FAKULTI KEJURUTERAAN ELEKTRIK

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LAPORAN PROJEK

SARJANA MUDA

A FORMAL METHOD FRAMEWORK FOR AUTOMATED VERIFICATION OF A DEAERATOR SYSTEM

Nur Amirah Binti Othman

Bachelor of Electrical Engineering (Control,Instrumentation and Automation)

June 2014

" I hereby declare that I have read through this report entitle "A Formal Method Framework for Automated Verification of A Deaerator System" and found that it has comply the partial fulfillment for awarding the degree of Bachelor of Electrical Engineering (Control, Instrumentation and Automation)"

Signature : ……

Supervisor's Name : DR SAIFULZA BIN ALWI @ SUHAIMI

Date : 9 JUNE 2014

A FORMAL METHOD FRAMEWORK FOR AUTOMATED VERIFICATION OF A DEAERATOR SYSTEM

NUR AMIRAH BINTI OTHMAN

A report submitted in partial fulfillment of the requirement for the degree of Bachelor of Electrical Engineering (Control, Instrumentation and Automation)

Faculty of Electrical Engineering

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2014

I declare that this report entitle "*A Formal Method Framework for Automated Verification Of A Deaerator System*" is the result of my own research except as cited in the references. The report has not been accepted submitted in candidature of any other degree.

Signature : ……

Name : NUR AMIRAH BINTI OTHMAN

Date : 9 JUNE 2014

Specially dedicated:

To my beloved father Othman bin Mohamad Noor,

To my beloved mother Nor Haizan binti Embong,

My beloved sister and brothers,

My supervisor and all my lecturers,

All my friends.

For their encouragement, support and motivation through my journey of education.

ACKNOWLEDGEMENT

Bissmillahirrahmanirrahim,

Alhamdulillah. Many grateful and thanks to Allah SWT for His continuous blessing and giving me the consent to complete this Final Year Project. This Final Year Project was organized by Faculty of Electrical Engineering (FKE), Universiti Teknikal Malaysia Melaka (UTeM) for student in final year to complete the undergraduate program in Bachelor of Electrical Engineering Major in Control, Instrumentation and Automation with Honors.

First of all, my sincere gratitude goes to my supervisor, Dr Saifulza bin Alwi @ Suhaimi to give me the opportunity to be under his supervision for the Final Year Project. Many thanks for the encouragement, suggestions and guidance in achieving the goal and maintain the progress in track. The discussions and the meetings give me a lot of new knowledge to explore regarding to my project. Next, I also want to thanks to all the lecturers of FKE, UTeM for their support and motivation to complete the project.

Many thanks to my friends, Munirah Binti Mohd Siraj, Mohd Mohaimin bin Miswon and Nurrafidah binti Mohammad Rashid who help me and give me the suggestion and motivation to make my best for this project. Not to forget to all my classmates in 4 BEKC and other friends,thank you very much for the support and concern to my final year project directly or indirectly. This four years experience will be remembered as an important memory before enter the new chapter of line as an engineer soon.

Last but not least, deepest thanks and appreciation to my parents for their moral supports, love, sacrifice throughout my life. I am thankful for their sacrifice, patience, and understanding during completing this project. Their sacrifice had inspired me from day I learned to write and read until I am now.

ABSTRACT

Deaerator is important equipment in feed water system of a power plant. The role of deaerator system is to remove dissolved gases which are oxygen and carbon dioxide that comes from the water leaving of condenser and to give the adequate level of water to the deaerator storage tank. In deaerator system, the flow of steam and water has their own principles which are the flow of steam before supply to the deaerator storage tank and the flow of water from condenser flow before supply to the boiler. The principle of deaerator system must in the correct order to make sure it is in the safe condition to the plant system. Thus, formal verification of correctness of a property is used as an approach to ensure all the specification created meets the actual behavior for the system. All the specifications must always *hold* during the verification process to ensure that the model designed will not violate. The verification procedure is also need to eliminate the errors that decrease the safety of the automation system. Hence, in this project, it will show on how the computational method such as temporal logic model checking can be used to verify the correctness of the design of an automation system. The project involves the deaerator model and the design of the ladder diagram (LD) using Programmable Logic Controller (PLC). The project used Computational Tree Logic (CTL) as the temporal logic to determine the specification. By using several logical specifications to the deaerator system, the designed model of deaerator model and control logic should verify so that it will not violate the required specification. If none of the behaviors of the system violates the given specification, the model of the system will correct. Otherwise, the model checker will automatically execute the counterexample of the model system to show why the specification is false. The verification of the system will be performed by using Symbolic Model Verify (SMV) model checker software.

ABSTRAK

Deaerator ini memberikan peranan penting dalam sistem air suapan loji kuasa. Peranan sistem deaerator adalah untuk membuang gas-gas terlarut iaitu oksigen dan karbon dioksida daripada air pemeluwap dan menghantar air yang mencukupi ke tangki simpanan deaerator . Dalam sistem deaerator , aliran wap dan air mempunyai prinsip-prinsip mereka sendiri yang merupakan aliran wap sebelum bekalan kepada tangki simpanan deaerator dan aliran air dari aliran kondenser sebelum disalurkan kepada tangki dandang. Prinsip sistem deaerator mesti dalam susunan yang betul untuk memastikan ia berada dalam keadaan yang selamat untuk sistem kilang. Oleh itu , pengesahan rasmi kebenaran ciri-ciri sistem yang digunakan sebagai pendekatan untuk memastikan semua spesifikasi yang dicipta memenuhi kelakuan sebenar untuk sistem itu. Semua spesifikasi mesti sentiasa berada pada tempat yang betul bagi memastikan model yang direka tidak akan melanggar . Prosedur pengesahan juga perlu untuk menghapuskan kesilapan-kesilapan yang mengurangkan keselamatan sistem automasi. Oleh itu, dalam projek ini , ia akan menunjukkan bagaimana kaedah pengiraan seperti duniawi model logik semakan boleh digunakan untuk mengesahkan kebenaran reka bentuk sistem automasi. Projek ini terdiri daripada model Deaerator dan reka bentuk gambarajah tangga (LD) Format menggunakan Programmable Logic Controller (PLC) . Projek ini menggunakan pengiraan Tree Logic (CTL) logik duniawi untuk terjemahan spesifikasi. Dengan menggunakan beberapa spesifikasi yang logik untuk model Deaerator itu, tingkah laku model yang disahkan dan hasil pengesahan digambarkan untuk operasi yang selamat. Jika tiada tingkah laku sistem melanggar spesifikasi yang diberi, model sistem akan membetulkan. Jika tidak, pemeriksa model secara automatik akan melaksanakan penyangkal sistem model untuk menunjukkan mengapa spesifikasi itu adalah palsu.Pengesahan terhadap sistem itu akan dilakukan dengan menggunakan Model simbolik Sahkan (SMV) perisian model pemeriksa.

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURE

LIST OF SYMBOLS

| , ∨ - OR gate

& - AND gate

~ - NOT gate

-> - THEN

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

This chapter briefly discussed about the motivation and the problem of this project. Besides, the objective and the project scope should be achieved at the end of the project.

1.1 Motivation

In power plant industry, steam power is the largest sector of the electrical generating industry and without it, the world will be in a big trouble. Electricity we use nowadays comes from the generation of steam from the power plant industry for example in thermal power plant, coal power plant and others.

In many years, the use of formal method in software development would help the industry meets the criteria or goals for their system as the software system in much important to engineering field. In the other disciplined of formal method approaches, such as object in structured design, it offer a methods to simplify the view of the system especially for the designer and the customer used. Formal method is a method that described the view or the behavior of the system immediately. Mathematical approached is very important to describe the behavior of a system and it will help the engineer to create the right system and help to create the system to right.

Thus, by all, the main motivation by doing this project is to enable applying the tools and techniques to check the property of reachability and resettability. It is important technique to make a checking in order to make sure the system not violate to the specification.

1.2 Problem Statement

Deaerator of a power plant is one of the important components for feed-water system. It is a feed-water heater which is widely used for remove entrained air that contained oxygen and carbon dioxide, CO_2. The example of deaerator that usually used in the power plant is Boilermate deaerator, Spraymaster deaerator and others. The deaerator system can control the steam pressure and water level of deaerator storage tank. In the deaerator system, it requires the heat which is comes from the steam at desired operating value. The water and steam will agitated together and remove the dissolved gases. The steam has high pressure steam that need to be reduced to maintain the desired pressure of deaerator operating pressure. Accurate pressure control is very important to get the saturation temperature of deaerator. The failure to maintain the steam pressure and temperature will cause too little inlet steam to remove the entrained air.

Besides remove the entrained air, the deaerator also must to keep the deaerator storage tank roughly half levels full of water to make sure enough supply feed water to the boiler. Too low water level makes the pump cavitations and the boiler shut down. Hence, adequate level control is very important in deaerator system. Hence, by all the behavior and principle flow of the deaerator system, the application of formal verification via model checking can be checked by using the software system. It is very important to check the correctness of the mathematical model of the model designed because in the plant system, the smallest change in the input will result to the different change in the output of the system. The verification is also required to eliminate design errors that decrease the safety of the system and to check the system from enters the undesired states. Thus, this proposed project is to introduce a formal method framework for automated verification of the deaerator system based on the prescribed logical assumption.

1.3 Objective of the Project

1. To determine the behavior of a deaerator system for the purpose of transformation to logical behavior.
2. To model the mathematical expression of deaerator system based on the prescribed logical assumption.
3. To verify the logical behavior of deaerator control system through Symbolic Model Verifier model checker software based on the Boolean model.

1.4 Project Scope

In power plant, there are several different types of design for deaerator which are steam flow pressurized deaerator and Boilermate deaerator. For this project, the Boilermate deaerator is used as to describe the behavior of deaerator system. deaerator system control two functions which are steam pressure and water level of deaerator storage tank before transfer to the boiler feed water pump. This project is only use logical of deaerator system based on continuous variable. The logical behavior of deaerator system is described by using the flowchart for the purpose of transformation to logical behavior. The transformation to logical behavior is described by using ladder diagram (LD) format of Programmable Logic Controller (PLC) in order to check whether the controller safe or not. Next, the designed controller, mathematical model and other temporal properties are transformed to Boolean equations before performing the verifications. The Computational Tree Logic (CTL) is used in this project as a type of temporal logic for specification and verification purposes. For the FALSE verification result, the detail process of counterexample will not be explained in this project. The verification of the behavior for deaerator system is carried out through SMV model checker software based on Boolean model.

CHAPTER 2

LITERATURE REVIEW

This chapter consists of three parts which are theory, research work and summary of literature review that are related to this project. The theory and information obtained from the published paper is very useful and as a guide to finish this project.

2.1 Theory

2.1.1 Basic Process of Deaerator System

In power plant industry, the steam and water system is in closed loop which means the water leaving the condenser will be fed back to the feed pumps and flow to the boiler [1]. The process will repeat continuously in the power plant system. Figure 2.1 shows the flowchart of main process in the power plant system.

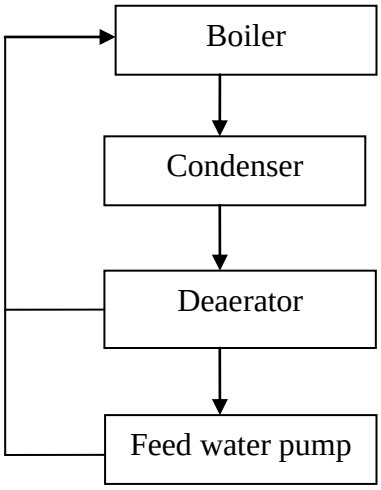

Figure 2.1 : The main process in power plant system

Based on Figure 2.1, the deaerator is one of important system in power plant. The water leaving from condenser cannot flow directly to the feed water pump without pass through the deaerator first. It is because the water from the condenser is cold and contained entrained air that must to be removed before it is transferred to the feed water pump and the boiler. The entrained of air contain dissolved gases which are Oxygen and Carbon dioxide. These two dissolved gas will make corrosion in the boiler, condensate line, steam lines and heat transfer equipments. The basic process of removing the dissolve gases in deaerator has two stages of operations. The first stage is in the Spraymaster, the water leaves the condenser and enter the top of deaerator through the self adjusting spray nozzles into a steam-filled primary heating and vent concentration section. At this stage, the temperature increase at 2 or 3°F of the steam temperature and most of dissolved gases are released at this point.[2] The second stage is in the Boilermate, the steam from the exhaust steam sources flow to the top of deaerator tank. It then flows at the bottom of the deaerator storage tank and flow upward through exchange packing. At the exchange packing, the hot water flow downward and meets the hot steam, deaeration occur and the heating water falls down to the deaerator storage tank and flow to the boiler feed pump.

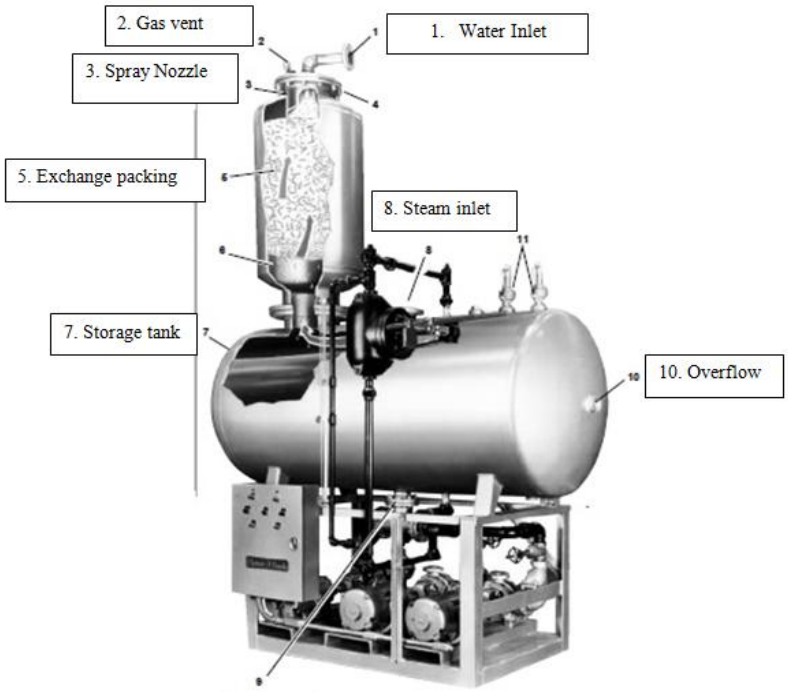

Figure 2.2 The Boilermate deaerator

2.1.2 Formal Method

The formal is frequently supported by tools, it uses mathematically rigorous semantics so that the analysis tool can give high quality of the design and software. The formal method made the interest to the researchers and engineer. It is because it can detect error early and hence reduce the cost of it use. Beside the name of formal method, it also called as mathematically method in determine the specification of the system designed which then can described the correctness with the actual system. The formal method or mathematical modeling is importance because it not possible the software system have free of error, sometimes the data that used in the software possible to become failed, hence the concept of formal method will be check and led to the correct result [3]. The formal method can be proven by using model checking and the theorem proving. The model checking technique can be check through the Symbolic Model Verify (SMV) model checker software.

2.1.3 Model Checking

Model checking is an automated verification technique which focused on determines the temporal logic and sees whether specification is same with the system designed or not. The tools of model checking can be check through SMV model checker software. Besides, by model checking, it also can detect the errors use in software system with the actual system and can give counterexample execute of model system on why the system is violated.

Three main creating the model checking technique are modeling, specification and verification. Modeling means convert the design into a suitable formal form which is compatible the model checking software that usually use formalism. Next, specification means ensure the properties of the design system are stated by using logic expression. The last one is verifying means determination the model obtained in first state is true with the next state or not.

Model checking has several of advantages. The first one is this verification technique has no proofs means it does need to construct the correctness proof. When enter

model description or diagram into the software, the checking will automatically run. Second is it has counterexample means if the specification is not correct, the model checking software will show why the specification is not same with the system. Next is model checking can have many temporal logic properties for concurrent systems. A concurrent system means several behaviors that occur simultaneously and connected to each other [4].

2.1.4 Temporal Logic

The first step in formal verification is the representation of formal specification of the design consisting of a description of the desired behavior. Temporal Logic is a logic expression the ordering events in time without introducing time explicitly [5]. It is also one of the formal verification techniques that can be used to verify the correctness of a finite state concurrent system. There are two types of temporal logic in order to express the properties for verification which are linear temporal logic (LTL) and Computational Tree Logic (CTL). In LTL, time s treated as if each moment has a unique possible future. The Boolean connectives as well as temporal connectives usually uses X ("next"), G ("always"), F ("eventually"), and U ("until").

CTL is also called as branching temporal logic. It is refer to the fact that at each moment there is several different possible futures. This type of temporal logic is described the tree of states rather than sequences. The tree is possibly representing all possible computations. CTL explicitly introduces path quantifiers which are "all path" and "Exist a path". "All path" represent "A" notation which mean the temporal logic is true in all paths starting in the current states while "Exist a path" represent "E" notation which mean the temporal formula is true in some path starting in the current state [6]. These two notation are combined with other alternative notation are used for temporal operators. The first one is "AF *p*" describes that for all the path starting from a state, eventually in the future, condition *p* must be hold. Second, "EF *p*" describes that there exists some path that eventually in the future satisfies *p*. Third, "AG *p*" describes that condition *p* is always or globally, true in all states of all the possible paths. Fourth, "EG *p*" describes that there is some path along which condition *p* is continuously true.

2.1.5 SMV Model Checker

SMV is symbolic model checking tools which is one of the software that can be verifying the temporal logic properties of finite systems [7]. SMV verifies every possible behavior of the system's behavior of the system satisfies the specification. A specification for SMV is a collection of properties. The properties can be created or can be specified in a notation using temporal logic.

2.2 Research Work

Through out the research that had done in order to understand this project, there are several terms meets from the previous paper. The first term is the basic about the formal method. Formal method is an effective techniques for automation software verifications which is increasingly been recognized. Software verification of formal method is an integral part of the software development which is to ensure the software system is satisfies with all the requirements model system. Researchers have been developed many different approach, but technique of mathematical modeling of this formal method is focused since the formal method can finding the errors of the model system [8]. The application of formal method by the other research is presents the formal method of Partition-and-Recur (PAR) method. It is used to design and prove the algorithmic programs. It also is an effective formal method on solving the Combinatory problems by using PAR method. This formal method not only simplifies the process of algorithms and correctness the testing but also improves the atomization, standardization and corrects the algorithm by changing many creative labors to mechanized labors. It used the C++ language [9]. Next is, formal method in requirement engineering and its application. The formal method divide into two forms which are in model checking and the theorem proving. The tool of model checking is by using NuSMV model checker and SPIN model checker. Model checking is a verification of finite state system. Finite state mean when all its variable range over discrete domain hence, number of possible state is finite. Next is by theorem proving. It is another approach to proving a specification is correct. The tool of theorem that usually used is Z "Zed" [10].

The second term covered in this research work is the automated verification. The automated verification is by verifying the properties of model system. It has several steps by doing verification in this paper. The first one is state the initial conditions that must be followed by input of model system. Next are the verifiable of the properties needed to be described as formula of MCDL in VMTS and finally the proofs of the properties of the model system detailed [11].

The third term is model checking technique. The paper presents the application of model checking technique in two system design of two nuclear power plant. Model checking technique is one of the methods for verifying whether the model of system is fulfills the specification by determine all the possible behaviors that have in the system. By the given a model and the specification, the model checker which is NuSMV can determine whether the software system used is behave with the model system or not. If the system is violates, the model checker do the counterexample which it will execute the model system and determine why it's false or not behave as the model system. The model used in this paper use the flow chart to describe the emergency cooling system. It used the state variable with the different possible states. "high", "low" and "medium". The model of the system use the principle of when no water flow into reactor container, the water will remain same or decrease and if water is flowing in, the water level will remain same [12]. The example of model checking on the other research.The paper discussed the verifying the design of satellite software control system which is called attitude and orbit control system (AOCS) by using model checking technique. The system behavior is to maintain the attitude of the satellite and for performing fault at detection, isolation and recovery decision of satellite. The verifying is use by symbolic model checker NuSMV 2. The diagram is transform to temporal logic properties by using BDD-based LTL model checking to prove the model system [13].

Besides, the other terms on the research work is Boolean expression. The use of Boolean Expression Manipulator from the research by using BDDs**.**The paper presents the LSI design system using Binary Decision Diagram (BDDs) which is use the Boolean expression. It uses Arithmetic Boolean Expression Manipulator (BEM-II) which is also on BDD technique. It calculates the Boolean expression that contains mathematic expression which is subtraction, addition, multiplication and comparison and then transform to the other various format [14].