree =5) or (Excellent=5 and Poor=1) has been used to rate the services on the basis of customer satisfaction. Table 2 explains the overall mean and standard deviation of the level Customer Satisfaction towards various services of the risk. It is clear from the table that from Good to Very Good (mean value being more than 3) but however the value of standard deviation is more than 1.0 which indicates a wide variation in the perspective. Even though the statistic said about various perspectives but at least we know when we adjust risk tolerance on various unwanted event which might be lower than risk appetite, we still keep trust and commitment to manage satisfaction of customers.

4.1.37 Conclusions

In this paper, on the idea of hypothesis testing, all factors of SERVQUAL appear to be most significant dimensions of service quality influencing client satisfaction with the telecommunication suppliers. Therefore it is suggested that the telecom service representatives must provide services as or near frequency of unwanted event and magnitude of impact of desired outcomes, so it will not undermine the trust and tolerance level of customers. If the customers feel they get attention both individualized and quality then it will make a chance big opportunity since when there is trust and commitment then customer satisfaction will become a loyalty.

As future work, we can discuss again inter-corelation between risk appetite, risk tolerance, risk culture about how big the impact of revenue when we miss-calculating the risk tolerance.

References

[1] S. Youcef, C. Djelloul, and B. Abderrezak, “The Impact of Customer Satisfaction for their Loyalty with the Existence of Trust and Commitment as Intermediate Variables : The Case Study of the Algerian Mobilis Telecom,” *Management*, vol. 5, no. 1. Scientific & Academic Publishing, pp. 1–5, 2015.

[2] H. Oh, “Service quality, customer satisfaction, and customer value: A holistic perspective,” *Int. J. Hosp. Manag.*, vol. 18, no. 1, pp. 67–82, Mar. 1999.

[3] M. Arora, “Role of Customer Service Quality in Customer Satisfaction : an Empirical Study of Select Telecom Service,” vol. 3, no. 3, pp. 85–94, 2015.

[4] ISACA, “Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf,” 2009. [Online]. Available: http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf. [Accessed: 07-Nov-2015].

[5] S. Bhargava, “The concept of service,” *altius.ac.in*, no. 2004, pp. 1–23.

Glossary

Satisfaction: Oliver (1996, P13) defines satisfaction as a judgment of enough level of satisfaction offered by a product or service throughout consumption [2]

Trust: is defined because the level of dependability ensured by one party to a different inside a given exchange relationship, Hosmer (1995) defines trust as reliance by one person, group, or firm upon a voluntarily accepted duty on the a part of another person, group, or firm to acknowledge and shield the rights and interests of all parties engaged during a cooperative endeavour or economic exchange. [2]

Commitment: in relationship promoting literature, commitment has wide been acknowledged to be associate integral a part of any long-run account [2]

Loyalty: is a psychological character fashioned by sustained satisfaction of the client as well as emotional attachment fashioned with the service supplier that ends up in a state of volitionally and systematically being within the relationship with preference, patronage and premium. [2]

The Annual Conference on Management and Information Technology (ACMIT) 2016

Comparison of Software Licensing and Development Models Using Val IT

Arief Abdul Hamid
Swiss German University, EduTown BSDCity, Kav. II.1, Bumi Serpong Damai, Tangerang Selatan, Banten 15339, Indonesia

Abstract

Today Small Medium Enterprise (SME) in Indonesia increasingly growing, along with the growth of business done, of course must be offset by existing IT in the company, due to support the performance of the company. Who originally used it daily jobs done manually will be diverted to use software to help the work. But sometimes to develop the IT application, the obstacle typically encountered is about the budget for the investment of IT itself, therefore in this paper the authors compare the advantages and disadvantages between open source software and software Proprietary using VAL IT as a framework. For the result of the Open Source Software is low cost because the the code it is free but company should spend budget for the training and for the report the company need to learn to create the reporting. While for software Proprietary is high cost but support is conducted regularly for operational and for just ask the vendor to create report.

Keywords: Open Source, Proprietary Software, Micro Small Medium Enterprise, VAL IT Framework

1. Introduction

To get a good operational in the company can only be realized by the use of appropriate software, therefore, before the company implemented an application / software to support the day to day operational activities they have to do the analysis first. Often times when they want to develop a system that already exists in the company, the leaders would normally consider the software that will be use. whether will be using Proprietary software or open source software. beside that the leader should be thinking about their budget if they want to upgrade the system. moreover for SME they often have problematic about budget for implementation system. So they should be more detailing about the advantage and disadvantage if we using Proprietary software or open source software, in open source inspection process is managed by independent developers or user it's different with proprietary software have sophisticated testing tools [1] [2].
This research is driven by the question of which type of software licensing is suitable for medium class enterprises, Open Source or Proprietary Software ?
VAL-IT section Investment management is apply for comparison these software for a material consideration for management. Because it related to the cost of investment by management.

2. Open Source Definition

As we all know before there is different between Free Software and Open Source Software. According to OSI (Open Source Initiative) there area unit some criteria could be comply if the software want to call an "Open Source" [3].
1. Free distributor
2. Source Code
3. Derived Works (The license should permit the modification code)
4. Integrity of The Author's Source Code
5. No discriminate resist to person or groups
6. There is no discrimination against areas of business
7. Distribution of license (The rights attached to the program must apply to all to whom the program is redistributed while not the necessity for execution of an extra license by those parties.)
8. License Must Not Be Specific to a Product

9. License should not restrict another software (the license should not insist that every one alternative programs distributed on an equivalent medium should be open source software.)
10. License should be technology – neutral.

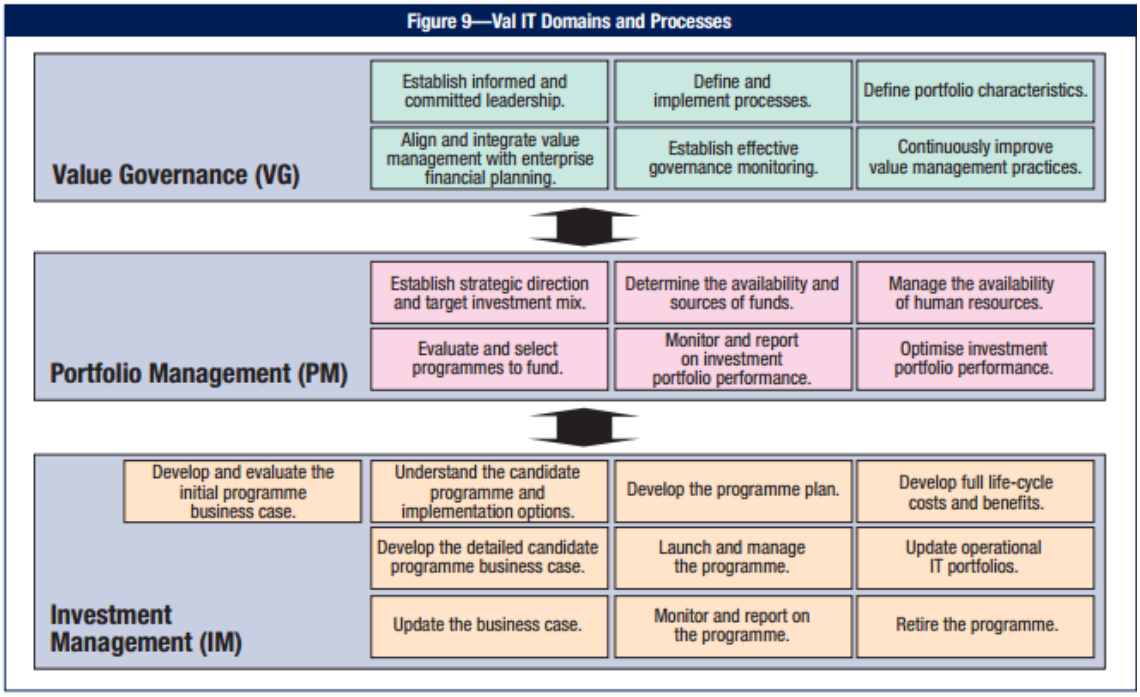
And today Open Source has flourished in many Category e.g operating systems, web servers, database [4].

2.1 Proprietary Software Definition

As we know that the opposite the open source is Proprietary software, which is to using the software we should buy the license first. And usually proprietary software owned by an individual or company. There are almost always on its use and for the source code it secret, according to [5] for proprietary software the e.g are Microsoft and child,adobe, Accpac (Accounting software), Symantec, Checkpoint etc. And Proprietary software development mostly the are using waterfall model, and have 5 phase [6], the first step is Requirement phase, the second phase is system and software design, third phase is implementation and unit testing phase, fourth phase integration and system-testing, and the last phase support and maintenance.

2.2 VAL-IT

Val IT Framework is Framework that focus on IT investment [7] . And because this paper related to investment on IT and to clarify the function of IT and Business functions. Author uses VAL-IT Framework for this paper to assist enterprises optimize the conclusion valuable from IT- enabled investments at an affordable cost, and with a better-known and acceptable level of risk, the Val IT initiative includes analysis activities, publication, and complementary resources, supporting its principal centerpiece [8], [9].
In the picture 1.0 [8] below shows Val-IT Domain and Processes :



Picture 1.0 VAL-IT Domain And Process

And as picture above we can sees there are 3 domains [7], [8] :

- Value Governance (VG) Value governance consists of 11 key management practices that cover the establishment of a governance, monitoring, and control framework, provides strategic direction for investments, and defines the investment portfolio characteristics

- Portfolio Management (PM) Portfolio management consists of 15 key management practices that cover the identification and maintenance of resource profiles; define investment thresholds; provide for the evaluation, prioritization and selection, deferral or rejection of investments; manage the overall portfolio; and monitor and reports on portfolio performance.
- Investment Management (IM) Investment management consists of 15 key management practices that cover the identification of business requirements; develop a key understanding of candidate investment programs; analyze alternatives; define and document detailed business cases for programs; assign clear accountability and ownership; manage programs through their full economic life cycle; and monitor and report on program performance.

2.3 COST

As we know that the one of advantage using open source is the open source approach strongly affects software distribution. People can try the software before buying it, having access to internal documentation and code [2], so we can modify the code to fit what the company need. and open source can achieve a high level of efficiency and the software patches or correction, is might be more faster then proprietary software because open source they have a one of big community [2], [6].

2.4 SECURITY

Besides the price issue of course to be considered from selecting a software is about security, because if the system are vulnerable to threats it can be affect business continuity. For security open source software is not intrinsically more secure than proprietary code [10]. Maybe for some people open source security is not good because the code is open to everyone but it opposite with open source mania like Eric Raymon as he said "Given enough eyeballs, all bugs will feel shallow" [9], [11].

2.5 MSME Definition

According to UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 20 TAHUN 2008 TENTANG USAHA MIKRO, KECIL, DAN MENENGAH.

This table show MSME describe the distribution of SME Category.

Enterprise Category	Net Asset	Annual sales revenue
Micro	Rp50.000.000,00	Rp 300.000.000,00
Small	>50.000.000,00-500.000.000,00	>Rp300.000.000,00 - Rp2.500.000.000,00
Medium	>Rp500.000.000,00 - Rp10.000.000.000,00	> Rp2.500.000.000,00 - Rp50.000.000.000,00

Table 1.0 Category of Micro Small Medium Enterprise

3. Methodology

For the methodology this paper will be analyzed with Investment Management module from Val IT Framework will be used to meet the company needs. Because this will relate to the investment of the company

3.1 IT Val - Investment management Procedure

The procedure of IT Val module there are 10 process as below [8]:

- Develop and assess the initial programme conception business case
- Understanding the candidate program and implementation options.
- Develop the program plan.
- Create full life-cycle costs and benefits.
- Create the detailed candidate program business case

- Launch and managing the program
- Enhance operational IT portfolios
- Update the business case
- Monitor and report on the program
- Retire the program

4. Result

PT.XYZ business is in outsourcing in Indonesia wants to develop the IT they had, because of the current IT system that they had not relevant to the business that has been developed at this time, there are many procedures are still do manually, which could be a possibility of error in jobs, Hence the company is currently wants to use the software for daily operations, to reduce the occurrence of Administrative mistakes in their daily work. There are several alternatives that are being considered and already can be classified in two types of open source software and software Proprietary. Where to evaluate both the author using Val IT Framework to analyze it. And of Val IT Framework authors chose Domain investment management procedures, relevant because this domain is relevant to the problem. And from the domain of the 10 existing processes, the author only took 4 process because the process that allows for compare. 4 process are:

- **Understand the candidate programme and implementation options**
- **Develop full life-cycle costs and benefits**.
- **Update operational IT portfolios**
- **Monitor and report on the programme**

1. Understand the candidate programme and implementation options

Based on the initial conversation with the CEO of PT. XYZ, The result are:

- **using Proprietary software or open source software**

2. Develop full life-cycle costs and benefits

For ERP Proprietary cost Efforts aimed at ongoing maintenance and enhancements cost approximately $1.5 million annually per ERP implementation [12] . In the picture 2.0 [13] below shows ERP Cost year to year :

Year	Cost	% of cost overruns	Duration	% of duration overruns
2012	$7.1MM	53%	17.8 months	61%
2011	$10.5MM	56%	16 months	54%
2010	$5.5MM	74%	14.3 months	61%
2009	$6.2MM	51%	18.4 months	36%

,

Table 2.0 ERP Cost year to year from Panorama Consulting Group

and Open source cost is depend on company requirement. And some research said cost for Open Source is the training cost of people in the company who deploy the application.

For the Benefit
ERP Proprietary **:** Support and update program will be conducted regularly
ERP Open Source **:** Can modify the program until meet with company requirement

3. Update operational IT portfolios

For the reflect changes that result ether open source and Proprietary operational almost similar.

4. Monitor and report on the programme

Open Source : For reporting we should be learn for creating the report.
Proprietary : For reporting the will be easier than open source because we just ask the vendor to create the report.

5. Conclusion

Based on the research above it is concluded that if Software Proprietary cost is High but the support is conducted regularly for operational, it can be delivered easier and the report delivering is also become easier. It is because if using the Software Proprietary the owner or company just ask the vendor to create report. While for Open Source Software, the cost is more cheaper than Software Proprietary but the benefit is we can modify the program until meet with the company requirement for operational IT which similar to Software Proprietary . But for reporting, the company should be learn the application to create the report.

The results of this research will propose to the owner to be weighted and assessed in each variable and it is necessary to perform decision making process in the future research

References

[1] M. S. Carvalho, "Why open source?," *Cad. Saúde Pública*, vol. 31, no. 2, pp. 221–222, 2015.

[2] A. Onetti and F. Capobianco, "Open source and business model innovation. the funambol case," in *Proceedings of the first International Conference on Open source Systems*, 2005.

[3] O. S. Initiative, *Open Source Initiative*. 2008.

[4] H. Kim, C. Boldyreff, and others, "Open source ERP for SMEs.," 2005.

[5] The Linux Information Project., "Proprietary Software Definition." Jul-2005.

[6] A. Boulanger, "Open-source versus proprietary software: Is one more reliable and secure than the other?," *IBM Syst. J.*, vol. 44, no. 2, pp. 239–248, 2005.

[7] C. Symons, "Measuring the business value of IT," *Forrester Res. Inc Camb. Mass. USA*, 2006.

[8] I. G. Institute, *Enterprise Value: Governance of IT Investments, the Val IT Framework, Version 2. 0*. ISACA, 2008.

[9] P. Afzali, E. Azmayandeh, R. Nassiri, and G. L. Shabgahi, "Effective governance through simultaneous use of COBIT and val IT," in *Education and Management Technology (ICEMT), 2010 International Conference on*, 2010, pp. 46–50.

[10] C. Payne, "On the security of open source software," *Inf. Syst. J.*, vol. 12, no. 1, pp. 61–78, 2002.

[11] E. Raymond, "The cathedral and the bazaar," *Knowl. Technol. Policy*, vol. 12, no. 3, pp. 23–49, 1999.

[12] J. Bonasera, "AMR Research Report Evaluates the Costs," *Chall. Added Benefits ERP Upgrad. AMR Res.*, 2002.

[13] Panorama Consulting Group, 2013., "2013 ERP REPORT." .

The Annual Conference on Management and Information Technology (ACMIT) 2016

Digital Era Paradox: Integrating Technology Acceptance Model with Governance Risk & Compliance to Reduced the Perceived Digital Risk

Triya Rachmatika

Abstract

Today societies are highly dependent to digital. This dependency is called Digital Darwinism (Institut Akuntan Publik Indonesia (IAPI).2015). This paper analyses customer's behavior in digital era. Customer behavior were learned and become one of the factors of digital implementation paradox. The paper found that Professional due care is important to analyze customer behavior. The paper identifies the gap between company's readiness with technology acceptance to deal with customer's trust and the increase of perceived digital risk. The results of this paper will find the best technology acceptance model base on literature studies and actual cases in companies. The result of this paper is the extension of the Technology Acceptance Model by focusing on the mean of reducing perceived digital risk with Governance Risk and Compliance.

1. Background

Digital era has increase digital dependency and cause societies to struggle for their existence. In auditor terms, this phenomenon is called digital Darwinism [6]. According to Darwin, the struggle of company could happen because societies can adapt to technology faster than the companies themselves. The evolution of companies will naturally occur if the company cannot survive [14]. In the era of Digital Darwinism, there are three dominant traits to survive that consist of relevance, interactivity, accountability [19]. In marketing perspective, Digital Darwinism is a main challenge to all companies. The digital environments changes create challenges for every company that uses IT as their services. IT services may give companies a lot of advantages, but there will be some paradox if companies don't know how to accept the risk and control the internal and external behavior.

Governance plays important roles in this era. Governance ensures the enterprise objectives are achieved by effective monitoring.

Technology acceptance is a key of corporate success nowadays. Technology acceptance in Indonesia should be accompanied by the awareness of technological risk and an act to response to the risk. A lot of companies will struggle when they have to adopt technology in their companies. There are risks which have not been foreseen by companies. Perceived risk in Technology Acceptance Model have been found in various studies. Some of them resulted in people readiness and behavioral uncertainties. Perceived risk has been added to technology acceptance model for increasing managerial focus to create corporation's safer and more effective technological use [9]. Those risks can result from the gap of management expectancies to technology effectiveness and outcome, or can be called as paradox. Base on companies' point of view, the paradox of technology resulted comes from companies' survival to adopt the technology [2}.

In author audit experienced, technology doesn't make the financial audit process easier, but also more complex. Technology adoption makes every audit has to be done by internal audit first to assess the risk level, and followed by external audit process. The awareness of people have became the major factor in the problem arises in IT audit. The impacts of perceived risk with technological adoption also have been studied in various studies, such as internal banking [4]. This paper also wants to investigate about the awareness and the risk response of technology adoption and the impact to perceived risk.

The needs to understand of costumer behavior and implement the technology governance in the company are important. This era will create more unauthorized access and modification of access that lead to be the vulnerabilities of company. Modification of access can resulted not only from internal but also external.

Companies have to protect themselves and all of their customer by implementing IT Governance Risk and Compliance (IT GRC) to increase the efficiency and the effectiveness of the digital. This

paper discusses professional due care including customer monitoring, customer due diligence and access management in the relation to decrease digital risk.

The research problems are as follows:

- How to control the customer behavior in digital era with professional due care?
- How to decrease the perceived digital risk in technological acceptance?

According to the audit experience, author will explain today's situation and create a model, which added the IT GRC factors, that impact to increasing the readiness of technological acceptance and reducing the effect of perceived risk.

2. Literature Review

2.1 Technology Acceptance Model (TAM)

Davis (1986) has introduced Technology Acceptance Model (TAM) . This study assess the extension Theory of Reasoned Action (TRA) as a part of Technology Acceptance Model by combining IT GRC model,. Author developed a new model to assist companies in managing their internal and external misused of information system or intention to conduct unethical things [10]. There were many of researches in the area of Technology Acceptance Model (TAM). Perceived risk is the factor that decrease perceived benefit of IT [3]. To make it efficient, companies should decreasase perceived risk of digital adoption.

Recently, TAM has found perceived risk as the factor that could reduces intention to use. A study of Technology Perceived Behavior has also been conducted in the area of customer satisfaction [13].

There are number of models explaining the acceptance of new technologies. There are also researches that combine TAM with behavioural science because the use of e-commerce [15]. The research that combines TAM with perceived risk as one of behavioral science, is shown in figure 1 below,

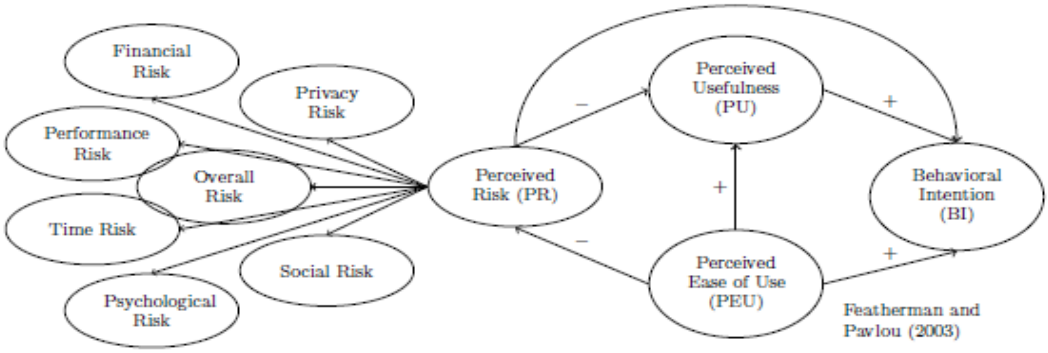


Figure 1. Featherman and Pavlou (2003)

2.2 Perceived Risk

Featherman and Pavlou have measured perceived risk that could reduce the perceived usefulness and perceived ease of use to the digital implementation. [3].

2.3 IT-Governance Risk Compliance

Previous study has developed integrated model of IT and GRC. High level process of IT GRC have integrated IT governance, IT Risk Management, and IT Compliance [14]

2.4 Technology Perceived Behavior

Human behavior was found to be the important factor of TPB and affected attitude and human behavior [5]. Recently many studies were conducted to understanding the user behavior toward user technology acceptance

2.4.1 Customer Due Diligence

Customer due diligence is a part of internal control. Companies, especially financial companies have to strengthen their policy and procedure in this digital era [20]. The practice of customer due diligence and the monitoring of customer's transaction become more important to know the customer's behaviour in digital era [7].

2.5 Professional Due Care

Professional Due care means the company's readiness in technology adoption and preparedness of its risk reduction. It can be done by regulating customer monitoring, customer due diligence and strengthen the access management.

A study has found the factor that support and can help customer to overcome the internal and external risk. Base on the journal that examining multidimensional risk, they could be reduced by some factors. The major factor, which are self-efficacy or the perceived capability, trust disposition and structural assurance or trust toward technology have been found could give impact to reduce the risk [13]. That studyr didn't include the GRC factor which found in this study can`be another major factor to reduce the risk.

3. Research Method

For that objective, author created an extent of Technology Acceptance Model according to two field studies. The dimension of this study is to overcome the risk perception by implementing these following steps:

- Literature studies in various journals.
- Field studies by observing the result of company's internal audit in 2015.
  This paper discussed about the implementation of digital service to customers that conducted by several companies. Professional due care to implement regulation has found more important in this study according to the increasing of digital risk nowadays.

4. The case of IT –GRC

Data Sample

Study 1. First author study of IT-GRC Risk [16] It can be illustrated as below

2015 Period (Monthly)	**Total of PT. ABC's User**			
	PT. ABC's Manual Report		**Reporting System**	
	External	**Internal**	**External**	**Internal**
1	65	1	60	0
2	63	1	59	0
3	66	1	62	0
4	58	1	55	0
5	50	1	49	0

Figure 2 Total of PT. ABC user

System should be monitored regularly to ensure the accuracy of data in the system. It needs the professional due care to monitor and ensure the customer's identities had been corrected before the input process to the system. To ensure the compliance of company, customer's identities, including the job of customer are important to measure customer's risks and customer due diligence. In this case, it was found that a customer still registered as a student while he had been an employee in the fact. The implication of such case was the monthly membership of that customer had to be paid by the company because he was still registered as a student in the period of free-students program.

The missing of company's professional due care to make session time out and update customer's identities regularly were other important things because it could give a chance for perpetrator to do irresponsible things.

Study 2

`Another case was found in an energy trading company. PT. XYZ, which provides fuel for Oil Company has the process that need to be validated manually so the money which has been received from customer can't be changed by unauthorized person. The usability of this kind of technology can make fraud by internal companies. This kind of technology needs governance from company, such as the regulation. The process of XYZ [16] was as below,

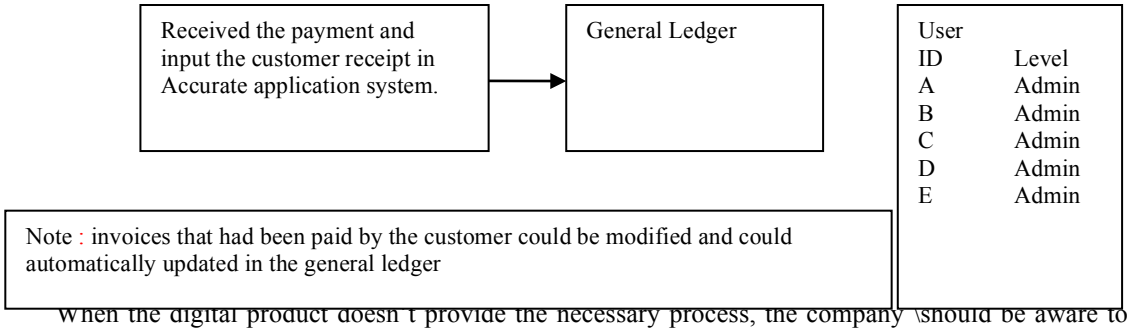


Figure 3. The process of invoice input to General Ledger Administrators

When the digital product doesn't provide the necessary process, the company should be aware to add the proce ensitivity of general ledger report in acc portant in this era. There must be a control of input, process and output as regulation stated. That's why supervisor first before general ledger input should review it. It was because of the fact that accurate application system cannot provide validation process.

The companies have to survive for winning the competition. In this era, our focus are not only about who have responsibility but the accountability also matter. Since the goal of every company is customer satisfaction, some authority has been shifted from staffs to customers. Those customers's ability has to be maintained regularly. It was also supported by one relevant study that resulted in Technology Acceptance Model extension. [8].

By learning from previous studies, this study pointed out that beside the structural assurance and self efficacy for internal and external companies the governance risk compliance also matter to decrease the risk. To add the governance risk compliance aspect, according to author audit experience, author made the TAM extension as below,

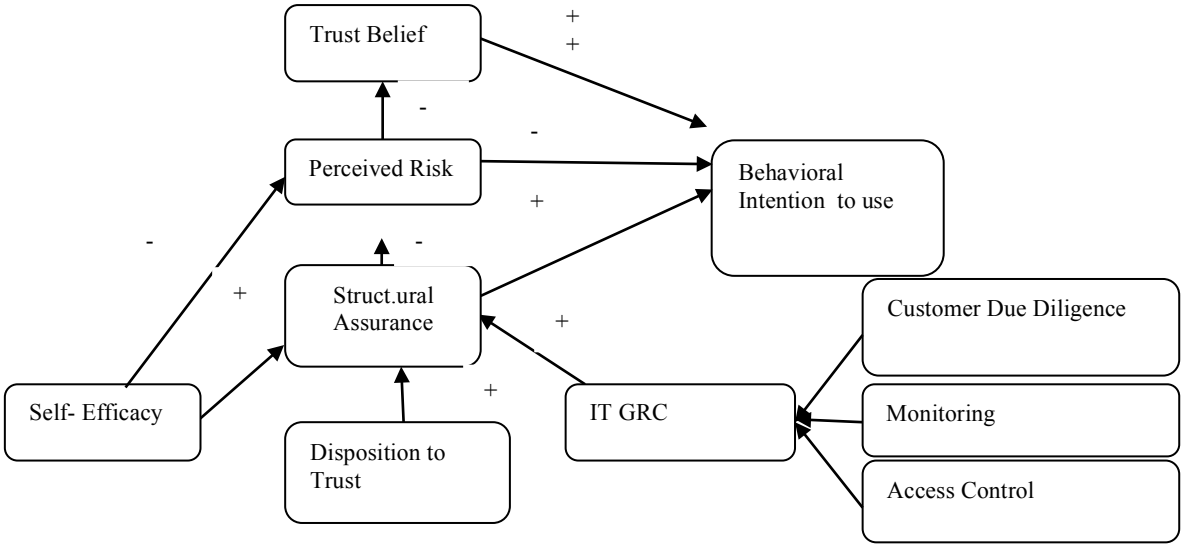


Figure 4 TAM-Governance Extension

5. Result of Previous Study

The result from both studies were supported the important of IT GRC for companies.

Study (1) Management has made changes regarding access control to the report format which will be monitored monthly [16] . The IT GRC has made the usage of IT more effective.

Number of Users Access Interactive Real Time	Incorrect Total User	Correct Total User

Management Feedback:
The differences were the result of different perception, which has just been the attention of management.

The external user which logged monthly	63	59

Figure 5. Feedback

Study (2) Segregation of duties also already made by company, and the procedure has been updated. Accurate application system only can be used by finance division or authorized people.

6. **Conclusion & Future Research**

This paper added the IT-GRC to reduce the risk for companies that adopt technologies. By Professional due care of IT GRC over information system control through regulate the customer due diligence, monitoring, and access control management could decrease perceived digital risk and increase the effectiveness of technology adoption.

IT-Governance Risk and Compliance (IT GRC) emphasize on the awareness and readiness of the technology acceptance and the following risk of adopting technology. The application of IT-Governance Risk and Compliance include but not limited to technical and non-technical things.

IT-GRC could be a potential key to solve technology acceptance problem to increase companies' structural assurance in order to decrease digital risk nowadays. Beside technical things (e.g. self-efficacy), companies should also consider the IT-GRC about non-technical things associated to technology acceptance and technology adoption. Professional due care including customer monitoring, customer due diligence and access control management could do IT-GRC regarding non-technical things associated to technology acceptance and technology adoption.

References:

[1] Allen, W. T., Jacobs, J. B., & Strine Jr, L. E. (2001). Realigning the Standard of Review of Director Due Care with Delaware Public Policy: A Critique of Van Gorkom and its Progeny as a Standard of Review Problem. *Nw. UL Rev.*, *96*, 449.

[2] Carlos Roca,J.,Jose Garcia,J.,& Jose de la Vega, J.(2009).The importance of perceivedd trust,security and privacy in online trading system. *Information Management & Computer Security ,17(2),96-113*.

[3] Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: a perceivedd risk facets perspective. *International journal of human-computer studies*, *59*(4), 451-474.

[4] Hanafizadeh, P., & Khedmatgozar, H. R. (2012). The mediating role of the dimensions of the perceivedd risk in the effect of customers' awareness on the adoption of Internet banking in Iran. *Electronic Commerce Research*, *12*(2), 151-175

[5] I. Ajzen, The theory of planned behaviour, Organizational Behavior and Human Decision Process 50, 1991, pp. 179–211.

[6] Institut Akuntan Publik Indonesia (IAPI)."Digital Darwanism –Adapt or Die". 2015.

[7] Isern, J., Porteous, D., Hernandez-Coss, R., & Egwuagu, C. (2005). AML/CFT Regulation: Implications for Financial Service Providers That Serve Low-Income People. *Focus Note*, *29*.

[8[Kim, S., & Garrison, G. Investigating mobile wireless technology adoption: An extension of the technology acceptance model. *Information Systems Frontiers*, *11*(3), 323-333.)2009

[9Kesharwani, A., & Singh Bisht, S. (2012). The impact of trust and perceivedd risk on internet banking adoption in India: An extension of technology acceptance model. *International Journal of Bank Marketing*, *30*(4), 303-322.

[10] Ingram, R., Skinner, S. J., & Taylor, V. A. (2005). Consumers' evaluation of unethical marketing behaviors: The role of customer commitment. *Journal of Business Ethics*, *62*(3), 237-252.

Lee, Ming-Chi. "Predicting and explaining the adoption of online trading: An empirical study in Taiwan." Decision Support Systems 47..2009.

[11]Lee, M. C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceivedd risk and perceivedd benefit. *Electronic Commerce Research and Applications*, *8*(3), 130-141.

[12] Looney, C. A., Valacich, J. S., Todd, P. A., & Morris, M. G. "Paradoxes of Online Investing: Testing the Influence of Technology on User Expectancies". *Decision Sciences*, *37*(2), 205-246.2006

[13]Luo, X., Li, H., Zhang, J., & Shim, J. P. (2010). Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision support systems*, *49*(2), 222-234.

[14] Racz, N., Weippl, E., & Seufert, A. (2010, July). A process model for integrated IT governance, risk, and compliance management. In *Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010)* (pp. 155-170).

[15]Riek, M., Böhme, R., & Moore, T. Understanding the influence of cybercrime risk on the e-service adoption of European Internet users. In *Workshop on the Economics of Information Security (WEIS)*.2014

[16] RSM Indonesia Final Audit Report.2014

[17] Schwartz, E. I. "Digital Darwinism: 7 breakthrough business strategies for surviving in the cutthroat Web economy". *Crown Business*.2002.

[18] Salo, J., & Karjaluoto, H.. A conceptual model of trust in the online environment. Online Information Review, 31(5), 604-621.2007

[19] Vollmer, C. "Digital Darwinism. Strategy+ Business", (54).2009

[20] Warkentin, M., & Willison, R. Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, *18*(2), 101.2009)

The Annual Conference on Management and Information Technology (ACMIT) 2016

Engineering Design and Simulation of Integrated Control System for Optimization of Transport System in Coal Handling Facilities with Automated Surge Bin

Ari Apriandi
Swiss German University, Edu Town BSD City, Tangerang, 15339, Indonesia

Abstract

At this time, technological developments continue to rise and get into all aspects such as telecommunications, banking, construction, oil and gas, trade, marine, mining, etc. Technology creates the change to become more effective and efficient. It is also happening in the world of mining with infrastructure facilities. In this study focuses on automation in the coal handling facility. The automation of control system has been developed from two stations into one integrated station that can increase production time and the system becomes more efficient and also reduce the failure of operator to start on the right time. Integration of the system is created with designing surge bin system with installing the sensors and to be connected to PLC device. Then, simulations have been done by developing ladder logic program using a PLC. This study focuses designing the sensors into surge bin until doing PLC simulation for integrated control system so both systems can be connected automatically and having the main control.

Keywords: PLC ; Ladder Logic ; Surge Bin ; Sensor ; Automation

1. Introduction

Currently coal mining industries are required to have more initiatves to reduce their manual operation to become automation for all handling facilities so that operation will be more effective and efficient [4]. The technology of these industries has developed since many years ago and get into their operation system including also the coal handling facilities [1]. The coal handling facilities take an important role for these industries. The role is to deliver raw coal from mine pit to be processed becoming coal product until shipped stage. Almost of the coal industries have the transport system in their concession area but their infrastructures have the different types but the process stages have almost same typically.

This research carried out a study case in one of coal mining company that the facilities contain Coal Processing Plant (CPP), Overland Conveyor (OLC) and Port and the flowsheet is illustrated in Fig 1.
The flow sheet describes the process stages of coal handling plant. The CPP (Coal Preparation Plant) is process stage from dumping coal truck, crushing the raw coal with primary crusher and then go through to secondary crusher via conveyor (CV11) and stacking (CV12) in stockpile (125ktons capacities). Then product coal in stockpile conveys into the reclaim tunnel to conveyor (CV13) until surge bin (500tons).
The OLC (Overland Conveyor) is process stage to convey product coal along 6.2 km to the port. The Port is process stages to stacking product coal into stockpile (50ktons capacities) or direct to convey coal via jetty conveyor (CV03) to loading barge.

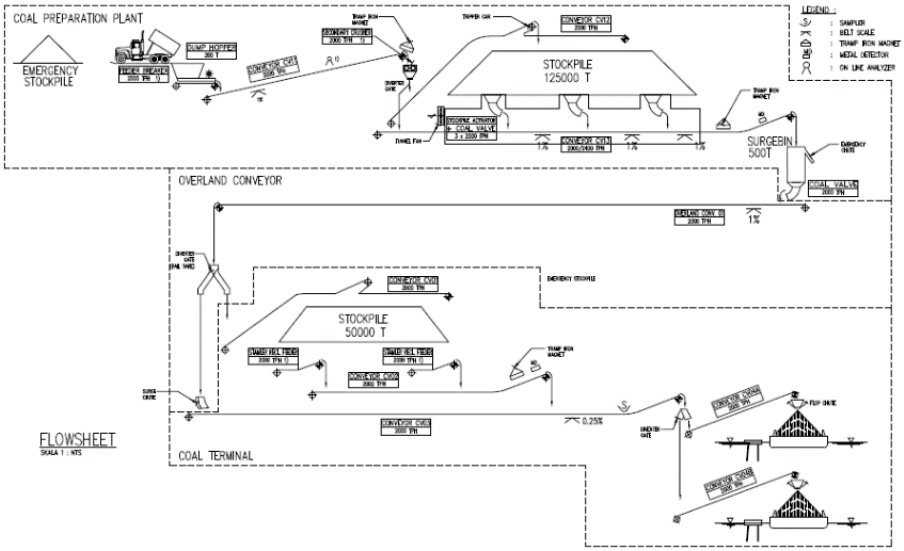


Fig. 1. Flow sheet of coal handling facilities

The coal handling facilities have been controlled by PLC/SCADA system [8]. They have two control rooms to operate the facilities where the first control room handles the CPP and other control room handles the OLC and port. Both of control rooms located in different places within 8 kilometres and the both operators have communicated with radio communication or room phone. This project will optimize

the existing system with combining two separate systems that can operate automatically. The existing facilities are seen in Fig 2.

Fig. 2. CPP, OLC and Port

4.1.38 Principles of Surge Bin

The quantities of coal, which pass through surge bin annually is considerable and continually increasing. This trend applies not only to the coal producers and export market facilities, but to coal users in such industries as steelmaking, electricity generation and cement manufacture. The achievement of reliable gravity flow is essential, particularly with the increasing size of the storage units and the automation of bulk solid material handling and processing systems.

In the field of bulk solids handling it is essential that both the storage and the discharge from storage of materials is carried out in an effective and efficient manner. However, it is known that flow out of bins and hoppers is often unreliable and as a result considerable costs can be incurred due to the consequential losses in production. This is very often the case with coal handling plant due to the cohesive and variable nature of coals. Problems that commonly occur in the operation of storage bins (including solids segregation, erratic flow, flooding, arching, piping and adhesion to the bin wall) can reduce the bin capacity below the designed values, or lead to flow blockages.

There are two basic modes of flow, mass flow and funnel flow [2]. These are illustrated in Fig 3. Each mode has its own advantages and disadvantages and it is important that designers and operators of bins be aware of their individual characteristics as these can have a significant effect of bin performance, and the characterictics of mass flow and funnel flow bins is shown in Table 1. The surge bin in this research is mass flow type and is needed for the bulk handling facilities to reduce lose time due to long process every started running.

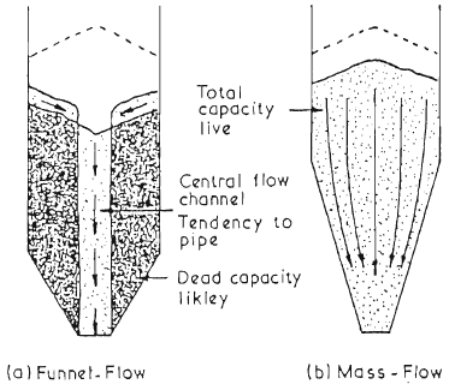


Fig. 3. Flow Patterns in Symmetric Funnel Flow and Mass Flow Bins

Table 1. Characteristics of Mass Flow and Funnel Flow Bins Funnel Flow	Mass Flow
Unless outlet size exceeds critical rathole dimension a considerable percentage of the contents may be non-reclaimable.	Total bin contents live.
Flow pattern is variable and difficult to predict. Depends on the time history of bin operation since last emptied.	Flow pattern predictable and reliable.
Last-in, first-out flow pattern promotes segregation, product deterioration, bin corrosion in dead regions, flooding of fine powders.	Outlet size to prevent cohesive arching and relatively small.
Feeders are larger and more expensive than mass flow.	Wall loads more predictable when flow pattern is symmetric.
Wall loads difficult to predict, especially if bin and/or flow pattern is non-symmetric.	First-in, first-out flow pattern; required when segregation, product deterioration are problems or fine powders are to be handled.
Capable of storing large quantities of bulk solid which can be gravity reclaimed if free-flowing.	Requires steep smooth hoppers with protection of hopper walls from impact wear and corrosion.
Bin wear can be a problem if flow pattern causes high velocities down a segment of the bin wall. This situation is promoted by outloading chutes or incorrectly designed feeders.	Detailing of bin structure important to ensure mass flow is maintained.
	Abrasive wear of hopper may be a problem with some bulk solids.
	May be difficult to achieve satisfactory geometry for large storages, without requiring excessive heights.
	Hopper wear and flow problems can occur if feeder design prevents mass flow operation.

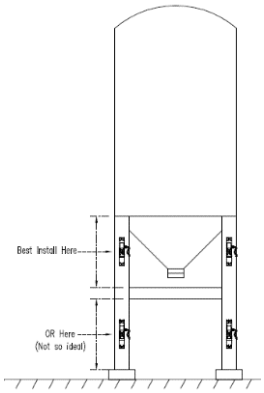
4.1.39 Sensors Design for Surge Bin

3.1 Load sensor with strain gauges

Strain gauges consist of a metal foil strip, flat length of metal wire or a strip of semiconductor material which can be stuck onto surfaces like a post stamp. When the wire, foil, strip or semiconductor is stretched, its resistance *R* changes. The fractional change in resistance *AR/R* is proportional to the strain *ε*. Metal strain gauges typically have gauge factors of the order of 2.0. While such a strain gauge is stretched its resistance increases, when compressed its resistance decreases.

Strain is (change in length per original length) and so the resistance change of a strain gauge is a measurement of the change in length of the gauge and hence the surface to which the strain gauge is attached [3]. A problem that has to be overcome with strain gauges is the resistance of the gauge changes when the temperature changes and so methods have to be used to compensate for such changes in order that the effects of temperature can be eliminated.

This research uses one of strain gauge models and its name is extensometer. Extensometer is a load sensor designed for force measurement on any load bearing structure. The sensor has some features such as strain gauge type, alloy steel



construction, 2 bolt holes and IP66 hermetically sealed protection and ATEX EEx ia IIC T4 hazardous approval, it is shown in Fig. 4 and the specification is shown in Table 2.

(a) (b)

Fig. 4. (a) Extensometer sensor; (b) Installation at Surge Bin

Table 2. Specifications of Extensometer

Parameter Value Unit	Value	Unit
Calibrated Output	1.7	mV/V at 500 με
Overload Capability (zero)	300	% of rated output
Overload Capability (max)	500	% of rated output
Input Resistance	350 ± 10	
Output Resistance	350 + 10	Ω
Insulation Resistance	>200	MΩ
Excitation, Recommended	10	Vdc
Excitation, Range	5 - 20	Vdc
Thermal Effect on Zero	0.025	± of FSO/°C
Compensated Temperature Range	-30 to + 80	°C

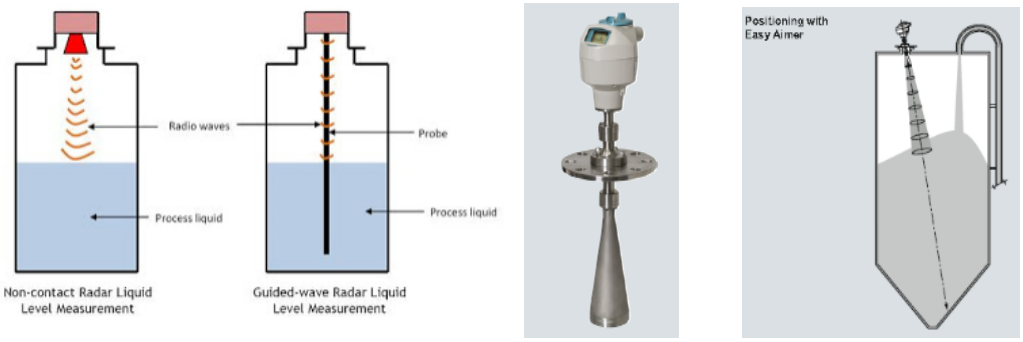
Construction	Painted Steel
Environmental Protection	IP66

3.2 Radar Level Measurement Sensor

Radar level instruments measure the distance from the transmitter or sensor (located at some high point) to the surface of a process material located further below in much the same way as ultrasonic level sensor, by measuring the time-of-flight of a traveling wave and then determine the level of the process material. And they are regarded as continuous level measurement devices because they continue to measure the level even as the level of the liquid in the vessel changes [3].

There are two basic types of level radar instruments are guided-wave radar and non-contact wave radar. Guided-wave radar instruments use wave guide "probes" to guide the radio wave into the process liquid while non-contact radar instruments send radio wave out through open space to reflect off this process material. Note that guided-wave radar instruments are used in applications where the dielectric of the process liquid is quite low and all radar level instruments use an antenna to broadcast or send radio signals to the process liquid whose level is to be determined. The Fig. 5a illustrates these two approaches.

The research also uses the sensor is non-contact wave radar which is a 2-wire 25 GHz pulse radar level transmitter for continuous monitoring of solids in storage vessel including extreme levels of dust and high temperatures, to a range of 30 m (98.4 ft), the sensor is shown in Fig. 5b.



(a) (b)

Fig. 5. (a) The diagram of level radar types; (b) Radar SITRANS LR260 "Level Measurement"

4.1.40 Integrated System with PLC

PLC (A programmable logic controller) is an industrial computer control system that continuously monitors the state of the input devices and makes decision based on the custom program to control the state of the output devices [5]. The first PLC offered relay functionality, thus replacing original hardwire relay logic, which used electrically operated device to switch electrical circuits mechanically. They met the requirement of modularity expandability, programmability and ease of use in an industrial environment. The PLC wiring can be easily understood and are being easily installed, use less space [4].

From output of both sensor, the PLC can make integrated system that become automatically. PLC is designed with its input/output module that continuously monitors the status in input devices connected, a programmable memory, processor and the power supply [6]. The input module has terminal into which outside process electrical signal generated by sensor or transducer are entered. The output module has terminal to which output signal are sent to actuate relays, solenoids, various, solid state switching, motor, devices, etc.

Ladder logic is a graphical programming language and ladder logic can be described as a rule based language rather than procedural language [7]. A rung in a ladder represents a rule, when implemented in PLC, the rules are typically executed sequentially by software in continues loop (scan), ladder logic has contact that makes or breaks circuit to control coils. The coils may represent a physical output which operates some device connected to PLC. Ladder program process inputs at the beginning of a scan and output at the end of the scan. Each rung on ladder diagram represents an operation on control process [5]. The processor scans the ladder program and then evaluates the logical continuity of each rung referring the input condition. If the input conditions are met then output will turn on (1) and if condition are not met then output will turn off (0). Ladder diagram is illustrated in Fig. 6.

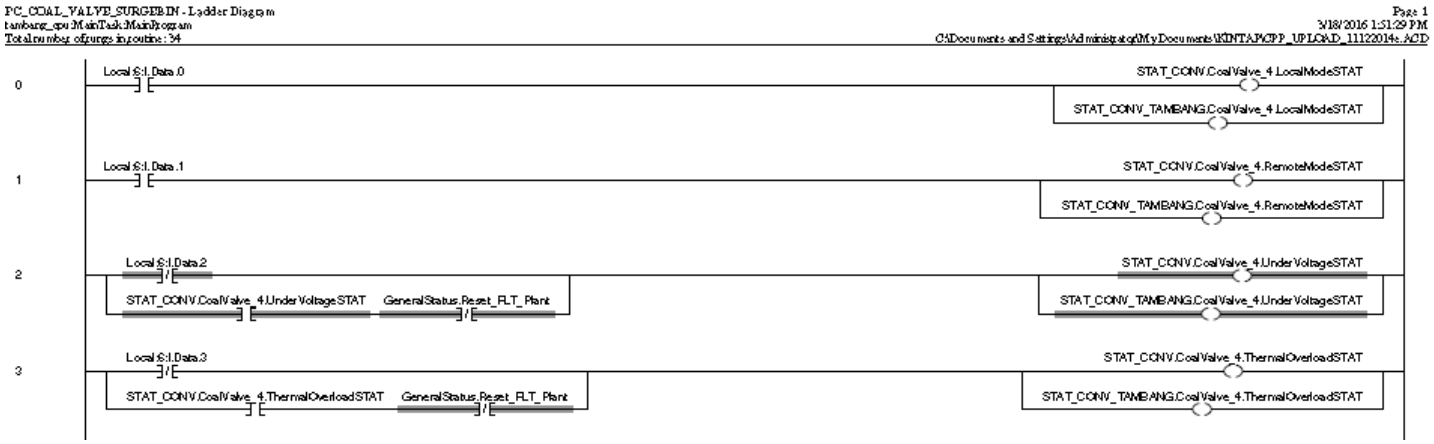


Fig. 6. Ladder diagram

The Extensometer sensor after was connected with transmitter panel shall give analog and digital outputs and both outputs shall be connected to PLC device and then the PLC program is created into ladder logic. The analog input in PLC can read the mass of bins with real time and the digital input in PLC can be used for instruction of high and low level limits. At the other option, if using radar level measurement sensor is simple to be connected to PLC without transmitter panel because the sensor gave the digital output directly but the PLC controls and decides for high and low level limits only. For its wide function, the extensometer sensor looks better than the radar level measurement sensor for this experiment with real time to show mass of bin whereas the radar can't do that.

4.1.41 Methodology

The working of our project summed up by the two control operations. The first operation is based on the coal passing through coal conveyor belt (CV1.3) into surge bin (CPP). The second operation is based on the coal level in the surge bin by locating both option sensors at different height in the coal storage tanks giving out the signal to PLC for open and close the bottom gate of surge bin to flow the coal into overland conveyor (OLC-Port). Block diagram is illustrated in Fig. 7.

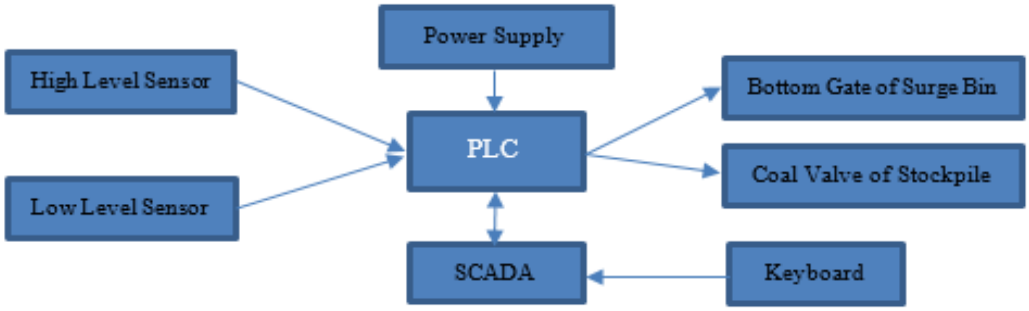


Fig. 7. Control system diagram

Activation of level sensors for low limit and high limit gave the system automatically and easy to operate the both operations and had an integrated control system to operate these handling facilities. The system shall be saving more 10 minutes for production time every starting the handling plants. Supervisory Control and Data Acquisition (SCADA) is a monitoring system that communicates and operates over

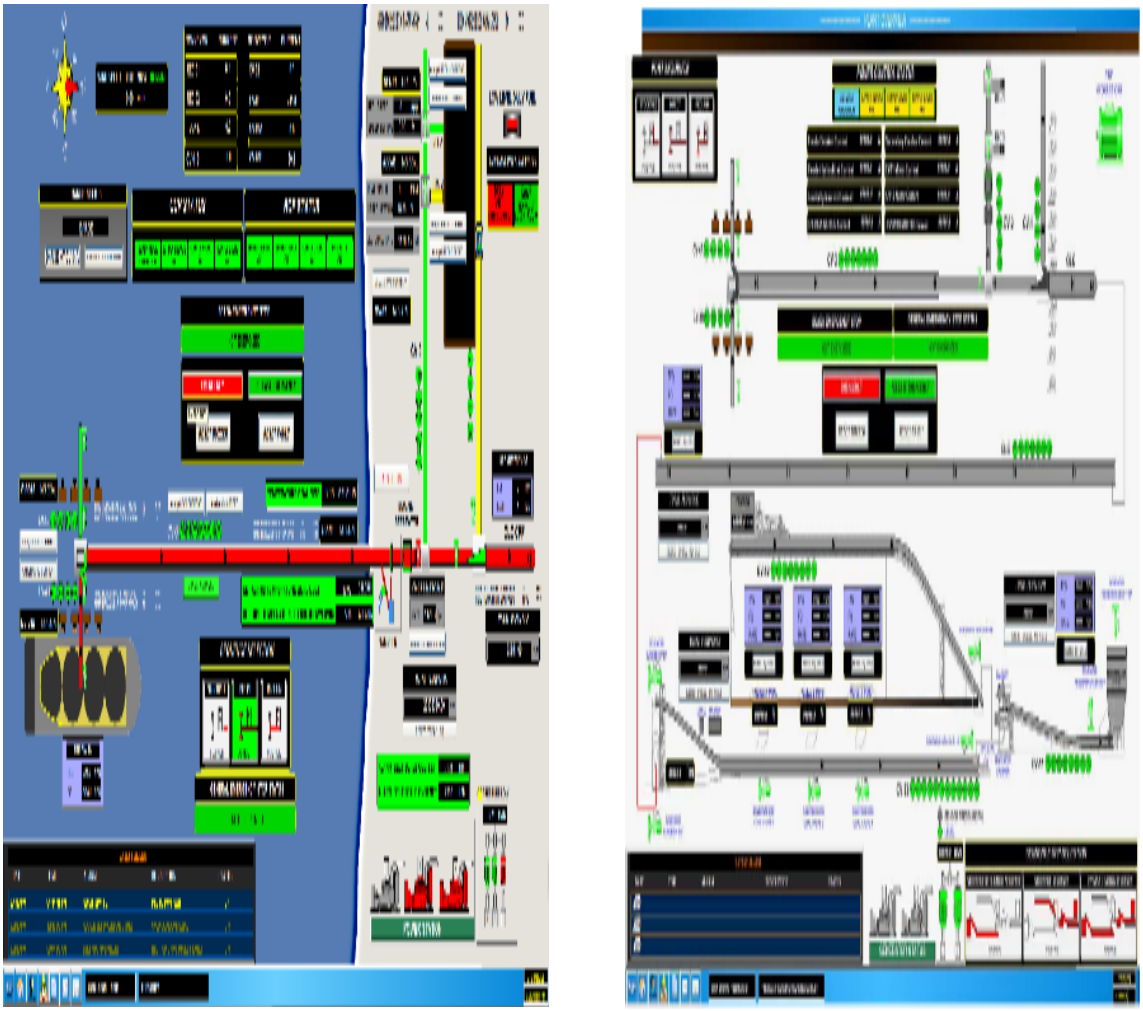


Fig. 8. SCADA (citect) in Control Room

special communication channel [8]. SCADA system shows the interface or display of process stages with good control, description and information. SCADA is illustrated in Fig. 8.

4.1.42 Conclusion

Thus with the adaption of modern PLC technology the coal level in the surge bin can be well controlled by the PLC without introducing the external human errors. The main objective behind the project is to avoid the failure of operator to start the plant for the right time, the longer production time and less usage of electricity power. Hence, through the project model is designed keeping in mind about the need for mining area and thermal power plant, the use of this technology can also be extended for implementing in the other process industries and further research application as well.

References

[1] Conveyor Equipment Manufacturers Association, "Belt Conveyors for Bulk Materials", 6th edition
2nd printing, Florida USA, 2007.
[2] Brian A. Moore, "Flow Properties and Design Procedures for Coal Storage Bins", in University
of Wollongong Thesis Collection, 1988.
[3] Jacob Fraden, "Handbook of Modern Sensors", 4th edition, California USA, 2010.
[4] R. Mandal, A. Kumar, "Application of Programmable Logic Controller for Gases Monitoring in
Underground Coal Mines", in journal of 2013 ESTIJ, India, 2013.
[5] John R. Hackworth, Frederick D. Hackworth. J, "Programmable Logic Controllers:
Programming Methods and Applications".
[6] Avvaru Ravi Kiran, "The Principle of Programmable Logic Controller and its role in Automation",
in journal of 2013 IJETT,Bangalore-India, 2013.
[7] Prof. Anup Dakre, Rupesh Bhosale, Omkar Nalawade, Akshay Chavan, "PLC Based Coal
Conveyor Automation and SCADA", in journal of 2016 IJTRE, Pune.
[8] Arindam Dutta, Ankush Chowdhury, Sabhyasachi Karforma, SubhabrataSaha, Saikat Kundu and
Dr. Subhasis Neogi, "Automation of Coal Handling Plant", January 2010, Kolkata-India.

The Annual Conference on Management and Information Technology (ACMIT) 2016

Reaction Time Difference Electric Actuator and Pneumatic Actuator Using Simulation X program

Abdullah Hawari

Abstract

Electric actuator and pneumatic actuator have some difference in the system, but need to find which one that have better efficiency and applicable on the designed system. Comparing two different system is not an easy task, need to find the right variable to be compared to define which one is more applicable. Reaction time is one of the variable determined by the velocity and the distance reached by the actuator to find which one is applicable. Using simulation X 3.3 to take the simulation on the pneumatics and the electronics using another parameter to find the reaction time of each system.

Keyword : Pneumatic; Actuator; Simulation X3.3

1. Introduction

Actuator is a type of motor that is responsible for moving or controlling mechanical system using source of energy, electric current, hydraulic fluids or compressed gas. There is also two types of movement that can be done by actuator the first is reciprocating move and the second one is rotary move. Commonly in industry commonly used actuator is hydraulic and pneumatic type. In this modern time when a company insist to have efficiency as high as possible. Hydraulic and pneumatic actuator have so many energy loses because of their energy source and phase change, in the other hand electric cylinder have higher efficiency because have fewer phase change.

2. Pneumatic Cylinder

Pneumatic cylinder are mechanical devices which use the power of compressed gas to produce a linear reciprocating force. Because the operating fluid is a gas, the leakage will not drip out and contaminate the surroundings, making pneumatics more attractive where cleanliness is a necessity. The challenges are created by the properties of the working liquid (compacted air): high compressibility and low consistency.

Speed and position are strongly related: an accurate positioning can be achieved only if a rigorous control of the actuated load speed exists[1]. Normally the control of the velocity is accomplished by incorporating a relative pneumatic stream controller (corresponding throttle or a relative directional control valve) inside the structure of the framework. The last form rearranges the structure of the framework, halting the heap in the modified focuses by hindering the weight supply circuits of the dynamic councils of the pneumatic engine. Because the pneumatic actuator work low pressure, when there is pressure loss, even only a little will cause a big loss on performance,

one of the treat of power loss is by infected by unwanted object. Unwanted object can cause power loss because it can damage the seal, rod and tube in actuator and make internal leaking.

3. **Electric Cylinder**

Electric cylinder is an actuator (cylindrical shaped) assisted by a motor to drive aligned worm gear to gain reciprocating movement. Typically, an electric motor is mechanically connected to rotate a lead screw. A lead screw has a constant helical string machined on its circuit running along the length (like the string on a fastener). Strung onto the lead screw is a lead nut or ball nut with relating helical strings. The nut is kept from turning with the lead screw (normally the nut interlocks with a non-pivoting part of the actuator body). Subsequently, when the lead screw is turned, the nut will be driven along the strings. The direction of motion of the nut depends on the heading of pivot of the lead screw. By associating linkages to the nut, the movement can be changed over to usable straight uprooting. Most current actuators are built for high speed, high force, or a compromise between the two. While considering an actuator for a specific application, the most vital particulars are regularly travel, speed, power, exactness, and lifetime.

There are many types of motors that can be used in a linear actuator system. These incorporate dc brush, dc brushless, stepper, or at times, even instigation engines. Everything relies on upon the application prerequisites and the heaps the actuator is intended to move. For instance, a straight actuator utilizing a basic pull AC motor driving a lead screw can be utilized to work a vast valve in a refinery. In this case, accuracy and high movement resolution aren't needed, but high force and speed are. For electromechanical linear actuators used in research center instrumentation mechanical autonomy, optical and laser hardware, or X-Y tables, fine resolution in the micron range and high precision may require the use of a fractional horsepower stepper motor linear actuator with a fine pitch lead screw. There are numerous varieties in the electromechanical direct actuator system. It is basic to comprehend the outline prerequisites and application imperatives to know which one would be ideal.

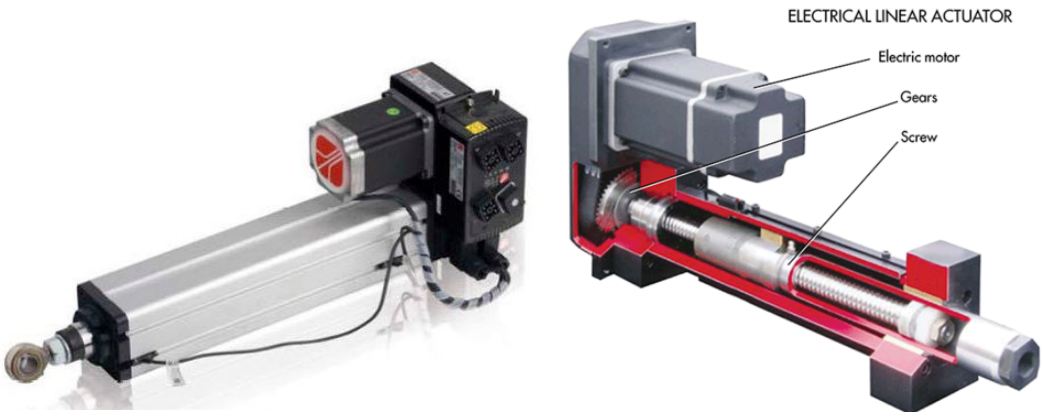


Fig 2.2 Electric Actuator

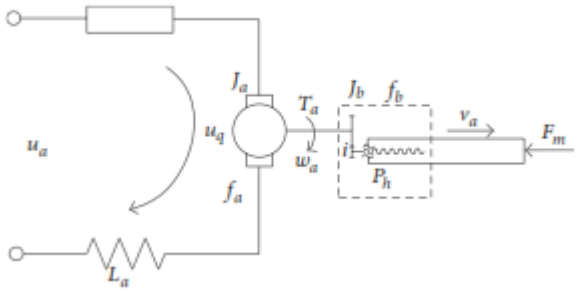


Fig 1.3 Schematic Drawing of Electric Cylinder

4. **Simulation X**

Using simulation X 3.3 we put on the parameter of the pneumatic and electric actuator, the problem with the simulation is we need to calculate all the variable first, we can't just put the type of the seal we need to directly put the friction of the seal that may be make the result inaccurate, also it's hard to determine the system for the electric actuator so make the simulation not completely done.

5. **Simulation Result**

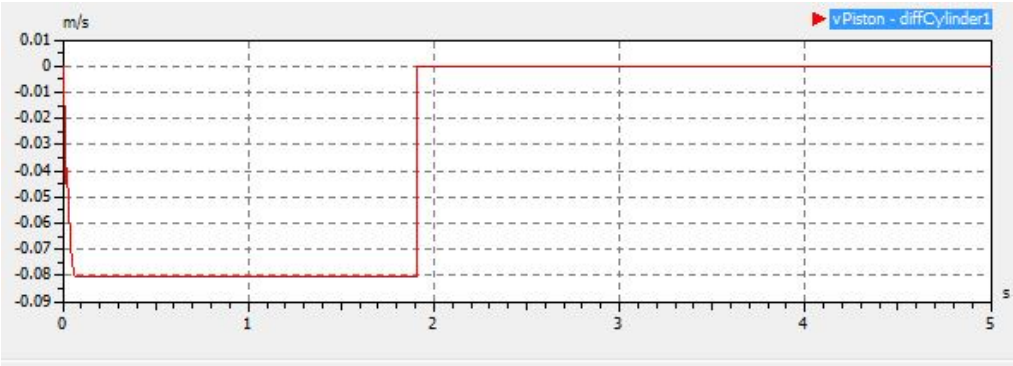


Fig.1.4 Velocity of

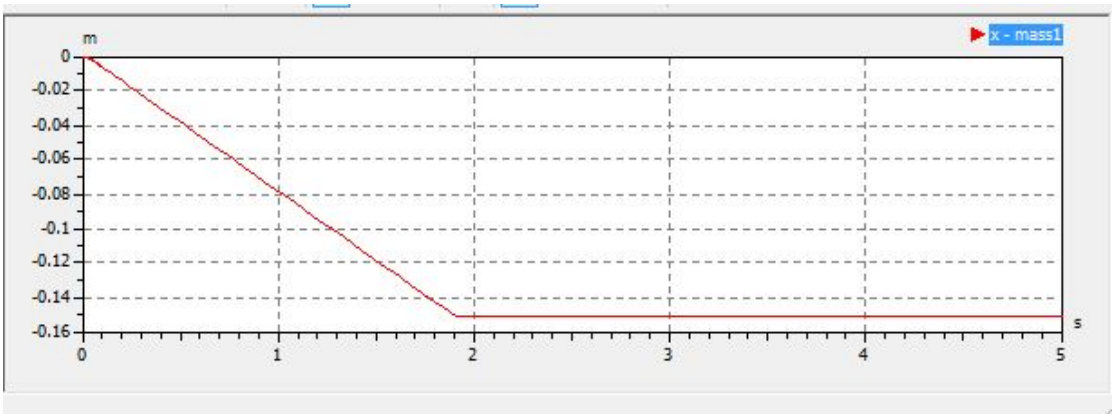


Fig 1.5 Distance Result Pneumatics

6. **Conclusion**

We find the time of the pneumatics to reach is full stroke is near 2 seconds, with the maximum velocity is 80 mm/s. Because we can't quite simulate the electric actuator properly we need to determine the speed of the electric actuator based on the

specification. As long it can achieve 151 mm of displacement on 2 seconds it can be determine that have same reaction time as the pneumatics one.

References

1. Avram, M. (2015). Control of speed and position of pneumatic actuator, 1-3.
2. Hassani, Meisam (2015). Dynamic Modeling of Linear Actuator Using Fuzzy System to Approximate Magnetic Charateristic, 1-6
3. Takahashi, Daiki (2016). Bilateral control of a velocity control system using electric and hydraulic actuators, 1-2
4. Bissal, Ara. (2015). Electric to mechanical energy conversion of linear ultrafast electromechanical actuators based on stroke requirements, 1-2
5. Liu, Yongguang (2015). Research of control strategy in the large electric cylinder position servo system, 1-7

The Annual Conference on Management and Information Technology (ACMIT) 2016

Experimental Vision Robot for General Working Application using Raspberry Pi and Single Camera with Python-OpenCV

Hendra Hermawan
Master Mechanical Engineering (Mechatronic), Swiss German University,EduTown BSD City, Tangerang, 15339 Indonesia.
email: hendra.hermawan@student.sgu.ac.id

Abstract

Development a visual-guided autonomous arm robot for general working application in service workshop require some preliminary works/research to ensure the quality and reliability of robot mainly on object detection/recognition and object pose estimation. We have experimented robot vision for this purpose using Raspberry Pi and single web camera supported by Python-OpenCV programming using color-base and contour-base detection algorithm for object recognition and Triangulation similarity method for object pose estimation.
Experiment results showed that color-base detection is 22% faster than contour-based object detection for colorful tooling object without disturbance same color from environment. However, contour-base detection is more effective for target working object detection than color-base. Light illumination and disturbance from environment should be managed for successful object detection. Triangulation linearity method is simple and fastest method for tooling object position estimation when tooling object is a known sized object. Experiment result showed error only 2% for distance estimation using this method compared with actual.

Keywords : General working, Raspbery Pi, Python-OpenCV, Object detection and recognition, Object pose estimation,

1. Introduction

The application of robotic system is increasing found on wide area implementation such as industry, military, consumer, medical, research and education. The needs of new robot which capable to imitate human behavior has driven many researchers and robot makers to develop an autonomous mobile vision arm robot from now and future. Basic design of an autonomous mobile vision arm robot consist integration of main subsystem : Mobile robot (2, 3 or 4 wheel driven), Arm and gripper robot with n degree of freedom (DOF), Vision system (camera and image processing computer) as presented in fig. 1.(a).

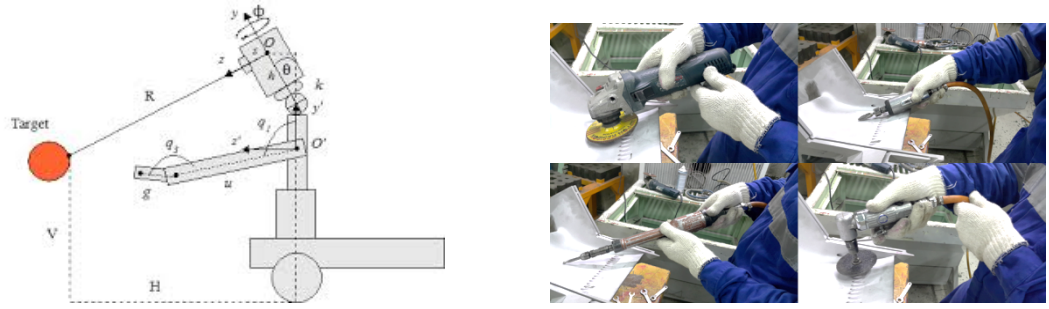
In this paper, we will report some experiments in development of vision arm robot for application in general working mainly found in service workshop. General working job normally is done by human worker to handle general tools (eg. hand drill, cutting tool, dressing tool) on working object (e.g component under repair) in service workshop as presented in fig. 1.(b). The normal activities of human worker in general working has sequence tasks as follows :

- Take general tools from its location
- Bring general tools to working area
- Perform general work at precise working object
- Return general tool to its location

Replacing general working activities by an autonomous vision robot from human worker has some benefits mainly whenever speed, accuracy/consistent result or safety issue (on harsh environment) are most likely desired. In this paper, will focus only on how robot can identify/ recognize general tools and repair object and also in how robot can estimate their position by vision, therefore development of mechanical action of arm robot and mobility of robot are not parts of this paper.

In vision detection and recognize object, such experiments have been reported by other computer vision researches. These include detection static object on fixed arm robot at indoor environment [1][8], moving object using single camera or omni-camera on mobile robot at outdoor environment [2][3], stereo vision to guide the robot arm return to the nominal home position [4]. While in vision

object pose estimation, such experiments have been done which are using camera monocular for highway driver assistance outdoor environment [5], 3D arm robot position indoor environment [6][8] and using visible laser diode in large surface measurement outdoor environment [7].



1.(a) 1.(b)

Fig. 1(a) typical autonomous vision robot [9]; 1.(b) typical general working activities in service workshop

2. Object detection and recognition

Object detection is all about finding an object or area of interest in a field of view. There are 2 methods evaluated in this report for object detection which are Color-base and Contour-base method.

2.1. Color-base detection

The picture color of image generally represented in color space either in RGB/BGR, YUV, YCrCb, HSV or Grayscale. RGB is one most popular color space model. In RGB space, every pixel image has color represented as a weighted combination of the Red, Green, and Blue. Each RGB value ranges between 0 and 255 with higher values corresponding to brighter pixels. This color space is widely used because it corresponds to the three photoreceptors of the human eye [8]. While in HSV space, each pixel color represented as combination of the Hue, Saturation and Value.

In color-base detection method, object detection is performed by selecting predefined color space (RGB, HSV or grayscale intensities) that will identify the object in an image while the rest of color will be neglected or marked as White/Black color background. The sequence algorithm in Color-base detection and recognition is presented in fig. 2.

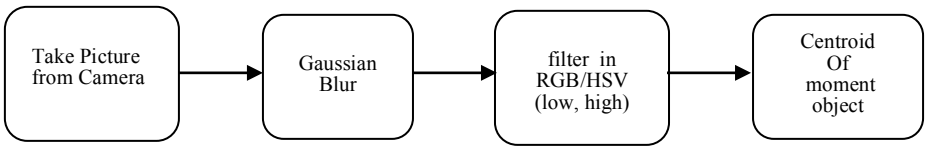


Fig. 2. flow diagram of color-base detection and recognition

To calculate centroid of moment object then image moment should be considered. An image moment is a certain particular weighted average (moment) of the image pixels' intensities, or a function of such moments, usually chosen to have some attractive property or interpretation. An image moment defined as [9] :

$$M_{xy} = \sum_i \sum_j i^{\cdot x}\, i^{\cdot j} f(i,j) \tag{1}$$

From the spatial moments M_{xy}, we can compute central moments which are invariant to translation (i.e. the position of the shape within the image). The centroid of image moment are C_x and C_y[9]:

$$C_x = \frac{M_{10}}{M_{00}} \quad C_y = \frac{M_{01}}{M_{00}} \tag{2}$$

The speed of this algorithm makes it very good for use in a controlled environment where disturbances of objects with similar color is not present[8].

2.2. Contour-base detection and recognition

There are some algorithm on contour-base (feature-base) method but on this report only evaluate Canny-edge and ORB.

2.2.1 Canny-edge

The Canny Edge detector is a multistage edge detection method developed by John F. Canny in 1986. It is a multi-stage algorithm with could be summarize each stages in fig. 3. After image is taken from camera then in first step the noise in the image is removed with a 5x5 Gaussian filter. In second step, the smoothened image is then filtered with a *Sobel* kernel in both horizontal and vertical direction to get first derivative in horizontal direction (G_x) and vertical direction (G_y).

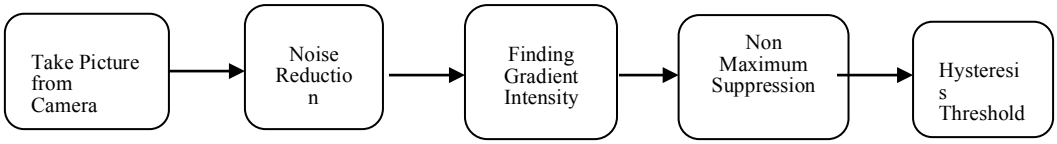


Fig. 3. flow diagram of Canny edge

From these two images, edge gradient and direction for each pixel can be found as follows [10]:

$$Edge\_Gradient\ (G) = \sqrt{G_x^2 + G_y^2} \quad (3)$$

$$Angle\ (\theta) = \tan^{-1}\left(\frac{G_y}{G_x}\right) \quad (4)$$

Gradient direction is always perpendicular to edges. It is rounded to one of four angles representing vertical, horizontal and two diagonal directions.uppression. In third step, after getting gradient magnitude and direction, a full scan of image is done to remove any unwanted pixels which may not constitute the edge. For this, at every pixel, pixel is checked if it is a local maximum in its neighbourhood in the direction of gradient. Finally in last step, all edges will be decided which are really edges and which are not. For this, there are two threshold values minVal and maxVal. Any edges with intensity gradient more than maxVal is included in the edge set and those below minVal is excluded (be non-edges), so discarded. Those who lie between these two thresholds are classified edges or non-edges based on their connectivity. If they are connected to "sure-edge" pixels, they are considered to be part of edges. Otherwise, they are also discarded.

For object matching, Canny edge use The maximum value of the correlation coefficient occurs when the template and the region in the input image are identical. This indicates the maximum correlation or the best possible match. The minimum occurs when the template and the region in the input image are least similar.

2.2.2 ORB (Oriented FAST and Rotated BRIEF)

ORB is basically a combination of FAST keypoint detector and BRIEF descriptor with many modifications to enhance the performance. First it use FAST (to find keypoints, then apply *Harris* corner measure to find top N points among them. It also use pyramid to produce multi scale-features. It computes the intensity weighted centroid of the patch with located corner at center. The direction of the vector from this corner point to centroid gives the orientation. To improve the rotation invariance, moments are computed with x and y which should be in a circular region of radius r, where r is the size of the patch. For descriptors, ORB use BRIEF descriptors with modification to make it rotation invariant.

For object recognition, ORB detector can be combined with Brute-Force Matching (BFM) method. It takes the descriptor of one feature in first set and is matched with all other features in second set using some distance calculation ad the closest one is returned.

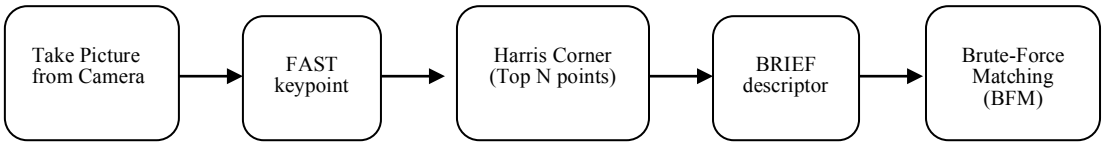


Fig. 4 flow diagram of ORB detection and recognition

3. Object distance estimation

Using Triangulation geometry method, distance of known object from camera could be estimated by vision. In this method, a known actual width of target object W with known distance D from camera and pixel length this object in camera is P then perceived focal length F of camera equation is [7] :

$$F = (P \times D) / W \quad (5)$$

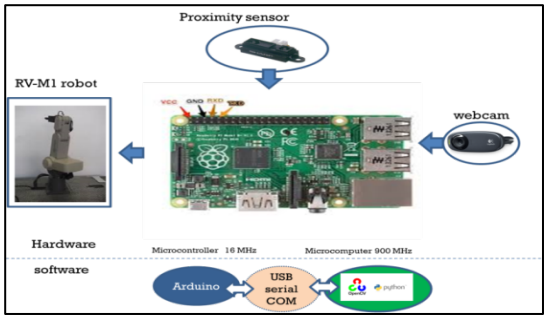
Since focal length F of camera and actual width W is constant, therefore for any new position of this object which calculated by vision of pixel P_1 could be estimated new distance D_1 [7]:

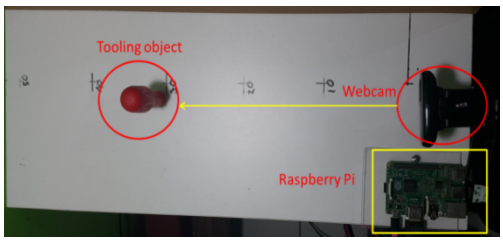
$$D_1 = (W \times F) / P_1 \quad (6)$$

4. Experiment Result

In our experiment, we use some hardware and software configuration as presented in fig. 5.(a) which consist of :

- Raspbery Pi 2 model B as microcomputer 900 MHz speed
- Webcam Logitech C310 with resolution 5 megapixels (1280 X 720 pixels)
- Distance Sensor of Sharp GP2Y0A21YK0F
- Analog to Digital Conversion 4 channels ADC 0804 (interface Raspberry to Distance sensor)
- Simulated for both general tools and target working object
- Experiment board
- Python programming software with Numpy and Matplotlib
- OpenCV libraries for vision computer software





5.(a) 5.(b)

Fig. 5. (a) Experiment Configuration; (b) Experiment setup

Since in this paper will focus only on how robot can identify/recognize object and also in how robot can estimate their position by vision therefore in experiment we did for scenario test as follows :

- Identification and recognize both of general tools and working object
- Identification and recognize of single general tools placed on others non target general tools
- Distance measurement of general tools and working object .

4.1 General tools detection and recognition

4.1.43 Color-base detection and recognition

.

In experiment, red tool (as target object)t was positioned among 2 other tools with different color. A sequence process of filtering image with color-base to get single general tools is presented in fig.6. It was observed, that a metallic part of tooling object could not filtered among other tools since the same black color with other tools. Hence image filtering using color-base in RGB format only effective to grasping area (red color) since it had different color with others. Also, from experiment color filter selection (lower and high) must carefully defined to get unique compared to other objects. Finally, grasping point for arm robot could be identified after centroid calculation be made (small circle in detected object was drawn for centroid location).

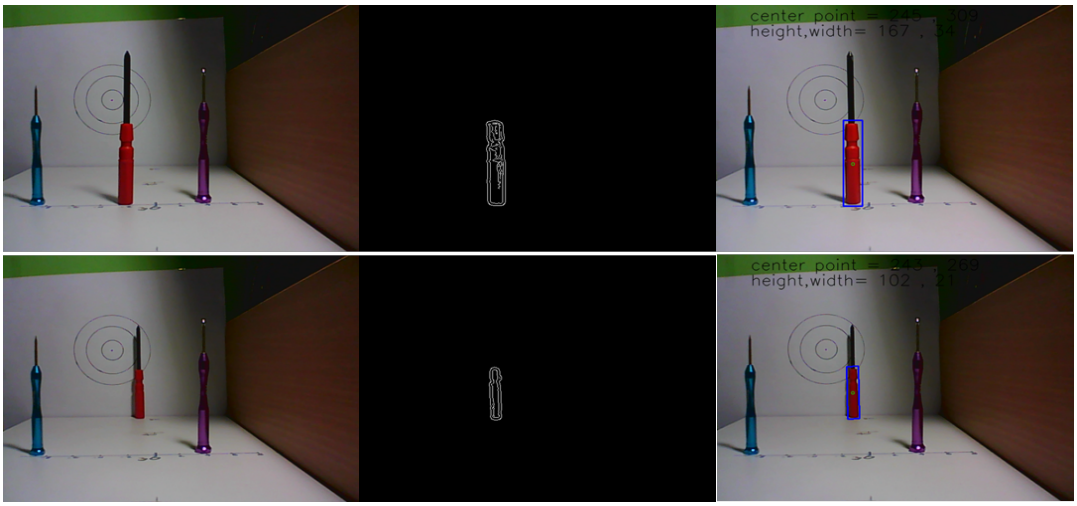


Fig. 6 sequence image result from camera, color-base masking, and end result detected of red tool

It was found that different light illuminations on the the tooling object will cause different RGB value setting to get target object even for the same color (red color). Also, when the same color exist on target tooling object and surrounding other tools (on metallic part) color base detection was not able to separate it. Therefore, Color base detection only able to select on holding part of target tooling object instead of whole parts of target tooling object.

4.1.44 Contour-base detection and recognition

4.1.2.1 Contour-base (Edge detection)

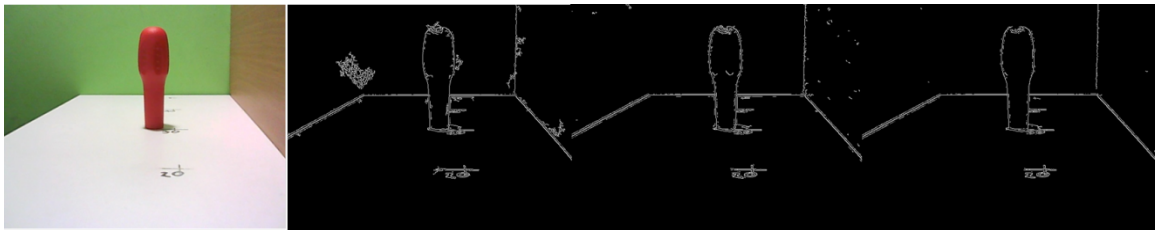


Fig. 7 edge detection result of general tools with different threshold at distance 30 cm

From experiment as shown in fig.7, we conclude at object distance 30 cm from camera the minimum threshold should be 30 and maximum threshold between 50 to 90 in order to get good edge image.

4.1.2.2 Contour-base (ORB detection)

By using ORB algorithm as presented before in figure (4), the red general tool as target was placed between two others general tool and then computed ORB's keypoint and compared and matched with BFM with ORB's keypoint from master single red general tools. Finally, 10 best matches were drawn among ORB's keypoints. The result of ORB detection and recognition is presented in fig. 8.

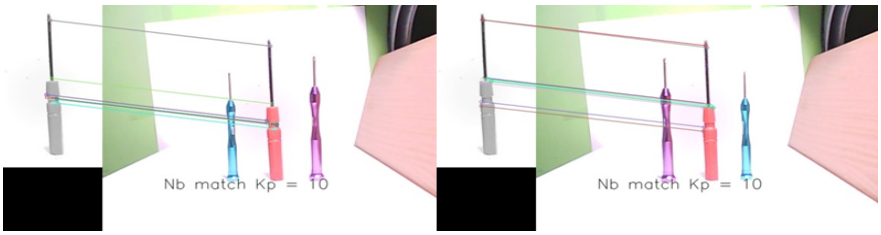


Fig. 8 The result for ORB detection and recognition is with number keypoint 10

4.1.45 Comparison Cycle time

This experiment was performed to evaluate cycle time processing among color-base and contour-base detection (ORB Match). The result is showed in figure (9). Base on the result experiment, cycle time of color base is 334.69 millisecond and 431.16 millisecond or 22% (96.47 millisecond) faster on color base.

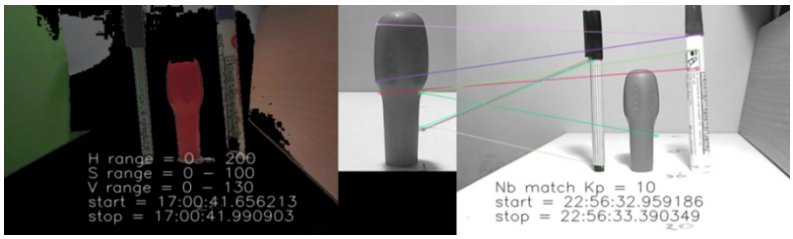


Fig. 9 cycle time between Color-base and Contour-base (ORB Match)

4.2 Target working object detection and recognition

In this experiment, the target of working object simulated by circle area which must be detected by vision system of robot. For this purpose, a finding circle method using Hough transform from Python-openCV library was used. Having detected, then red color circle is re-drawn using detected circle center point and its radius as presented in fig. 9.

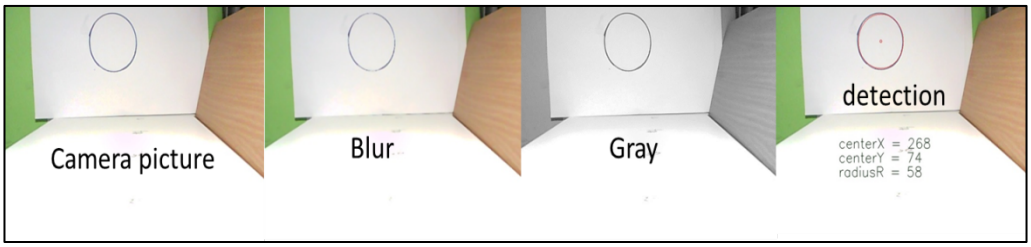


Fig. (9).The result for ORB detection and recognition is with 10 keypoints

4.3 Distance estimation of general tools

For this purpose, we choose red general tool (actual height of hand grasped is 6.5 cm) as master to calculate camera focus length. Using contour analysis of image we got image size of tool height is 164 pixel. Hence, using equation(5) the camera focal length is 756. This value was set to estimate distance of red general tool at any point placed in front of camera. In figure(10), the raspberry pi-

based vision computer could detect red general tool and estimate distance location from camera.

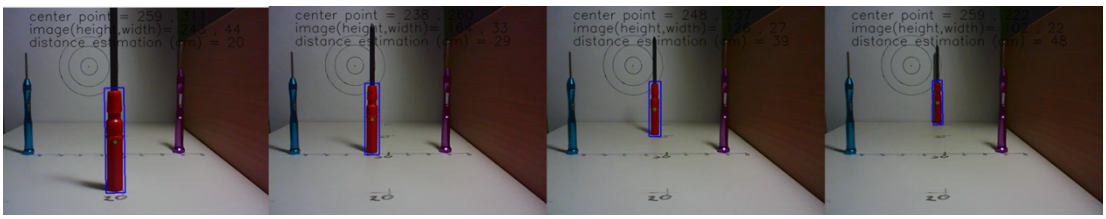


Figure (10). Image result of business card object at 20, 30, 40,50 cm distance

With refer to these experiment, pixel length of each object could be computed and presented as in table 1.

Table 1 Image pixel length measurement.

Description	Distance=20 cm	Distance=30 cm	Distance=40 cm	Distance=50 cm
Image height (pixel)	243	164	126	102
Distance estimation (cm)	20	29	39	48

With four distance points as sample data, the error of distance estimation is 2%.

4.4 Distance estimation of working object

For this experiment, Sharp GP2Y12 distance sensor has been utilized as comparison with vision method to estimate location of working object and result showed in table 2.

Table 2 Working object position estimation.

Experiments	Center point (pixel)		Radius		Distance	
	X-axis	Y-axis	Actual (cm)	Visual (pixel)	Actual (cm)	Sensor (cm)
Single circle	268	74	4.175	58	57	55
Outer circle	288	94	4.8	71	57	56
2nd outer circle	295	95	3.3	48	57	57
Inner circle	292	96	1.4	21	57	56

5. Conclusion and Further Work

This paper has reported some experiments using Raspberry Pi Raspberry Pi 2 and Web Cam that was sufficient as embedded computer vision for autonomous vision robot with cycle time between 330-435 millisecond for object detection and recognition. Tooling object detection using color-base method is faster 22% in cycle time compared with contour-base detection. However, this method only effective for tooling object with significant color. For tooling object with not significant color and unstructured shape, it should be used contour-based detection.

Object distance estimation using Raspberry-base vision computing and Triangulation similarity method give result error 3% from actual when object placed within 50 cm from camera. Light intensity, disturbance environment and proper filtering criteria are very critical factors must be managed properly for successfully Vision guided object detection/ recognition and object distance estimation for arm robot. Also, camera parameters both intrinsic and extrinsic should be considered when precision position is highly desired.

Future work is recommended to be done for validation of arm robot action in grasp of object using object position from this paper. Also using more real general tools and working object (part under

repair) will make more realistic experiments. This research still use single camera and it is recommended for expansion using stereo camera in order to get 3D object reconstruction for determine more accurate grasping point of general tools.

References

[1] Amit Agrawal , Yu Sun , John Barnwell, Ramesh Raskar. *Vision Guided Robot System for Picking Objects By Casting Shadows.* Mitsubishi Electric Research Laboratories. 2009

[2] Boyoon Jung , Gaurav S. Sukhatme. *Detecting Moving Objects using a Single Camera on a Mobile Robot in an Outdoor Environment.* In the 8th Conference on Intelligent Autonomous Systems; 2004

[3] Domagoj Herceg, Ivan Markovi´c, Ivan Petrovi. *Real-Time Detection of Moving Objects by a Mobile Robot with Omnidirectional Camera.* Image and Signal Processing and Analysis 7th International Symposium. .p. 289 – 294; 2011

[4] Yi Jin, Ming Xie. *Vision Guided Homing for Humanoid Service Robot.* Pattern Recognition Proceedings 15th International Conference . p. 511 - 514 Volume 4; 2000

[5] Geng Lei, Xiao Zhitao, Wu Jun, Zhang Fang, Miao Jinghong. *Monocular Vision Distance Measurement Method Based on Dynamic Error Compensation*. International Journal of Digital Content Technology and its Applications. Volume 7, Number5, 2013

[6] Cheng-Hao Huang, Chi-Sheng Hsu, Po-Chien Tsai, Rong-Jyue Wang, Wen-June Wang. *Vision Based 3-D Position Control for a Robot Arm International Journal of Digital Content Technology and its Applications*. Systems, Man, and Cybernetics (SMC), IEEE International Conference; 2011

[7] Cheng-Chuan Chen, Ming-Chih Lu, Chin-Tun Chuang, Cheng-Pei Tsai. *Vision-Based Distance and Area Measurement System.* Wseas Transactions on Signal Processing. Issue 2, Volume 4,; 2008

[8] Eirik Anfindsen Solberg, *Vision Based Robotic Control*, Master Thesis Norwegian University Science and Technology. 2014

[9] Kennet Dawson, Howe, *A Practical Introduction to Computer Vision with OpenCV*, Dublin, Ireland, Willey Publishing. 2014

[10] Ashwin Pajankar, *Raspberry Pi Computer Vision Programming,* Birmingham, Mumbai, Packt publishing. 2015

The Annual Conference on Management and Information Technology (ACMIT) 2016

[Poster Paper] Information Technology Risk Management for Data Center With Physical Security Methods

Moh. A. Amin Soetomo*, Teddy Septiawan*
[a]*Swiss German University, EduTown BSD City, Tangerang 15339, Indonesia*
[b]*PT. Sigma Cipta Caraka (Telkomsigma), German Center BSD City, Tangerang 15321, Indonesia*

Abstract

Management of IT data-based risk becoming an important part to deal with all the threats that arise from an information system. The method used in managing risk starts from identifying risk, assessing risk, and establish strategies to manage them through the available resources. Risk management in a data center must be related to data security and security policy in force. So it is not enough just to apply the methods and techniques of electronic data security but need to be supported physically securing data.

Keywords: Risk Management; Data Center; Physical Security;

The Annual Conference on Management and Information Technology (ACMIT) 2016

[Poster Paper] Risk Assessment for Android Malware Using Permision Based Analysis

Yohanes Syailendra Kotualubun
yohanessyailendra@gmail.com
Edu Town BSD City, Serpong, Indonesia

Abstract

Smartphone have been becoming the most used mobile handset and most users are relying on smartphones to store their private information. Starts from personal contact, personal schedule, until banking accounts are still been stored in the smartphone's storage. All of the information is put at risk because of many "trusted" Applications stored at Application Store. Major threat of Android users is malware that uploaded into App Store. This paper will try to calculate qualitative Risk Assessment based on Static Analysis, focusing on permission based analysis.

Keyword : Android, Risk Analysis, Malware Detection

SWISS GERMAN UNIVERSITY
MASTER OF INFORMATION TECHNOLOGY
Kavling EduTown II.1
BSDCity Tangerang 15339
Telp. 021 3045 0045, Ext 1501-1505
acmit2016@sgu.ac.id | sgu.ac.id

ISSN : 977-2355-020-149