1-1-2013

Fault Tolerant Control Design for Feedwater System

Mohammed Eltayb
Ryerson University

FAULT TOLERANT CONTROL DESIGN FOR FEEDWATER SYSTEM

by

Mohammed Eltaybb

A project

presented to Ryerson University

in partial fulfillment of the
requirement for the degree of
Master of Engineering
in the Program of
Electrical and Computer Engineering.

Toronto, Ontario, Canada, 2013

AUTHOR'S DECLARATION FOR ELECTRONIC SUBMISSION

I hereby declare that I am the sole author of this MRP. This is a true copy of the MRP, including any required final revisions.

I authorize Ryerson University to lend this MRP to other institutions or individuals for the purpose of scholarly research

Signature _____

I further authorize Ryerson University to reproduce this MRP by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

I understand that my MRP may be made electronically available to the public.

Signature_____

FAULT TOLERANT CONTROL DESIGN FOR FEEDWATER SYSTEM

Master of Engineering 2013
Mohammed Eltayb
Electrical and Computer Engineering
Ryerson University

Abstract

Fault tolerant control (FTC) is essential nowadays in the automation industry. It provides a means for higher equipment availability. Fault in dynamical systems can occur due to the deviation of the system parameters from the normal operating range. Alternatively, it can be a structural change from the normal situation of continuous operation such as the blocking of an actuator due to the mechanical stiction. In this research project, a fault tolerant controller is designed with Matlab Simulink for a feedwater system.

The feedwater system components are modified to work under embedded controller design with FTC attached to it. Feedwater systems usually consist of a de-aerator or simply a water storage tank, feedwater pumps, control valves, piping and support fitting elements such as chock valves, flanges, hoses and relief valves, beside instrumentation devices like level transmitters, flow transmitters, pressure regulators. The faults are injected separately for each device. Fault diagnostic is used to detect and identify the faults by Limit-checking method. Then a controller is reconfigured to take the action of correcting the hardware failures in the control valve, level sensor, and feedwater pump.

The simulation results revealed that the redundant components can take over and handle the process operation when the fault occurs at the duty components. Level sensors are set to work in on-line mode, while the control valves are set to work in off-line mode, due to the mechanical parts movement. Setting the control valves in off-line mode reduces the probability of valve stiction and elongates the component availability.

The results reveal the operation of feedwater system is not stopped when a hardware failure takes place in all feedwater system major components. Moreover, the disturbances are not considered in this research as there are many control techniques that can be used to handle the disturbance in a robust way.

Acknowledgments

Thanks to Allah.

My deepest and most sincere gratitude to Dr. Vadim Geurkov, my supervisor at Electrical and Computer Engineering Department, Ryerson University. With his encouragement I could achieve this research work.

Also I would like to thank my family and my friends for their kind support.

Contents

List of Figures

Chapter 1

Introduction

The complexity of automation in processes is continuously growing due to the increasing demands of making safety first for personnel, equipment, and environment, as well as the requirement for higher performance and quality and cost efficiency of production. In this industry environment, a fault free process is not guaranteed.

In process and manufacturing industries, reliability, availability, and safety, are always in a high demand. The continuous operation of machine tools such as actuators, instrumentation, and controllers, is vulnerable to disturbances and errors, and in order to achieve a continuous high quality products, the standard controllers such as proportional, integral, and derivative (PID) controller, model predictive controller (MPC), etc. are designed to maintain a robust control system by compensating for many types of disturbances. Sometimes, there is a change in process operation that such controllers can not handle. These include, for example, a hardware defect, fault output, and large process transients[1]. Fault is defined as unpermitted deviation from the actual measurement. Therefore, designing a fault tolerant controller to avoid such faults is becoming more important in automation industry. Fault tolerant controller is a controller that monitors all process equipment, detects most possible faults, and takes action by reconfiguring the process controller to continue handle the process operation. Fault detection and diagnosis (monitoring and supervision) is a key component of many automation systems. Fault detection is the recognition that a problem has occurred, even if the root cause is unknown. Faults may be detected by a variety of quantitative or

qualitative means. This includes many of the multi-variable, model-based methods. It also includes simple, traditional techniques for single variables, such as alarms based on high, low, or deviation limits for process variables or rates of change. Fault diagnosis is the pinpointing of one or more root causes of problems, to the point where corrective action can be taken. This is also referred to as fault isolation, especially when emphasizing the distinction from fault detection[1].

In common, casual usage, fault diagnosis often includes fault detection, so fault isolation emphasizes the distinction. A fault does not have to be the result of a complete failure of a piece of equipment, or even involve specific hardware. For instance, a problem might be defined as non-optimal operation or off-spec product. In a process plant, root causes of non-optimal operation might be hardware failures, but problems might also be caused by poor choice of operating targets, poor feedstock quality, poor controller tuning, low steam system pressure, sensor calibration errors, or human error. A fault may be considered a binary variable in which the component is faultless or faulty, or there may be a numerical extent, such as the amount of a leak or a measure of inefficiency. Fault tolerant control systems are needed in process control to reduce the potential hazards and hidden risks in a technological systems to a safe level with respect to human, environments and production.

1.1 Background

Modern control systems are vulnerable to malfunction due to possible faults and failures in actuators, sensors or other components. To deal with this issue, the fault-tolerant controller design has been an active research area for several years, and aims to design a controller to guarantee a satisfactory performance for a given system under both normal and fault environments. This kind of controller was used in the early 1970s for safety critical systems of aircraft, space craft, chemical plants and power plants.

Fault tolerant control systems can be classified as passive or active. In the passive case, the controller is designed to be sufficiently robust to predetermine faults so that no modification in the control process is needed after experiencing a fault. In the active case,

some preliminary actions are first taken to detect and diagnose the fault, and the controller is then reconfigured based on an off-line or online strategy[2].

Fault in dynamical systems is the deviation of the system parameters from the nominal situation or structural change from the normal situation like the blocking of an actuator due to the mechanical stiction. Faults will change the performance of a closed loop system which further result in production loss or degradation in system stability. It is very important to distinguish between fault and a disturbances. Faults are usually represented as additional external signals or as a parameter deviations, but disturbances are represented by unknown signals that have to be added to systems output signals. Additive faults are the faults that represented as additional external signals while the multiplicative faults are the parameters signal deviation. Modeling the uncertainty signal is the same as dealing with multiplicative faults. Robust control design can handle the uncertainty signals and the disturbances in the dynamic systems, but to deal with faults, a fault tolerant control design must be established to reconfigure the main controller to cancel the faults effect or to attenuate them to acceptable levels[3, 4, 5].

The process industries are a broad group of businesses comprising both the primary and secondary industrial sectors. The primary industries look after the first stages of processing raw materials, or producing the primary energy requirements for our society. These basic industries are the heavy industries such as oil production facilities, coal power generation, and pulp and paper, or the utilities such as water treatment and waste water sectors. The so-called secondary industries are those in which the first stage of product manufacturing is initiated. Second group industries would include petrochemicals, pharmaceutical, refineries, distillers, food producers, and textile manufacturers. Manufacturing is the third industrial layer which combines the primary outputs of energy with the partially refined raw materials to produce finished goods for consumer-based society[1].

Distributed control systems (DCS) are usually used to control and monitor process operation for all industrial layers. The advance control techniques are built inside the DCS controller to provide robust control. The hardware failure of process components must be

avoided by DCS, which is usually not affordable by such advanced techniques. The emergency shutdown system (ESD controller) is often built to work in parallel with DCS. The function of ESD controller is to protect the plants from hazards associated with plants operation, for example such hazardous are classified by ISA standards. Class 1 hazards is defined as flammable gases or vapors are present in the air in quantities sufficient to produce explosive or ignitable mixtures. Class 2 hazards is combustible or conductive dusts are present in the plants surrounding area. Class 3 hazards is ignitable fibers or flyings that are present, but not likely to be in suspension in sufficient quantities to produce ignitable mixtures, such as typical wood chips, cotton, flax and nylon[1].

1.2 Motivation

The reason of developing such fault tolerant control design for the feedwater system is to minimize the risk of boiler shutdown due to components hardware failure. Simultaneously, the need of this design is to maintain the feedwater tank level. The equipment such as instrumentation and valves of the ESD system are not intended for connection to the DCS, according to many standards and regulations[6, 7]. They are designed to work in the event of an emergency situation. In this thesis, a proposed design using the signal only, and not the hardware wiring (e.g., field instrument), that is connected between two systems through a communication bus is proposed. For example, a level transmitter is wired to ESD system as an analog input and at the same time a signal from ESD to DCS carrying the level value is transmitted. This value is used as virtual transmitter working as a second sensor to design a fault tolerant controller. The need for such design will provide a cost reduction in using a redundant instruments and less wiring to a DCS[8].

The feedwater system is used in many industrial layers. It has a major impact on the overall plant efficiency and performance. Poor control of the feedwater can cause for example, the level in the boiler to overflow and dumping of the valuable treated feedwater. In addition, the boiler may trip resulting in unplanned plant shutdown that could impact the production performance. In the normal range of plant operation, the boiler feedwater

regulator experiences high flow rates with low differential pressure. However, during startup, this valve experiences low flow rates with very high differential pressure, which can cause severe cavitation damage. Hardware failure of the feedwater components has also a major economy impact for causing unpredictable plant shut down. For the above reasons, the needs of designing a fault tolerant controller is necessary to carry out the feedwater system protection layer that can be attached with the existing DCS controller[1, 8, 9].

1.3 Objectives

The aim of this research work is to modify the feedwater system components to work under embedded controller designed with FTC attached to it. The faults are to be simulated and injected separately for each component. Fault diagnostic and isolation method is to be used to detect and identify the faults. Then a controller (with FTC attached to it) is to be reconfigured, when hardware failure happened in one of the feedwater system components. The controller is expected to take action of correction. The expected result is to have a smooth process operation of the feedwater system freed from any high transients. A higher components availability is to be achieved for sensors level, control valves at the tank inlet, and feedwater pumps. Availability is the ability of the components to perform their functions when required.

1.4 Contribution

The major contribution of this research work is to implement the right fault tolerant identification method as well as the right redundancy strategy that will result in a reliable process operation of the feedwater system. Utilizing a Matlab-Simulink to design fault tolerant controller is also a challenge in modeling a process functions of dynamic systems such as feedwater system, although there are many standards such as IEC and ISA recommend the use of function block diagram (FBD) language, which has a very simple way of designing process control functions in its library. The thesis also reflects some ideas about a research based on an industrial experience of how the operation and the safety of the feedwater system

is designed and controlled. The terminologies of fault tolerant control have been described in the literature with a very broad definitions. This thesis tries to present a simple way of definitions that can describe the basic concept of fault tolerant control and the feedwater system through the literature review chapter.

1.5 Work Structure

The introduction to the thesis has been given in chapter one, to familiarize the reader with a brief description and background of the feedwater system. The motivation behind conducting this research work is also given in chapter one. To explain the overall structure of the fault tolerant control and how the the feedwater system works, chapter two is designated to carry out a literature review for fault tolerant control and the feedwater system. Chapter three is to describe how the proposed model is designed with Matlab-Simulink to configure a fault tolerant controller for a feedwater system. The proposed model results are also showed in this chapter. Discussion is needed as well to verify how the proposed model is effective in solving the problem of the hardware components failure in the feedwater system. The conclusion is discussed with a suggested future work in chapter four. All the circuit diagrams of Matlab-Simulink are given in the appendix.

Chapter 2

Literature Review

2.1 Introduction

The Feedwater System collects water from the condenser hot wells, where the steam generated during operation is condensed, through the condensate pumps and feedwater heaters to the deaerator storage tank, moves it through redundant, isolable pumps, valves, and heaters to the steam generators to maintain the proper water level within the boiler[10]. The function of the boiler is to raise the pressure of the hot well water sufficiently to drive it into the steam generator, against steam generator pressure. Also it provides a means to isolate the steam generators from the main feedwater system in the event of a feed line or steam line rupture, as well as to provide a means to inject chemicals to maintain feedwater chemical properties within design specifications. Fig. 2.1 depicts the structure of the feedwater system. Feedwater system components can be described as follows:

1-Feedwater pump

Usually it has a high horsepower, motor-driven centrifugal pump that takes a suction, via the feedwater pump suction header, from the deaerator storage tank. The feedwater pump draws a suction from the deaerator storage tank; it raises pressure of the feedwater before discharging to its associated feedwater pump. The feedwater pump has a minimum flow line, returning flow to the deaerator. This minimum flow control system allows the feedwater pump to operate at a sufficient rate (e.g., when the feedwater control valves have the feed-

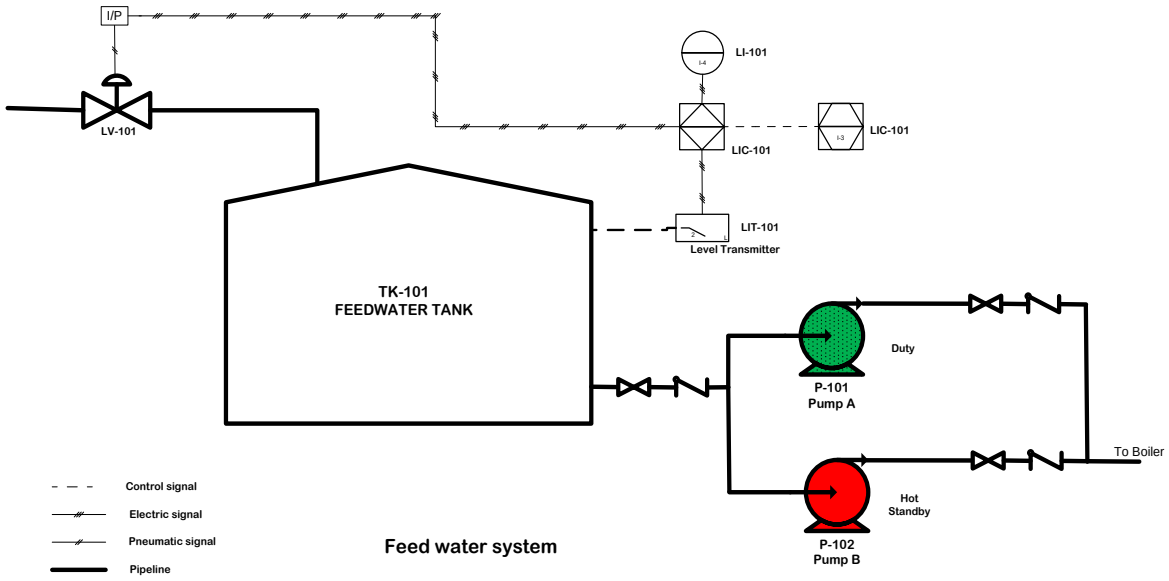

Figure 2.1: Feedwater system

water flow essentially shut off) to prevent damage to the pump (due to dead-heading)[10].

2-Feedwater valves

The feedwater isolation valves, are usually designed as gate valves type connected in series. Each valve is equipped with an electro-hydraulic operator designed to fail closed on loss of electric power. The signal to shut the valves comes from either a manual signal sent from the main control room or a main steam isolation signal. The isolation valves will completely shut within a few seconds of a main steam isolation signal[10].

3-Feedwater instrumentation

A temperature detector well, with local temperature indication, is mounted in the inlet header of the feedwater tank, on the discharge line of each of the main feedwater pumps,

and on the inlet and outlet piping of each train of high pressure feedwater tank. A pressure indicating transmitter, with plant monitoring input functions, is mounted on the common supply header feeding to the boilers, on the discharge of each of the feedwater pumps. The pressure indicator transmitter is used for plant monitoring system input. Level transmitters are mounted on the feedwater tank to provide the controller with a continuous monitoring of the water level[9].

4-Feedwater control system

The feedwater control system provides the capability for stable system level control during steady-state operation and in case of transients. The fault tolerant control is attached to the main feedwater controller providing a protection layer incase hardware failure or high system transients.

2.2 Fault Tolerant Control

The structure of fault tolerant control (FTC) is depicted in Fig. 2.2. The diagnostic block is to carry the fault detection method as well as to identify the fault type. This block will send the fault signal to the controller redesign block to take action of modifying the existed controller in order to tolerate the errors and maintain stabilized plant operation. All small arrows represent signals, and the large arrow is to represent the connection between the controller redesign block (Reconfiguration block) and system main controller[11].

Fault tolerant controller works in such a way to compensate for faults so they do not lead to system failure. The most common way to reach that is to use component redundancy. The down side of redundancy is that, the system will be more complex and costly[11]. Such redundancy schemes can be designed for hardware, software, and information processing. An example of mechanical and electrical components that have a redundant scheme is sensors, actuators, micro-computer, buses, etc.

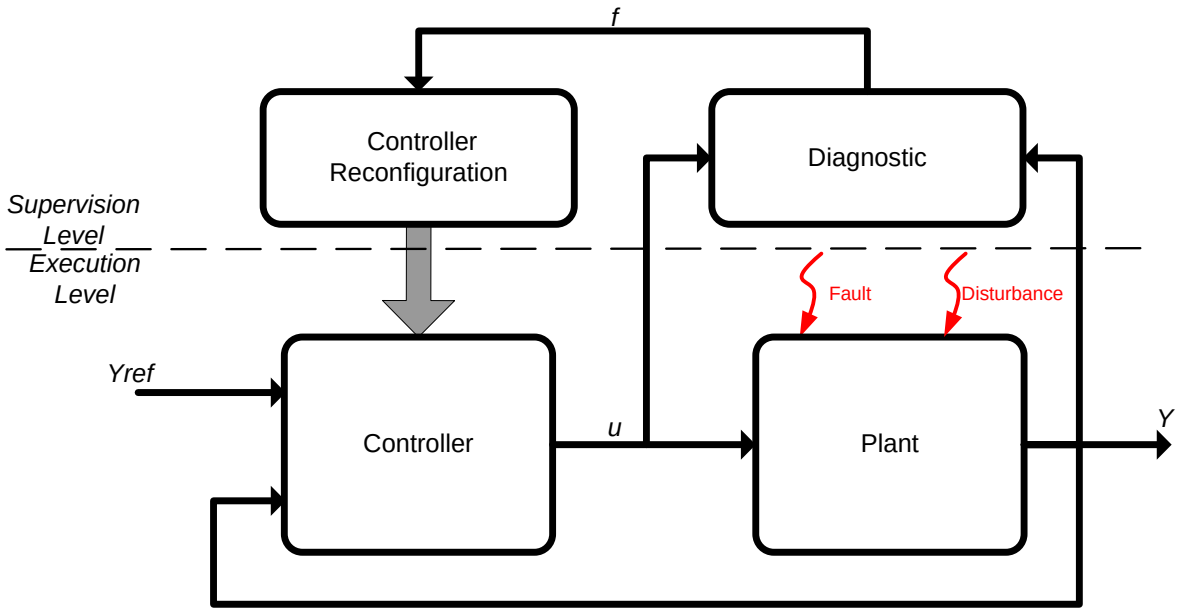

Figure 2.2: The structure of fault tolerant control(FTC).

2.2.1 Supervision and Fault Management

In supervision and fault management, the measurable variables are checked with regard to tolerances and alarms are generated for the operator. In the case of a dangerous process state, the monitoring function automatically initiates an appropriate counteraction, and based on that, symptoms are generated via change detection, a fault diagnosis is performed and decisions are made for controller reconfiguration[12]. A simple limit checking method can be applied for monitoring the process variables, which works especially well if the process operates approximately in a steady-state. However, the situation becomes more complicated if the process changes rapidly at the set points[11].

2.2.2 Fault Detection Methods

The goal for early detection and diagnosis is to have enough time for counteractions like other operations, triggering of redundance, configuration, maintenance or repair. Earlier detection

can be achieved by gathering more information, specifically by using the relationship between the measurable quantities in the form of mathematical models. For fault diagnosis, the knowledge of cause-effect relations must be used. Models-based methods can be used for prediction of the impacts of faults as well as diagnosis. In most cases, the model-based method is independent of the process controller. Application development is formalized; often easier to review and re-use with fewer errors for multiple instances of the same equipment. Assumptions and limitations are likely to be clearer especially for first principles models. They are likely to reflect physical laws rather than observed coincidences that might only be true under certain conditions[11].

Quantitative models are numerical models such as algebraic equations and differential equations. For example, the gross error detection and diagnosis methods associated with traditional data reconciliation are based on quantitative, static models: algebraic equations (and inequality constraints)[1].

Qualitative models generally do not include information on the magnitude of faults or their effects. Rather, they use terminology such as high temperature, often using variables that are binary or a few discrete values. A state transition diagram is another example of a qualitative model. Fault propagation models (cause/effect models of abnormal behavior) are the most common. Dynamic models explicitly model behavior over time, while static models do not. In the case of numerical models, this is a difference between algebraic models vs. models based on differential equations or difference equations. Even qualitative models can incorporate dynamics. For instance, cause-and-effect models can include time delays. In another example, a state transition diagram or Petri net is a dynamic model, because it models changes in state that occur over time when triggered by events. Frequency response analysis is not common in fault diagnosis except for event generation, although it provides a way to describe some dynamic behavior through algebraic manipulations[1].

Level sensor measurements can show some oscillations with either a harmonic or stochastic nature, or both. Signal model-based fault detection may apply to correct or modify this oscillation. The task of fault detection is summarized in Fig. 2.3.

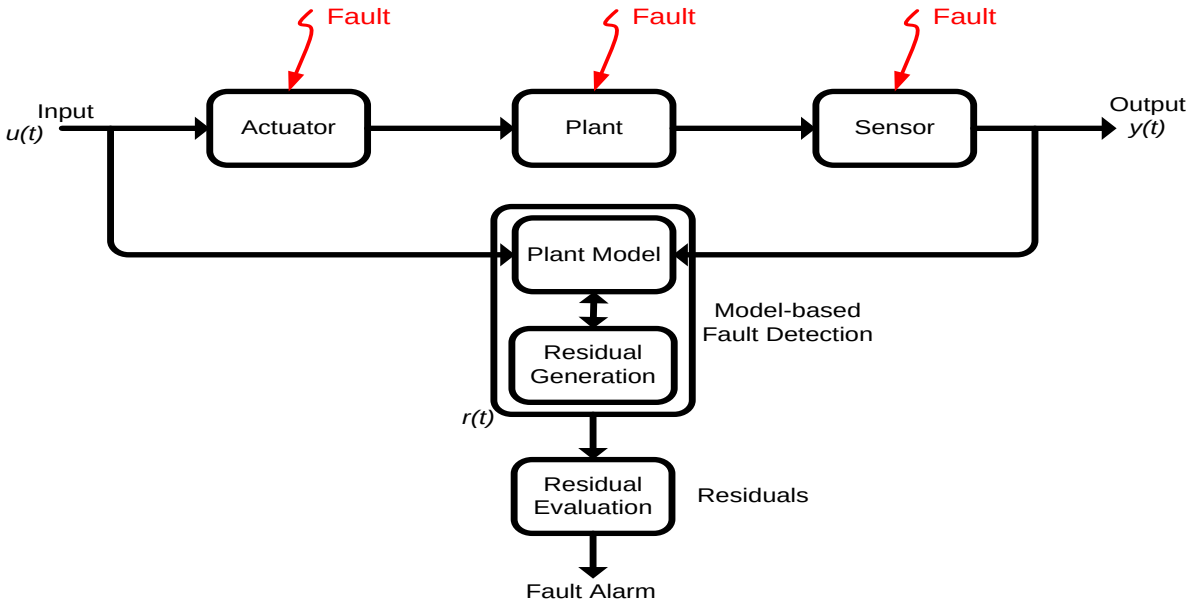

Figure 2.3: Structure of model-based Fault Detection and Isolation System.

Limit Check Based-model fault Detection

The big advantage of the classical limit-value based supervision method is its simplicity and reliability. It has the ability to react after a relatively large change of a feature, i.e. after either a large sudden fault or a long lasting gradual increasing fault. In addition, an in-depth fault diagnosis is usually not possible. Limit check is basically defined as a range of two values called threshold, allow a certain value to pass through the threshold and reject other values. If Y_{max} represent the maximum threshold value and Y_{min} for the minimum threshold value, a normal state can be defined as[11]:

$$Y_{max} < Y(t) < Y_{min} \tag{2.1}$$

In a normal situation, if $Y(t)$ stays with a certain tolerant area, and any increase value out of the threshold (i.e., the threshold is determined by Y_{max} and Y_{min}) will indicate a faulty value. This method can be applied to any measured values such as level, flow, pressure,

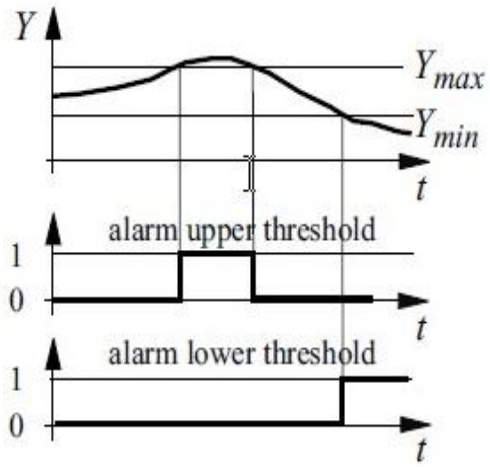

Figure 2.4: Limit-checking, the absolute value $Y(t)$

and temperature. The selection of the threshold range is usually based on experiments and trend history of system. There is a trade-off between narrow and wide threshold, and it is very important to avoid measurement fluctuation (see Fig 2.4). Another simple approach of limit-check is also use a trend checking. Trends use the previous values of the signal. by taking $\dot{Y} = dY(t)/dt$, monitored the variables, and check if[11].

$$\dot{Y}_{max} < \dot{Y}(t) < \dot{Y}_{min} \tag{2.2}$$

This equation can help identify whether the selected threshold is too small. Moreover, an alarm can be obtained earlier if the threshold is small than using a limit checking with absolute value. Limit checking of absolute value and of trend can be combined by making the absolute value dependent on the trends $Y_{max} = f(\dot{Y} > 0)$ and $Y_{min} = f(\dot{Y} < 0)$ in order to detect early deviations as well as avoiding false alarms for small trends[11].

Parity Equation Model-Based Fault Detection

Parity equation is a direct and straightforward method used to detect faults by comparing the process behavior with the process model. The difference in signals between the actual

process and the process model is called residuals. Residuals is a check of process parameters consistency. Residuals can be designed by using the transfer function or state space formulations. To explain how the parity equation method works, a multiple input multiple output model is considered (see Fig 2.5), and the process is described by the transfer function as follows[11]:

$$G_p(s) = \frac{y_p(s)}{u(s)} = \frac{B_p(s)}{A_p(s)} \tag{2.3}$$

The process model is

$$G_m(s) = \frac{y_m(s)}{u(s)} = \frac{B_m(s)}{A_m(s)} \tag{2.4}$$

Assuming the model parameters are known such that

$$G_p(s) = G_m(s) + \Delta G_m(s) \tag{2.5}$$

where $\Delta G_m(s)$ is the model errors, the output error is the residual and is formulated by:

$$r'(s) = y_p(s) - y_m = y_p(s) - G_m(s)u(s) \tag{2.6}$$

$$r'(s) = G_p(s)[u(s) + f_u(s)] + n(s) + f_y(s) - G_m(s)u(s) \tag{2.7}$$

$$r'(s) = \Delta G_m(s)u(s) + G_p(s)f_u(s) + n(s) + f_y(s) \tag{2.8}$$

For faultless process the residual is equal to zero, and in this case there is no addictive faults f_u and f_y and no noise (n represent the noise and u is the input signal) the polynomial error or equation error leads to:

$$r(s) = A_m(s)y_p(s) - B_m(s)u(s) \tag{2.9}$$

$$= A_m(s)[G_p(s)[u(s) + f_u(s)] + n(s) + f_y(s)] - B_m(s)u(s) \tag{2.10}$$

If the process and the model agree, ideally the residual becomes

$$r(s) = A_m(s)[f_y(s) + n(s)] + B_m(s)f_u(s) \tag{2.11}$$

Additives faults f_u are filtered by the model polynomial $B_m(s)$ at the input terminal and and f_y by $A_m(s)$ at the output. The above equation defined r and r' as a primary residuals for polynomial errors and output errors respectively

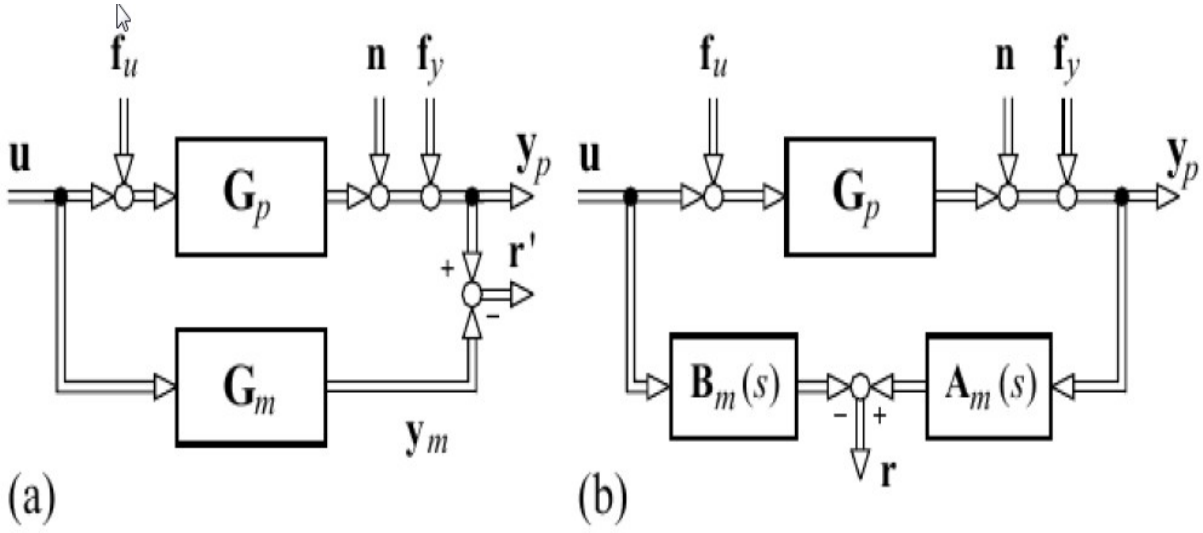

Figure 2.5: Residual generation with parity equations for multiple-input multiple-output process:(a) Output errors; (b) Polynomial errors

2.2.3 Controller Redesign

Controller redesign is responsible for changing the control structure after the fault has occurred in the process. It aims to satisfy the closed loop systems requirements in terms of having a continuous operation without any interruption. There are two principles of the controller redesign, one is fault accommodation which means to adapt the controller parameters to the dynamical properties of the faulty plant. The input and output of the plant used in the control loop remain the same as in the case of the faultless process. Faults accommodation is based on the controller predesign and is used to be configured off-line for a specific fault before putting the system in operation. This requires all the resulting control schemes to be stored in the control software. The second principle involves the controller reconfiguration, which is only acceptable in case of the controller accommodation, which is not a feasible solution. The complete control loop has to be reconfigured. This loop reconfiguration includes the selection of new control configuration where alternative input and output signals are used. The selection usually depends on the possible and existing process faults. As such, a new control law has to be designed on-line while the operation is running.

Control reconfiguration is very useful for correcting sensor faults, actuators faults, and plant faults[13].

2.3 Feedwater System

To understand and develop the fault tolerant control system, one has to be familiar with the basic operation of the targeted system. A feedwater flow control system is defined by ISA standards as a control system that uses input signals derived from the process for the purpose of regulating feedwater flow to the boiler to maintain adequate boiler drum level according to the manufacturers recommendations. The minimum design requirements for feedwater system include[6, 7]:

1. Process measurement for the water level, pressure, and flow. In some cases a temperature measurement is also required.

2. Control and logic, the control philosophy has to be set prior to system design (i.e., PID, MPC, or Fuzzy control.

3. Final control device. A careful selection of control valve sizing has to be taken into consideration.

4. System reliability and availability by measuring the individual system component availability and reliability.

5. Alarm requirements. Incase of faults, operator has to be notified by the controller to take a correct action such as reporting the faulty equipment to be serviced immediately and determine the selection of duty component according to the operating hours defined by the manufacturer.

6. Operator interface, for operator easy access and quick intervention to add or modify the process operation.

Feedwater systems consist of de-aerator or simply water storage tank, feedwater pumps, control valves, piping and support fittings elements such as chock valves, flanges, hoses and relief valves, beside instrumentation device like level transmitters, flow transmitters, pressure regulators. Feedwater systems is one of the most important parts in power plant system type steam turbine-generators. This is because if the supply to the water boiler is impeded, then the steam feeding the turbine will cease to function[14].

2.3.1 Control Valve

A control valve is defined as a mechanical device that fits in a pipeline creating an externally adjustable variable restriction. Most plants are still utilizing pneumatic spring and diaphragm actuators to actuate their feedwater recirculation valves. These types of actuators are sufficient for many, less critical, plant applications, which do not provide recognized payback for tighter control.

The use of pneumatic actuators inherently results in hysteresis due to stiction, which is caused by the need to overcome frictional forces created between the valve packing and valve stem. The main limitation with these actuators is due to the compressibility of air as a control medium. Recent years have seen an improvement in pneumatic control due to the advent of smart positioners. These positioners reduce the effect of stiction in pneumatic actuators by introducing advanced control algorithms in the positioners.

The downside to smart positioners is an additional increase in dead time, to help correct for stiction, particularly in valves with larger actuators, and when the control signal step change is small (2% or less). Another downside to pneumatic actuators is their lack of rigidity. Because air is the operating medium, and is compressible, they can often be moved by the process. Pneumatic actuators do not have the stiffness that is inherent to a hydraulic actuator and therefore do not have the ability to control as accurately when small steps are required. The rigidness of a hydraulic actuator is well suited for an application requiring fine control and tight shut-off such as boiler feedwater recirculation. Water is an incompressible fluid. Assuming a non-turbulent flow of water, the relationships between flow rates, flow

coefficients, related installation factors, and pertinent service conditions for control valves handling incompressible fluids is provided below[6, 7].

$$C = \frac{Q}{(N_1 \times F_R)} \sqrt{\frac{\rho_1/\rho_0}{\triangle P}} \tag{2.12}$$

where C is flow coefficient, F_R is Reynolds number factor, $\rho_1/\rho_0 = 1.0$ is the relative density for water at $15C^{\circ}$, N_1 is a constant, Q is the volumetric flow rate of water, $\triangle P$ is the differential pressure between upstream and downstream pressure taps$(P_1 - P_2)$. The equation for the flow rate of a Newtonian liquid through a control valve when operating under non-turbulent flow conditions is derived for Reynolds number $< 10,000$.

Fail Safe Actions

Before describing the type of failures that are commonly associated with the control valves, it is important to mention here, what will happen after the failure occurred. There are tow main actions that the process control designer has to consider before ordering and configuring the control valve: a) Fail-Closed action wherein the valve closure member moves to a closed position when the actuating energy source fails (pneumatic, hydraulic , or electric energy source) .b) Fail-Open action wherein the valve closure member moves to an open position when the actuating energy source fails.

The process behavior at the valve position will certainly determine which action that is appropriate to apply. For example, the feedwater system inlet valve has to be in a fail closed condition when a failure happened at the valve. Because of the valve position at the inlet, it is safe to keep the valve closed in case of failure to prevent the feedwater tank from overflow. In this case a fail-closed action has to be applied[7].

Control Valve Faults

Valve stiction, cavitation, dead band, and backlash are the major valve problems that could degrade the process performance in exhibiting non-linearity of the process. Because valve stiction is a usual control valve problem and used to develop an oscillatory in process control,

one needs to explain it more. According to American National Standard Institute (ANSI) and International Society of Automation (ISA), the definition of valve stiction is the resistance to the start of motion, usually measured as the difference between the driving value required to overcome static friction up-scale and down-scale. The dead band express the behavior of the valve when it is not moving, even when the input to valve keeps changing[6, 7].

Actuator Faults

One of the frequent faults of valve actuator is the positioner overshoot. It is one control valve problem that is more common now than a decade ago. Positioners are fast feedback controllers that measure the valve stem position and manipulate the valve actuator until the desired valve position is achieved. Most positioners can be tuned. Some are tuned too aggressively for the valve they are controlling. This causes the valve to overshoot its target position after a change in controller output. Sometimes the positioner is simply defective in a way that causes overshoot. If the process controller is also tuned aggressively, the combination with positioner overshoot can cause severe oscillations in the control loop. Another problem that associated with valve actuators is the actuator nonlinearity[15].

A valve with a nonlinear flow characteristic can also lead to tuning problems. A control valves flow characteristic is the relationship between the valve position and the flow rate through the valve under normal service conditions. Ideally the flow characteristic should be linear. With a nonlinear characteristic, one can have optimal controller response only at one operating point. The loop could become quite unstable or sluggish as the valve position moves away from this operating point.

2.3.2 Level Sensor

Liquid level measurements can be made using a differential pressure type transmitter or gauge pressure type transmitter. Typically, this is determined based upon whether the tank is open to the atmosphere or whether it is closed. A closed tank application is where the tank or vessel is sealed from the atmosphere. As process fluid filled or is emptied from the tank, the pressure inside the tank may go from positive to vacuum. This change in internal

tank pressure has a direct effect on measured fluid level, unless it is compensated for. Piping the low side of a differential pressure transmitter to the top of the tank does this[4]. Pressure transmitters can be used to measure the pressure of steam, gases and liquids in industrial plants. However, they are more commonly used to measure the flow rate of steam, gases or liquids, or the level of liquids in tanks. Robust and well-known, pressure transmitters (known as hydrostatic devices when measuring liquid level) are the most common measuring device for liquid level in a tank. The theory can be explained as follows[15]:

$$P = \rho \times g \times h \tag{2.13}$$

where P is the pressure exerted by a liquid column, ρ is the density of the liquid, g is the gravity, and h is hight of the liquid column. A simple level equation for feedwater system could be simplified in the following equation.

$$h = P/s.g \tag{2.14}$$

where $s.g$ is the specific gravity.

2.3.3 Feedwater Pumps

Feedwater pump functions as a mechanical device used to pump water from a storage tank into a boiler. The water supplied by the feedwater pump is needed to replenish the boiler water lost during normal operation. Used on most systems, the boiler feedwater pumps make use of a boiler to supply hot water for heating or steam to drive steam turbine. Typically, these feedwater systems operate automatically using sensors in the boiler and in the storage tank to switch the pump on when the water level reaches a pre-determined point and switching the second pump to avoid tank overflow. The pumps used on the systems are usually centrifugal types operated by electric or steam-driven motors. The duty pump should in charge for maintaining the tank level as well as the boiler need. The standby pump is to be started when the tank level reaches a very high level to drain the tank. In this case, a special control design is required to convert the water flow that is over the need of the boiler consumption[15].

Summary

The main function of the feedwater system is to supply high-pressure water to the boiler during startup, normal, and emergency operations. Fault tolerant controller works in such a way to compensate for faults so they do not lead to system failure by utilizing component redundancy. Limit-checking method can be applied for monitoring the process variables, which works well if the process operates approximately in a steady-state. The controller redesign means how to change the control structure after the fault has occurred in the process.

Chapter 3

The Fault Tolerant Control

3.1 Introduction

Dynamical system can be modelled based on system architecture or system behavior[12]. Designing fault tolerant control for dynamic systems has to be based on models. These models describe the normal system operation as well as the faulty operation. Dynamic system is defined as a set of interconnected components that must be designed to achieve some desirable functions. The output of the dynamic system allows the design engineer to configure system components. Specifically, if the design engineer is equipped with pressure set point, level, temperature parameters, this will allow the design engineer to configure the feed water system components. Some functions exploit physical principles, which are expressed by a relationships of constraints and time evolution of variable (Trajectory). The notions of these functions can be illustrated by taking a feedwater system as an example, which is explained in section 3.2 for dynamical system [12].

Many dynamical systems are very complex and nonlinear. linearization is used to describe nonlinear system around operating points. Differential equations are used to describe nonlinear system dynamics[5]:

$$x(t) = f(x(t), u(t)) \tag{3.1}$$

$$y(t) = h(x(t), u(t)) \tag{3.2}$$

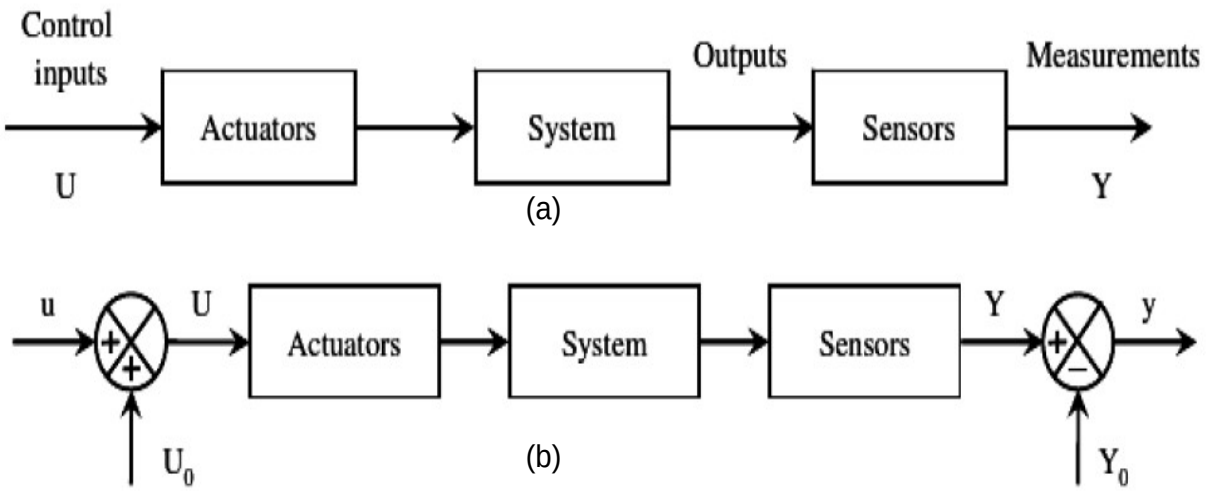

Figure 3.1: Dynamic system representation:(a) All operating zones;(b)Operating points (U_0, Y_0)

Or in recursive equation for discrete time domain:

$$x(k+1) = f(x(k), u(k)), y(k) = h(x(k), u(k)) \tag{3.3}$$

where x is the state vector, u is the control input vector, and y is the system output vector. f and h are nonlinear functions. A specific operating point has to be chosen in order to describe the relationship between the variations of system inputs and the variation of the system outputs of a dynamic system at this operating point. If the system of Fig. 3.1 is considered as a dynamic system with its actuators and sensors, with a range of its operating points of its inputs U and measurements Y, one can linearized it around an operating point (U_0, Y_0) such that, the relationship between the variation of system inputs u and output y can be described as:

$$u = U - U_0 \tag{3.4}$$

$$y = Y - Y_0 \tag{3.5}$$

Many real systems in industry can work in a nonlinear domain. Their equation can be

described by:

$$\begin{aligned} \dot{x}(t) &= f(x(t)) + \sum_{j=1}^{m}(g_i(x(t))u_j(t)) \\ &= f(x(t)) + G(x(t))u(t) \\ y_i(t) &= h_i(x(t)) \quad 1 <= i <= q \end{aligned} \tag{3.6}$$

$f(x)$ and $g_i(x)$ can be represented in the form of $n-$dimensional matrix of real-valued functions of the real-variables $x_1, x_2, ..., x_n$:

$$f(x) = \begin{vmatrix} f_{1j}(x_1, ..., x_n) \\ f_{2j}(x_1, ..., x_n) \\ \vdots \\ \vdots \\ f_{nj}(x_1, ..., x_n) \end{vmatrix}$$

$$g(x) = \begin{vmatrix} g_{1j}(x_1, ..., x_n) \\ g_{2j}(x_1, ..., x_n) \\ \vdots \\ \vdots \\ g_{nj}(x_1, ..., x_n) \end{vmatrix} \tag{3.7}$$

Functions $h_1, ..., h_q$ which characterize the output equation of the system my be represented in the form:

$$h_i(x) = h_i(x_1, ..., x_n) \tag{3.8}$$

And the corresponding discrete time representation is:

$$\begin{aligned} x(k+1) &= f_d(x(k)) + \sum_{j=1}^{m}(g_{di}(x(k))u_j(k)) \\ &= f_d(x(k)) + G_d(x(k))u(k) \\ y(k) &= h_d(x(k)) \end{aligned} \tag{3.9}$$

3.2 Feedwater System Model

The function of the Feedwater System is to supply high-pressure water to the boiler during startup, normal, and emergency operations. The system automatically maintains the proper flow to the boiler and water level in the feedwater tank. The system is shown in Fig. 2.1. The feedwater system spans from the deaerator (Feedwater tank) through to the boiler and

is used to provide feedwater to the boiler to match the steam flow demand. The major control components involved with the feedwater system include the boiler feed pump, the boiler feedwater regulator, and the boiler feedwater recirculation valve. The water flow into the tank is controlled by the valve. The valve control input signal is a current signal in mA which is converted into a pressure signal using I/P converter. This I/P is called the positioner in pneumatic control valves. The pressure signal is applied to the control valve actuator to change valve position toward valve opening or closing depending on the tank level as well as the outflow of the feedwater pumps. Thus, it dictates the amount of flow passing into the tank. The tank height is measured by the level sensor or transducer incase of using a pressure sensor to measure the level which produces an output in mA.

Modeling of the feedwater required determination of the relation between the input and output signals. Basically by determining the relation between the input flow, the output flow, and the water tank level. If $q_i(t)$ represents the input flow, $q_o(t)$ represents the outflow, the height is $h(t)$, and a constant cross sectional tank area A one can have these relations[1]:

$$\frac{\mathrm{dh(t)A}}{\mathrm{dt}} = q_i(t) - q_o(t) \tag{3.10}$$

assuming a constant outflow rate, the outflow is proportional to water hight in the tank

$$q_o(t) = h(t)/R \tag{3.11}$$

then,

$$A\frac{\mathrm{dh}}{\mathrm{dt}} = q_i(t) - q_o(t) = q_i(t) - h(t)/R \tag{3.12}$$

$$RA\frac{\mathrm{dh}}{\mathrm{dt}} + h(t) = Rq_i(t) \tag{3.13}$$

where R represents a parameter due to pipe restrictions.

3.3 FTC for The feedwater System

When it comes to engineering control systems for fault conditions, there many types of redundancies: cold, warm and hot. The use of each depends on the criticality of the process

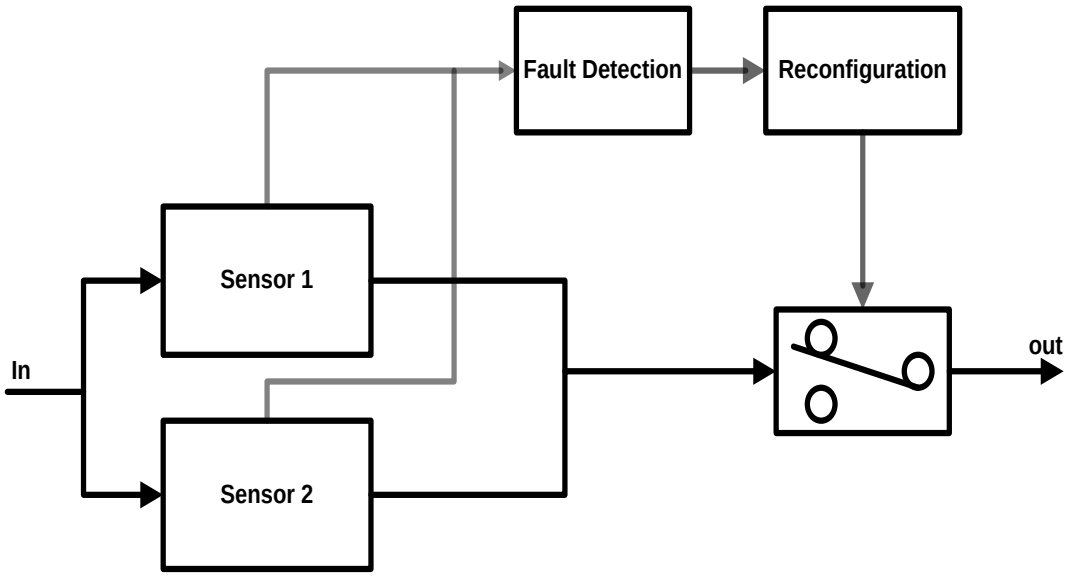

Figure 3.2: Dynamic redundancy for the sensor level

and the consequences of equipment failures. And failures are inevitable. Some processes require less intervention (cold redundancy such as a pump failure) while some cannot tolerate any failures or delays (hot redundancy for example communication systems processor failures). Some are in the middle where automatic action is necessary but the response time is not critical such as the control valve failure.

Redundancy in engineering systems is about providing reliability and a process alternative to a failing condition. For such reasons, a fault tolerant control method uses redundancy in system modules is a good choice. In the case of feedwater system, another valve is used as a redundant, as well as another sensor and transmitter are also duplicated. For feedwater pumps, a third pump is required to fulfill the modular redundancy and acting as a cold standby[1]. All the redundant modules are connected in parallel to the existed one. The redundancy of the level sensor and the control valve is depicted in Fig. 3.2 and Fig. 3.3 respectively. Static redundancy normally uses voters such as 1oo2 (One out of Two) and

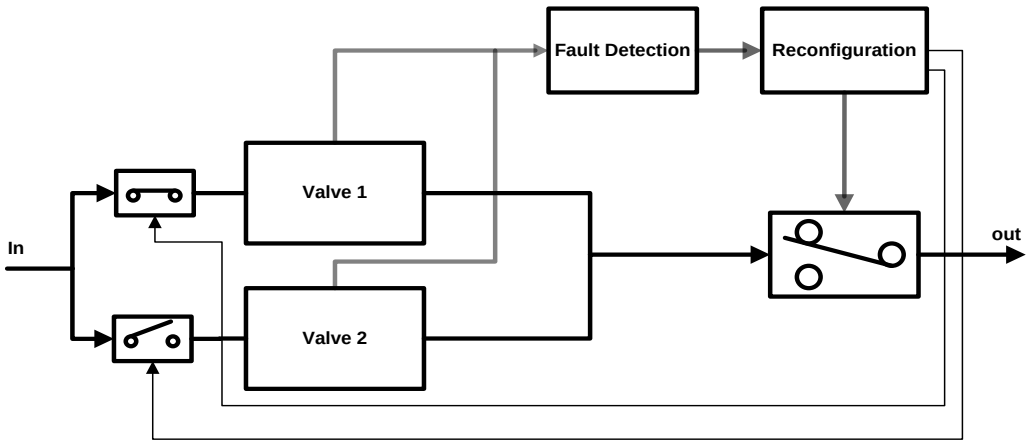

Figure 3.3: Dynamic redundancy for the control valve

2oo3 (Two out of Three), but in our case a dynamic redundancy is used, which needs a fewer modules at the cost of more information processing. In case of two modular, one is usually in operation mode, and if it fails, the standby or backup unit takes over. A modular can be represented by a valve, instrument or a pump. This action is performed by the fault tolerant controller. In the sensor case, the standby module will stay in operation, but for the valve case, the standby module will be in cold standby due to mechanical movement of the valve[1]. The standby module that is kept in operation is called the hot standby while the standby module that is not in operation during the normal situation is called cold standby. The redundancy of the sensor level and the redundancy of the control valve are combined together with the process plant in Fig. 3.4.

Fault tolerant controller is designed also to take care of pumps faults. For the feedwater system, tow pumps are designed to handle the process operation. A third one is needed to act as a cold standby pump. Fig. 3.5, is the representation of the pumps operation cases. In each case there is two possible ways to configure the selected pump. When the level reach it's high point, there is only one pump that has to be in duty and according to the

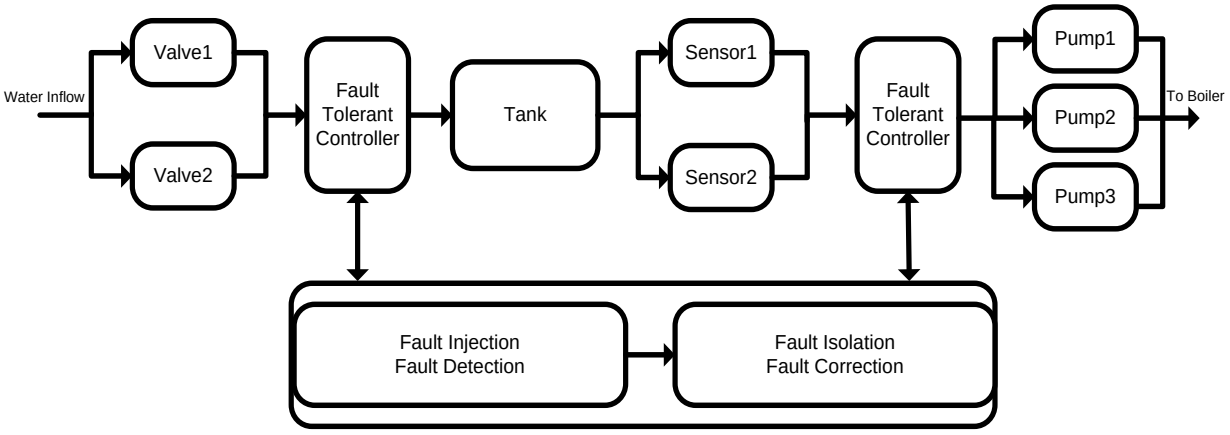

Figure 3.4: Fault tolerant controller with redundant system components.

status of the other pumps which is chosen by the operator, one has to be in hot standby and the other in cold standby. Fig. 3.5 represents a case of pump1 in duty by default. If one needed to have other feedwater pumps to work as a duty pumps, the selection has to be redesign for the desirable pump[1]. The overall physical system design or the flow diagram is depicted Fig. 3.6. The system consist of two level sensors at the tank wall that are connected to the plant controller via $4-20mA$ signals as well as connected to an indicator for local observation. The main controller is connected to the I/P converter via also a $4-20mA$ signal. The pneumatic signal is supplied to the valve actuators after conversion to move the valve position according to the desired value. Another signal from the main controller to start and stop the feedwater pumps. A human machine interface (HMI) is connected to the main controller for operator access in order to provide smooth and continuous monitoring for the process[1].

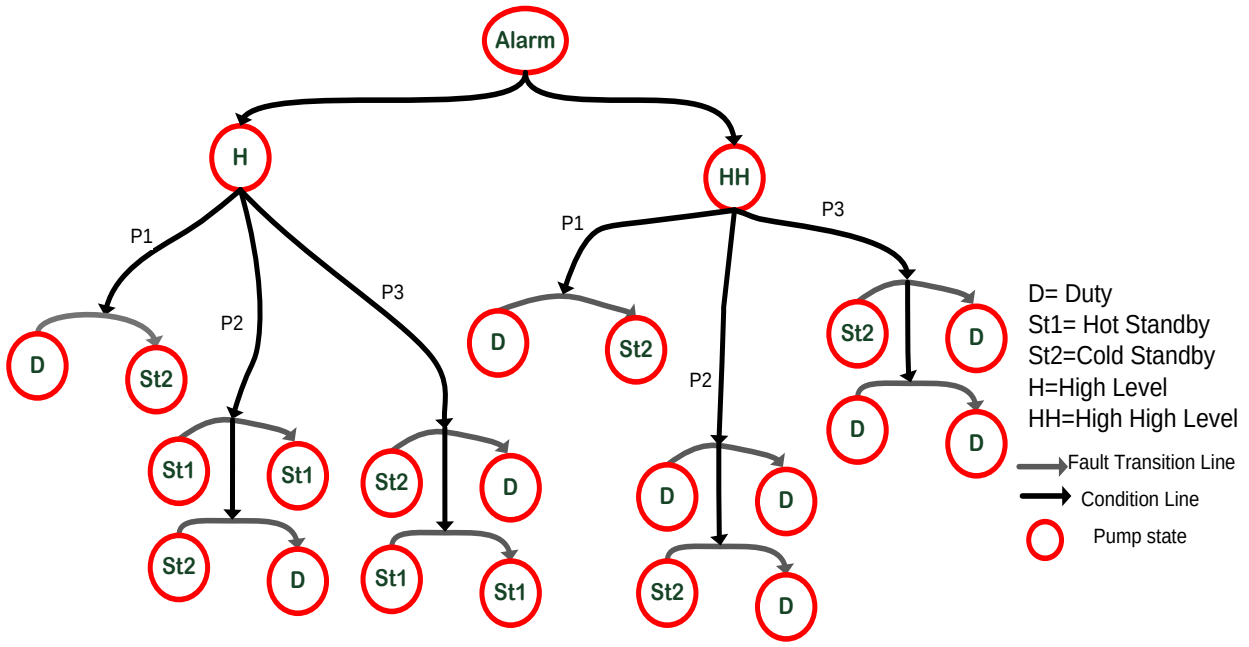

Figure 3.5: Pumps selection and transition states at fault of duty pump1

3.4 Results

The first simulation of feedwater system is designated to run for the normal operation, where there is no faults nor disturbance is occurred. This step will allow us to understand how the feedwater system works. The set point is changed at 100s from the high level case which is set at 60-85% to the high high level which is set at 85%. Then the PID controller will follow the change of the set point, allowing the tank level to raise by opening the inlet flow valve. At the same time the controller will start the standby pump in order to protect the tank from the overflow. Fig. 3.7, Fig. 3.8, and Fig. 3.9 show the normal operation of the sensor, the inlet control valve, and the pump respectively.

3.4.1 Sensors Fault

At the 150s on the simulation time, a fault is injected to the sensor circuit, and at 150.5s the second sensor that works as hot standby takes over and handles the level measurement.

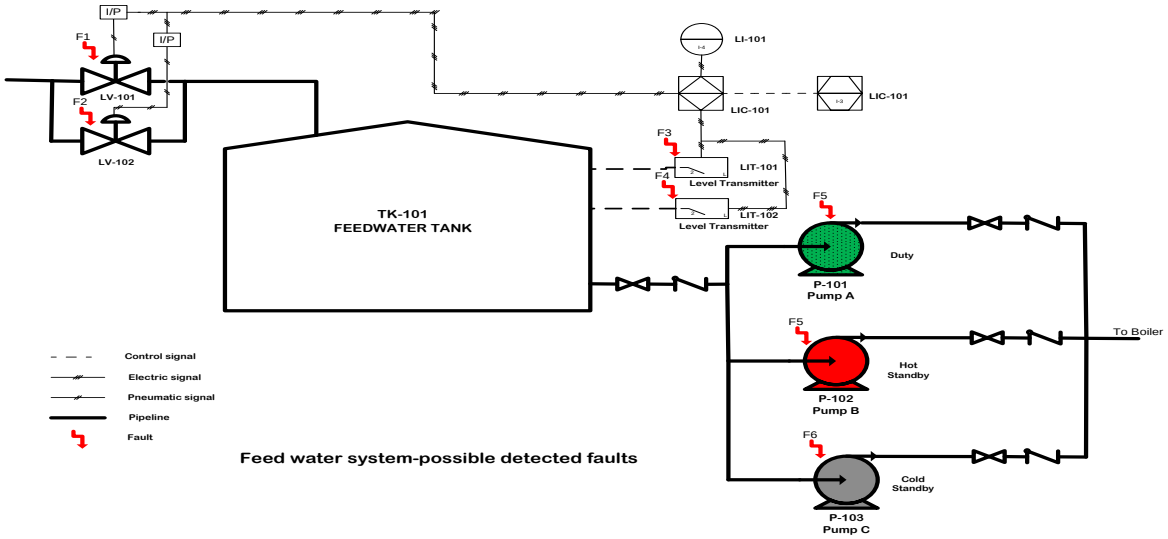

Figure 3.6: Feedwater systems with redundant components

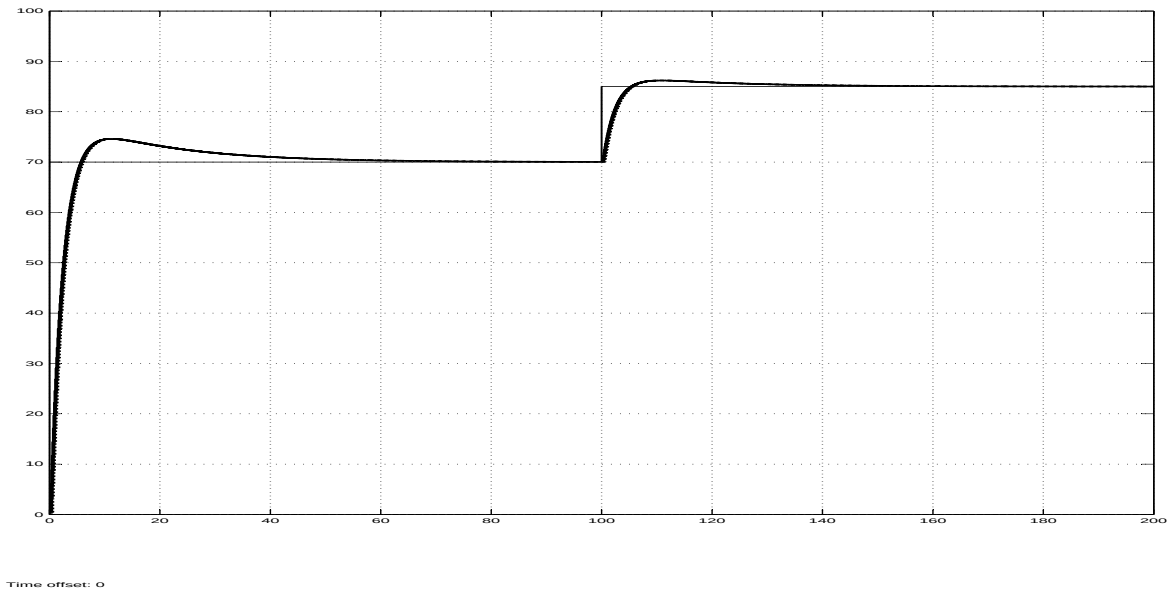

Figure 3.7: Normal operation of level sensor .

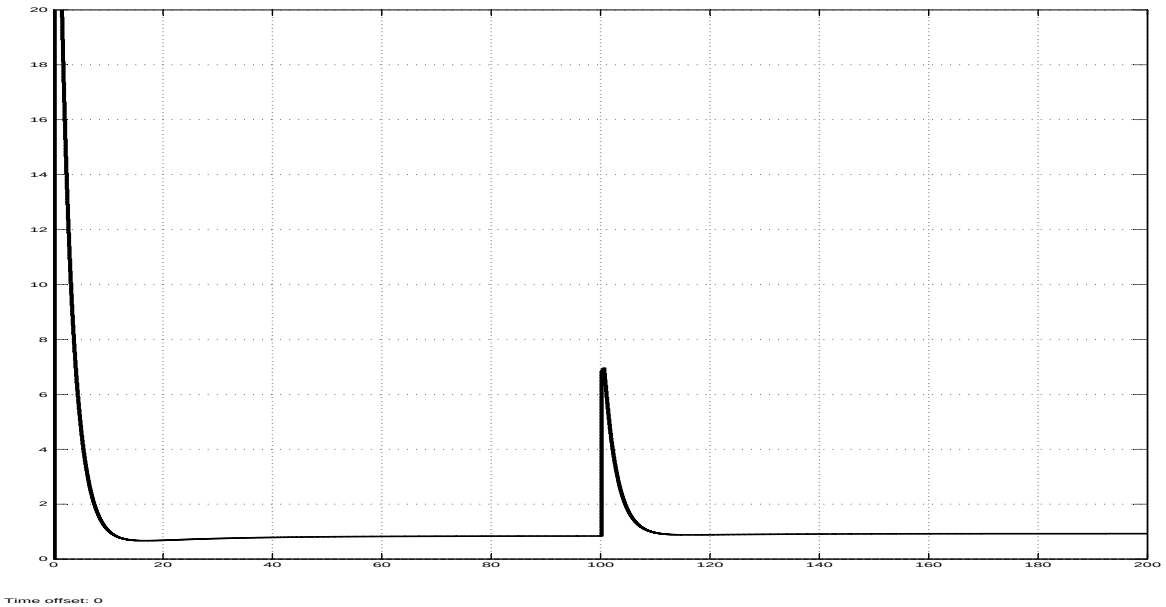

Figure 3.8: In-flow of feedwater tank under normal operation

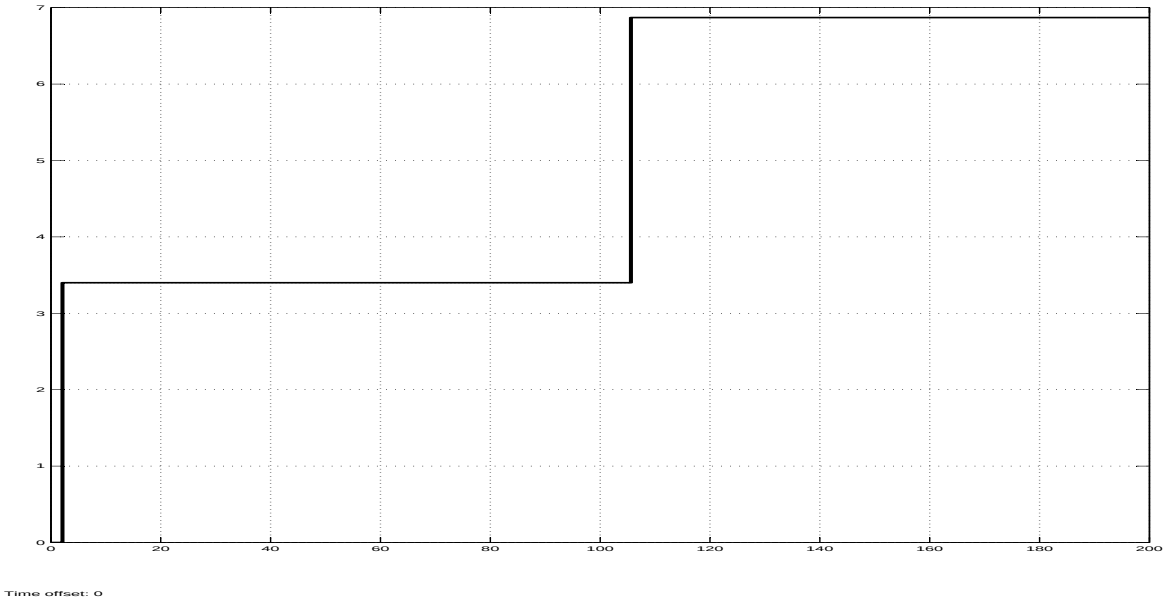

Figure 3.9: Normal pump operation of feedwater system

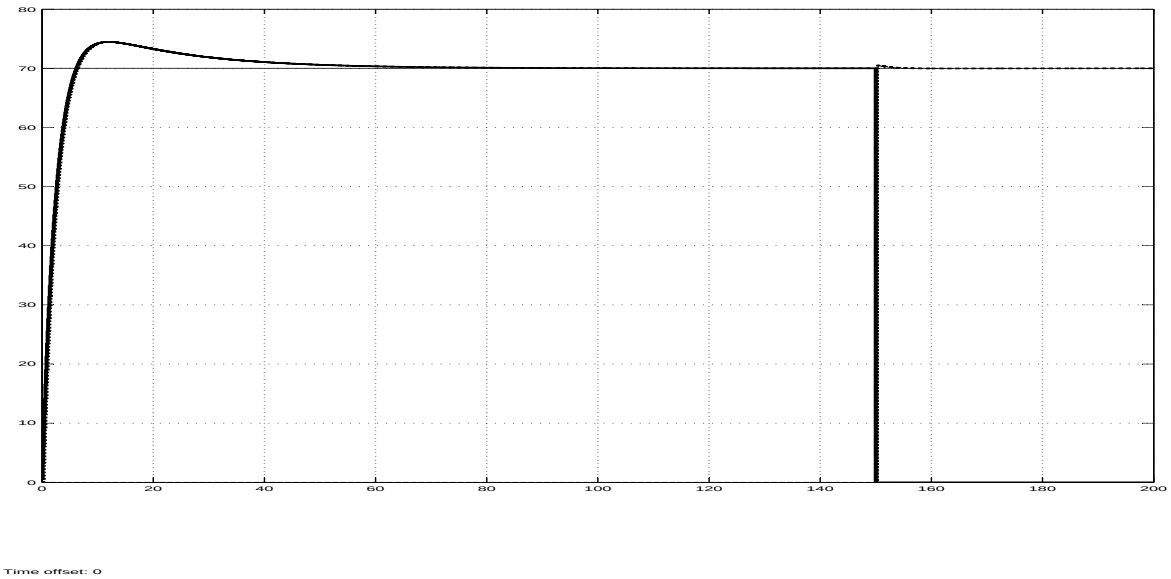

Figure 3.10: FTC take action at sensor fault.

This is depicted Fig. 3.10, and for magnified in Fig. 3.11. The fault is simulated by step change in the level from high high level to zero level, then a limit-check detecting method is used to identify the sensor fault.please see A. In reality, sensors design could be the same in a manufacturing point of view, but due to accuracy tolerance, their readings are slightly different. Taking that into account, simulation circuit is designed to represent this difference. Recently developed differential pressure transmitters have a higher accuracy and a complicated structure design, hence their maintenance is more complex than the other regular transmitter like radar or ultrasonic transmitters. The fault tolerant controller will increase the process availability by neglecting the repair time for components.

3.4.2 Control Valve Fault

Control valves are usually vulnerable to mechanical stiction due to their frequent movement parts. Setting the control in cold standby mode will reduce the valve stiction, but it has to be maintain regularly to assure continuous availably of the valve. In this simulation, a

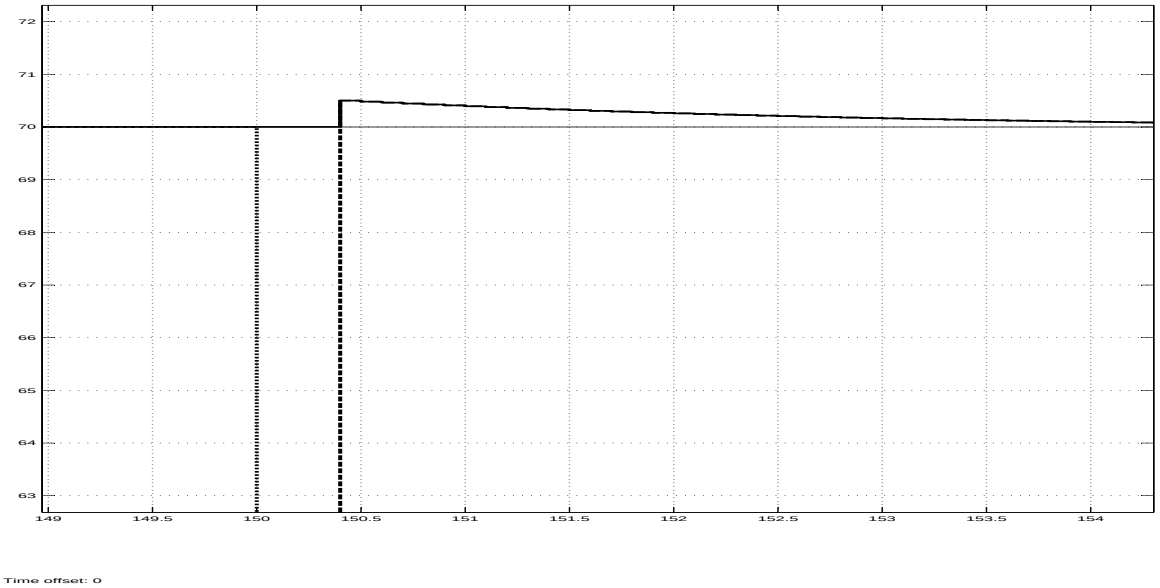

Figure 3.11: FTC take action at sensor fault. Magnified

fault injector is built to simulate the valve fault at 250s from the simulation run time, then fault identification is obtained by limit-check method. Controller reconfiguration is designed to switch from the duty faulty valve to the one in the cold standby. It is noticed that the nonlinearity of the control valve is very noticeable, and is illustrated in Fig. 3.12 and Fig. 3.13

3.4.3 Feedwater Pumps fault

The sequence of operation of the feedwater system usually consists of setting one of the pump to work in duty mode when the level is reach to high. (See Fig 3.5). The high level is set by the tank specification and the need of water supply. The second will be in a hot standby, waiting for the level to raise to a high high level. The high high level usually is set to be higher than the high level in order to prevent the feedwater tank from overflow. Fault tolerant controller uses a third pump to work as a cold standby. In case of, there is only one pump in duty, which means the tank level is high, thus the cold standby will be in charge to

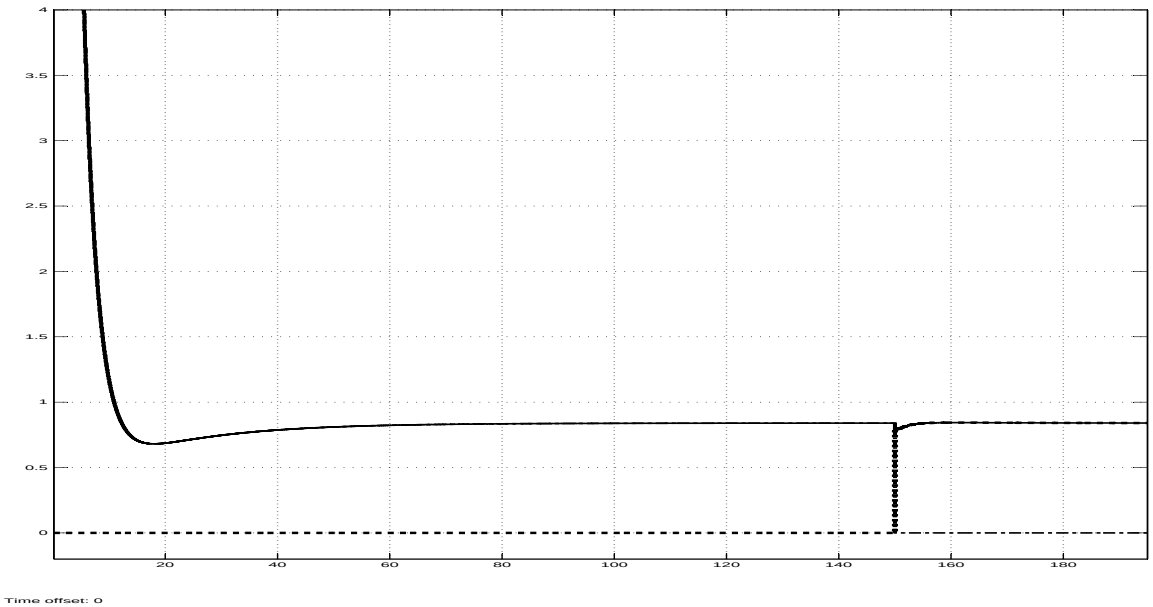

Figure 3.12: Control valve take-over when duty valve is faulty.

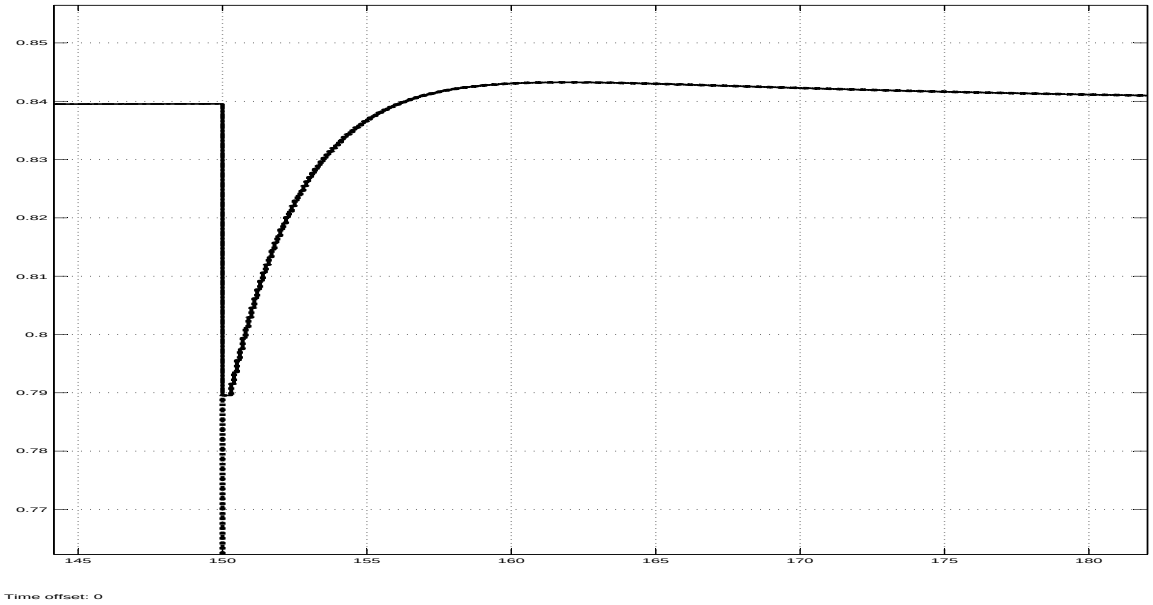

Figure 3.13: Control valve take-over when duty valve is faulty. Magnified

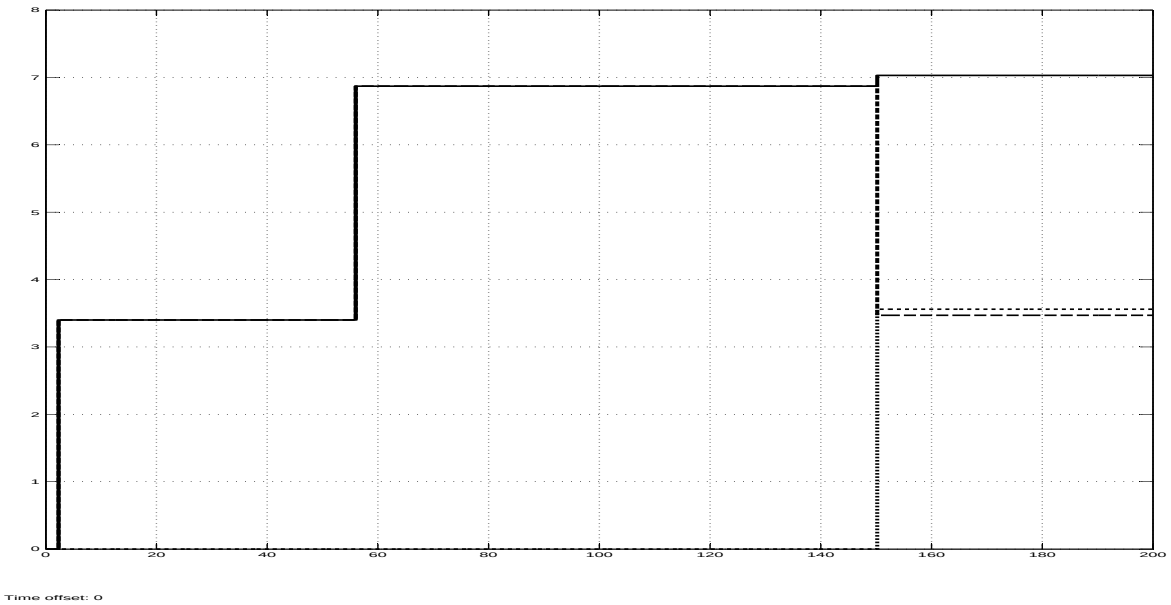

Figure 3.14: Pump1 switching-over using FTC.

replace the duty pump incase of pump fault. For the high high level, where both the duty and the hot standby pumps are in operation, the cold standby will switch over and handle the out put flow incase any of the operating pumps getting faulty.

Operator has to decide first before running the controller which pump has to be in duty, hot standby, or clod standby according to the pumps availability. In this simulation, a constant pump flow is assumed and small different between pumps flow is considered for illustration purpose.Fig. 3.14 shows pump 1 fault at 150s of the simulation run time. Pump 1 was in duty when the fault occurred, hence pump 3 is taking over as it was previously set by the operator in a cold standby. The level was at high high when the fault injected, so the total output flow before the fault is the sum of pump1 and pump2 output flow. After the fault, the total sum of the outflow is produced from pump2 and pump3.

For clear understanding, the same procedure of injecting the fault and detecting it is repeated for pump2 and pump3 when both are working as a duty pumps in two different scenarios.Fig. 3.15 and Fig. 3.16 showed the two scenarios of pump2 and pump3 respectively.

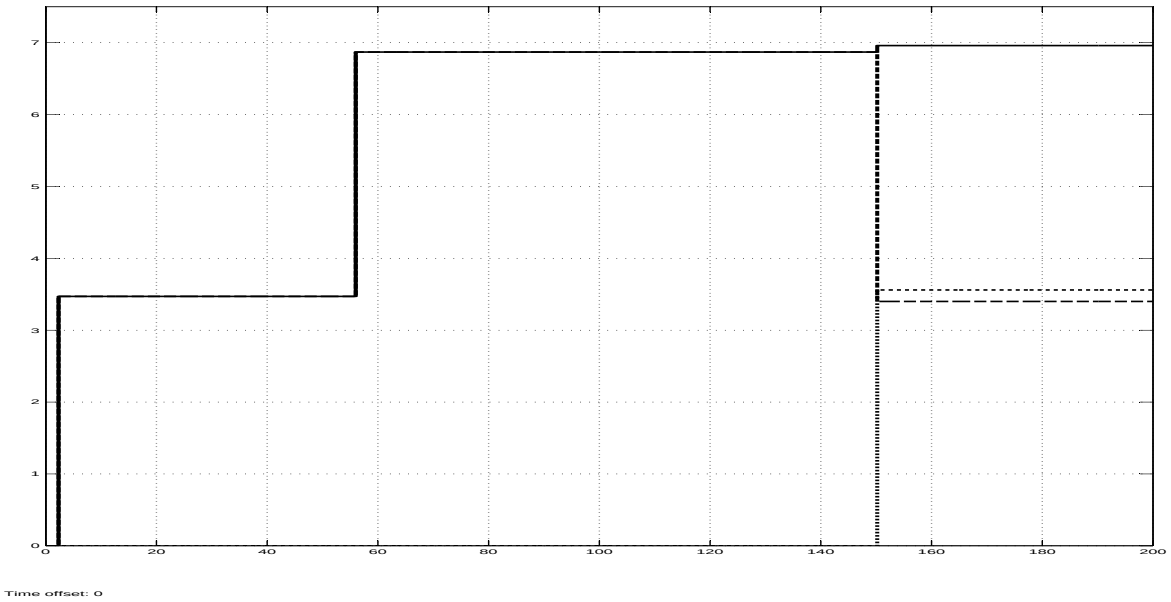

Figure 3.15: Pump2 switching-over using FTC.

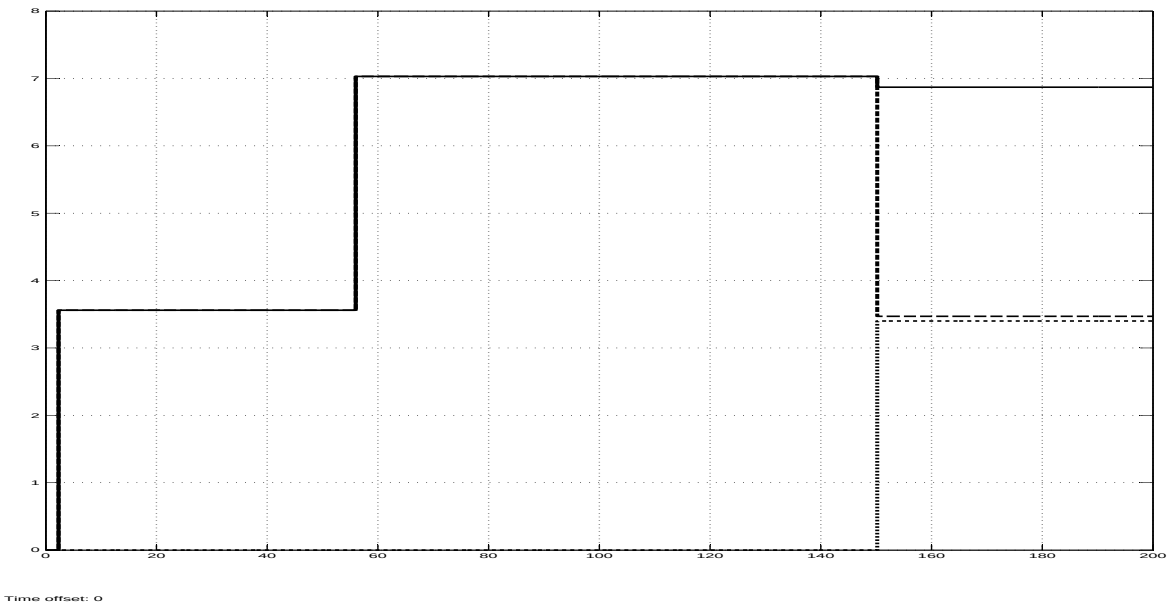

Figure 3.16: Pump3 switching-over using FTC.

Summary

Fault tolerant control for dynamic systems usually designed based on models. These models describe the normal system operation as well as the faulty operation. Modeling the feedwater systems requires a determination of the relationship between the input and output signals, by determining the relations between the input flow, the output flow, and the water tank level. linearization is used to describe nonlinear system around operating points. Redundancy for feedwater system is to provide reliability and a process alternative to a failing condition. For such reasons, so another valve is used as a redundant, as well as another sensor and transmitter are also duplicated. For feedwater pumps, a third pump is required to fulfill the modular redundancy and acting as a cold standby.

Chapter 4

Conclusion

A PID controller is developed in this project to control the level of the feedwater tank using Matlab Simulink. Then two components of each sensor and control valve are designed. The sequence of operation for pump logic is configured based on the pump selection that is discussed earlier in previous chapter. An option of selecting the duty pump as well as the duty control valve to the plant operator is set to provide flexible operation. The flexible operation will help the operator as well as the maintenance crew to identify the faulty equipment and corrected it. Fault simulation is injected in each component, and at specific time of the simulation run time, the fault tolerant controller action is observed and depicted for the illustration purpose.

The simulation on Matlab-simulink for the feedwater system model is designated to run for the normal operation first to understand how faultless systems works, where there is no faults nor disturbance is occurred. The set point is changed from the high level case to the high high level. Then the PID controller will follow the change of the set point, allowing the tank level to raise by opening the inlet flow valve. At the same time the controller will start the standby pump in order to protect the tank from the overflow.

At the next simulation step, a fault is injected to simulate the sensor failure, and at the fault time, the limit-checking model-based is used to detect the sensor fault. Once the controller sense the fault, action must be taken to isolate the faulty sensor and at the same time utilizing the backup sensor (usually called hot standby as it's state is an online backup)

the second sensor that works as hot standby takes over and handles the level measurement. The fault is simulated by step change in the level from high high level to zero level (please see appendix A).

Control valve fault simulation is carried out in the same way that, the sensor fault simulation is configured. Redundant control valve is put in an off-line mode as it has a moving parts, which can increase the probability of valve failures, such as valve stiction, backlash, and cavitation. Setting the control in cold standby (off-line) mode will reduce the valve stiction, but it has to be maintain regularly to assure continuous availably of the valve. In this simulation, a fault injector is built to simulate the valve fault at a certain simulation run time, then fault identification is obtained by limit-check method. Controller reconfiguration is designed to switch from the duty faulty valve to the one in the cold standby. It is noticed that the nonlinearity of the control valve is very noticeable due to the valve sizing characteristics.

In this feedwater system, only one pump is configured to work in duty mode when the level is reached to high. The tank high level point for pump operation is set by the tank specification and the need of water supply. The second pump is configured in a hot standby mode, so it must be activated at a high high level. The high high level usually is set to be higher than the high level in order to prevent the feedwater tank from overflow. Fault tolerant controller uses a third pump to work as a cold standby. In case of, there is only one pump in duty, which means the tank level is high, thus the cold standby will be in charge to replace the duty pump incase of pump fault. For the high high level, where both the duty and the hot standby pumps are in operation, the cold standby will switch over and handle the out put flow incase any of the operating pumps getting faulty.

It is very important to have a decision of the selecting the duty pump, hot standby pump, and cold standby pump, by the control room operator in order to start the pumps sequence of operation. A correspondence between the maintenance personnel and the operation personnel should establish the control strategies of the pumps. Start-up and shutdown procedures of the feedwater pumps has to be taken into account, to allow smooth running of the pumps

sequence of operation. For instance, a standby pumps will need amount of time to build the pressure at their head section when they started. In our simulation, these procedures are not considered, as they mainly depends on the pump manufacturer's specifications.

Faults are simulated for each pump when it is running. Once the controller has discovered the faulty one, the standby pump will be put on operation. As mentioned before, there is always a backup pump to handle the process operation in all mode of level (High or high high) to ensure a continuous operation.

4.1 Future Work

When developing a fault tolerant control, there are many methods to archive higher performance of fault detection and identification techniques. For instance, using a parity equation check model-based method can provide accurate results. The assumption of constant flow rate for feedwater tank outlet valves is consider to be constant. This assumption requires a fixed speed pump only to handle the outflow, which consumes more energy. The future work can consider a variable speed drive to operate the feedwater pumps.

Fault tolerant controller can be built in a very large scale to accommodate all the process equipments that their hardware failure could deteriorate the plants operation. Starting with the electronics controller, where any fault occurred in it will have a major impact on the plant production . In general, understanding and implementing the right fault tolerant identification method as well as the right redundancy strategy will result in a reliable system when equipment fails. And everything will eventually fail.

Summary

The sequence of operation for the feedwater pumps is designed in such a way, to give the operator the privilege of configuring which pump has to be in duty, hot standby, or cold standby. The redundancy of control valves and level sensors are configured in away that will satisfy the operation of feedwater system and the controller redesign of the FTC. The simulation on Matlab-simulink for the feedwater system model is designated to run for many

operation stage to understand process under normal operation and under faulty equipments as well. Future work is suggested to consider other fault detection methods that can achieve high performance of FTC for the feedwater system.

Appendix A

The Matlab-simulink circuit diagrams of the feedwater system are depicted in this appendix. The main circuit diagram is shown in Fig. A.1. More details of the main circuit blocks in Fig. A.2 which is the control valve logic and Fig. A.3 for the fault tolerant control that is designed for the control valve. The sensor logic is configured in Fig. A.4. It is important to mentioned that all the blocks in these circuits are a Simulink library blocks, except the ones that are defined as a user function blocks, sensor, valve, and pumps. Fig. A.5 is a user function block designated to represent the feedwater tank. Fig. A.6 and Fig. A.7 are the circuits diagram for the pumps logics and the FTC for feedwater pumps respectively. The limit-checking model-based is designed in Fig. A.8.

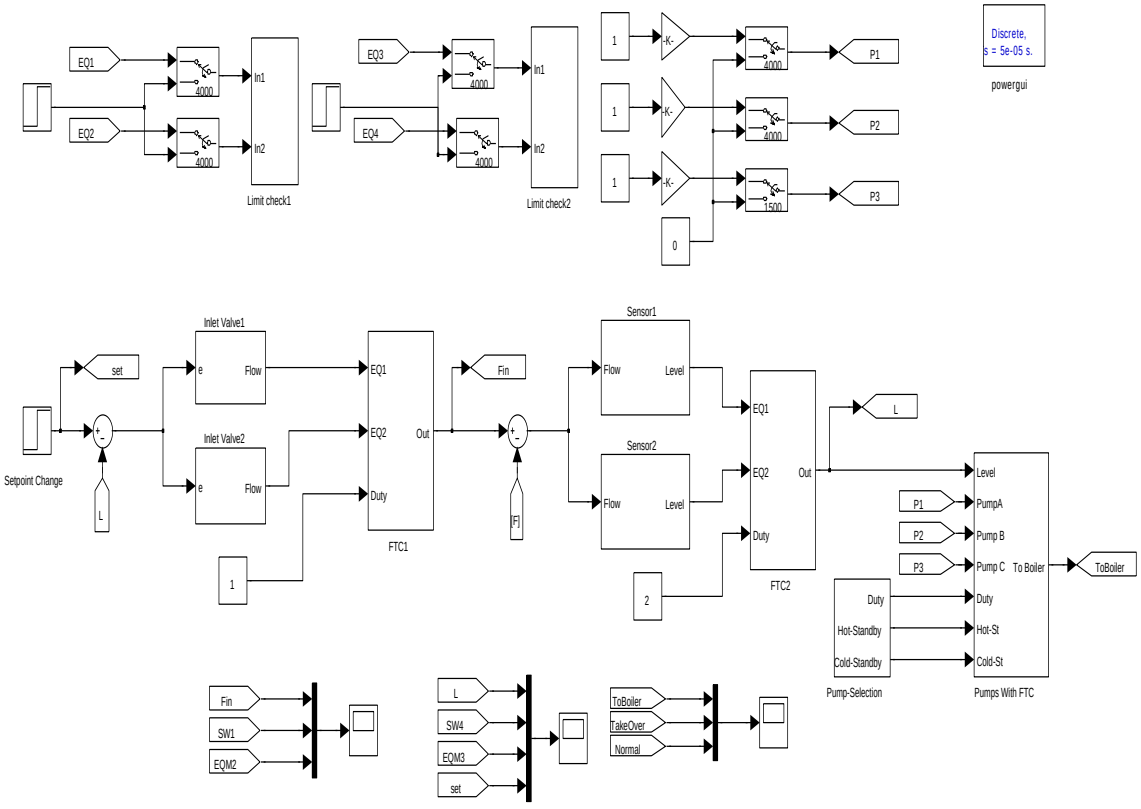

Figure A.1: Matlab Circuit Diagram for Feedwater System.

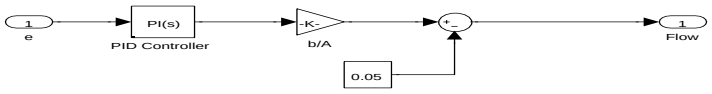

Figure A.2: Matlab Circuit Diagram for Control Valve.

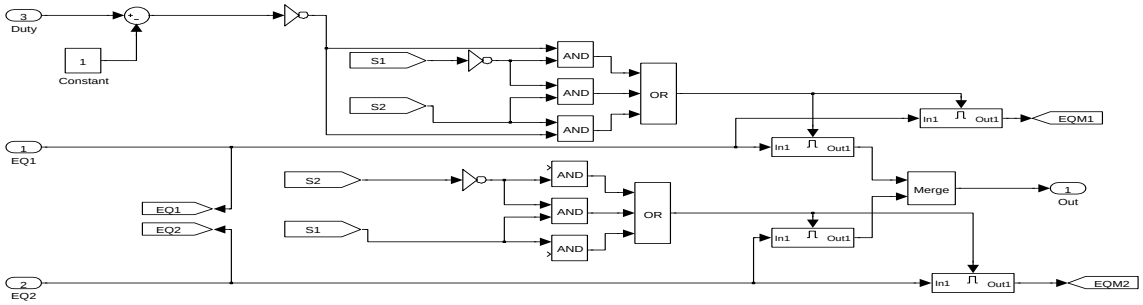

Figure A.3: Matlab Circuit Diagram for Valve FTC.

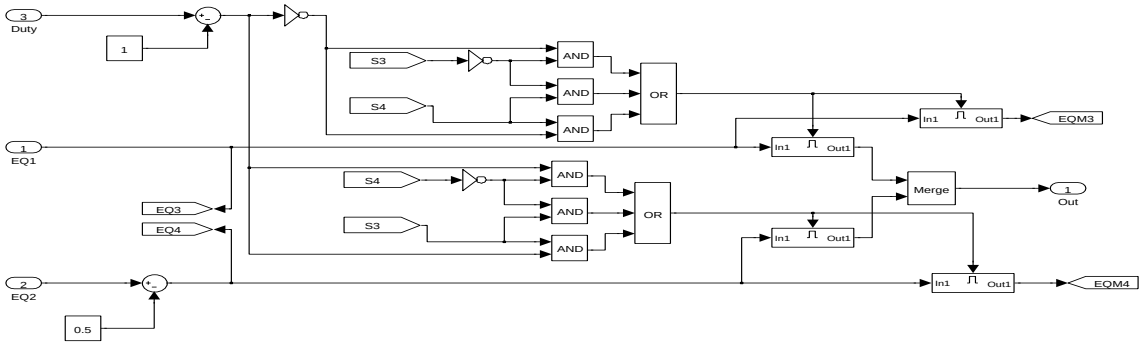

Figure A.4: Matlab Circuit Diagram for Level Sensor FTC.

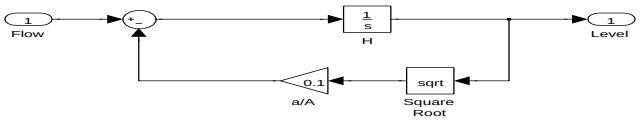

Figure A.5: Matlab Circuit Diagram for Feedwater Tank.

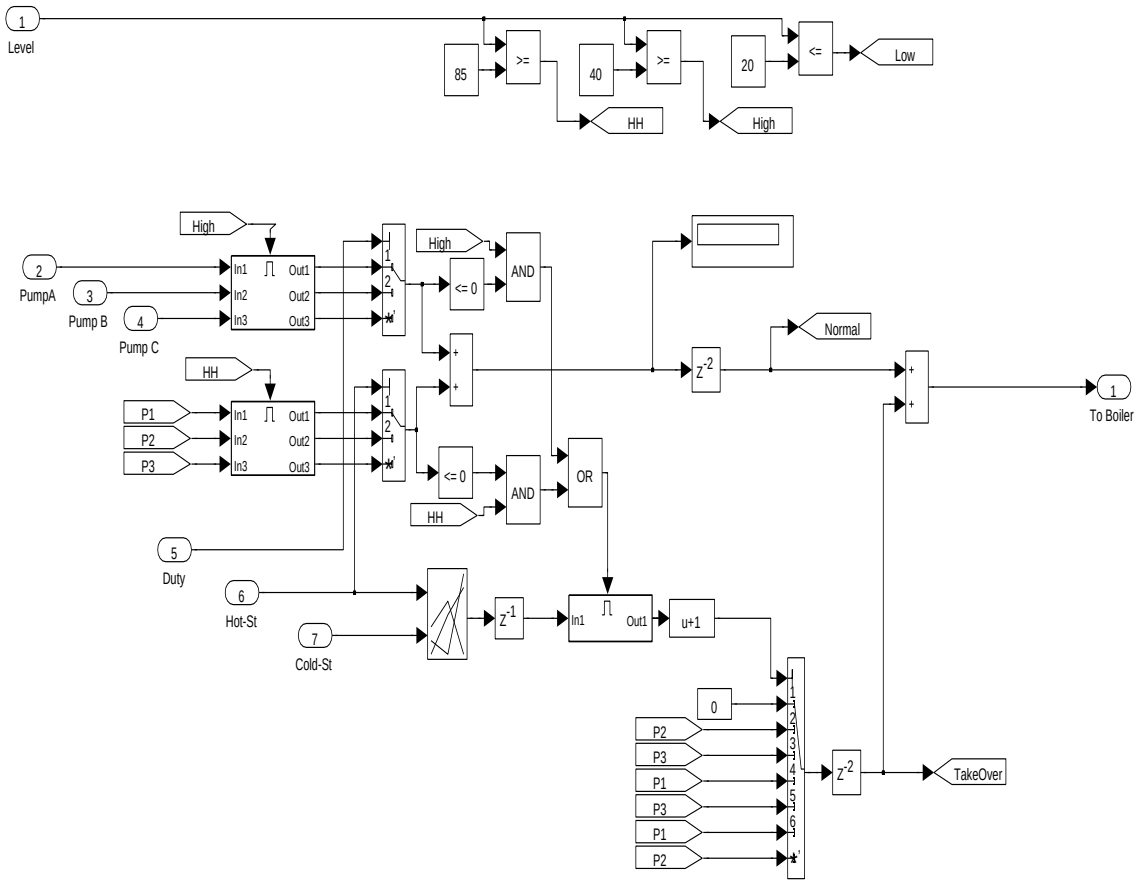

Figure A.6: Matlab Circuit Diagram for Feedwater Pumps.

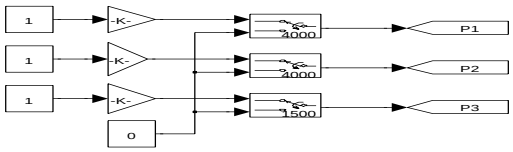

Figure A.7: Matlab Circuit Diagram for Pumps Logic with FTC.

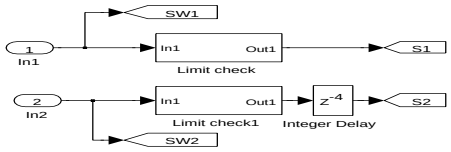

Figure A.8: Matlab Circuit Diagram for Fault Detection.

feedwater system parameters	
Hight of tank	4 m
Maximum fill level	3.5 m
Radius of tank	2 m
Tank volume	37.68 m^3
Process valve position	3.5-4 m
Proportional gain Kp	1.59934
Integral gain Ki	0.079967
Inflow rate constant	1
Outflow rate constant	0.4
Specification	
Pressure Output signals	4 to 20 mA
Span limit (max)	130 kPa
Range limit	-100 to 130 kPa
Control signal inputOutput	4 to 20 mA
Pump1 constant flow rate	3.40
Pump2 constant flow rate	3.47
Pump3 constant flow rate	3.56

Bibliography

[1] L. H. Chiang, E. L. Russell, R. D. Braatz, *Fault Detection and Diagnosis in Industerial Systems*, Advaned textbooks in control and signal processing , Springer 2001

[2] Sojoudi, S.; Lavaei, J.; Murray, R.M., "Fault-tolerant controller design with applications in power systems and synthetic biology,"*American Control Conference (ACC)*, 2011 , vol., no., pp.4135,4142, June 29 2011-July 1 2011

[3] S. Manz "Online Fault Detection and Diagnosis of Complex Systems based on Hybrid Component Models," *14 th International Congress on Condition Monitoring and Diagnostic Engineering Management,*,pages 0-8, COMADEM, Cambridge U.K., ISBN, 2001.

[4] Dengfeng Zhang; Zhiquan Wang; Shousong Hu, "Robust Satisfactory Fault-Tolerant Controller Design with Closed-Loop Poles and Variance Constraints," *Intelligent Control and Automation*, 2006. WCICA 2006. The Sixth World Congress on , vol.1, no., pp.1971,1975, 0-0 0

[5] Hassan Noura, Didier Theilliol, Jean-Christophe Ponsart, Abbas Chamseddine, *Fault-tolerant Control Systems,Design and Practical Applications*, Springer London, ISBN: 978-1-84882-653-3, 2009

[6] IEEE Recommended Practice-Adoption of IEC 61000-4-15:2010, Electromagnetic compatibility (EMC)–Testing and measurement techniques-Flickermeter-Functional and design specifications," *IEEE Std 1453-2011* , vol., no., pp.1,58, Oct. 21 2011

[7] Enterprise-Control System Integration, Part 5, "Business-to-Manufacturing Transactions",*ANSI/ISA-95.00.05-2007 CAP Learning*

[8] Zawawi, A.E.; El-Sayed, A., "Integration of DCS and ESD through an OPC application for upstream Oil and Gas," *Power and Energy Society General Meeting*, 2012 IEEE , vol., no., pp.1,5, 22-26 July 2012

[9] Stagg, T. A., "Digital implementation of a feedwater control system for a 500MW boiler," *Implementation Problems in Digital Control, IEE Colloquium on* , vol., no., pp.2/1,2/3, 9 May 1989

[10] Se-Jin Baik, "Main Steam and Feedwater System," *Primary Fluid System Engineering Dept. Korea Power Engineering Company Inc*

[11] Isermann, Rolf, "Fault-Diagnosis Systems : An Introduction from Fault Detection to Fault Tolerance," *Technical Report*, Springer, Pages: 477, 2006

[12] Blanke, Mogens Kinnaert, Michel Lunze, Jan, *Diagnosis and Fault-Tolerant Control.* ,Springer, Pages: 684, 2006.

[13] Hearns, G.; Grimble, M.J.; Johnson, M.A., "Integrated fault monitoring and reliable control," *Control '98. UKACC International Conference on (Conf. Publ. No. 455)* , vol., no., pp.1175,1179 vol.2, 1-4 Sep 1998

[14] Zezulka, F.; Bradac, Z.; Kucera, P., "Formal methods for higher reliability of the industrial automation," *Industrial Technology, 2003 IEEE International Conference on* , vol.2, no., pp.891,895 Vol.2, 10-12 Dec. 2003 ISBN 1-85233-327-8 ,Springer, 2001.

[15] Rolf Isermann, " Model-based fault-detection and diagnosis status and applications," *Annual Reviews in Control, Volume 29, Issue 1, 2005, Pages 71-85,*, ISSN 1367-5788, 10.1016/j.arcontrol.2004.12.002. 1989.

[16] H. Jamouli and D. Sauter, "A New Adaptive Kalman Estimator for Detection and Isolation of Multiple Faults Integrated in a Fault Tolerant Control," *Journal of Control Science and Engineering, vol. 2010, Article ID 497925, 11 pages,* 2010.

[17] ABB Manual, Engineered solutions for all applications,"Pressure Measurement Theory and Application Guide", *2600T Series Pressure transmitters*, Manual 3KXP000001R2901.2012

[18] Geurkov, V.L., "Diagnosis of microprocessor based measurement instruments, measuring parameters of passive complex quantities," *Instrumentation and Measurement Technology Conference, 1996. IMTC-96. Conference Proceedings. Quality Measurements: The Indispensable Bridge between Theory and Reality., IEEE* , vol.2, no., pp.792,796 vol.2, 1996

[19] Geurkov, V., "On the question of desired sensitivity assurance when testing linear systems by small number of test patterns," *Electrical and Computer Engineering, 2002. IEEE CCECE 2002.* Canadian Conference on , vol.1, no., pp.538,540 vol.1, 2002

[20] Grimble, Michael J. Johnson, Michael A. Choudhury, Shoukat M. A. A. ,*Diagnosis of Process Nonlinearities and Valve Stiction : Data Driven Approaches*, Pages: 289, Springer, Berlin/Heidelberg, DEU, 2008

[21] D. Steven, "Model-based fault diagnosis in dynamic systems using identification techniques, Silvio Simani, Cesare Fantuzzi and Ron J. Patton, Springer: London, 2003, 282pp. ISBN 1852336854," *International Journal of Robust and Nonlinear Control*, vol. 15, no. 11, 2005

[22] Poledna, Stefan, *Fault-Tolerant Real-Time Systems : The Problem of Replica Determinism*, Pages: 160, Springer, Boston, MA, USA, eISBN: 9780585295800, 1996

[23] El-Farra, N.H., "Integrating model-based fault detection and fault-tolerant control of distributed processes," *American Control Conference*, 2006 , vol., no., pp.6 pp.,, 14-16 June 2006

[24] Zhang Yongsheng; Ma Yunyi; Tang Ying, "Research on the condensation and feedwater control system for nuclear power plant," Computer Application and System Modeling (ICCASM), *International Conference on* , vol.3, no., pp.V3-63,V3-66, 22-24 Oct. 2010

[25] Holzenthal, L.L., Jr.; Masada, G.Y., "Utilization of a linearized model for the redesign of the feedwater control system of a drum boiler power plant," *Southeastcon '90. Proceedings., IEEE* , vol., no., pp.914,918 vol.3, 1-4 Apr 1990

[26] Broadwater, R.P., "A design approach for a power plant feedwater control system," *Control Systems Magazine, IEEE* , vol.3, no.1, pp.4,11, February 1983

[27] Chour, Q. B.; Acchione, P. N.; Kar, P. K., "Safety Considerations in the Design of a Unique Nuclear Steam Generator Feedwater Control System,"*American Control Conference,* 1985 , vol., no., pp.1451,1456, 19-21 June 1985

[28] Gee-Yong Park; Kee-Choon Kwon, "Application of On-Line Signal Recovery to Feedwater Control System," *SICE-ICASE, 2006. International Joint Conference* , vol., no., pp.1715,1718, 18-21 Oct. 2006

[29] Futao Zhao, Jing Ou, Wei Du, "Simulation modeling of nuclear steam generator water level process a case study" *, ISA Transactions*, Volume 39, Issue 2,Pages 143-151, April 2000