DYNAMIC FLOWGRAPH METHODOLOGY FOR RELIABILITY MODELLING OF NETWORKED CONTROL SYSTEMS

With Application to a Nuclear-Based Hydrogen Production Plant

by

Ahmad Wail Al-Dabbagh

A Thesis Submitted in Partial Fulfillment

of the Requirements for the Degree of

Master of Applied Science

in

The Faculty of Engineering and Applied Science

Electrical and Computer Engineering

University of Ontario Institute of Technology

December 2009

ABSTRACT

The use of communication networks in digital control systems introduces stability and reliability concerns. Standard reliability and safety assessment methods need further modification to accommodate the issue in the reliability assessment of networked control systems. In this thesis, it is demonstrated that the Dynamic Flowgraph Methodology (DFM) can be extended to model networked control systems. The modelling of the communication network influence on the performance of the control system is presented. The areas that can affect the reliability of the control system are identified using the methodology. The thesis also presents the application of the DFM to a nuclear-based thermochemical water splitting process for hydrogen production, the Copper-Chlorine (Cu-Cl) cycle. The architecture of a networked control system and configuration of instrumentation and control systems for the hydrogen production plant are proposed in the thesis.

Keywords: dynamic flowgraph methodology, networked control system, Cu-Cl cycle, instrumentation and control systems, communication network

DEDICATION

To my parents, Dr. Aala R. Ali and Dr. Wail Y. Al-Dabbagh. Your continuous encouragement and support help me succeed.

ACKNOWLEDGMENTS

I would like to thank and acknowledge those who made this work possible. Firstly, I would like to sincerely thank my supervisor and professor, Dr. Lixuan Lu for providing technical guidance throughout the course of my Master's program.

Also, I would like to thank my supervisory committee member, Dr. Mikael Eklund.

I am grateful to all my friends and colleagues at UOIT for providing an enjoyable learning environment.

TABLE OF CONTENTS

List of Figures.....viii

List of Tables.....xi

Chapter 1 Introduction

1.1 Objective of the Thesis.....1

1.2 Organization of the Thesis.....2

Chapter 2 Literature Review

2.1 Networked Control Systems.....3

2.1.1 Distribution of the Controllers.....5

2.1.2 Advantages of Networked and Distributed Control Systems.....6

2.1.3 Applications of Networked and Distributed Control Systems.....6

2.2 Reliability Assessment of Instrumentation and Control Systems.....9

2.2.1 Methods of Reliability Modelling and Assessment.....12

2.2.2 Requirements of Reliability Modelling.....12

2.2.3 Comparison of Modelling Methods.....14

2.2.4 Reliability of Networked Control Systems.....15

2.2.4.1 Reliability of Communication Networks.....17

2.2.4.2 Reliability of Communication Networks in Networked Control Systems.....18

2.2.5 Reliability Modelling of Networked Control Systems.....24

2.2.5.1 Previous Studies on Modelling of Networked Control Systems...24

2.2.5.2 Requirements for Reliability Modelling of Networked Control Systems.....27

2.3 The Dynamic Flowgraph Methodology.....28

2.3.1 Model Components.....29

2.3.2 Model Construction.....29

2.3.3 Model Analysis.....31

2.4 Chapter Summary.....33

Chapter 3 Dynamic Flowgraph Methodology for Modelling of Networked Control Systems

3.1 Modelling of Communication Network.....35

3.1.1 Preprocessing Time Component.....37

3.1.2 Waiting Time Component.....38

3.1.3 Transmission Time Component.....39

3.1.4 Postprocessing Time Component.....42

3.2 Networked Control System Example.....46

3.3 Model Analysis and Results.....58

3.4 Chapter Summary.....67

Chapter 4 Application of DFM to the Copper-Chlorine Thermochemical Cycle

4.1 Introduction to Nuclear-Based Hydrogen Production.....68

4.2 The Copper-Chlorine Thermochemical Cycle.....69

4.3 Networked Control System Design for the Hydrogen Plant.....72

4.3.1 Architecture of the Control System.....73

4.3.2 Communication Structure of the Control System.....73

4.4 Dynamic Flowgraph Methodology Modelling of the Hydrogen Plant.....78

4.5 A Case Study: The Hydrogen Reactor Unit (Step 1).....81

4.5.1 Piping and Instrumentation Diagram: Part 1.....84

4.5.2 Piping and Instrumentation Diagram: Part 2.....96

4.5.3 Piping and Instrumentation Diagram: Part 3.....103

4.6 Chapter Summary.....109

Chapter 5 Conclusions and Recommendations for Future Research

5.1 Conclusions.....110

5.2 Recommendations for Future Research.....110

References

Appendix

LIST OF FIGURES

Figure 2.1 A Generic Architecture of a Networked and Distributed Control System.....5

Figure 2.2 A Networked Control System.....16

Figure 2.3 Control Performance vs. Sampling Rate for Different Control Schemes..21

Figure 2.4 Timing Diagram of Message Transmission.....22

Figure 2.5 Waiting Time for Nodes on a Network Bus.....23

Figure 2.6 Communication Network Model.....25

Figure 2.7 DFM Modelling Elements.....29

Figure 3.1 A Simple Networked Control System.....35

Figure 3.2 DFM Model of Preprocessing Time Component.....37

Figure 3.3 DFM Model of Transmission Time and Waiting Time Components.....40

Figure 3.4 DFM Model of Postprocessing Time Component.....43

Figure 3.5 DFM Model of Communication Network.....44

Figure 3.6 A Simple Process System.....47

Figure 3.7 Simulink Model of the NCS Example.....48

Figure 3.8 Simulink Model for Calculating the Valve Position.....48

Figure 3.9 Flow vs. Valve Position with No Communication Delay.....49

Figure 3.10 Simulink Model of Communication Network Effect.....50

Figure 3.11 Flow vs. Valve Position with Communication Delay.....51

Figure 3.12 DFM Model of Networked Control System Example.....53

Figure 3.13 DFM Model of Controller Block in NCS DFM Model.....54

Figure 3.14 Prime Implicants of Communication Unavailability in NCS.....59

Figure 3.15 Flow vs. Valve Position with Reduced Communication Delay.....61

Figure 3.16 Timed Fault Tree Part 1.....62

Figure 3.17 Timed Fault Tree Part 2.....63

Figure 3.18 Timed Fault Tree Part 3.....64

Figure 3.19 Timed Fault Tree Part 4.....65

Figure 4.1 Conceptual Layout of Copper-Chlorine Cycle.....71

Figure 4.2 Architecture of Networked Control System for Cu-Cl Cycle.....74

Figure 4.3 Upper-Level Communication Diagram for Cu-Cl Cycle DCS.....76

Figure 4.4 DFM Model of the Hydrogen Plant.....80

Figure 4.5 Conceptual Schematic for the Hydrogen Reactor.....82

Figure 4.6 Auxiliary Equipment for the Hydrogen Reactor.....82

Figure 4.7 Block Diagram of Reactor 1.....83

Figure 4.8 P&ID of Hydrogen Production Reactor Unit.....85

Figure 4.9 DFM Model of Line 1-1 Flow.....86

Figure 4.10 DFM Model of Line 1-7 Flow.....89

Figure 4.11 DFM Model of Temperature Control of Line 1-1 and Line 1-7.....91

Figure 4.12 DFM Model of Line 1-2 and Line 1-3 Flow.....93

Figure 4.13 DFM Model of Hydrogen Production Reactor.....95

Figure 4.14 P&ID of Quenching and Sedimentation Unit.....97

Figure 4.15 DFM Model of Line 1-17 Flow.....98

Figure 4.16 DFM Model of Line 1-18 and Line 1-19 Flow.....100

Figure 4.17 DFM Model of Quenching Cell.....102

Figure 4.18 P&ID of HCl Absorption Unit.....104

Figure 4.19 DFM Model of Line 1-12 Temperature and Line 1-6 Flow.....105

Figure 4.20 DFM Model of Line 1-12 and Line 1-20 Flow.....108

LIST OF TABLES

Table 2.1 Reliability Modelling Methodologies and Requirements.....14

Table 3.1 Discretization of Source Hardware/Software Status (SHSS).....38

Table 3.2 Discretization of Preprocessing Time (PRE) and Source Delay (SD).....38

Table 3.3 Decision Table for T1 in Preprocessing Time DFM Model 38

Table 3.4 Discretization of Waiting Time (WAIT).....39

Table 3.5 Discretization of Bit Time (BIT).....40

Table 3.6 Discretization of Message Size (MS).....40

Table 3.7 Discretization of Transmission Time (TX).....40

Table 3.8 Decision Table for T2 in Transmission and Waiting Time DFM Model..41

Table 3.9 Discretization of Network Time Delay (NTD).....41

Table 3.10 Discretization of Network Availability (NTA).....41

Table 3.11 Decision Table for T3 in Network Time Delay DFM Model.....42

Table 3.12 Discretization of Destination Hardware/Software Status (DHSS).....43

Table 3.13 Discretization of Postprocessing Time (POST) and Destination Delay (DD).....43

Table 3.14 Decision Table for T4 in Destination Delay DFM Model.....43

Table 3.15 Discretization of Device Delay (DVD).....44

Table 3.16 Decision Table for T5 in Communication Network DFM Model.....44

Table 3.17 Discretization of Total Delay (DEL).....45

Table 3.18 Decision Table for T6 in Communication Network DFM Model.....45

Table 3.19 Discretization of Communication Network Effect (CN).....46

Table 3.20 Decision Table for T7 in Communication Network DFM Model.....46

Table 3.21 Parameters Used in Communication Network Model.....49

Table 3.22 Description of Process Variables in NCS DFM Model.....52

Table 3.23 Discretization of Main Stream Flow (MF), Flow (F), Flow Measurement in Previous Cycle (FMP), Flow Measurement (FM) and Flow Measurement Used by Controller (FMC).....54

Table 3.24 Discretization of Flow Sensor Status (FSS).....54

Table 3.25 Discretization of Flow Setpoint (FSP).....54

Table 3.26 Discretization of Flowrate Error (FE) and Flowrate Error in Previous Cycle (FEP).....55

Table 3.27 Discretization of Integral Control Term for Flowrate (IFE) and Integral Control Term in Previous Cycle (IFEP).....55

Table 3.28 Discretization of Controller Decision (CD), Controller Instruction to Valve (CI) and Change in Valve Opening (DFV).....55

Table 3.29 Discretization of Valve Opening (FV) and Valve Opening in Previous Cycle (FVP).....55

Table 3.30 Discretization of Valve Status (FVS).....55

Table 3.31 Decision Table for T8 in NCS DFM Model.....56

Table 3.32 Decision Table for T9 in NCS DFM Model.....56

Table 3.33 Decision Table for T10 in NCS DFM Model.....57

Table 3.34 Decision Table for T11 in NCS DFM Model.....57

Table 3.35 Decision Table for T12 in NCS DFM Model.....57

Table 3.36 Decision Table for T13 in NCS DFM Model.....57

Table 3.37 Decision Table for T14 in NCS DFM Model.....58

Table 3.38 Decision Table for T16 in NCS DFM Model.....58

Table 4.1 Reaction Steps of Copper-Chlorine Cycle.....70

Table 4.2 Description of Variables of Hydrogen Plant DFM Model.....79

Table 4.3 Description of Process Variables of Line 1-1 Flow DFM Model.....87

Table 4.4 Description of Process Variables of Line 1-7 Flow DFM Model.....88

Table 4.5 Description of Process Variables of Line 1-1 and Line 1-7 Temperature Control DFM Model.....90

Table 4.6 Description of Process Variables of Line 1-2 and Line 1-3 Flow DFM Model.....92

Table 4.7 Description of Process Variables of Hydrogen Production Reactor DFM Model.....94

Table 4.8 Description of Process Variables of Line 1-17 Flow DFM Model.....96

Table 4.9 Description of Process Variables of Line 1-18 and Line 1-19 Flow DFM Model.....99

Table 4.10 Description of Process Variables of Quenching Cell DFM Model.....101

Table 4.11 Description of Process Variables of Line 1-12 Temperature and Line 1-6 Flow DFM Model.....106

Table 4.12 Description of Process Variables of Line 1-12 and Line 1-20 Flow DFM Model.....107

CHAPTER 1

INTRODUCTION

Reliability assessment methods allow the evaluation of the reliability of systems. The methods provide important information on how to improve a system's life to reduce safety risks and hazardous. Several reliability assessment methods were defined and used over the past decades (Aldemir et al., 2007; Ebeling, 1996). With the advancement in technology, the existing methods were extended and new methods were adopted. The introduction of digital Instrumentation and Control (I&C) systems in many applications brought the need to further modify the existing reliability assessment methods. The deployment of communication networks in control systems dictates the use of dynamic reliability assessment methods with special features, such as time dependency and multi-state representation (Aldemir et al., 2006).

1.1 Objective of the Thesis

The objective of the thesis is to demonstrate the extension of the Dynamic Flowgraph Methodology (DFM) to reliability modeling of Networked Control Systems (NCSs). This thesis also shows how the method is applied to model the Cu-Cl thermochemical cycle used for hydrogen production. The modelling is performed subsequent to defining the configuration of I&C systems, and discussing the control flow and the architecture of the networked control system.

1.2 Organization of the Thesis

This thesis is structured as follows: in Chapter 2, a literature review is provided to present the findings in the area of reliability assessment of networked control systems. Chapter 3 presents the reliability modelling of networked control systems using the dynamic flowgraph methodology. In Chapter 4, the application of the DFM to the modelling of Cu-Cl thermochemical cycle is demonstrated. Chapter 5 concludes the thesis and provides recommendation for future research.

CHAPTER 2

LITERATURE REVIEW

This chapter presents a review of the results found in literature in the areas of networked control systems and their reliability assessment. The failure and performance degradation of the control system can lead to process instability (Huo & Zhang, 2008). Thus, the reliability of the control system is an essential part of the reliability of the controlled process. The failure of control system components (i.e., hardware, software and communication networks) is discussed herein. Methods for reliability assessment and modelling are compared. The dynamic flowgraph methodology is introduced. Also, the reliability modelling of communication network and its application in control systems is discussed.

2.1 Networked Control Systems

Instrumentation and control systems are deployed in order to regulate a process to provide a safe and reliable operation. The I&C systems consist of actuators, sensors and controllers. One promising technique for control and monitoring of processes is via the use of networked control systems (Soglo & Xianhui, 2006). They are used in many applications such as factories, hydraulic and thermal power plants, and aerospace industry (Hemeida, El-Sadek, & Younies, 2004). In a NCS, control elements are distributed throughout the process, as opposed to centralized control technique. The

distributed control elements are connected by a network for the purpose of communication and monitoring (Kim, Ji, & Ambike, 2006; Zhang, Branicky, & Philips, 2001). The use of a shared communication network introduces time delays in the transmission of messages between the control elements, which is identified as one of the concerns associated with this control methodology. However, NCSs offer significant advantages such as enhanced flexibility, and reduced wiring and maintenance (Hespanha, Naghshtabrizi, & Xu, 2007; Huo & Fang, 2007).

A basic schematic for the layout of a networked and Distributed Control System (DCS) is shown in Figure 2.1 (Al-Dabbagh & Lu, 2008). The device controllers control equipments and communicate with each other and with the group controller via a communication network. The combination of a group controller and the device controllers is usually referred to as a partition (Harber, Kattan, & MacBeth, 1996). Each partition can communicate with other partitions and with a Plant Display System (PDS), or a Human Machine Interface (HMI), via a communication network.

The data transfer is performed using communication protocols, such as Ethernet or other standards (Lian, Moyne, & Tilbury, 2001). There are several types of commercially available networks such as ControlNet, Foundation Fieldbus, Profibus, DeviceNet, Ethernet, Interbus, etc. The choice of a network protocol depends on the application requirement. For example, in process control applications, the communication network should handle real-time traffic among the control devices. In utilities networks control, the network should be able to perform remote monitoring and station control (Kadri, 2006). The different types of networks are suitable for different types of transmissions

(Zhang et al., 2001). For example, Ethernet can hold a maximum of 1500 bytes of data in a single packet. Thus, it is more efficient to lump data into one packet and transmit them together. On the contrary, DeviceNet can hold a maximum of 8 byte of data in a single packet. It is therefore useful in transmitting small-size control data.

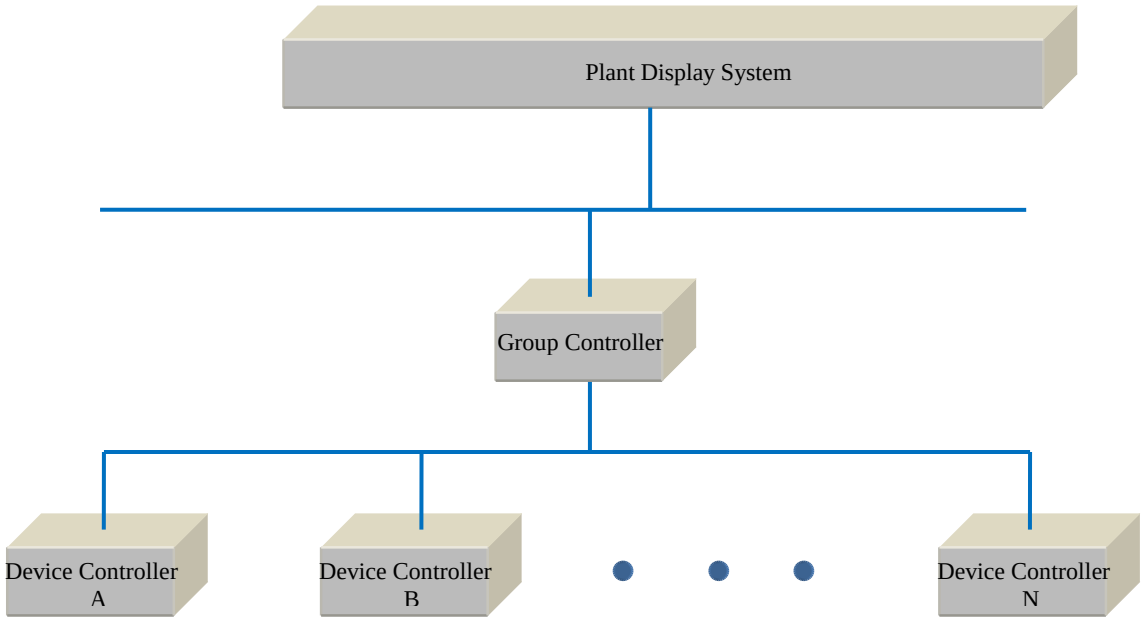

Figure 2.1 A Generic Architecture of a Networked and Distributed Control System

2.1.1 Distribution of the Controllers

The distribution of controllers may be performed according to two schemes (Fieguth, 2008): physical or functional distribution. In the physical distribution scheme, the nodes (partitions) are spread around the system in the most optimized manner, i.e., to reduce the amount of wiring. As a result, cabling costs can be lowered and there would be less congestion in the control room area. In the functional distribution scheme, the control application is divided into logical chuncks assigned to different partitions.

2.1.2 Advantages of Networked and Distributed Control Systems

Networked and distributed control systems offer a number of benefits that include (Fieguth, 2008):

- Easy maintenance, built-in redundancy and transfer of control.
- High performance and high level control oriented programming languages.
- Ability to include low level logic and minor control functions, and potential for reductions in plant wiring.

These benefits have made the use of distributed control systems very attractive for many applications. The next section presents a summary of designs of networked and distributed control systems for aircraft and nuclear power plants applications.

2.1.3 Applications of Networked and Distributed Control Systems

The distributed control methodology, where communication network is used to connect the control systems, is applied in a wide range of applications. In this section, a summary of the control system design is provided for an aircraft arm manipulator and nuclear power plants.

A networked and distributed control system design for a manipulator arm placed on the surface of a spacecraft was presented by Jia, Zhuang, Bai, Fan, & Huang (2007). The manipulator is composed of six joints to provide six degrees of freedom. In the design of the distributed control system for the manipulator, a main controller was set inside the spacecraft and six joint controllers were set inside the joints. The spacecraft was specified

to communicate with the manipulator by means of a 1394 serial data bus. The main controller was specified to communicate with the six joints through a RS422 serial data bus.

The main controller was specified to be responsible for: obtaining power from the spacecraft, communicating with both the spacecraft and with the manipulator, supplying power to the manipulator, and having online trajectory planning and collision detections. The joint controllers were specified to be responsible for: obtaining power from the main controller, communicating with the main controller, and controlling and driving a permanent magnet synchronous motor that controls the movement of the joint.

In traditional instrumentation and control systems for nuclear power plants, most connections are typically hardwired point-to-point (Kim, Lee, Park, & Kwon, 2000). Since they are based on analog technologies, they are slow and fragile to noise. Modern digital communication networks are fast and more immune to channel noise (Kim et al., 2000). The networked and distributed control system approach is also applied in the control and monitoring of nuclear power plants.

Atomic Energy of Canada Limited (AECL) has been investigating the use of DCSs for CANDU nuclear power plants. A DCS design was proposed for control of a CANDU 9 power plant (Harber et al., 1996). The DCS is composed of a set of control and monitoring partitions. The partitions are interconnected to each other as well as to the PDS by a communication network. The DCS was designed to use two types of bus for communication: a local bus and an intra-plant bus. The plant control functions are

assigned to the individual partitions. The functions of the group level control were specified to be able to:

- obtain inputs from several sources and drive several devices,
- implement relatively complex logic, and
- generate outputs which can drive actuators

The functions of the device level control were specified to be able to:

- perform control loops that may involve a small number of inputs,
- use setpoints or error signals computed at the group level,
- provide a facility for direct operator override in an output loop, and
- observe redundant analog outputs or devices.

The use of a DCS for Advanced CANDU Reactor (ACR) has been investigated by Brown & Basso (2004). In the proposed design, two dual-redundant networks are used to transfer information: data acquisition network and inter-partition network. The two networks are based on Hitachi's μ∑ Network-1000 architecture. The network is a 100 Mbps, fibre optic, token ring network. A single network can support 255 nodes over a total distance of 100 km. However, a limit of 32 nodes per μ∑ network was recommended for μ∑ networks used in control functions (Brown & Basso, 2004).

Several studies were performed in South Korea to propose the use of Ethernet-based networks for distributed digital control systems in nuclear power plants (Park, Lee, Choi, Shin, Kim, Lee, & Kwon, 2000; Choi, 2002; Kim et al., 2000). The design is composed of three levels of hierarchical networks: information network, control network and field network.

The information network is responsible for the exchange of data or commands among operator interface stations and engineering interface stations. For its network, the use of a protocol based on TCP/IP is proposed, since the information network is treated as a non-safety computer network and hence does not need redundancy of channels. The control network provides the mechanism for communication between the group controllers and was described as the core communication network in NPPs. This makes it extremely important to operate in a safe, reliable and stable manner. Among the high speed networks, such as Fast Ethernet, Fiber-channel, ATM and FDDI, the use of Ethernet was proposed because it is very cheap, easy to implement, and widely available (Kim et al., 2000). It was argued that Ethernet is very reliable and maintainable. The field network is responsible for communication between field controllers for sharing Input and Output (I/O) data. The use of High-level Data Link Control (HDLC) as its data link layer and the use of RS-485 scheme which has multi-drop as a physical connection were proposed.

The malfunction of the control system, especially the unavailability of communication mechanism, can jeopardize the stability of the process and lead to safety concerns. Thus, reliability assessment must be performed to identify those areas that can be major contributors to control system unreliability.

2.2 Reliability Assessment of Instrumentation and Control Systems

The impact of process systems failure can vary from being inconvenient with minimal cost to extremely significant in both economic loss and safety effects. The impact in safety-critical systems can be severe and may lead to catastrophic events. Reasons that

can cause system failure include: inadequate engineering design, equipment malfunction, human error and improper maintenance (Ebeling, 1996). Reliability assessment must therefore be performed for engineering systems to study potential threats to systems reliability and to find areas for improvement. In reliability engineering, attempts are made to investigate and measure the failure of systems in order to improve their optimal use (Smith, 2005). This can be achieved by increasing systems design life, and reducing the possibility of failure and safety risks. The malfunction of instrumentation and control systems can jeopardize the stability of a process and may lead to plant failure (Huo & Zhang, 2008). The reliability of the instrumentation and control systems is an integral part of the reliability of the plant. Thus, the impact of I&C systems malfunction must be analyzed. This supplies key information on component selection, and inspection and maintenance strategies determination, in order to increase systems life cycle, reduce plants failure frequency and improve systems safety. This section presents and compares the different methodologies used for modelling the reliability of systems, specifically the digital instrumentation and control systems in safety critical application such as nuclear power plants.

The use of digital instrumentation and control systems offers many advantages over their analog counterpart. The advantages include: potential to improve process safety and reliability, stability and improved failure detection capability, and reduced wiring and easier maintenance (Hespanha et al., 2007; Huo & Fang, 2007). Because of these advantages and obsolescence issues with current analog systems, analog I&C systems are no longer considered for new designs and there is an increased desire to use digital systems in both safety and non-safety systems in safety-critical systems, such as nuclear

power plants (Fullwood, Gunther, Valente, & Azarm, 1991; Aldemir et al., 2006). Some specific issues that were identified to be relevant to reliability modelling of digital I&C systems are listed as follows (Aldemir et al., 2006):

- Digital I&C systems use combination of software/firmware in information processing.
- Digital I&C systems rely on sequential circuits. Since they have memory, their outputs may be a function of system history.
- The rate of data transfer is affected by the choice of internal/external communication mechanisms and the communication protocol. This can affect the digital I&C system reliability and robustness.
- Tasks may compete for a digital controller's resources. This requires coordination between the tasks.
- A finer degree of communication and coordination between the controllers is necessary in order to coordinate multiple digital controllers directly and explicitly.
- A digital controller can remain active and not only react to data, but can anticipate the state of the system.
- Tight coupling and less tolerance to variations in operation increases the digital I&C system sensitivity to the dynamics of the controlled physical process.

However, in spite of the progress over the past few decades in studying the reliability of digital I&C systems, there are many areas that need to be established.

2.2.1 Methods of Reliability Modelling and Assessment

There exist several methods that can be used to model and assess the reliability of systems. The choice of the method depends on the several modelling requirements. The most commonly used methods are:

- Fault trees and event trees
- Markov models
- Petri nets

Current Probabilistic Safety Assessment (PSA) analytical tools that assess the safety of safety-critical systems typically involve fault tree analysis, often in combination with other methods such as event trees, Markov models and reliability block diagrams (Dugan, Bavuso, & Boyd, 1993; Bucci, Kirschenbaum, Mangan, Aldemir, Smith, & Wood, 2008). The increased use of digital I&C systems raises several concerns about the capability of the current PSA tools to account for the dynamic interactions between the digital control system elements and the controlled process. For example, software failures, time dependency of unavailability and incomplete independence of various systems (Lu & Jiang, 2004). Therefore, the models of digital systems must be able to interface with the current PSA tools (Kirschenbaum et al., 2006), which dictates the finding of methods to address digital I&C systems' reliability in combination with the current PSA tools.

2.2.2 Requirements of Reliability Modelling

The modelling methodology is chosen based on specified requirements. The requirements specified for modelling digital instrumentation and control systems are listed as follows (Aldemir et al., 2006):

1. The model must be able to predict encountered and future failures well.
2. The model must account for the relevant features of the system.
3. The model must make valid and plausible assumptions.
4. The model must quantitatively be able to accurately represent dependencies between failure events.
5. The model must be designed so its concepts are easy to implement and learn.
6. The data used in the quantification process must be credible to a significant portion of the technical community.
7. The model must be able to differentiate between a state that fails one or multiple safety checks.
8. The model must be able to differentiate between faults that cause function failures and intermittent failures.
9. The model must be able to provide relevant information to users, including cut sets, probabilities of failure and uncertainties associated with the results.
10. The methodology must be able to model the interaction of the digital I&C system portions of accident scenarios with non-digital I&C system portions of the scenarios.
11. The model should not require highly time-dependent or continuous plant state information.

2.2.3 Comparison of Modelling Methods

Table 2.1 provides details on the satisfaction of the requirements mentioned above when applying some of the methods for reliability modelling of digital instrumentation and control systems (Aldemir et al., 2006).

Table 2.1 Reliability Modelling Methodologies and Requirements

Requirement/Methodology	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Continuous Event Trees	X	X	X	X	O	?	?	X	?	?	O
Dynamic Event Trees	X	X	X	?	X	?	?	?	X	X	O
Markov Models	X	X	X	X	O	?	X	X	X	X	O
Petri Nets	X	X	X	X	O	?	?	?	X	X	O
Dynamic Flowgraph Methodology	X	X	X	?	X	?	?	?	X	X	X
Dynamic Fault Trees	X	?	?	?	X	?	X	?	X	?	X
Event Sequence Diagram	X	X	X	X	O	?	?	?	X	X	O

In the table, the entry ‘X’ indicates that the method fulfills the requirement, ‘O’ indicates that the method does not fulfill the requirement, and ‘?’ indicates that further study is needed to determine whether or not the method fulfills the requirement. As can be noted, no single method satisfies all requirements. Each method is associated with its own advantages and disadvantages. The methods that rank as top three with most positive features and least negative or uncertain features are the dynamic flowgraph methodology, dynamic event tree approach or Markov approach and event sequence diagram (Aldemir et al., 2006).

Although fault trees and reliability blocks diagrams are the easiest and most often used techniques in complex systems reliability assessment. These techniques are Boolean models and thus their aim is to show how a binary system (i.e., with two states) state depends on the binary states of the systems' components. In addition, those methods assume components independence and hence they are not suited to modelling systems in which there are dependencies between components (Ghostine, Thiriet, Aubry, & Robert, 2008). As many researchers have refined the static techniques for use in various industries, including aerospace, medical, and nuclear, efforts must be made to modify the dynamic techniques for integration in the current probabilistic safety assessment tools.

2.2.4 Reliability of Networked Control Systems

Networked control systems are defined as a control system whose sensors, controllers and actuators are connected via means of communication networks (Wu, Deng, & Gao, 2005; Cloosterman, Van de Wouw, Heemels, & Nijmeijer, 2006). Figure 2.2 illustrates a simple networked control system that consists of a sensor, controller and actuator. The operation of the networked control system is given as follows (Lian, Moyne, & Tilbury, 2002): the sensor node periodically samples a process parameter with a specified sampling time, or sampling rate, and converts the physical parameter to a digital message. It then packs and send the message to controller through a shared communication network. The controller node unpacks the message from sensor node and employs a control algorithm to calculate a control signal. The signal is then sent to the actuator node through the communication network. The actuator then performs its task according to the

received control signal. This section provides a literature review of the work conducted to investigate the reliability of networked control systems.

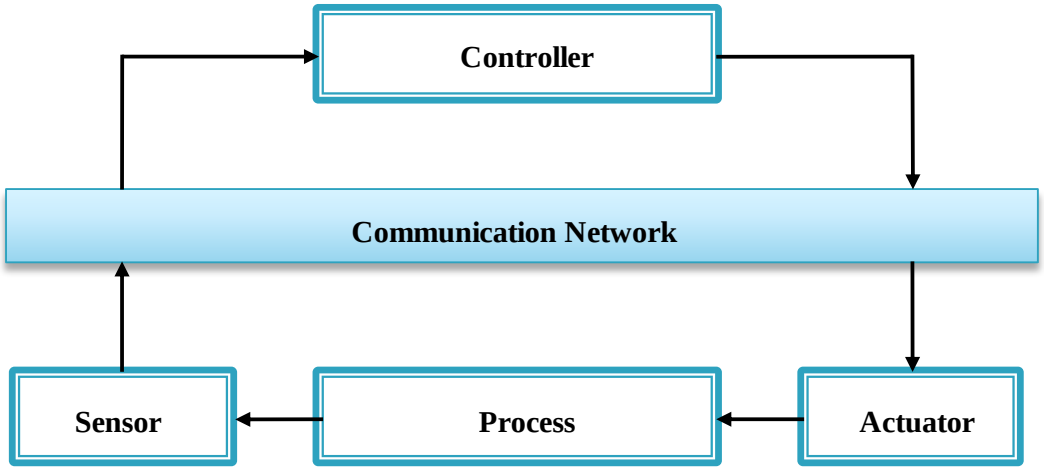

Figure 2.2 A Networked Control System

The main requirement for control systems is to obtain a sufficient level of Quality of Control (QoC) (Galdun, Takac, Lingus, Thiriet, & Sarnovsky, 2008). To guarantee a sufficient reliability level of the control system, a suitable control structure needs to be used to meet the requirements for better dependability parameters (Galdun et al., 2008). Dependability involves the following concepts (Zagar, 2005):

- Reliability: the solution must perform its specified task whenever requested.
- Availability: the solution must be available all the time for performing the task.
- Security: malicious third parties must not be able to take control of the solution and use it against or without knowledge of its authorized users.

Control systems are usually designed to be reliable and available under normal operating conditions. However, under unpredictable environmental influence (e.g., hardware failures, broken communication networks links), the reliability and availability may be affected (Zagar, 2005). Also, degradation in communication networks performance can affect the reliability of control systems.

Failure scenarios in networked and distributed control systems can be classified by (Zagar, 2005):

- A **communication failure** can be the cause of communication link's unavailability or degradation in communication network performance. It can occur at the control or field network levels. In either case, the control systems will be isolated, which may lead to process instability.
- A **node crash** can be the cause of the failure of hardware or software of sensor, actuator or controller.

2.2.4.1 Reliability of Communication Networks

This subsection presents details on the reliability of computer and communication networks. Several studies were conducted in the area of computer networks to investigate their reliability (Chiou & Li, 1986; Le & Li, 1989; Jian & Shaoping, 2006). The previous research conducted on network reliability has focused on models in which each component may be in one of two modes: operative or failed. However, a component may undergo degradations in performance before a complete outage and will therefore operate in more than two modes (Chiou & Li, 1986). Network components can be lying between the fully operative mode and the fully failed mode. For example, a digital transmission

link could have a high bit-error rate, erroneous data packets and a reduced effective capacity (Le & Li, 1989).

The reliability of a computer network is related not only with the reliability of the components and the topology of the network, but also with the configurations of the nodes and the traffic flowing into the network (Jian & Shaoping, 2006). Nodes consist of two failure modes: congestive failure and failure related with inactivation of the software and hardware. The latter is defined as the fixed reliability of the node. The study models the fixed reliability by Generalized Stochastic Petri Nets (GSPN). When studying the reliability of communication networks in networked control systems, several issues must be accounted for in the reliability modelling as will be discussed in the following subsection.

2.2.4.2 Reliability of Communication Networks in Networked Control Systems

The issues that may affect the performance of a communication network and thus influence the reliability of the NCS include (Galdun et al., 2008):

- Time delay or latency: they are defined as the time from the source sending a data packet to the destination receiving it. There is no guarantee for zero or even constant delay in the sending of messages between control devices (Hespanha et al., 2007). The delay can affect the accuracy of time-dependent computations in the control system.
- Data losses: when there is congestion in the communication network bus, some packets are dropped. In this case, the controllers have to make decisions with

incomplete information. It is assumed that messages can be lost if one of these conditions is satisfied: (i) the maximum number of retransmission for the message is reached, (ii) a new message of the same type is ready to be sent (Ghostine et al., 2008).

- Electromagnetic inferences (EMI): they can generate transient faults in electronic circuits that affect the normal operations. The component affected will be temporary unavailable. For example, if a communication network is affected by a transient fault, it may be unable to transmit data for a certain interval of time. External interferences occur stochastically in time which leads to variable delays on affected messages (Ghostine et al., 2008).

In real time systems, particularly control systems, delays or dropped packets may degrade control system's Quality of Performance (QoP), which may cause instability and lead to catastrophic events (Ghostine et al., 2008; Huo & Zhang, 2008; Kumar, Verma, & Srividya, 2009). In addition, research was performed in the area of stability analysis of communication networks with communication limitation, focusing on the delay and packet dropout components (Cloosterman et al., 2006; Zhang, Zheng, & Lu, 2006; Zhang, Zhong, & Wei, 2008; Tian & Levy, 2008). The use of a shared communication network introduces different forms of time delay uncertainty between sensors, actuators, and controllers. The time delay (i.e., time from the source sending a message to the destination receiving it) comes from the time sharing of communication medium and other functionality required for physical signal coding and communication processing (Lian et al., 2002). The characteristics of time delays could be constant, bounded, or even random, depending on the chosen network protocols and hardware. The time delay could

potentially degrade a system's performance and possibly cause system instability (Lian et al., 2002). Another issue is that process information may be transmitted using multiple network packets, due to bandwidth and packet size constraints in some networks types. Therefore, chances are all, part or even none of the packets could arrive by the time of control calculation (Zhang et al., 2001). For real-time feedback control data (e.g., sensor measurements and calculated control signals), it may be advantageous to discard an old, untransmitted message and transmit a new packet if it becomes available. This allows the controller to constantly receive fresh data for control calculations (Zhang et al., 2001).

The computational and operational schemes of sensors, controllers and actuators in a networked control system can be specified as (Zhang et al., 2001):

- Clock-driven sensors: the sensor periodically samples a parameter in the process at a given sampling rate
- Event-driven controllers: the controller calculates the control signal as soon as the sensor data arrives
- Event-driven actuators: the actuator changes the plant inputs as soon as the data become available

A performance chart was provided to compare the control performance of continuous control, digital control and networked control systems with sampling rates as presented in Figure 2.3 (Lian et al., 2002). It can be used as a guide to determine the appropriate sampling rate for an NCS.

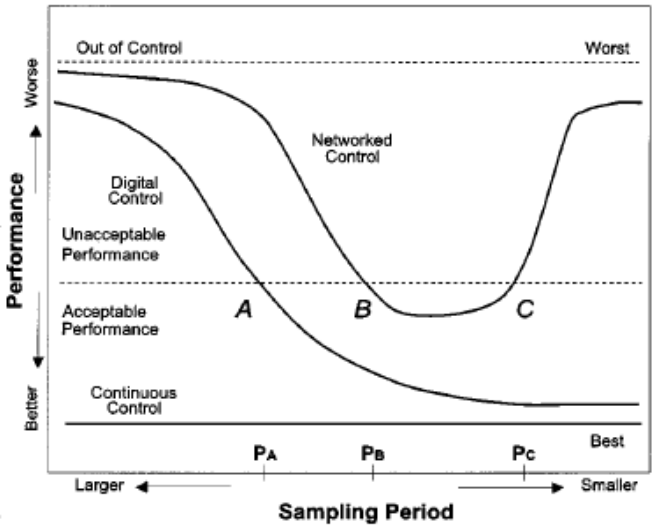

Figure 2.3 Control Performance vs. Sampling Rate for Different Control Schemes (Lian et al., 2002)

The worst, unacceptable, acceptable, and best regions can be defined based on the specifications of the control system such as steady-state error, overshoot and phase margin (Lian et al., 2002). For the networked control case, point B can be determined by analyzing the characteristics and statistics of network-induced delays and device processing time delays. As the sampling rate gets smaller, the network traffic load becomes heavier. The likelihood of more contention time or data loss increases in a bandwidth-limited network and hence longer time delays result. This condition causes the existence of point C in an NCS (Lian et al., 2002).

The important time delays that should be considered in networked control system analysis are the sensor to controller and controller to actuator end-to-end delays. In an NCS, the time delay can be broken into two parts (Lian et al., 2002): device delay and network delay. The device delay includes the time delays at the source and destination nodes. The time delay at the source includes the preprocessing time and the waiting time.

The time delay at the destination node is the postprocessing time. The network time delay includes the total transmission time of a message and the propagation delay of the network. The timing behaviour of message transmission from source node to a destination node is shown in Figure 2.4.

The preprocessing time at the source node, T_{pre} is the time needed to acquire data from the external environment and encode it into the appropriate network data format. This time depends on the device software and hardware characteristics. In many cases, it may be assumed that the preprocessing time is constant or negligible.

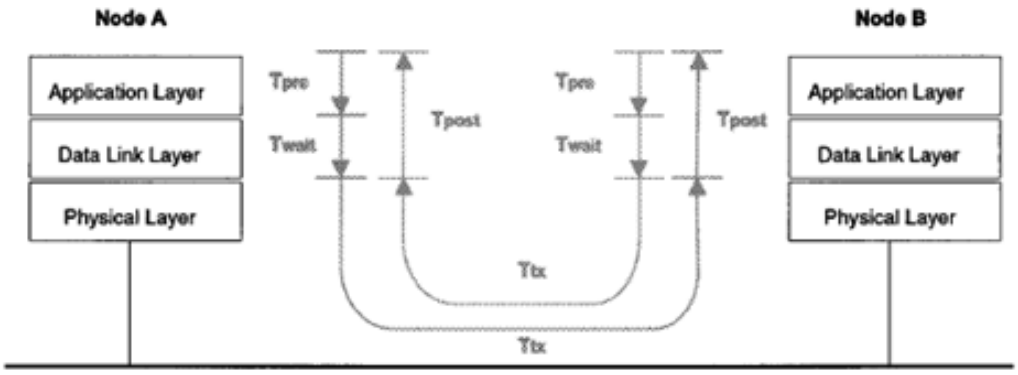

Figure 2.4 Timing Diagram of Message Transmission (Lian et al., 2002)

A message may spend time waiting in the queue at the sender's buffer before transmitting. It could be blocked by other messages on the network. Depending on the traffic on the network and the amount of data the source node needs to transmit, the waiting time, T_{wait} may be significant. For example, if Slave 1 in Figure 2.5 is transmitting a message, the other eight nodes must wait until the network medium is idle.

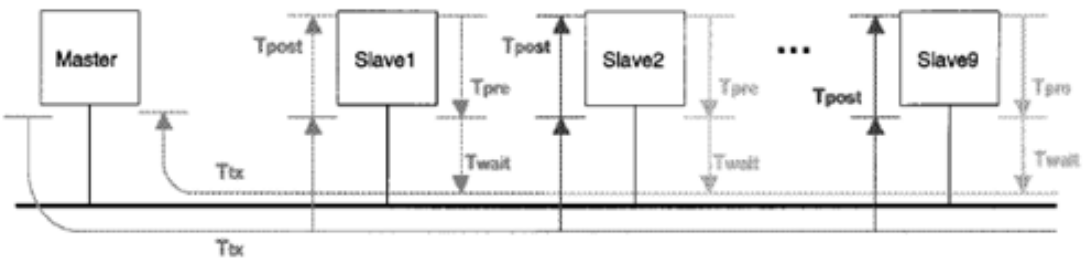

Figure 2.5 Waiting Time for Nodes on a Network Bus (Lian et al., 2002)

The Transmission time, T_{tx} is the most deterministic parameter in a network system. It depends on the network protocol (i.e., data rate and message size) and the distance between the two nodes. The postprocessing time, T_{post} at the destination node is the time taken to decode the data into the physical data format and output to the external environment.

Due to the interaction of the network and control requirements, the selection of the best sampling rate is a compromise. Based on the previous analyzes, smaller sampling rates guarantee a better control QoP. However, in a bandwidth-limited control network, the use of smaller sampling rates introduces high-frequency communication which may degrade the network QoS. The degradation of network QoS could further deteriorate the control QoP as a result of longer time delays when the network is near saturation (Lian et al., 2002).

2.2.5 Reliability Modelling of Networked Control Systems

This subsection describes related studies that model the networked control systems for reliability analysis. The limitations of the studies are discussed and the requirements for a modelling framework are defined.

2.2.5.1 Previous Studies on Modelling of Networked Control Systems

Some studies have investigated reliability and safety models of networked control systems (Campelo, Yuste, Rodriguez, Gil, & Serrano, 1999; Ghostine et al., 2008). In performing the reliability modelling, Stochastic Activity Networks (SAN) and the UltraSAN tool were used (Campelo et al., 1999). SAN are extensions to timed Petri nets.

This technique provided the capability of using two types of activities, timed and instantaneous activities. Timed activities represent delays by a probabilistic distribution. Instantaneous activities are used if the time to complete an operation is insignificant. A communication network model was included in their study, as shown in Figure 2.6.

Activities represent an exponentially distributed variable with a rate equal to the expected failure rate of the corresponding component. In this model, there are four activities modelling the network's behaviour.

Activities "fnsr_1" and "fnsr_2" have a rate of: $\lambda_n \; x \; (1 - \; P_p) \; x \; (1 - \; C_n)$, where:

- λ_n is the network failure rate.
- P_p is the probability of the failure being permanent.

- C_n is the network error coverage (i.e., the probability of the error being covered by the error detection mechanisms in the system).

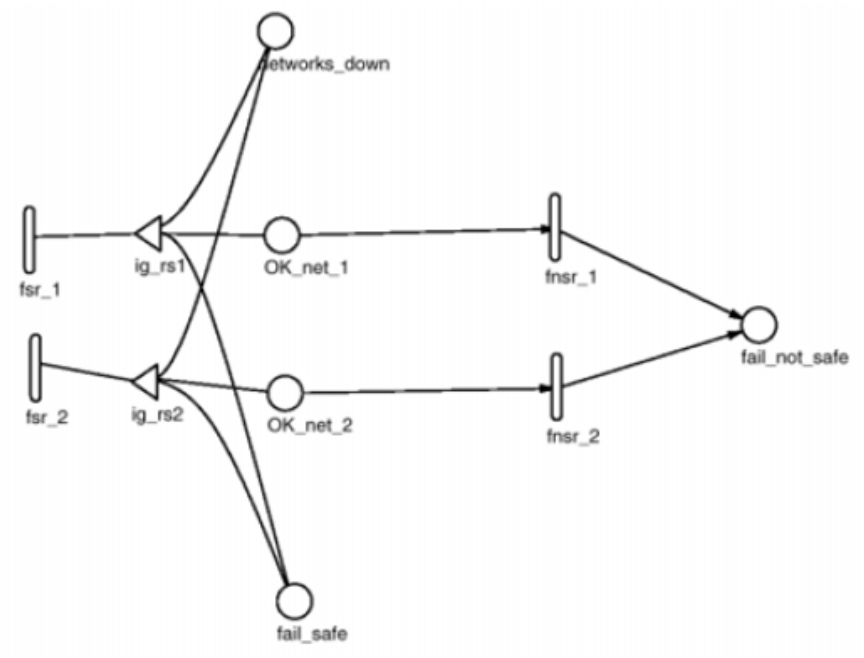

Figure 2.6 Communication Network Model (Campelo et al., 1999)

All non-permanent uncovered network errors will take the system to the "fail_not_safe" state. Activities "fsr_1" and "fsr_2" have a rate of: $\lambda_n \, x \, P_p$. This means that all permanent network errors will be detected and if the system is unable to reconfigure itself (if there are no spare networks left), it will go to "fail_safe" state. Input gates are in charge of deciding when activities are enabled and what to do upon completion of the activity (Campelo et al., 1999).

The network modeling is based on communication networks being available or unavailable. It does not include the performance degradation factors such as network

induced delays. The input gate predicate in the model is a Boolean expression. This technique does not allow the representation of multi-state systems in the model.

Another study investigated the influence of the transmission faults on the reliability of a networked control system (Ghostine et al., 2008). Their approach is composed of two parts: a modelling part in which all the basic components of a networked control system are modelled and a simulation part in which simulation is done on the models to evaluate the reliability. In their work, Petri nets extensions are used. The network model is defined as the central model, where all other models are linked to it by sharing places. The model takes account of CSMA/AMP strategy used in CAN-based communication network and aims at evaluating some performance parameters on the network for a running time. The parameters include:

- The sum and the average time delays for each node on the network.
- The efficiency of the network.
- Network utilization.
- The ratio of lost messages for each node on the network.

This study only takes into account CAN-based networks and is not generic. Hence, it cannot be used for modelling the behaviour of other networks. Although attempts were made to study the reliability of networked control systems, there exist many areas that need to be considered.

2.2.5.2 Requirements for Reliability Modelling of Networked Control Systems

A modelling framework for assessing the reliability of networked control systems must be established. The following features must be provided by the modelling technique:

1. The model must capture the behaviour of the hardware, software and communication systems of the networked control system.
2. The model must be generic. (e.g., it can be applied to model different types of communication networks).
3. The model must take into account the degradation in systems' performance.
4. The model must incorporate time dependency and multi-state behaviour.
5. The model must be easy to learn, adopt and incorporate into existing PSA tools.

Several studies were conducted to model the reliability of software-driven control systems using dynamic flowgraph methodology (Garret, Guarro, & Apostolakis, 1993; Yau, Guarro, & Apostolakis, 1995; Garrett, Guarro, & Apostolakis, 1995; Cosgrove, Guarro, & Romanski, 1996; Guarro, Yau, & Motamed, 1996; Guarro & Yau, 1996; Houtermans, Apostolakis, Brombacher, & Karydas, 2000; Garrett & Apostolakis, 2002). This methodology offers the advantage of having one model that can be used to derive many failure or success scenarios. In addition, the modelling technique can account for time dependency and multi-state representation of systems' parameters. These two important features in modelling the reliability of digital I&C systems are not provided by traditional fault tree analysis. Further details on the dynamic flowgraph methodology and its advantages are presented in the following subsection.

2.3 The Dynamic Flowgraph Methodology

The dynamic flowgraph methodology is a digraph (directed graph) based approach to model and analyze the behaviour and interaction of software and hardware within an embedded system for the purpose of safety and reliability assessment and verification (Garret et al., 1993; Garrett et al., 1995; Yau et al., 1995; Cosgrove et al., 1996; Guarro et al., 1996; Guarro & Yau, 1996; Houtermans et al., 2000; Garrett & Apostolakis, 2002). The dynamic flowgraph methodology has been mainly applied in modelling software driven control systems. It was also presented as an approach to model an operating team, where the performance of individuals in the team and their interaction with the system hardware was modeled (Milici, Wu, & Apostolakis, 1996). In the DFM approach, system models are developed in terms of causal relationships between physical variables and temporal characteristics of the execution of software modules. The DFM model can also capture time dependent behaviour and switching logic. When modelling a digital control system, both the controlling software and the system being controlled can be represented in the DFM model (Guarro & Yau, 1996). The methodology has two fundamental goals (Guarro & Yau, 1994):

- To provide an integrated hardware/software model of the system
- To identify how certain critical events of interest may occur

Although DFM is based on digraphs, it shares more similarities with the state machine approach (Garret & Apostolakis, 2002). Instead of using static models with continuous partial derivates to model the relationships between process variables, the system state is dynamic and state transitions are expressed using decisions tables. The difference is that

DFM also models the system hardware (including failure behaviour) and operating environment in addition to software (Garret & Apostolakis, 2002).

2.3.1 Model Components

The DFM uses a set of basic modeling elements to represent the system parameters and their relationships as described below and shown in Figure 2.7.

1. Process variable and conditioning nodes,
2. Causality and conditioning edges, and
3. Transfer and transition boxes and their associated decision tables.

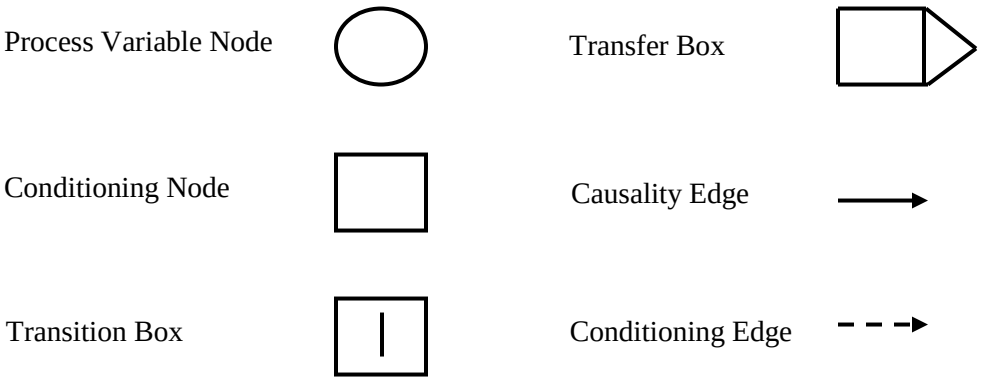

Figure 2.7 DFM Modelling Elements

2.3.2 Model Construction

The modelling strategy is a two step process: construction of a model and analysis of the constructed DFM model.

The construction of DFM models is performed using a detailed multi-state representation of the cause-and-effect and time-varying relationships that exist between key system parameters. The nodes represent the systems' parameters, components or variables. They are discretized into a finite number of states and therefore represent more than just an operative or failed scenario. For example, a node can represent a range of operating pressure reading. The process variable nodes are used to represent physical or software parameters. The condition nodes are used to identify component failure states, software switching actions and changes of process operation modes (Guarro et al., 1996). The edges are used to visually represent the type of relationships that exists between parameters (i.e., cause-and-effect or conditioning relationship). Transition boxes and transfer boxes are used to express the detailed representation of the function and temporal relationships that exist among parameters states. Transition boxes differ from transfer boxes in that a time lag is assumed to occur between the time when the input variable states become true and the time when the output variable states are reached (Guarro et al., 1996). The boxes contain decision tables that are used to incorporate a multi-state representation of the relationships that exist among the parameters. Decision tables are a mapping between possible combinations of the input states and output process variable nodes (Guarro et al., 1996). They can be implemented from empirical knowledge of the system, physical equations that describe the behaviour of the system, or software code and/or pseudo code (Cosgrove et al., 1996).

A model is always a compromise between faithfulness and simplicity. A model can be very detailed to represent all the system behaviour and dynamics, yet at the same time, can be intractable. Thus, assumptions should be made to simplify the model, while

leaving it relatively faithful and tractable (Ghostine et al., 2008). In other words, careful selection of the number of states should be made while maintaining sufficient amount of information in order to capture more details of the behaviour of the system (Guarro et al., 1996).

2.3.3 Model Analysis

The second step involves the analysis of the constructed model. This allows for identification of the modes by which specific system and process failure states can take place. An implemented DFM model can be analyzed by tracing sequences of events inductively and/or deductively through the model structure. This identifies the paths by which combinations of basic events can propagate through the system to result in system events of interest, whether desirable or undesirable. The DFM Software Toolset allows for performing the deductive and inductive analysis of an implemented DFM model.

The inductive DFM analysis follows a bottom-up approach. It is performed by specifying a set of component states and then investigating the propagation through the system and finding the influence on the system state level of interest. The deductive DFM analysis follows a top-down approach. It is performed by specifying a state of interest and finding the combination and sequences of parameters that lead to the specified state. When performing deductive analysis, timed prime implicants can be found. A prime implicant is defined as a conjunction of primary events which are sufficient to cause the top event and which does not contain any shorter conjunction of the same events which is also sufficient to cause the top event (Cosgrove et al., 1996). Prime implicants can be helpful in identifying unknown systems hazards, prioritize the disposition of known systems

hazards, and guide lower-level design decisions to eliminate or mitigate known hazards (Garrett & Apostolakis, 2002). In addition, timed fault trees can be derived for any top event to visually represent the combination and sequences of events that lead to the occurrence of the specified top event. In the inductive and deductive DFM analysis, the model is analyzed by automated forward- and back-tracking procedures, respectively. The analysis can be continued for several steps forward or backward in time. The information associated with each step is presented in the form of intermediate transition tables. Transition tables are logically equivalent to gates in a time-dependent fault tree.

The deductive DFM analysis shares key conceptual features with traditional fault tree analysis. However, DFM uses a multi-state and time dependent representation of system and parameter conditions. In addition, timed fault trees, derived using DFM deductive analysis, systematically and formally account for the timing relations between system and parameter states (Garrett et al., 1995). DFM is reported to offer major advantages over conventional safety and reliability methods. It represents the capabilities of FMEA, FTA and HAZOP in one tool (Houtermans et al., 2000). Only one DFM model is needed to capture the complete behaviour of a system. A model can be used for performing failure analysis, verifying design requirements and defining test cases. In addition, a model provides the capability of executing the equivalent of a large number of fault tree derivations for different possible top events of interest. Thus, it is not necessary to perform separate model constructions for each system's state of interest (Garrett et al., 1993). The DFM approach provides a documented model of the system behaviour and interactions as well as a framework to model and analyze time-dependent behaviour (Yau et al., 1995).

2.4 Chapter Summary

The chapter provided literature review of networked control systems and their reliability assessment. Methods for reliability assessment of digital instrumentation and control systems were compared. The dynamic flowgraph methodology was introduced and the advantages of the method were discussed. In addition, the features that should be provided by reliability assessment methods were listed. The following chapter demonstrates the extension of the dynamic flowgraph methodology to modelling of networked control systems.

CHAPTER 3

DYNAMIC FLOWGRAPH METHODOLOGY FOR MODELLING OF NETWORKED CONTROL SYSTEMS

A major issue in reliability modelling is how to compose hardware reliability, software reliability and timely correctness to arrive at a reasonable system's reliability model (Nolte, Hansson, & Norstrom, 2003). Reliability modelling of systems using the dynamic flowgraph methodology offers many advantages over other reliability modelling methods (Garret et al., 1993; Garrett et al., 1995; Yau et al., 1995; Cosgrove et al., 1996; Guarro et al., 1996; Guarro & Yau, 1996; Houtermans et al., 2000; Garrett & Apostolakis, 2002). The use of DFM allows for modelling of systems as a whole. The method can be used to capture the behaviour and interactions of the hardware and software components of systems. It allows the incorporation of multistate systems and time dependency into the analysis. One DFM model can be used to study different events of interests. The modelling technique provides the following capabilities:

- Modelling of systems' behaviour, and
- Investigation of the effect of components' reliability

This chapter demonstrates the extension of the methodology to the modelling of networked control systems. Figure 3.1 shows the schematic of a simple networked control system. The system consists of a controller, actuator and sensor that are connected using a communication network. The sensor periodically samples and sends

data to the controller. The controller's decision and instructions are sent to the actuator to take action in the process (e.g., change valve position, change motor speed, etc.). The communication is made possible through the use of a shared communication network.

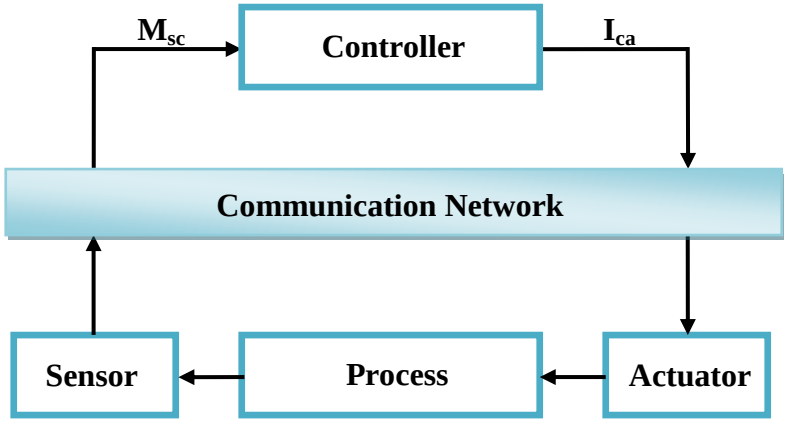

Figure 3.1 A Simple Networked Control System

3.1 Modelling of Communication Network

This subsection demonstrates the modelling of the behaviour of the communication network in a NCS using the dynamic flowgraph methodology. The reliability of the communication network influences signals transmission between the communicating nodes. For example, in Figure 3.1, if communication is available, messages will be transmitted on time. This is modelled by allowing the controller to use the current transmitted message. Otherwise, if communication is unavailable, the controller will not receive the current value. Consequently, it will use the message transmitted from the previous cycle.

From the controller point of view, if transmission is completed on time, the sensor measurement used by the controller is defined by Eq. 3.1. Otherwise, the sensor measurement used by the controller is defined by Eq. 3.2.

$$M_{sc} = R_x(n) \tag{3.1}$$

$$M_{sc} = R_x(n-1) \tag{3.2}$$

where, M_{sc} is the sensor measurement used by the controller, n is a discrete sampled value, $R_x(n)$ is the message at n, $R_x(n-1)$ is the message at $n-1$ (i.e., from the previous cycle). From the actuator point of view, if transmission is completed on time, the controller instruction used by the actuator is defined by Eq. 3.3. Otherwise, the controller instruction used by the actuator is defined by Eq. 3.4.

$$I_{ca} = T_x(n) \tag{3.3}$$

$$I_{ca} = T_x(n-1) \tag{3.4}$$

where, I_{ca} is the controller instruction used by the actuator, $T_x(n)$ is the message at n, $T_x(n-1)$ is the message at $n-1$ (i.e., from the previous cycle). The model takes into account the availability of the communication link and the performance degradation of the communication network. The communication system is seldom robust to loss of data or data latency (Zhang et al., 2001). Time delays are indicated to be the main source of degradation in the control performance.

As mentioned in Section 2.2.4.2, in a networked control system, time delays are broken into preprocessing time, T_{pre}, waiting time, T_{wait}, transmission time, T_{tx}, and postprocessing time, T_{post}. The total time delay is expressed by Eq. 3.5. The time delay components are used in implementing the DFM model. DFM models are implemented for each component of the time delay as discussed below.

$$T_{delay} = T_{pre} + T_{wait} + T_{tx} + T_{post} \tag{3.5}$$

3.1.1 Preprocessing Time Component

The preprocessing time at the source node is defined as the time needed to acquire data from the external environment and encode it into appropriate network data format. For example, data is sampled and decoded into digital format. The time is the sum of the computation time and the encoding time. It depends on the device software and hardware characteristics. The model is shown in Figure 3.2, where SHSS, PRE and SD represent source hardware/software status, preprocessing time and source delay, respectively. The discretization of the variables shown in Figure 3.2 is provided in Tables 3.1 – 3.2.

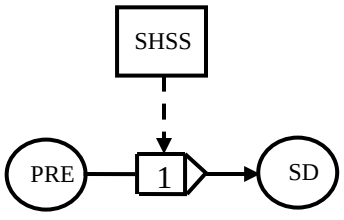

Figure 3.2 DFM Model of Preprocessing Time Component

Table 3.1 Discretization of Source Hardware/Software Status (SHSS)

0	Available
1	Unavailable

Table 3.2 Discretization of Preprocessing Time (PRE) and Source Delay (SD)

0	τ_{PRE}
1	τ_x

The source preprocessing time is assumed to be τ_{PRE} when the corresponding processor is functional. In case of an unavailability or failure of the hardware or software components of the processor, a time delay of τ_x is assumed. Numerical representations of the variables are left unassigned for the sake of generality. Table 3.3 provides the decision table for transfer box T1 to express the mapping between the variables.

Table 3.3 Decision Table for T1 in Preprocessing Time DFM Model

Input		Output
SHSS	PRE	SD
0	0	0
1	0	1

3.1.2 Waiting Time Component

The waiting time, which is also referred to as network access time, is defined as the time a message may spend in the queue at the sender's buffer before transmission. The waiting time is the sum of the queue time and the blocking time. The time depends on the amount of data the source node must send and the traffic on the network. The main factors affecting waiting time are network protocol, message contention type and network traffic load. The model of this component is included in the next subsection. The waiting time is

discretized into two ranges, an acceptable range, 0 - τ_{WAIT1} and an unacceptable range, τ_{WAIT1} - τ_{WAIT2}. Table 3.4 describes the discretization of the variable, where WAIT represents the waiting time.

Table 3.4 Discretization of Waiting Time (WAIT)

0	0 - τ_{WAIT1}
1	τ_{WAIT1} - τ_{WAIT2}

3.1.3 Transmission Time Component

The transmission time is the time required to transmit a message between two nodes. The formula for transmission time is described as shown in Eq. 3.6 (Lian et al., 2002).

$$T_{tx} = N \, x \, T_{bit} + T_{prop} \tag{3.6}$$

where, N is the message size in terms of bits, T_{bit} is the bit time and T_{prop} is the propagation time between any two devices. The propagation time is negligible in a small scale control network (100 m or shorter) since typical transmission speed in a communication medium is 2 x 10^8 m/s (Lian et al., 2002).

The DFM model of the transmission time and waiting time components is shown in Figure 3.3. Tables 3.5 – 3.6 demonstrate the discretization of the variables that represent the bit time, BIT and message size, MS, respectively.

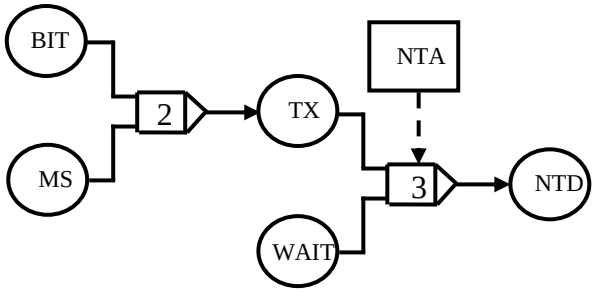

Figure 3.3 DFM Model of Transmission Time and Waiting Time Components

Table 3.5 Discretization of Bit Time (BIT)

0	0 - τ_{BIT1}
1	τ_{BIT1} - τ_{BIT2}

Table 3.6 Discretization of Message Size (MS)

0	0 – ms_1
1	ms_1 – ms_2

The transmission time is discretized into three ranges as shown in Table 3.7, where TX represents to the transmission time variable. The discretization of the variable is given by Eq. 3.7 – Eq. 3.9.

Table 3.7 Discretization of Transmission Time (TX)

0	0 – τ_{TX1}
1	τ_{TX1} - τ_{TX2}
2	τ_{TX2} - τ_{TX3}

$$\tau_{TX1} = m_{s1} \, x \, \tau_{BIT1} \tag{3.7}$$

$$\tau_{TX2} = m_{s1} \, x \, \tau_{BIT2} \tag{3.8}$$

$$\tau_{TX3} = m_{s2} \, x \, \tau_{BIT2} \tag{3.9}$$

where, m_{sx} is the message size and τ_{BITx} is the bit time. The ranges represent the required, acceptable, and unacceptable transmission times, respectively. The decision table for transfer box T2 is given in Table 3.8.

Table 3.8 Decision Table for T2 in Transmission and Waiting Time DFM Model

Input		Output
BIT	MS	TX
0	0	0
1	0	1
0	1	1
1	1	2

The network delay is the sum of the transmission delay and the waiting time. The discretization of the network delay and network availability is shown in Tables 3.9 – 3.10, where NTD and NTA represent the network time delay and network availability, respectively. The discretization is given according to Eq. 3.10 – Eq. 3.12. Table 3.11 provides the decision table for transfer box T3.

Table 3.9 Discretization of Network Time Delay (NTD)

0	$0 - \tau_{NTD1}$
1	$\tau_{NTD1} - \tau_{NTD2}$
2	$\tau_{NTD2} - \tau_{NTD3}$

Table 3.10 Discretization of Network Availability (NTA)

0	Available
1	Unavailable

$$\tau_{NTD1} = \tau_{TX1} + \tau_{WAIT1} \quad (3.10)$$

$$\tau_{NTD2} = \tau_{TX2} + \tau_{WAIT2} \quad (3.11)$$

$$\tau_{NTD3} = \tau_{TX3} + \tau_{WAIT2} \quad (3.12)$$

Table 3.11 Decision Table for T3 in Network Time Delay DFM Model

Input			Output
NTA	TX	WAIT	NTD
0	0	0	0
0	1	0	1
-	-	1	2
-	2	-	2
1	-	-	2

3.1.4 Postprocessing Time Component

The postprocessing time at the destination node is defined as the time taken to decode the network data into the physical data format and output to external environment. It is the sum of the decoding time and the computation time. The DFM model of this component is shown in Figure 3.4. The discretization of the variables is given in Table 3.12 – 3.13, where DHSS, POST, and DD represent the destination hardware/software status, the post processing time and the destination delay, respectively. The device delay at the destination node is assumed to be τ_{POST} when the corresponding processor is functional. In case of an unavailability or failure of the hardware or software components of the processor, a time delay of τ_y is assumed. The decision table for transfer box T4 is provided in Table 3.14.

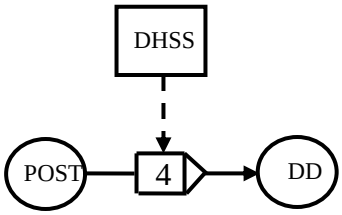

Figure 3.4 DFM Model of Postprocessing Time Component

Table 3.12 Discretization of Destination Hardware/Software Status (DHSS)

0	Available
1	Unavailable

Table 3.13 Discretization of Postprocessing Time (POST) and Destination Delay (DD)

0	τ_{POST}
1	τ_y

Table 3.14 Decision Table for T4 in Destination Delay DFM Model

Input		Output
DHSS	POST	DD
0	0	0
1	0	1

The DFM models of the time delays are combined to form the DFM model of the communication network effect, as shown in Figure 3.5. In the model, the total device delay, represented by DVD, is the sum of the delays at the source node and the destination node. This is expressed in Eq. 3.13. The discretization of the total device delay is given in Table 3.15 and the decision table for transfer box T5 is given in Table 3.16.

$$\tau_{DVD} = \tau_{SD} + \tau_{DD} \tag{3.13}$$

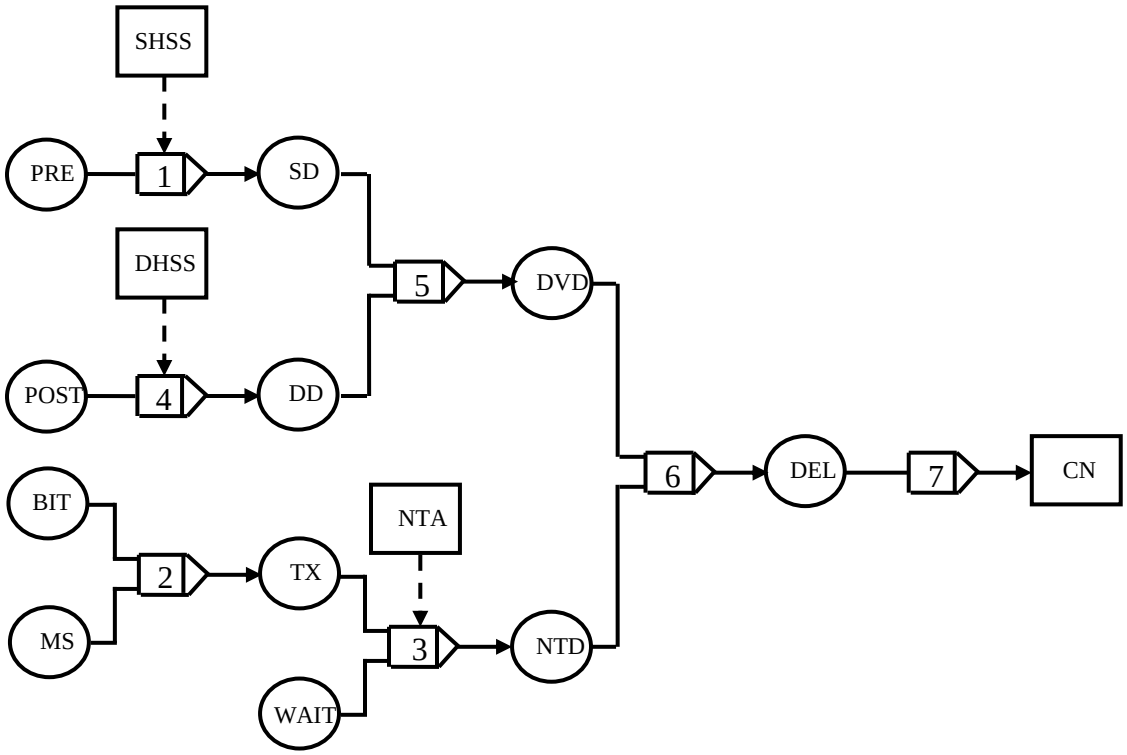

Figure 3.5 DFM Model of Communication Network

Table 3.15 Discretization of Device Delay (DVD)

0	τ_{DVD}
1	τ_z

Table 3.16 Decision Table for T5 in Communication Network DFM Model

Input		Output
SD	DD	DVD
0	0	0
1	-	1
-	1	1
1	1	1

The total time delay is expressed in terms of the total device delay and the network delay. The discretization of the total time delay, represented as DEL in the DFM model, is given

in Table 3.17. The decision table for transfer box T6 is given in Table 3.18. The total time delay is calculated according to Eq. 3.14 – Eq. 3.16.

Table 3.17 Discretization of Total Delay (DEL)

0	0 - τ_{DEL1}
1	τ_{DEL1} - τ_{DEL2}
2	τ_{DEL2} - τ_{DEL3}

Table 3.18 Decision Table for T6 in Communication Network DFM Model

Input		Output
DVD	NTD	DEL
0	0	0
0	1	1
-	2	2
1	-	2

$$\tau_{DEL1} = \tau_{DVD} + \tau_{NTD1} \tag{3.14}$$

$$\tau_{DEL2} = \tau_{DVD} + \tau_{NTD2} \tag{3.15}$$

$$\tau_{DEL3} = \tau_{DVD} + \tau_{NTD3} \tag{3.16}$$

The equations represent required, accepted and unaccepted time delays, respectively. The total delay is compared to a threshold (i.e., sampling rate) to determine whether the communication between the nodes is affected. The discretization of the node CN that represent the communication network effect is shown in Tables 3.19. The decision table for transfer box T7 is given in Table 3.20.

Table 3.19 Discretization of Communication Network Effect (CN)

0	will affect performance
1	will not affect performance

Table 3.20 Decision Table for T7 in Communication Network DFM Model

Input	Output
DEL	CN
0	1
1	1
2	0

The implemented DFM model can study the reliability of different types of communication networks. The aim of this study is to implement a generic model. When a network type is determined, the message transmission rate, message size, etc. can be used as inputs to the model. Based on knowledge about the system, specifications can be determined (e.g., sampling time requirement, etc.). The model also incorporates multi-state representation of components behaviour. For example, the node 'DEL' is discretized into 3 states that represent different ranges of delays. These features make this methodology much more powerful than other reliability assessment tools.

3.2 Networked Control System Example

Figure 3.6 shows a simple process. The main components of the process are the main stream pipe, the flow pipe, the flow sensor, the control valve, the controller and communication the network. Details of these components are discussed below.

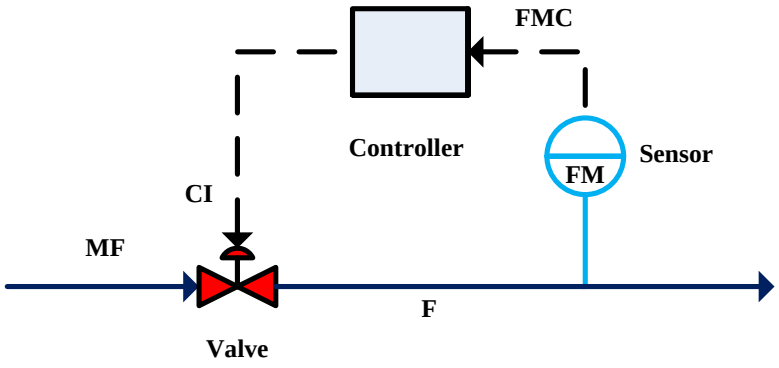

Figure 3.6 A Simple Process System

- Pipes: the diameter of the pipes is 10 cm. The length of both the main stream pipe, MF and the flow pipe, F is 1 m.
- Sensor: the sensor periodically samples and sends data to the controller. The sampling rate is 100 ms.
- Valve: the control valve is driven based. The valve can be throttled from 5% opened all the way to fully opened.
- Controller: the controller's function is to maintain the flowrate through the flow pipe at 40 cm^3/s by throttling the control valve. The controller receives flow measurements, FMC from the sensor, implements the control logic and then sends instructions, CI to the control valve. The controller compares the measured flowrate with the setpoint. If the values differ, the controller calculates the change in the valve position. If they are the same, the valve position is left unchanged. The change in the control valve position is determined using a Proportional-Integral (P-I) control law. The P-I controller used in the NCS example has a proportional gain, K_P of 0.8 and an integral gain, K_I of 1.

MATLAB/Simulink is used to implement a computer model that simulates the process. The computer model is used subsequently to demonstrate the applicability of the DFM technique. The model is shown in Figure 3.7.

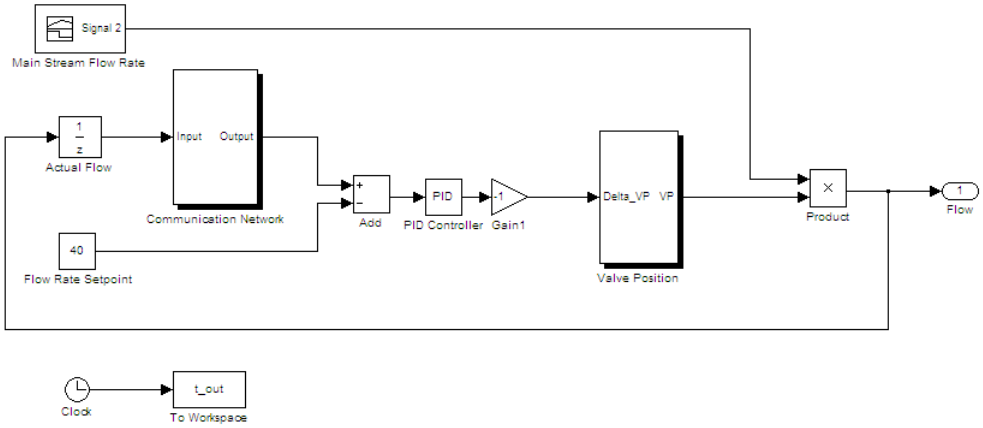

Figure 3.7 Simulink Model of the NCS Example

In the model, the flow in the main stream (before the valve) is initially set at 55 cm^3/sec. At time t = 30 seconds, the flow increases gradually until it reaches 75 cm^3/sec at time t = 32 seconds. The P-I controller attempts to maintain the flow rate at 40 cm^3/sec (after the valve) by adjusting the valve position. The PID controller block was used in the Simulink model, where the deferential gain was set to zero and the proportional and integral gains were those given above. Figure 3.8 presents the sub-model used to calculate the valve position, which is from 5% - 100% opened.

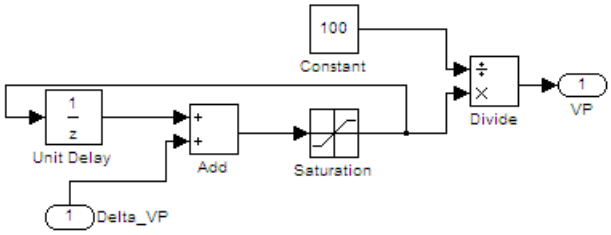

Figure 3.8 Simulink Model for Calculating the Valve Position

The flow in the main stream (before valve), the controlled stream (after the valve) and the valve position are shown in Figure 3.9. In the figure, communication delay is not included (i.e., time delay = 0 seconds). Between 30 and 30.3 seconds, the flow in the flow stream increases to reach a maximum value of 42.5 cm^3/sec and then begins to decrease to meet the flow requirement.

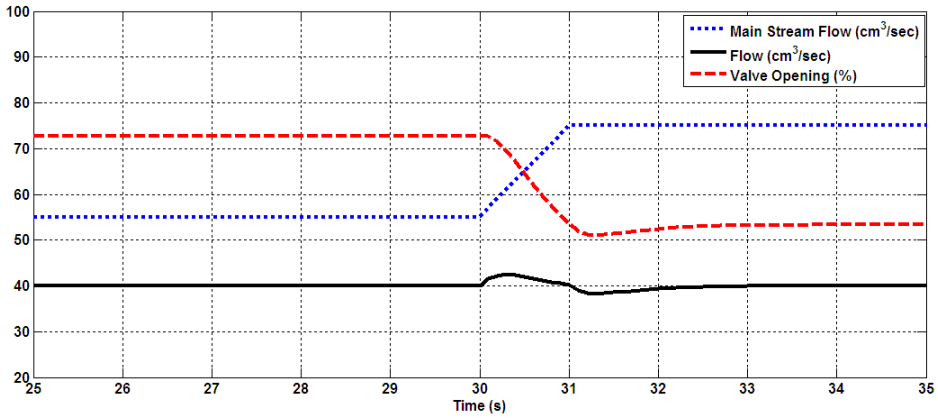

Figure 3.9 Flow vs. Valve Position with No Communication Delay

The next step in the modelling of the process is to include the effect of the communication network. The type of the control network chosen for this example is ControlNet. ControlNet has a data rate of 5Mb/s, bit time of 0.2 µs and minimum message size of 7 bytes (56 bits) (Lian et al., 2001). The parameters assumed in the communication network model are those listed in Table 3.21.

Table 3.21 Parameters Used in Communication Network Model

Parameter	**Value**
Preprocessing time	1 µs
Postprocessing time	1 µs
Message size	240 bits
Bit time	0.2 µs
Waiting time	Random

In this type of network, the random waiting time is bounded. The maximum waiting time is the Token Rotation Time (TRT), which is assumed to be 1.2 seconds. The calculation of the total communication delay is performed using a MATLAB routine, which is included in the Appendix. The calculated value is used in the Simulink model. The communication network effect is introduced between the flow sensor and the controller to represent sensor-to-controller delay. Figure 3.10 shows the block that implements this effect. The effect of communication delay is most evident when process variables change. Thus, in the Simulink model, the delay is introduced when the flow in the main stream starts to change at t = 30 seconds.

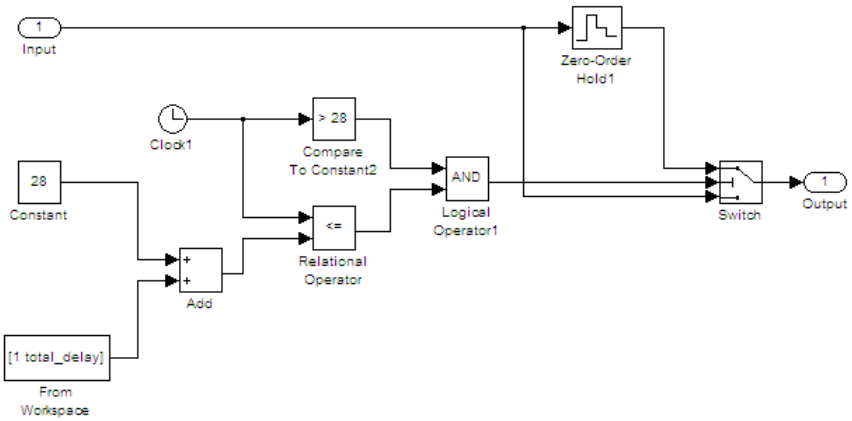

Figure 3.10 Simulink Model of Communication Network Effect

The total time delay generated by the MATLAB routine is 0.8775 seconds. The resulting plots are shown in Figure 3.11. Between 30 and 30.8775 seconds, updated measurement data are not transmitted due to the introduced time delay and they are considered to be lost from the controller's perspective. The loss of data dictates the controller to use the most recent sensor measurement, which was obtained at t = 30 seconds (55 cm^3/sec). Therefore, the controller maintains the position of the valve at approximately 73%.

At time t = 30.8775 seconds (0.8775 seconds after the insertion of the delay), the controller receives the actual flow in the main stream and determines the new valve position in order to maintain the flow at 40 cm^3/sec. Between time t = 30 and 30.8775 seconds, the flow increases significantly since it is not properly controlled. The flow increases to reach a maximum value of 51.65 cm^3/sec and then it begins to decrease. In safety-critical applications, the flow increase of 9.15 cm^3/sec (51.65 – 42.5 cm^3/sec) may cause process instability and may lead to catastrophic events.

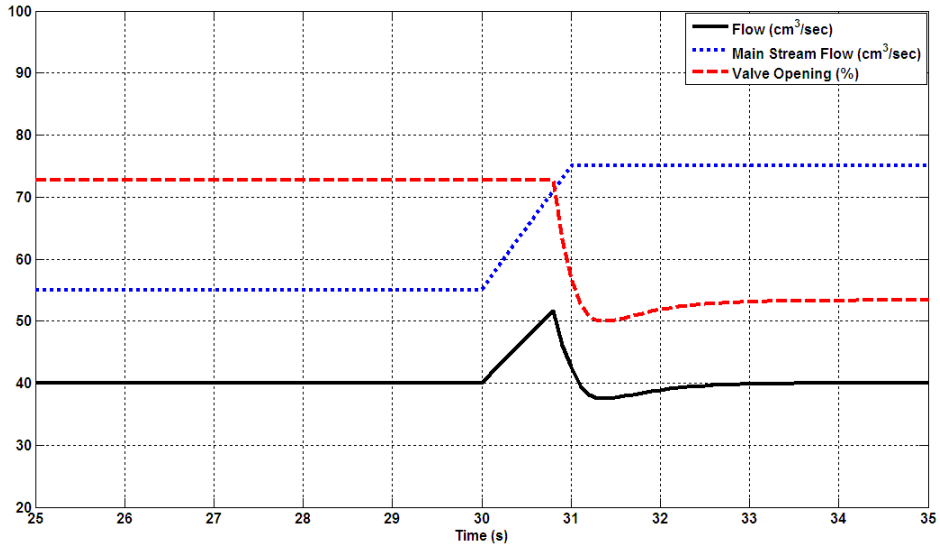

Figure 3.11 Flow vs. Valve Position with Communication Delay

In applying DFM to the networked control system example presented in Figure 3.6, assumptions similar to those used by Guarro et al. (1996) were made with regard to the possible failure modes of system components. The flow sensor can fail high, fail low or fail as-is. The control valve can fail open, fail closed or fail as-is. These multistate representations are included in the DFM model. The DFM model of the system is implemented as shown in Figure 3.12. In the figure, the controller model, C and the

communication models, the communication between sensor and controller, CSC and controller and valve, CCV are represented as black boxes. The controller model is expanded as shown in Figure 3.13. The modelling technique of the controller is similar to that given by Guarro et al. (1996). The model of both communication blocks is similar to that discussed in the previous subsection. The description of the model variables is presented in Table 3.22. In Figure 3.12, transfer box 8 and transfer box 9 represent the control valve and the flow sensor, respectively. Transfer box 10 represents the flow stream pipe. Transition box 11 and transition box 12 represent sensor-to-controller and controller-to-actuator communication, respectively. Transfer boxes 13, 14 and 15 in Figure 3.13 represent the P-I logic that determines the change in the control valve position.

Table 3.22 Description of Process Variables in NCS DFM Model

MF	Main flow stream
F	Flow
FMP	Flow measurement in previous cycle
FSS	Flow sensor status
FM	Flow measurement
FMC	Flow measurement used by the controller
FSP	Flow setpoint used by the controller
FE	Flowrate error term used by the controller
FEP	Flowrate error term in previous cycle
IFE	Integral control term for flowrate
IFEP	Integral control term for flowrate in previous cycle
CD	Controller decision
CI	Controller instruction to the valve
DFV	Change in valve opening
FVP	Valve opening in previous cycle
FVS	Valve status
FV	Valve opening
CSC	Communication between sensor and controller
CCV	Communication between controller and valve

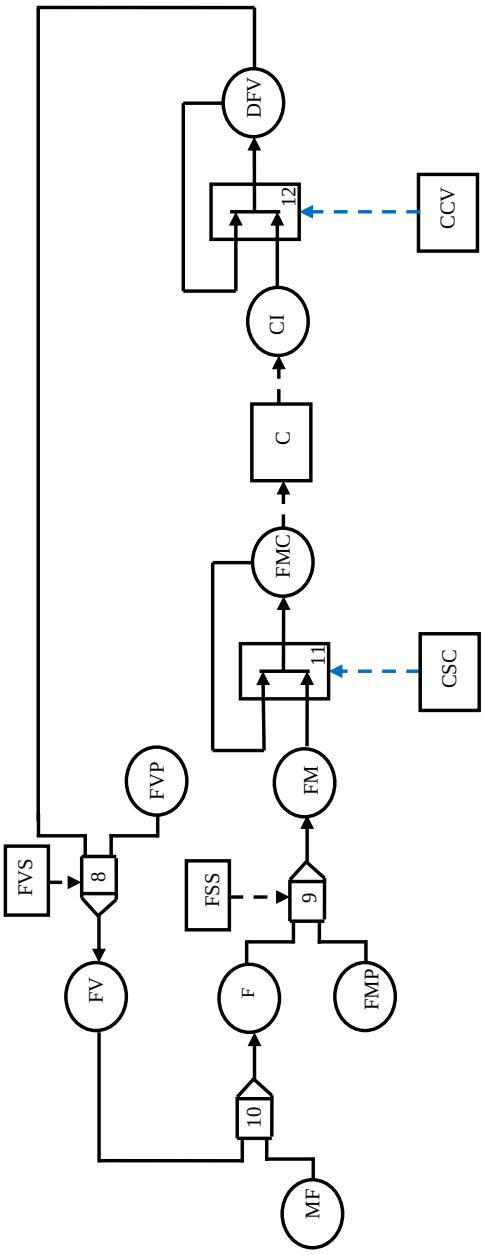

Figure 3.12 DFM Model of Networked Control System Example

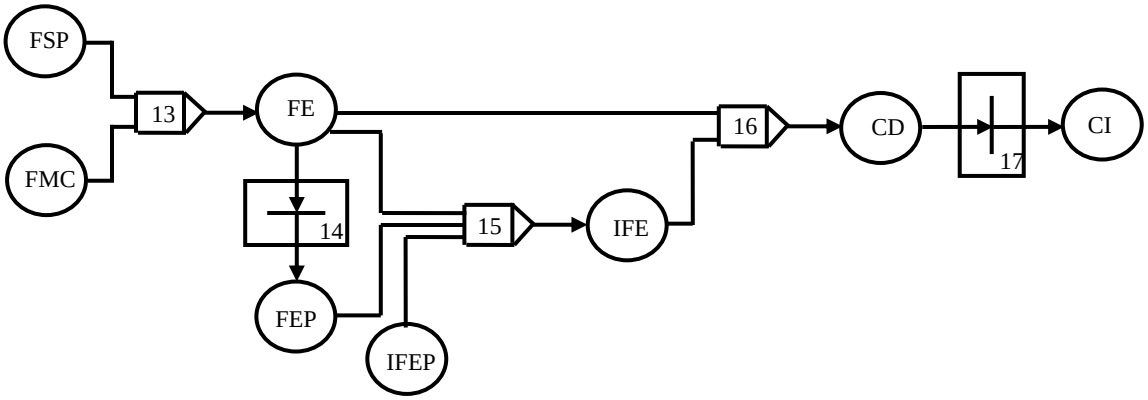

Figure 3.13 DFM Model of Controller Block in NCS DFM Model

The nodes in the DFM model are discretized into finite number of states. The discretization scheme is shown in Tables 3.23 – 3.30. The tables demonstrate the knowledge about the system and the assumptions regarding the failure modes of the components.

Table 3.23 Discretization of Main Stream Flow (MF), Flow (F), Flow Measurement in Previous Cycle (FMP), Flow Measurement (FM) and Flow Measurement Used by Controller (FMC)

0	0 - 40 cm^3/s
1	40 cm^3/s
2	40 - 80 cm^3/s

Table 3.24 Discretization of Flow Sensor Status (FSS)

0	Failed low
1	Normal
2	Failed high
3	Failed as-is

Table 3.25 Discretization of Flow Setpoint (FSP)

0	40 cm^3/s

Table 3.26 Discretization of Flowrate Error (FE) and Flowrate Error in Previous Cycle (FEP)

0	0 cm^3/s
1	0 to +40 cm^3/s
2	-40 cm^3/s to 0

Table 3.27 Discretization of Integral Control Term for Flowrate (IFE) and Integral Control Term in Previous Cycle (IFEP)

0	0 cm^3/s
1	0 to 200 cm^3/s
2	-200 to 0 cm^3/s

Table 3.28 Discretization of Controller Decision (CD), Controller Instruction to Valve (CI) and Change in Valve Opening (DFV)

0	Open by some percentage
1	No change
2	Close by some percentage

Table 3.29 Discretization of Valve Opening (FV) and Valve Opening in Previous Cycle (FVP)

0	5-40% open
1	40-60% open
2	60-100% open

Table 3.30 Discretization of Valve Status (FVS)

0	Failed open
1	Normal
2	Failed closed
3	Failed as-is

The mappings between the process variables are presented in the decision tables, Tables 3.31 – 3.38. The tables were constructed based on logical and dynamical interaction between process parameters. In the tables, the item '-' indicates a 'does not matter' entry.

It can be noted from Table 3.38 that the representation of the integral of flow error used by the controller, IFE, is not taken into making the decision for T16. This is because the limited number of states in both node variables, FE and IFE. Thus, a decision table for T15 is left unimplemented.

Table 3.31 Decision Table for T8 in NCS DFM Model

Input			Output
FVS	DFV	FVP	FV
0	-	-	2
2	-	-	0
3	-	0	0
3	-	1	1
3	-	2	2
1	0	0	1
1	0	1	2
1	0	2	2
1	1	0	0
1	1	1	1
1	1	2	2
1	2	0	0
1	2	1	0
1	2	2	1

Table 3.32 Decision Table for T9 in NCS DFM Model

Input			Output
FSS	F	FMP	FM
0	-	-	0
2	-	-	2
3	-	0	0
3	-	1	1
3	-	2	2
1	0	-	0
1	1	-	1
1	2	-	2

Table 3.33 Decision Table for T10 in NCS DFM Model

Input		Output
FV	MF	F
0	0	0
0	1	0
0	2	1
1	1	0
1	2	1
1	0	0
1	1	1
1	2	2

Table 3.34 Decision Table for T11 in NCS DFM Model

Input			Output
CN	FM	FMC^{--}	FMC
0	-	0	0
0	-	1	1
0	-	2	2
1	0	-	0
1	1	-	1
1	2	-	2

Table 3.35 Decision Table for T12 in NCS DFM Model

Input			Output
CN	CI	DFV^{--}	DFV
0	-	0	0
0	-	1	1
0	-	2	2
1	0	-	0
1	1	-	1
1	2	-	2

Table 3.36 Decision Table for T13 in NCS DFM Model

Input		Output
FSP	FMC	FE
0	0	2
0	1	0
0	2	1

Table 3.37 Decision Table for T14 in NCS DFM Model

Input	Output
FE	FEP
0	0
1	1
2	2

Table 3.38 Decision Table for T16 in NCS DFM Model

Input		Output
FE	IFE	CD
0	-	1
1	-	2
2	-	0

3.3 Model Analysis and Results

The DFM Software Toolset can be used to implement and analyze the DFM model. The toolset allows inductive and deductive analysis. Once the DFM model is implemented in the toolset and nodes states and decision tables are specified, timed prime implicants can be obtained by analyzing the implemented model. Alternatively, a timed fault tree can be constructed manually to provide a visual representation of the combination of basic events that lead to the top event.

In this section, the derivation of both the timed prime implicants and timed fault tree is demonstrated. The prime implicants technique is used for analysis of the communication network model explained in Section 3.1. The fault tree technique is used to demonstrate the analysis of the NCS example explained in Section 3.2.

The prime implicants for the unavailability of communication between control systems, CN = 0 are determined using the DFM Software Toolset. There are 5 prime implicants that can lead to the top event, as shown in Figure 3.14.

```
For the top event:
At time 0  ,    CN = 0     (performance affected)

There are 5 prime implicants

Prime Implicant #1
     At time 0  ,  WAIT = 1     (Tau_wait1-Tau_wait2)

Prime Implicant #2
     At time 0  ,   BIT = 1     (Tau_bit1 - Tau_bit2)      AND
     At time 0  ,    MS = 1     (ms1 - ms2)

Prime Implicant #3
     At time 0  ,   NTA = 1     (Unavailable)

Prime Implicant #4
     At time 0  ,  DHSS = 1     (Unavailable)

Prime Implicant #5
     At time 0  ,  SHSS = 1     (Unavailable)
```

Figure 3.14 Prime Implicants of Communication Unavailability in NCS

The prime implicants provided by the DFM can be used to enhance systems' performance. For example, for the NCS example given above, a delay higher than or equal to 100 ms is considered unacceptable. It makes the communication unreliable and leads to system instability. In order to reduce the delay below the unacceptable level, the prime implicants can be used in making decisions to modify the design of the networked control system. Based on Prime Implicant #1 in Figure 3.14, excessive waiting time is one of the factors that can affect the performance of the networked control system. The waiting time is dependent on the control network type and the configuration of the network nodes. The reduction of the waiting time can significantly enhance the

performance of the control system. Figure 3.15 shows the plots of the flow and the valve position for a waiting time of 80 ms. Between 30 and 30.3 seconds, the flow increases to reach a maximum value of 42.5 cm^3/sec. This is very similar to the results obtained for the case where no communication delay is introduced. It can be noted in Figure 3.15 that the insertion of 80 ms waiting time does not affect the performance of the control system and the controlled process. Prime Implicant #2 suggests that the combination of large bit time and message size is another factor that leads to the top event. The bit time is dependent on the network type and cannot be changed. The message size can be varied by the system designer. In the example given above, the bit time is 0.2 μs and the message size is 240 bits, as previously listed in Table 3.21. The two parameters are considered small since they result in a transmission time delay of 48 μs. Thus, for this example, selecting a different network type or reducing the message size will not enhance the performance of the system. When using DeviceNet as the communication network, the bit time is 2 μs and the minimum message size is 47 bytes, which is equal to 376 bits (Lian et al., 2001). Those parameters can lead to a transmission time delay that may affect systems' performance. It is therefore recommended to pay additional attention to determining the message size used when deploying networks such as DeviceNet. Based on Prime Implicant #3, 4 and 5, the availability and functionality of the communication link and nodes' processors are severe factors that affect communication reliability. Thus, the selection of those systems must receive careful consideration.

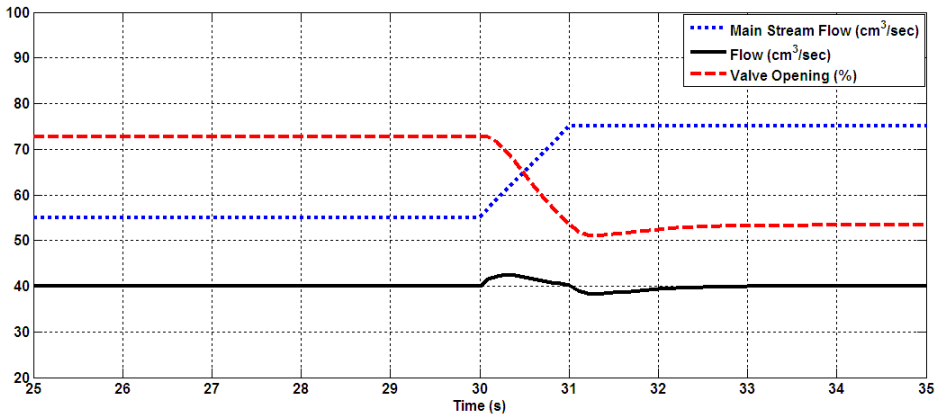

Figure 3.15 Flow vs. Valve Position with Reduced Communication Delay

In addition, the DFM model can be used for inductive analysis. This assists in verifying designs and identifying potential threats to systems instability. For example, the designer can use the DFM Software Toolset to investigate the consequences of having the following basic events: waiting time in the range τ_{WAIT1} - τ_{WAIT2}, bit time of τ_{BIT1} - τ_{BIT2}, postprocessing time of τ_y, etc. or other combinations of events.

The next step is to analyze the implemented DFM model of the NCS example. A timed fault tree is derived to perform the analysis. Given reliability data of basic events (e.g., unavailability of communication link, etc.), the reliability of the top event can be calculated. Timed prime implicants can also be generated either from the implemented fault tree or using the DFM Software Toolset. The analysis allows the identification of areas of potential improvement to minimize risk and enhance safety. The timed fault tree for the top event 'flow measurement is above 40 cm^3/s' is presented here as an example. Fault trees can be derived for any other event of interest (e.g., flow is below 40 cm^3/s, communication will affect performance, etc.). In order to derive the timed fault tree, the

decision tables are used. A “does not matter” table entry is not included in the fault tree since it does not affect the occurrence of events.

The implemented timed fault tree is composed of several parts, as shown in the figures below. Based on Table 3.32, the condition ‘flow measurement is above 40 cm^3/s (FM = 2)’ occurs if any of the following conditions is met:

{{FSS = 1} AND {F = 2}},

{FSS = 2}, or

{{FSS = 3} AND {FMP = 1}}.

Part 1 of the fault tree for the top event is shown in Figure 3.16. Based on Table 3.33, the flow is above 40 cm^3/s (F = 2) if the following condition is met:

{{FV = 2} AND {MF = 2}}.

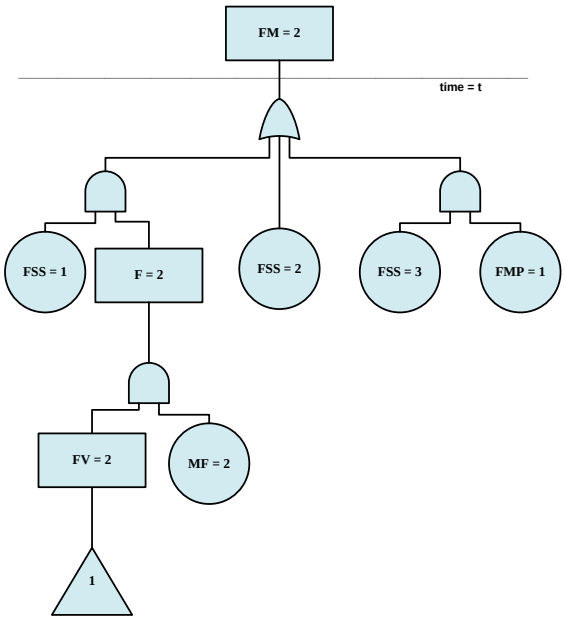

Figure 3.16 Timed Fault Tree Part 1

Figure 3.17 shows the partial fault tree for the event ‘FV = 2’. Based on Table 3.31, the event occurs if any of the following conditions is met:

{FVS = 0},

{{FVS = 1} AND {DFV = 0} AND {FVP = 1}},

{{{FVS = 3} AND {{FVP = 2}}, or

{{FVS = 1} AND {FVP = 2}} AND {{DFV = 0} OR {DFV = 1}}.

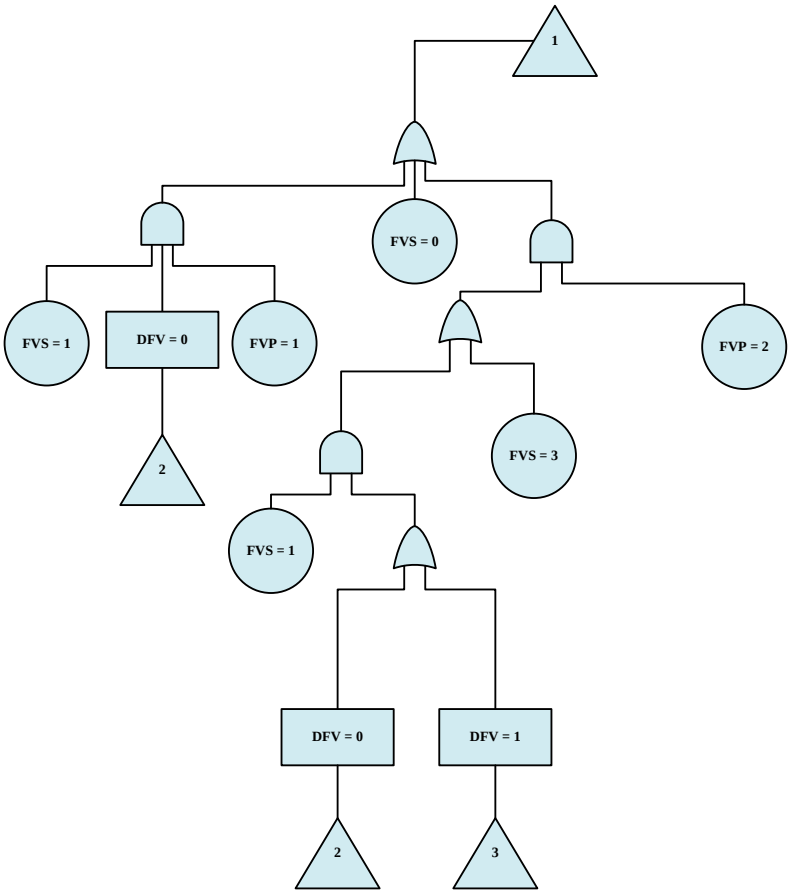

Figure 3.17 Timed Fault Tree Part 2

Based on Table 3.35, the event ‘DFV = 0’ occurs if any of the following conditions is met:

{{CN = 0} AND {DFV^{--} = 0}}, or

{{CN = 1} AND {CI = 0}}.

The event ‘DFV = 1’ occurs if:

{{CN = 0} AND {DFV^{--} = 1}}, or

{{CN = 1} AND {CI = 1}}.

The corresponding partial fault trees are shown in Figures 3.18 and 3.19, respectively. The remaining parts of the fault tree can be derived by following a similar technique. The fault tree is considered complete once basic events are reached for all branches, such as FVS = 0 in Figure 3.17. The time dependency shown in Figures 3.18 and 3.19 is useful for observing the time for the occurrence of the combination of events.

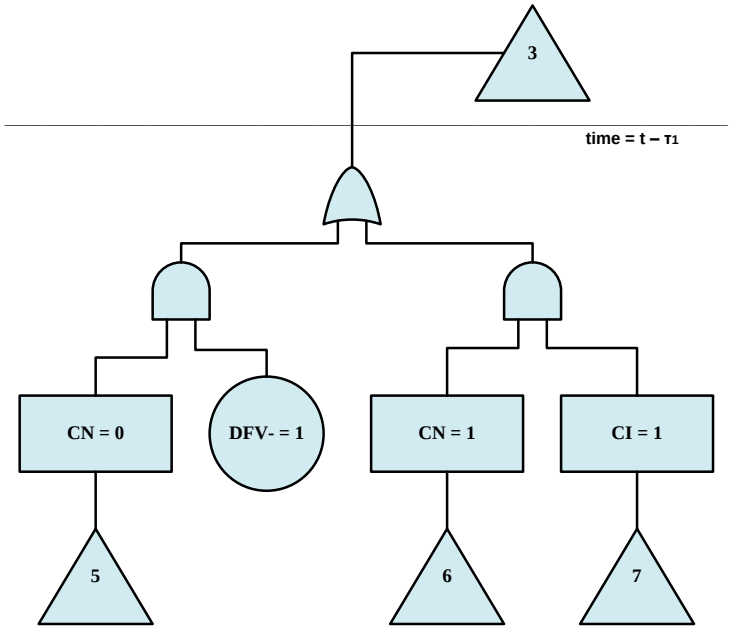

Figure 3.18 Timed Fault Tree Part 3

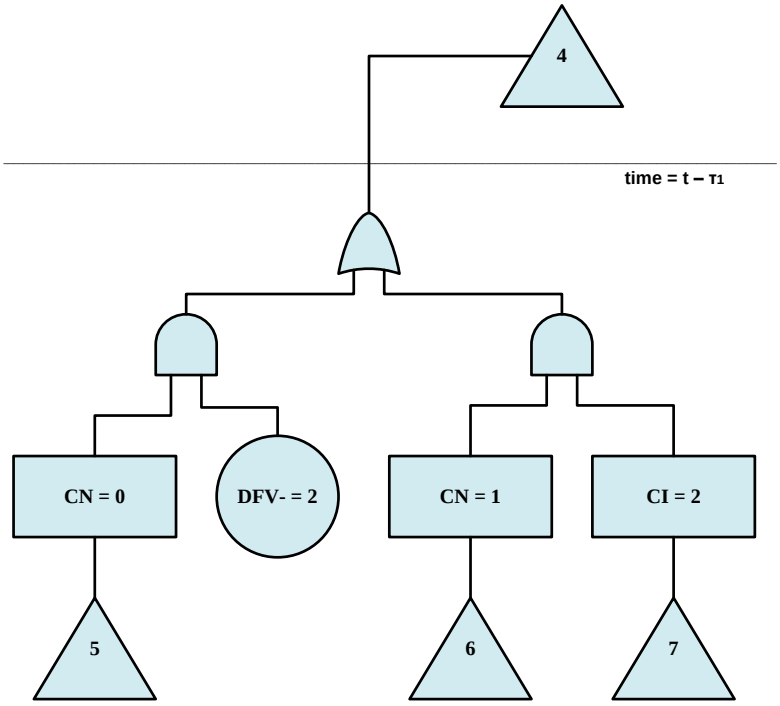

Figure 3.19 Timed Fault Tree Part 4

In conclusion, the dynamic flowgraph methodology can be used to evaluate the performance of physically existing systems and potential systems design. In evaluating physically existing systems, the dynamic flowgraph methodology can be used to model the behaviour of the system. By selecting an event of interest, the combination of events or conditions that lead to the top event can be determined using deductive analysis. This can be accomplished by generating the timed prime implicants for the DFM model using the DFM Software Toolset. Also, a timed fault tree can be constructed manually to provide a visual representation of the combination of basic events that lead to the top event. Knowledge of the combination of events is useful in determining the components with major contribution to systems reliability. This can assist in determining maintenance strategy and inspection frequency.

In evaluating the design of systems prior to their implementation, similar analysis can be performed as explained above (derivation of timed prime implicants and timed fault trees) to determine the combination of events that lead to the top event of interest. Reliability data of basic events can be used to determine the reliability of the event of interest. This can demonstrate whether the system meets the reliability requirements. In addition, it can be used to study the use of various components to determine the most potential candidate. This provides the capability of selecting components that will meet the reliability requirements in order to minimize systems risk.

The dynamic flowgraph methodology can also be used to predict systems' behaviour using inductive analysis. This can be performed by selecting a basic event and investigating the consequences of its occurrence. This helps in identifying the areas that should receive careful attention in their components selection and maintenance strategies determination.

The methodology is found to meet the requirement given in Section 2.2.5.2 for establishing a modelling framework for the reliability of networked control systems. The modelling methodology captured the behaviour and interaction of the three components of a NCS (i.e., hardware, software and communication systems). The methodology can be applied to model any process and any type of communication network protocol by specifying the states of the basic events. In addition to the availability of systems, their degradation in performance was included in the model. The model incorporated time dependency and multi-state representation.

3.4 Chapter Summary

In this chapter, the modelling of the behaviour and reliability of communication networks in networked control system applications was presented using the dynamic flowgraph methodology. Also, the applicability of the method to model networked control systems was demonstrated. A networked control system example was specified and analyzed. The deductive analysis was shown using derived timed prime implicants and a timed fault tree.

CHAPTER 4

APPLICATION OF DFM TO COPPER-CHLROINE THERMOCHEMICAL CYCLE

In this chapter, the application of DFM to the copper-chlorine thermochemical cycle is demonstrated. An overview of nuclear-based hydrogen production methods is given while focusing on the Cu-Cl thermochemical cycle.

4.1 Introduction to Nuclear-Based Hydrogen Production

As the demand for hydrogen usage increases, methods for its large-scale production must be available. Nuclear energy can become a primary energy source for hydrogen production plants. Yildiz & Kazimi (2006) presented various possibilities to produce hydrogen using Nuclear Power Plants (NPPs). Those are:

1. The use of the generated electricity for liquid water electrolysis.
2. The use of both the generated high temperature heat and the electricity for high temperature steam electrolysis.
3. The use of the generated heat for thermochemical water splitting processes.

Although water electrolysis is a commercially proven technology, it is an expensive method for centralized hydrogen production due to its low energy efficiency. On the other hand, in thermal processes, a series of thermally assisted chemical reactions occur

to release hydrogen from hydrocarbons or water. Some of the promising options include Steam Methane Reforming (SMR), Sulfur-Iodine (S-I), Calcium-Bromine-Iron (UT-3) and Copper-Chlorine (Cu-Cl) thermochemical cycles. In SMR, hydrogen is produced from hydrocarbons. Although it is the most economical and widespread hydrogen production method, it is not favourable for a long-term hydrogen economy due to its associated emissions of carbon dioxide (Yildiz & Kazimi, 2006). The S-I and UT-3 thermochemical cycles were found to have the highest commercialization potential and practical applicability to nuclear heat sources. However, some endothermic reactions are necessary to occur at very high temperatures in both S-I (830 – 900 ˚C) and UT-3 (730 ˚C) cycles (Yildiz & Kazimi, 2006). The Cu-Cl thermochemical cycle is emerging as another promising method for large-scale hydrogen production for its offering of many advantages over other types of thermochemical water splitting processes.

4.2 The Copper-Chlorine Thermochemical Cycle

A collaborative effort has taken place by Argonne National Laboratories, Atomic Energy of Canada Limited, University of Ontario Institute of Technology (UOIT) and other partners to design the Cu-Cl thermochemical cycle for hydrogen production. In the Cu-Cl cycle, water is decomposed into hydrogen and oxygen through intermediate copper and chlorine compounds with a highest heat temperature input of 530 ˚C (Rosen, Naterer, Sadhankar, & Suppiah, 2006). The relatively low heat temperature input requirement allows the Cu-Cl cycle for future linkage with a wider range of NPP choices. This factor makes the Cu-Cl cycle more advantageous over other thermochemical cycles for hydrogen production. More specifically, the heat input at temperatures less than 530˚C

make the cycle suitable for coupling with Canada's Generation IV reactor, Super-Critical Water Reactor (SCWR), which is based on the proven CANDU technology (Wang, Naterer, & Gabriel, 2008). The cycle offers other key advantages that include reduced demands on materials of construction, minimal solid handling and the requirement of inexpensive raw material. Further, its reactions can proceed nearly to completion without significant side reactions and the cycle can utilize low-grade waste heat from power plants for several thermal processes within the cycle (Wang et al., 2008). These advantages demonstrate the potential of the Cu-Cl cycle to become a sustainable method for large-scale hydrogen production.

Rosen et al. (2006) presented a conceptual layout of the Cu-Cl thermochemical cycle, as shown in Figure 4.1. The cycle consists of five interconnected reaction vessels, or reactor units, with intermediate heat exchangers. Five reactions occur in the cycle according to those recorded in Table 4.1 where each reaction is achieved in a reactor unit. The five reactor units are: hydrogen reactor, electrochemical cell, spray drying unit, fluidized bed and oxygen reactor.

Table 4.1 Reaction Steps of Copper-Chlorine Cycle (Rosen et al., 2006)

Step	**Reaction**	**Temperature Range (˚C)**
1	$2Cu\,(s) + 2HCl\,(g) \rightarrow 2CuCl\,(l) + H_2\,(g)$	430-475
2	$2CuCl\,(s) \rightarrow 2CuCl\,(aq) \rightarrow CuCl_2\,(aq) + Cu\,(s)$	Ambient (electrolysis)
3	$CuCl_2\,(aq) \rightarrow CuCl_2\,(s)$	<100
4	$2CuCl_2\,(s) + H_2O\,(g) \rightarrow CuO*CuCl_2\,(s) + 2HCl\,(g)$	400
5	$CuO*CuCl_2\,(s) \rightarrow 2CuCl\,(l) + 1/2O_2\,(g)$	500

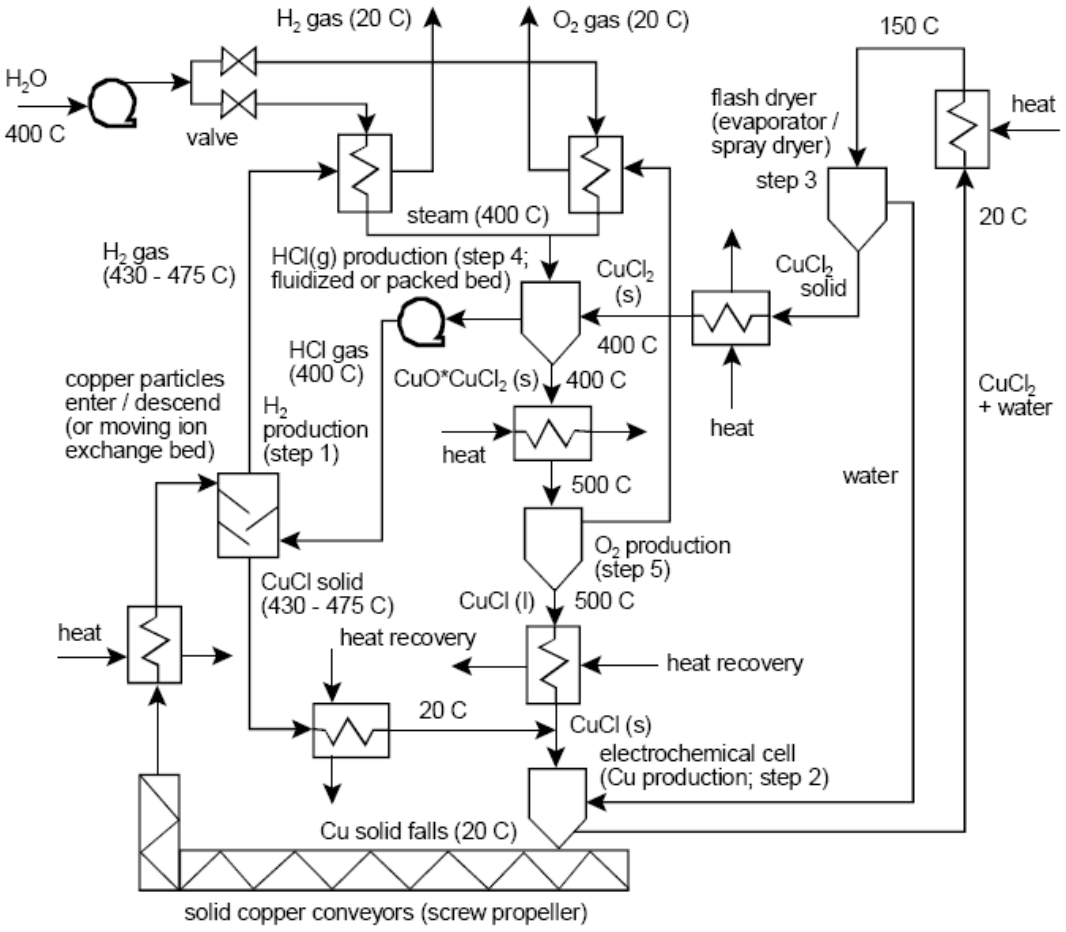

Figure 4.1 Conceptual Layout of Copper-Chlorine Cycle (Rosen et al., 2006)

In Step 1, copper particles and HCl gas enter a hydrogen production reactor to react and generate CuCl solid and H_2 gas. A conceptual layout of the auxiliary equipment for this step is discussed in Section 4.5. Rosen et al. (2006) indicated that Step 2 of the cycle may be implemented by means of an electrochemical cell. The CuCl solid produced in the hydrogen reactor along with that from the oxygen reactor (Step 5) are used in the electrochemical cell reactor (Step 2) to produce aqueous $CuCl_2$ and solid copper particles. The solid copper particles exiting from the electrochemical cell are then collected and transported by a conveyer to the hydrogen reactor. Naterer, Daggupati, Marin, Gabriel, & Wang (2008) mentioned that the aqueous cupric chloride, $CuCl_2$ of the electrolysis step is

necessary to be dried to provide particles that are subsequently reacted to produce copper oxychloride, $CuO*CuCl_2$, hydrogen chloride gas, HCl, as well as hydrogen. The aqueous $CuCl_2$ dried in the flash dryer unit is used for supply of solid $CuCl_2$ to the fluidized bed reactor unit (Step 4). In the fluidized bed, the solid $CuCl_2$ and high temperature steam react to produce solid $CuO*CuCl_2$ and HCl gas. The HCl gas is used in the hydrogen reactor unit and the solid $CuO*CuCl_2$ is supplied to the oxygen reactor unit (Step 5) to produce liquid CuCl and oxygen gas.

In order to apply the DFM to the modelling of the hydrogen production plant, a preliminary design or knowledge of the control system must be available. In the following subsections, the architecture and communication structure of the networked control system for the Cu-Cl thermochemical cycle are provided. The hydrogen reactor unit is used as a case study to demonstrate the detailed design of the control system by defining the configuration of the instrumentation and control systems.

4.3 Networked Control System Design for the Hydrogen Plant

In the Cu-Cl thermochemical cycle, heat input is used to decompose water into hydrogen and oxygen through intermediate copper and chlorine compounds. The conceptual layout of the Cu-Cl thermochemical cycle presented in Figure 4.1 is used as the basis for the design of the networked control system. As previously mentioned, the cycle consists of five interconnected reaction steps, i.e., hydrogen reactor, electrochemical cell, spray drying unit, fluidized bed and oxygen reactor.

In order to regulate and monitor the operation of the hydrogen production plant, instrumentation and control systems must be deployed. The I&C systems drive the reactions to occur in proper sequence while maintaining safe and reliable plant operation. In this section, the description of a NCS design for the hydrogen production plant is provided.

4.3.1 Architecture of the Control System

The design of the networked and distributed control systems for the hydrogen plant is based on a functional distribution scheme. In the scheme, the control functions are divided into logical chunks assigned to different control partitions. The architecture of the DCS consists of one Plant Display System (PDS) and five partitions, as shown in Figure 4.2 (Al-Dabbagh & Lu, 2009). Each partition is responsible for the control of one of the reactor units. The PDS allows user intervention through an HMI system. It offers the capability of displaying alarms and transients of the hydrogen production plant and allowing control room operators to specify setpoints and control commands.

4.3.2 Communication Structure of the Control System

The communication structure of the DCS proposed in Figure 4.2 has three levels: information network, control network and field network. Figure 4.3 presents an upper-level communication diagram for the hydrogen production plant with the Cu-Cl thermochemical cycle.

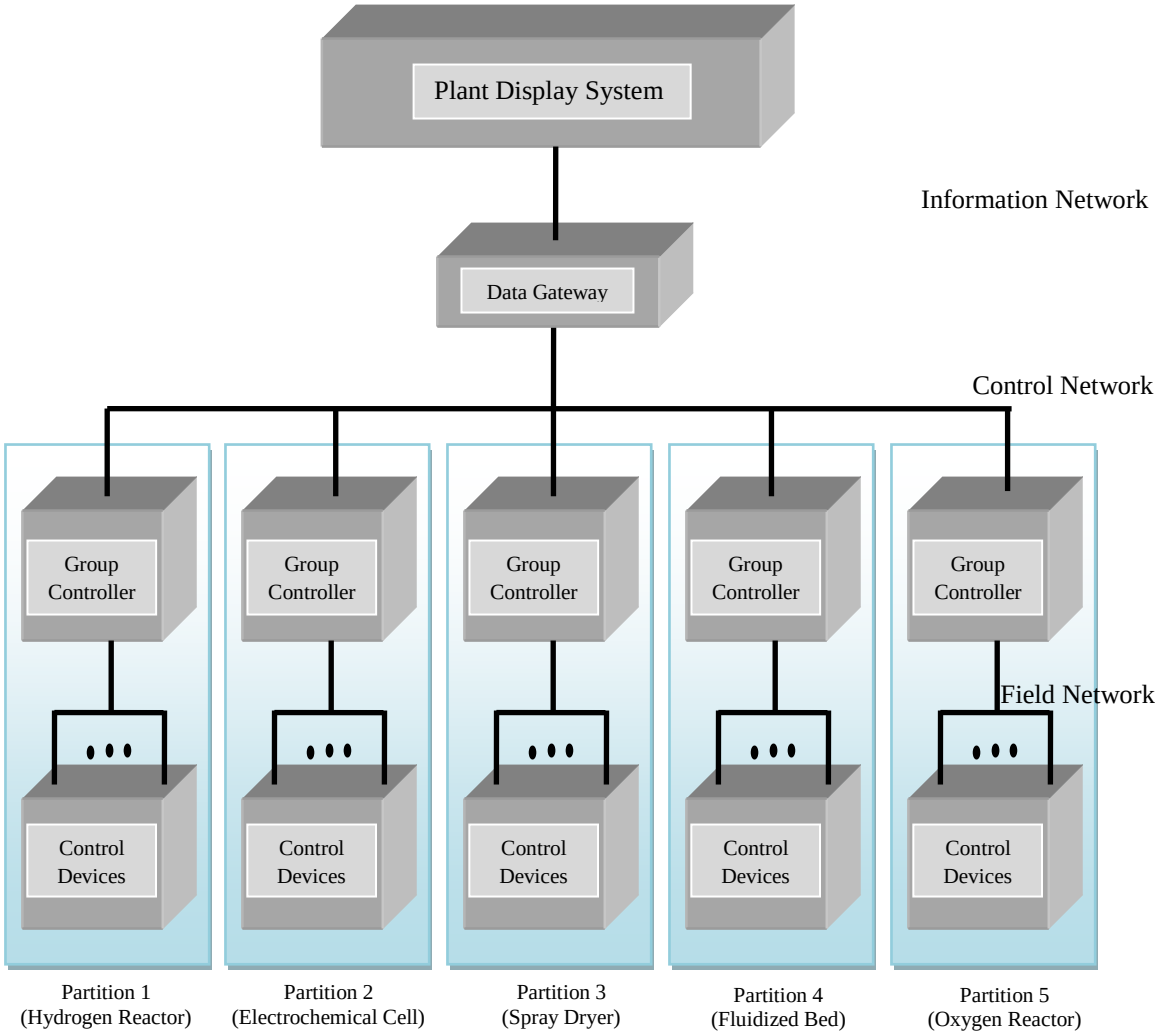

Figure 4.2 Architecture of Networked Control System for Cu-Cl Cycle

In figure 4.3, the type of information exchanged between the partitions and the PDS is presented. The PDS communicates with the group controller of each partition using the information network through a data gateway. The data gateway supports communication interface between two different communication protocols. It is used to prevent fault propagation from information network (non-safety system) to the control network (safety-system) (Kim et al., 2000). TCP/IP network protocol is proposed for implementing the information network since it is considered a non-safety system and

does not need a highly reliable communication network. The role of the PDS is to monitor the production of hydrogen and oxygen gases produced in reactor units 1 and 5, respectively. It provides the following instructions to the control partitions:

- Plant start command
- Plant shutdown command
- Target hydrogen (i.e., the required amount of hydrogen production)

Given the above instructions, the partitions govern the plant to meet the hydrogen demand. Each partition of the DCS is responsible for achieving one of the five reactions in Table 4.1. The group controller of each partition is responsible for executing complex control logic, and monitoring device controllers in the respective reactor unit. The group controller of Partition 1 adjusts the hydrogen production rate while sending its copper and HCl gas demands to the group controller of partition 2 and 4, respectively. The group controller of Partition 2 then communicates with the group controller of Partition 1 and Partition 5 to request the necessary amount of CuCl inflow. The group controller of Partition 4 communicates with the group controller of Partition 2 to request the necessary amount of $CuCl_2$ solid. The group controller of Partition 3 requests the necessary amount of $CuCl_2$ aqueous from the group controller of Partition 2. Finally, the group controller of Partition 5 communicates with the group controller of Partition 4 the necessary amount of $CuO*CuCl_2$ production.

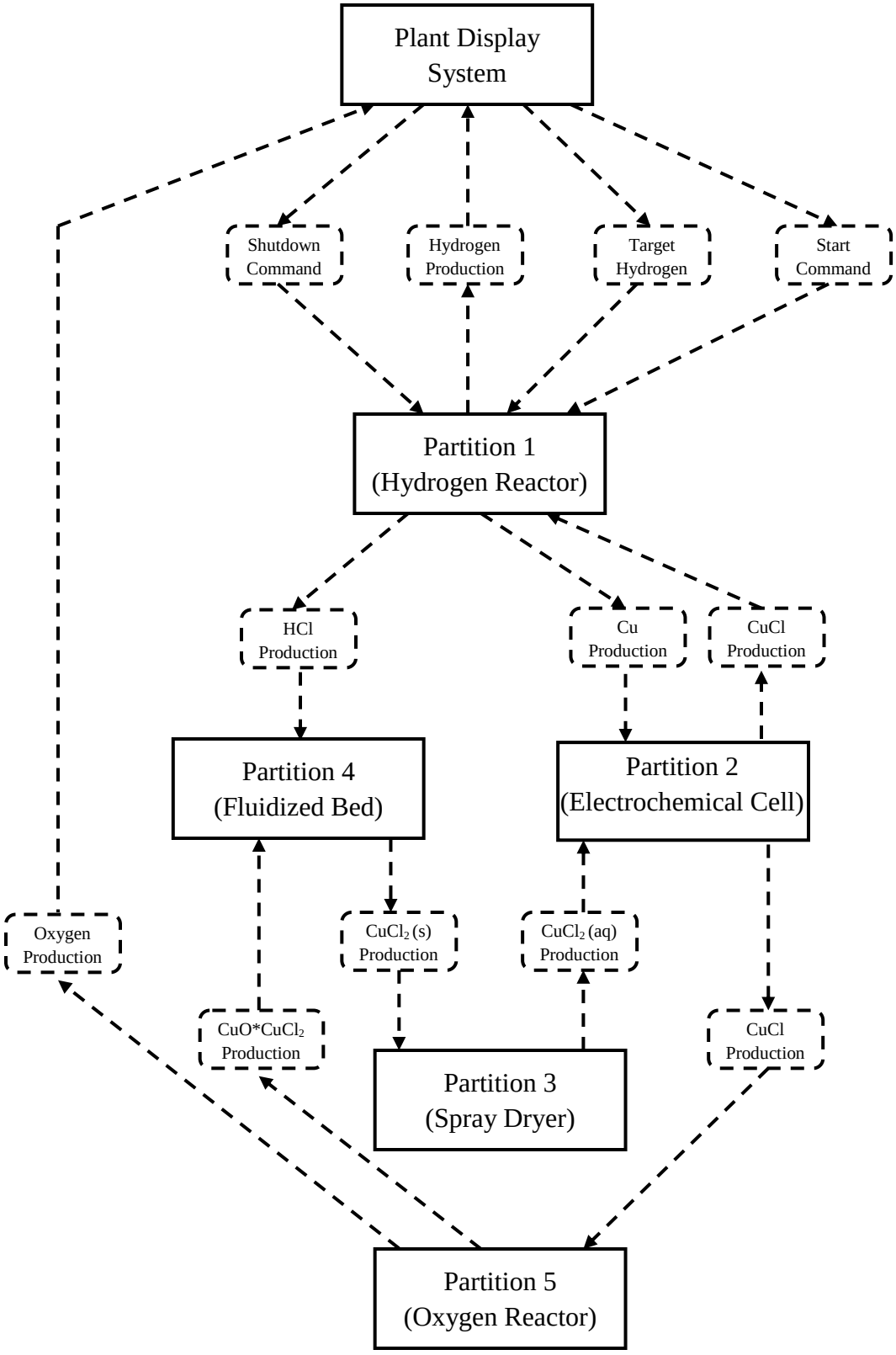

Figure 4.3 Upper-Level Communication Diagram for Cu-Cl Cycle DCS

The group controllers communicate with each other using a control network. Important characteristics which the control network possesses are high reliability, high data transmission speed and maintainability. In the literature, several Ethernet-based network protocols were proposed to satisfy the strict requirements of safety-critical systems, such as those used in nuclear power plants. For example, the use of a Control Network Interface Card (CNIC) based on the microprocessor MPC8260 with Fast Ethernet controller was suggested by Kim et al. (2000). A new high speed real-time network called Plant Instrumentation and Control Network+ (PICNET+) was recommended by Park et al. (2000). A network called Ethernet based Real-Time Control Network (ERCNet) which uses ring topology, token passing mechanism and physical media of Fast Ethernet was proposed by Choi (2002). The control network in the hydrogen production plant utilizes a Fast Ethernet based technology: Gigabit Ethernet. Gigabit Ethernet is an extension of original Ethernet technology with faster data transmission speed of 1 Gbps. It employs all specifications of original Ethernet such as the support of CSMA/CD (Carrier Sense Multiple Access with Collision Detection) mechanism. The mechanism can resolve contention on the communication medium (Lian et al., 2001). For data transmission, a node listens to the network before transmission. If the network is busy, the node waits until the network is idle. Otherwise, it transmits its data packet immediately. If two nodes find the network idle and decide to transmit their packets simultaneously, the packets of the two nodes will collide and their content will be corrupted. Subsequently, the nodes wait a random length of time before retransmission. The maximum number of allowable transmission attempts is 16.

The device controllers within each partition are responsible for executing simple logic and control of field devices such as valves, motors, pumps, compressors, etc. Device controllers of one partition can communicate with each other to acquire necessary data for making control decisions. Within one partition, the device controllers can also communicate with their group controller to exchange data and instructions. Many commercially available fieldbus technologies such as Profibus, DeviceNet, Foundation Fieldbus, etc. can be used for implementing a field network. Foundation Fieldbus (FF) H1 (Kadri, 2006) is proposed for selection as the field network in the hydrogen plant. Its use can result in reduction of wiring, decrease in maintenance costs and ability of online addition of field device. Further, its ability to connect different devices from different vendors makes the network interoperable. Its data transfer rate is 31.25 Kbps and can form either a bus or tree topology. It uses a single twisted pair wire with a maximum length of 1900 m. The maximum number of field devices that one network segment can accommodate is 32. However, if repeaters are used, the network can accommodate up to 240 field devices (Kadri, 2006).

4.4 Dynamic Flowgraph Methodology Modelling of the Hydrogen Plant

This section demonstrates the use of dynamic flowgraph methodology in modelling the dynamical and logical interactions between the reactor units in the Cu-Cl cycle. The model represents the relationships between the process variables of the reactors and the communication between reactors. Figure 4.3 is used as the basis for the modelling of the hydrogen production plant. The model is shown in Figure 4.4. In the model, the term T_x and R_x of the model nodes denote the transmission and receive of the corresponding

variable, respectively. The process nodes are described in Table 4.2. The boxes that represent the control partitions, the PDS and the communication network influence are expanded to contain a DFM model that emulates the behaviour of the corresponding system. The DFM model of each box is used to produce output variables which are used as inputs to the DFM models of the other boxes.

Table 4.2 Description of Variables of Hydrogen Plant DFM Model

$P1_a$	Cu Production Requirement
$P1_b$	HCl Production Requirement
$P1_c$	H_2 Production
$P2_a$	CuCl Production Requirement from Partition 1
$P2_b$	CuCl Production Requirement from Partition 5
P4	$CuCl_2$ Solid Production Requirement
P3	$CuCl_2$ Aqueous Production Requirement
$P5_a$	$CuO*CuCl_2$ Production Requirement
$P5_b$	Oxygen Production
HT	H_2 Target

The conditional edge of each transition box is connected to the communication network model. The model represents the effect of the communication network on the transmission of signals between the group controllers. This model is similar to that implemented in the previous chapter. The decision tables for each transition box can be determined when the relationships between the process variables are specified. In the model, it is assumed that all controllers and transmitted messages share similar characteristics (i.e., processors, message size, bit time, etc.). Given the complete DFM model with decision tables, timed prime implicant and timed fault trees can be generated for any event of interest in the hydrogen production plant with Cu-Cl cycle, whether desirable or undesirable.

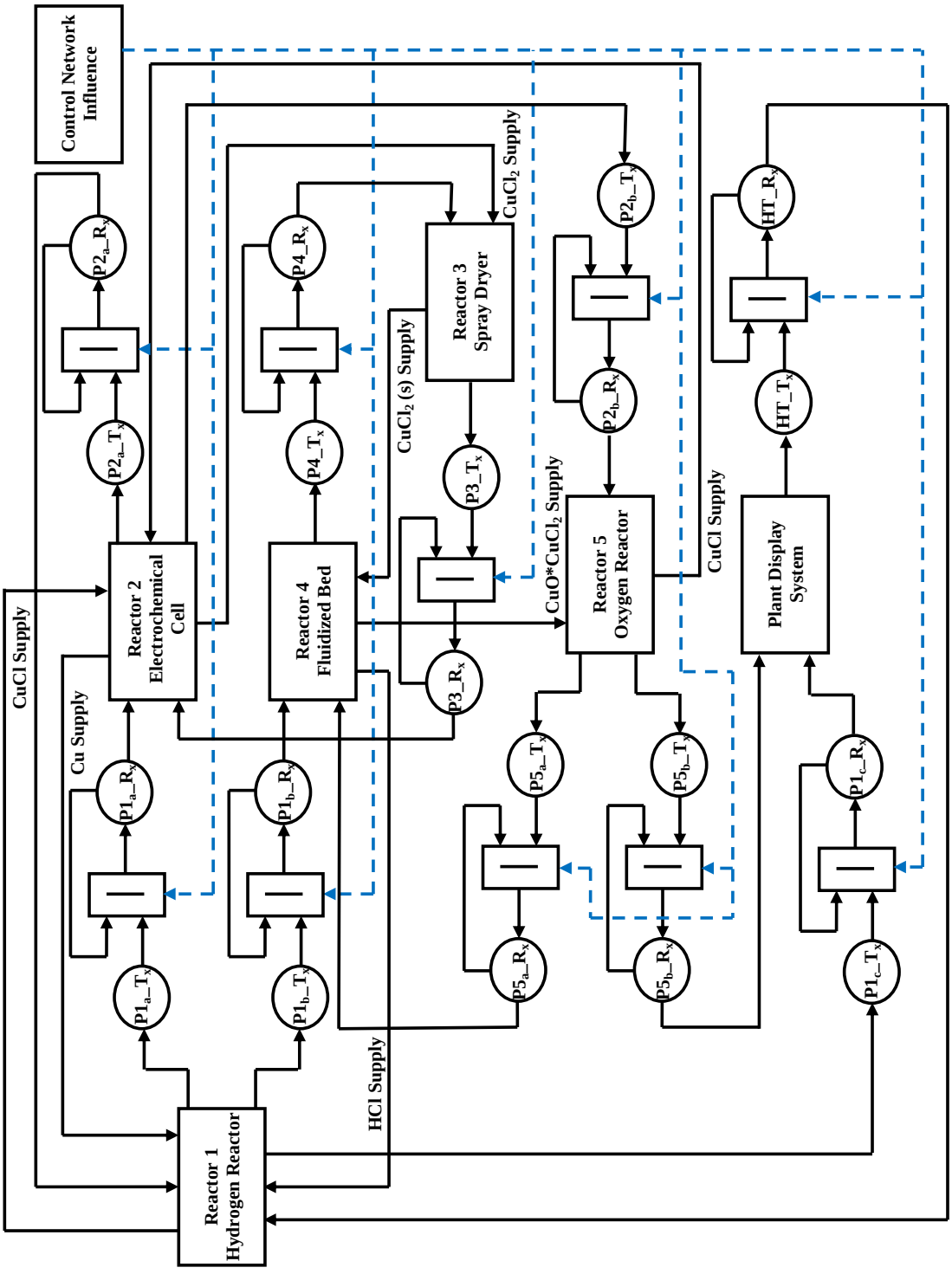

Figure 4.4 DFM Model of the Hydrogen Plant

4.5 A Case Study: The Hydrogen Reactor Unit (Step 1)

In this section, the hydrogen reactor unit (Partition 1 in Figure 4.2) is used as a case study. The Reactor 1 Hydrogen Reactor black box shown in Figure 4.4 is expanded. In order to implement the DFM model, the control methodology and specifications are discussed.

In Step 1, copper particles enter the mixing chamber in the hydrogen reactor, descend along an inclined bed and then melt to produce CuCl liquid at the exit. At the same time, HCl gas passes through the mixing chamber (shown in Figure 4.5) to react and generate H_2(g) in a second exit stream (Rosen et al., 2006). Wang et al. (2008) presented a possible layout for the auxiliary equipment associated with the hydrogen reactor as shown in Figure 4.6. During the start up of the reaction process, HCl and copper particles are heated to 400 ˚C and 80 ˚C, respectively. The HCl and hydrogen mixture of gases that are produced from the mixing chamber are cooled to less than 60 ˚C before applying the alkali solution. The alkali solution absorbs the HCl gas and allows the hydrogen gas to be separated for storage. Wang et al. (2008) stated that the preferred alkali solution is sodium hydroxide since it will not produce carbon dioxide when it reacts with HCl gas. In the other stream, some unreacted copper particles may exit the reactor with molten CuCl. Therefore, a sedimentation vessel is needed to separate the copper and return it to the reaction chamber. The molten CuCl product is then quenched using cold water in a quenching cell.

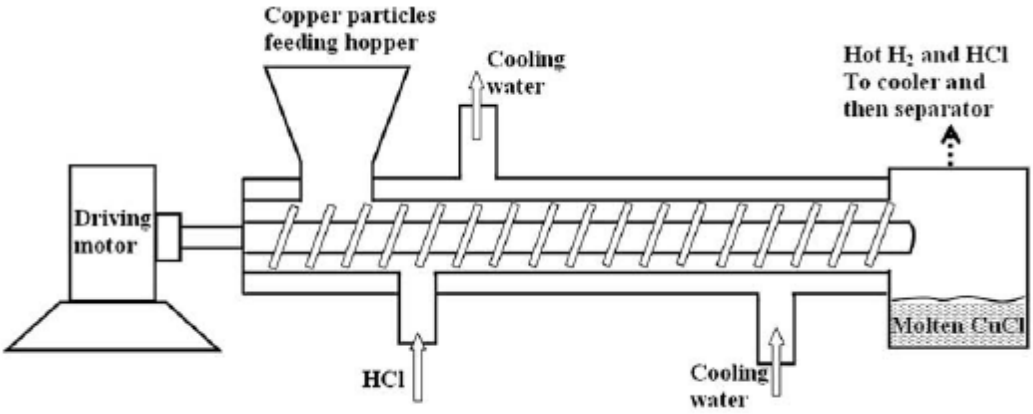

Figure 4.5 Conceptual Schematic for the Hydrogen Reactor (Wang et al., 2008)

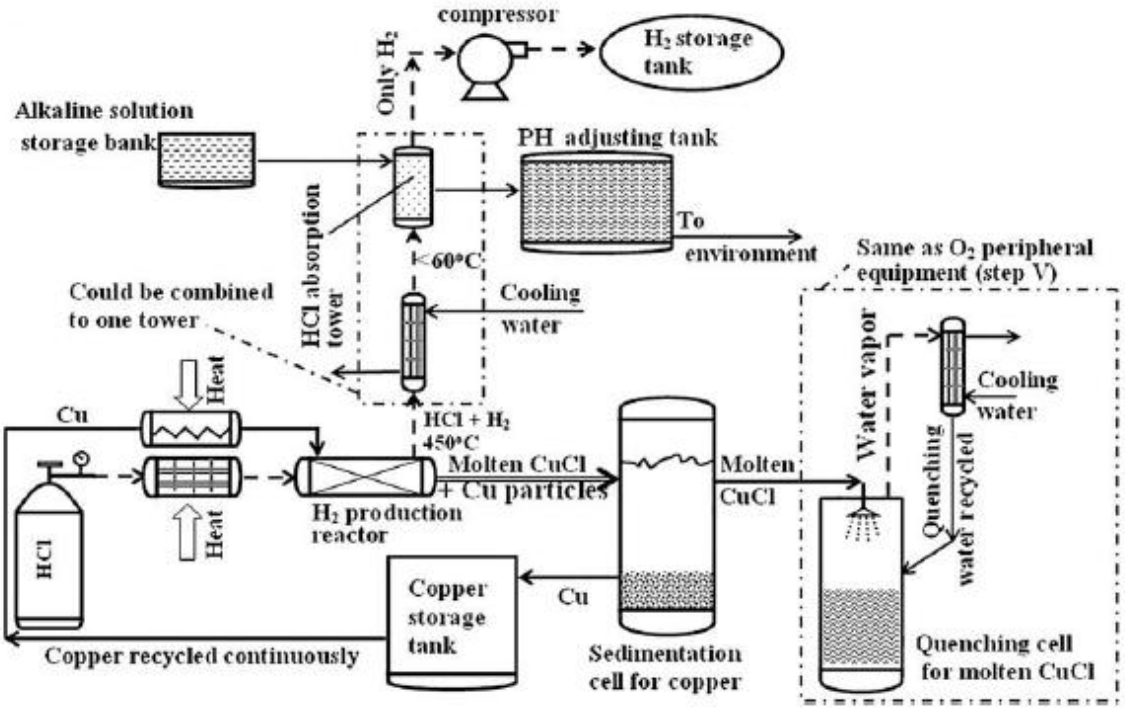

Figure 4.6 Auxiliary Equipment for the Hydrogen Reactor (Wang et al., 2008)

As shown in Figure 4.4, the input reactants to the hydrogen reactor unit are HCl gas, from the fluidized bed unit (Step 4), and copper particles, from the electrochemical cell (Step 2). The products are hydrogen gas and CuCl. The hydrogen gas is stored in a hydrogen

storage tank and the CuCl is used in the electrochemical cell (Step 2). As shown in Figure 4.2, the partition that governs the hydrogen reactor unit consists of one group controller, several device controllers and a fieldbus network. The group controller performs the following tasks: (i) communication with the PDS to exchange hydrogen production data and plant start/shutdown commands (ii) communication with the group controller of the electrochemical cell partition to control and monitor the copper particles inflow and CuCl production and outflow; (iii) communication with the group controller of the fluidized bed partition to control and monitor the production and inflow of HCl gas and (iv) communication with the device controllers of its partition to meet the production demands and ensure a proper and controllable operation of process equipments. Figure 4.7 shows the block diagram of the hydrogen reactor unit's input and output variables.

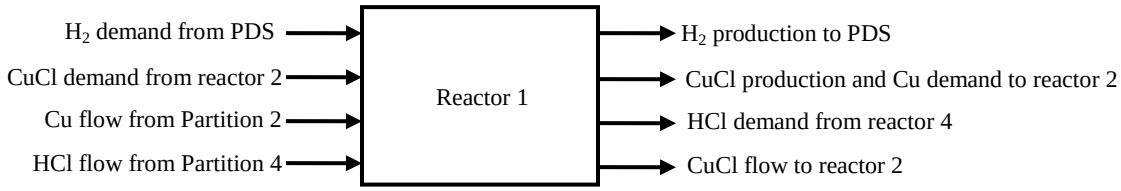

Figure 4.7 Block Diagram of Reactor 1

To facilitate the implementation of the DFM model for the reactor unit, detailed design of the control methodology must be established. For this reason, the configuration of the I&C systems is discussed. The responsibility of the device controllers is to govern the field devices (i.e., valves, motors, pumps, compressors, heat chambers and heat exchanges). The Piping and Instrumentation Diagram (P&ID) described below is implemented to demonstrate the configuration of the control devices. The P&ID for the

hydrogen reactor unit is developed based on the layout for the auxiliary equipments in the unit shown in Figure 4.6. The P&ID is decomposed into three parts: hydrogen production reactor unit, sedimentation and quenching units and HCl absorption unit. The description and corresponding DFM model of each part is described.

4.5.1 Piping and Instrumentation Diagram: Part 1

Figure 4.8 demonstrates the first part of the P&ID. In the figure, HCl gas enters the hydrogen production reactor through Line 1-1. The flow is controller initially by control valves V1-1 and V1-2. It is also controlled by pump and valve, P1-1 and V1-4 or P1-2 and V1-3. Flow measurements are provided to the controllers through the use of sensors F1-1 to F1-10. The redundancy of actuators and sensors is included to provide a higher degree of reliability in order to improve the performance. The DFM model of the flow through Line 1-1 is demonstrated in Figure 4.9.

The input to the model shown above is the HCl requirement sent from the group controller of the partition to controller C1B. The controller C1B can control the valve and pump combination and can send command to controller C1 to adjust the valve opening position. The output of the model is the following: HCl requirements from reactor 4 sent from C1 to group controller, HCl flow into hydrogen reactor unit, and measurement of HCl flow into hydrogen production reactor sent from C1B to group controller. The description of the variables in the DFM model is shown in Table 4.3.

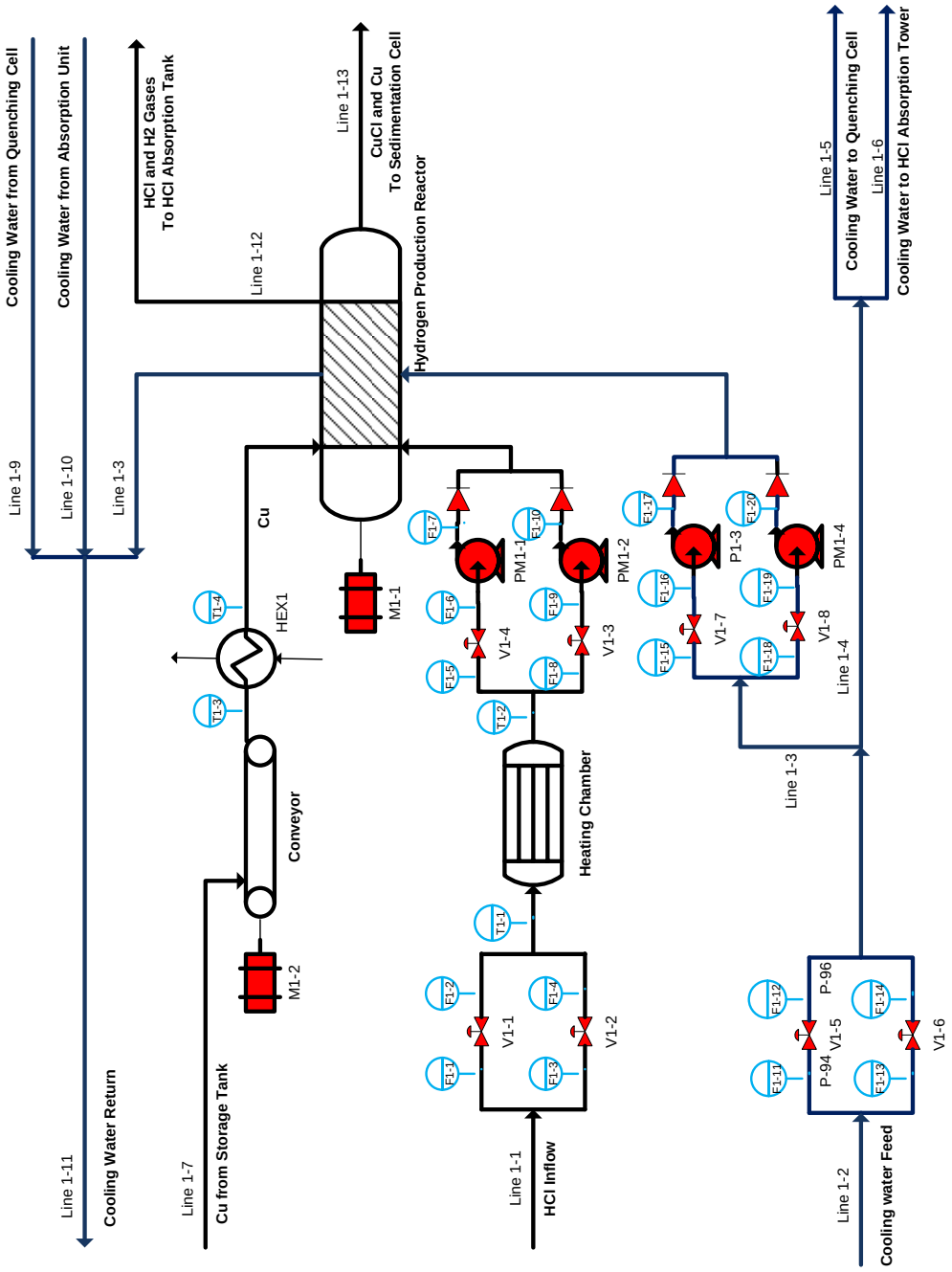

Figure 4.8 P&ID of Hydrogen Production Reactor Unit

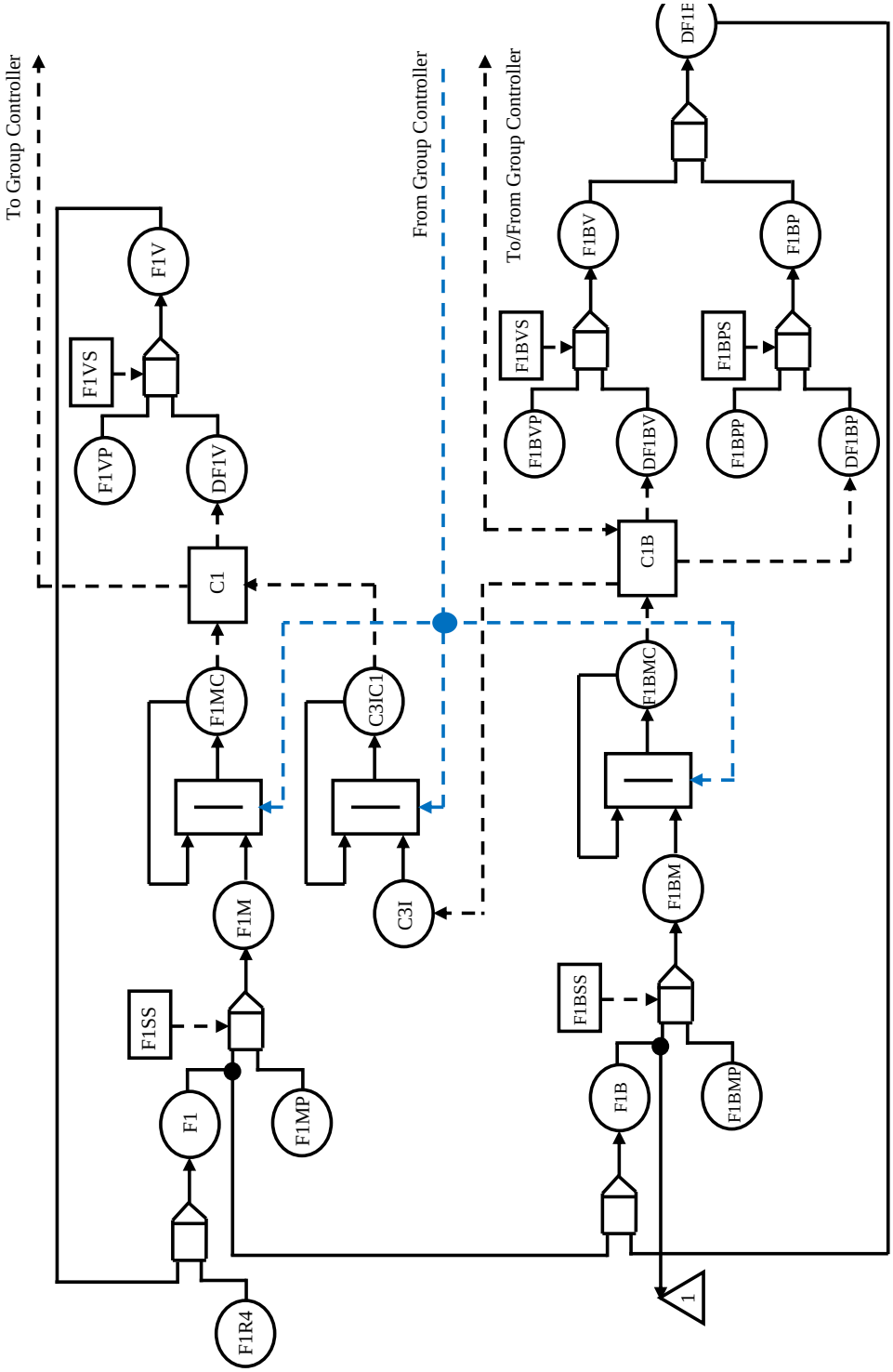

Figure 4.9 DFM Model of Line 1-1 Flow

Table 4.3 Description of Process Variables of Line 1-1 Flow DFM Model

F1R4	Line1 flow from reactor 4
F1	Line 1 flow
F1MP	Measurement of line 1 flow in previous cycle
F1SS	Line 1 flow measurement sensor status
F1M	Line 1 flow measurement
F1MC	Line 1 flow measurement used by controller
C1	Controller 1
DF1V	Change in flow 1 valve position
F1VP	Line 1 flow valve position in previous cycle
F1VS	Line 1 flow valve status
F1V	Flow 1 valve position
C3I	Instruction from controller 3
C3IC1	Instruction from controller 3 used by controller 1
F1B	Line 1 flow after heating
F1BMP	Line 1 flow measurement after heating in previous cycle
F1BSS	Line 1 flow measurement status after heating
F1BM	Line 1 flow measurement after heating
F1BMC	Line 1 flow measurement after heating used by controller
C1B	Controller 1B
F1BVP	Line 1 flow valve position after heating in previous cycle
DF1BV	Change in line 1 flow valve position after heating
F1BVS	Line 1 flow valve status after heating
F1BV	Line 1 flow valve position after heating
F1BPP	Line 1 flow pump speed in previous cycle
DF1BP	Change in line flow pump speed
F1BPS	Line 1 flow pump status
F1BP	Line 1 flow after heating in previous cycle
DF1B	Change in line 1 flow after heating

Copper particles enter the hydrogen production reactor through Line 1-7. The speed of motor M1-2 governs the flow of the Cu particles. Flow sensors are used to measure the amount of Cu particles flow into the production reactor. The DFM model of this process is shown in Figure 4.10. The input to the model is the Cu requirement sent from group controller to C7. The output of the model is the Cu requirement from reactor 2 sent from C7 to group controller and Cu supply to hydrogen production reactor. The description of variables included in the model is shown in Table 4.4.

Table 4.4 Description of Process Variables of Line 1-7 Flow DFM Model

F7	Line 7 flow
F7R2	Cu supply from reactor 2
F7MP	Line 7 flow measurement in previous cycle
F7SS	Line 7 flow sensor status
F7M	Line 7 flow measurement
F7MC	Line 7 flow measurement used by controller
DM2	Change in motor 2 speed
M2P	Motor 2 speed in previous cycle
M2S	Motor 2 status
M2	Motor 2 status
COVS	Conveyor status
DF7	Change in line 7 flow

The role of heat exchanger HEX1, and heating chamber in the P&ID is to adjust the temperature of the Cu particles and the HCl gas to 400 ˚C and 80 ˚C, respectively, before entering the hydrogen production reactor. The controller of each device obtains temperature measurements at its inlet and outlet from temperature sensors provided along each stream. The DFM model of the temperature of both streams is shown in Figure 4.11.

The inputs to the model are the HCl and Cu flow temperature requirement sent group controller to C1T and C7T, respectively. The outputs of the model are the following: HCl and Cu flow temperature measurement sent from C1T and C7T to group controller, respectively, and temperature of the HCl and Cu flow to hydrogen production reactor. The description of the variables in the model is shown in Table 4.5.

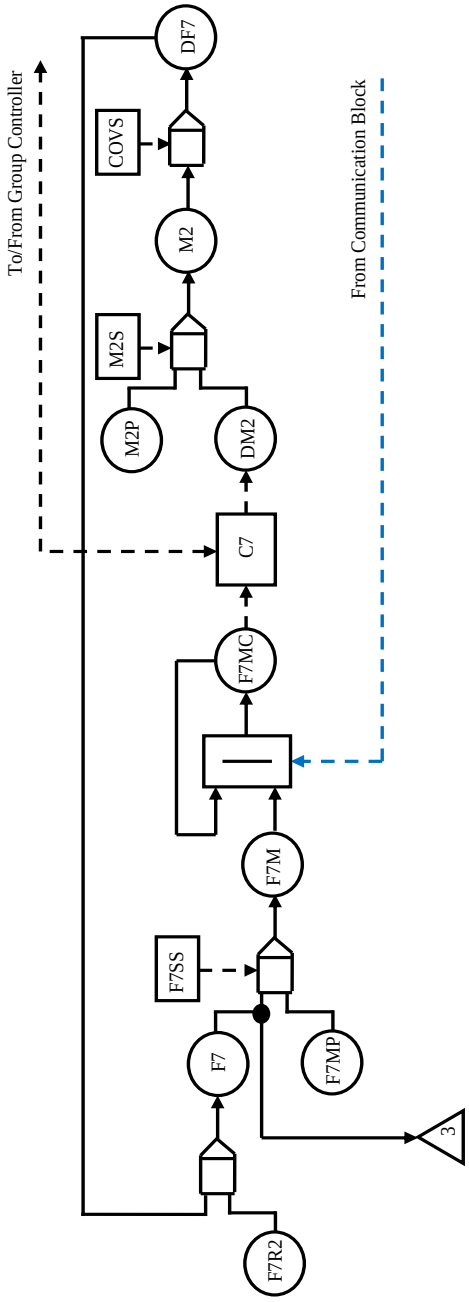

Figure 4.10 DFM Model of Line 1-7 Flow

Table 4.5 Description of Process Variables of Line 1-1 and Line 1-7 Temperature Control DFM Model

TF1BH	Temperature of line 1 flow before heating
TF1SS	Line 1 flow temperature sensor status
TMF1	Measurement of line 1 flow temperature before heating
TMF1C	Measurement of line 1 flow temperature before heating used by controller C1T
DTF1	Change in temperature of line 1 flow
TF1P	Temperature of line 1 flow in previous cycle
HCS	Heating chamber status
TF1A	Temperature of line 1 flow after heating
TMF1A	Measurement of line 1 temperature after heating
TF1AC	Measurement of line 1 flow temperature after heating used by controller
TF1AS	Line 1 flow temperature sensor status after heating
TF7BH	Temperature of line 7 flow before heating
TF7SS	Line 7 flow temperature sensor status
TMF7	Measurement of line 7 flow temperature before heating
TMF1C	Measurement of line 7 flow temperature before heating used by controller
DTF7	Change in temperature of line 7 flow
TF7P	Temperature of line 7 flow in previous cycle
HEXS	Heat exchanger status
TF7A	Temperature of line 7 flow after heating
TF7AS	Line 7 flow temperature sensor status after heating
TMF7A	Measurement of line 7 temperature after heating
TF7AC	Measurement of line 7 flow temperature after heating used by controller

The role of the main and standby valves and pumps along 1-3 is to govern the flow of cooling water into the reactor, where flow sensors are placed along the stream to provide measurements to the controllers of the valves and pumps. The valves along Line 1-2 control the flow from the main water stream to Line 1-3, Line 1-5 and Line 1-6. The DFM model of the flow through both streams is shown in Figure 4.12. The description of the variables of the model is shown in Table 4.6.

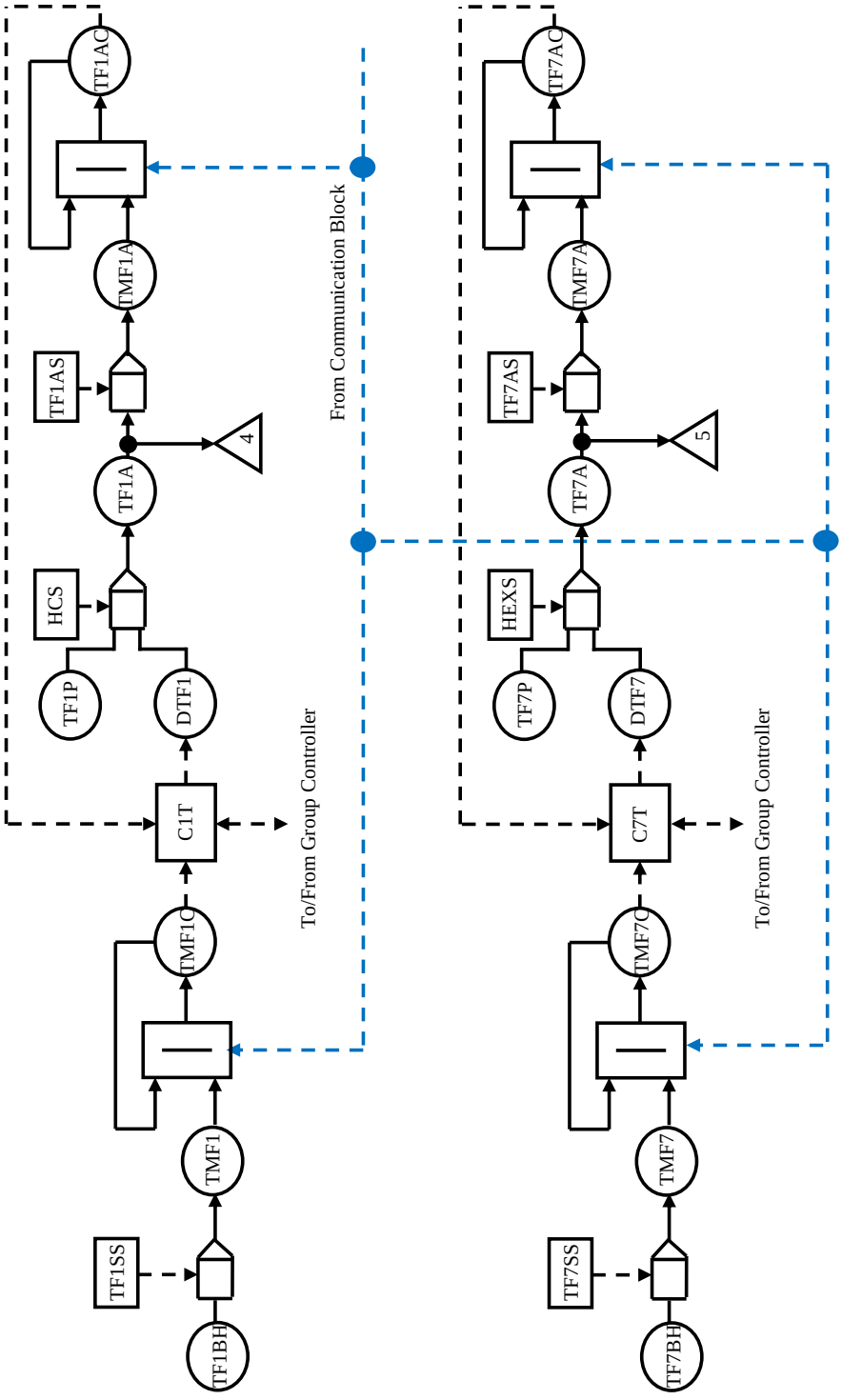

Figure 4.11 DFM Model of Temperature Control of Line 1-1 and Line 1-7

Table 4.6 Description of Process Variables of Line 1-2 and Line 1-3 Flow DFM Model

F2	Flow through line 2
F3	Flow though line 3
F3MP	Measurement of line 3 flow in previous cycle
F3SS	Line 3 flow sensor status
F3M	Measurement of line 3 flow
F3MC	Measurement of line 3 flow used by controller
DF3V	Change in line 3 flow valve position
F3VP	Line 3 flow valve position in previous cycle
F3VS	Line 3 flow valve status
F3V	Line 3 flow valve position
DF3P	Change in line 3 flow pump speed
F3PP	Line 3 flow pump speed in previous cycle
F3PS	Line 3 flow pump status
F3P	Line 3 flow pump speed
DF3	Change in line 3 flow
F2T	Line 2 flow from tank
F2	Line 2 flow
F2MP	Line 2 flow measurement in previous cycle
F2SS	Line 2 flow sensor status
F2M	Line 2 flow measurement
F2MC	Line 2 flow measurement used by controller
DF2V	Change in line 2 flow valve position
F2VP	Line 2 flow valve position in previous cycle
F2VS	Line 2 flow valve status
F2V	Line 2 flow valve position

The input to the model are the H_2O requirement sent from group controller to C3 for flow into the hydrogen production reactor and to C2 for flow into the three water supply lines Line 1-3, Line 1-5 and Line 1-6. The outputs of the model are the following:

- H_2O flow into hydrogen production reactor sent from C3 to group controller
- H_2O flow requirement from line 2 sent from C3 to group controller
- H_2O flow into hydrogen production reactor
- H_2O supply to two lines
- H_2O supply measurement sent from C2 to group controller

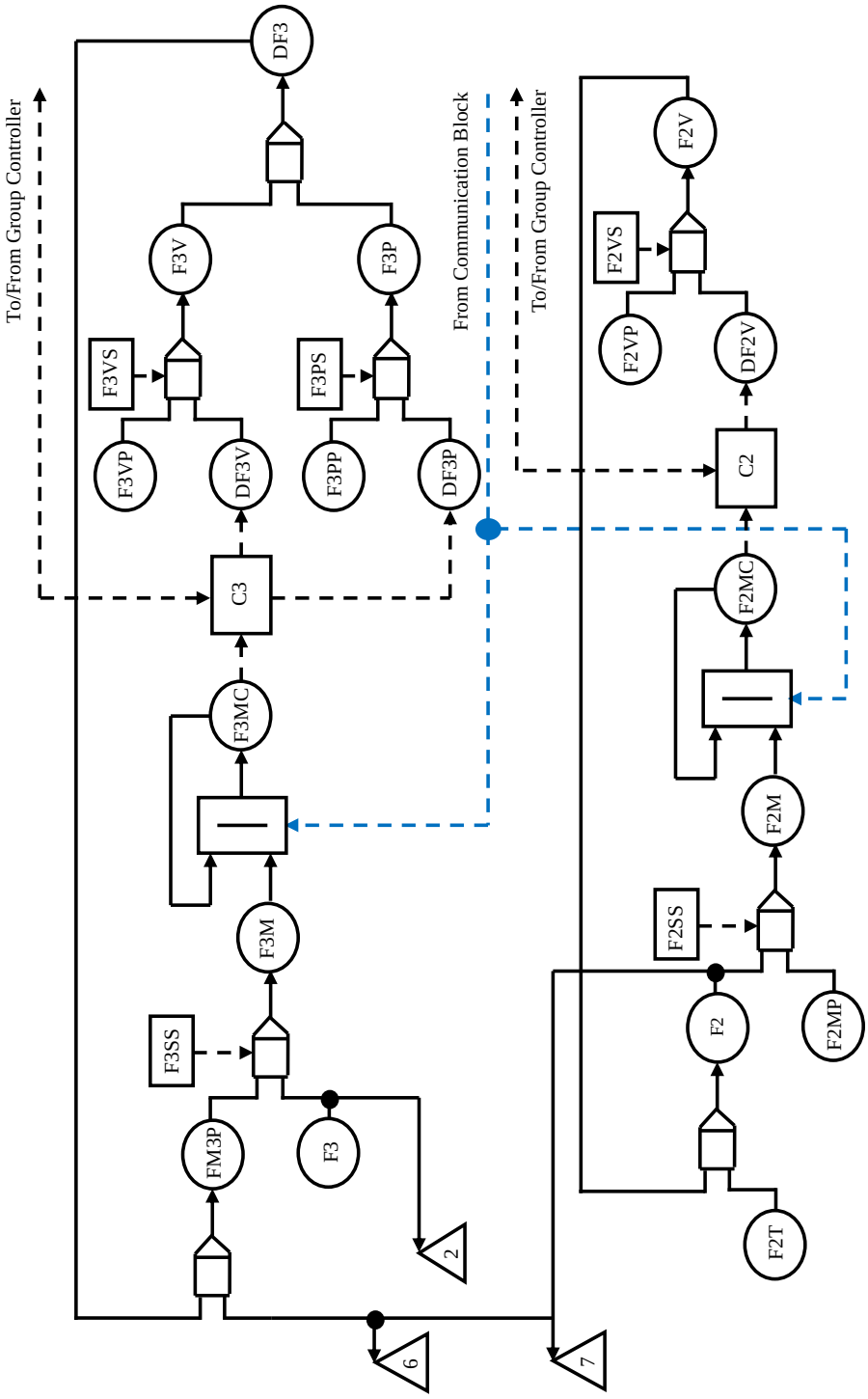

Figure 4.12 DFM Model of Line 1-2 and Line 1-3 Flow

The role of the device controller of the hydrogen production reactor motor M1-1 is to govern its speed to adjust the hydrogen production rate to meet production demand. The production rate calculation is based on a comparison of the hydrogen production demand, and the hydrogen flow rate through Line 1-21 in Part 3 of the P&ID. Once the production rate is determined, the device controller of the hydrogen production reactor communicates with the device controllers of the devices along Line 1-1, Line 1-7, and Line 1-3 to control the inflow of HCl gas, Cu particles, and cooling water, respectively. The DFM model of the hydrogen production reactor operation is shown in Figure 4.13. The inputs to the model are the following: instruction from group controller to C8, HCl flow, H_2O flow, HCl temperature and Cu temperature. The outputs of the model are HCl and H_2 outflow and CuCl and Cu outflow. The description of the variables in the DFM Model is shown in Table 4.7.

Table 4.7 Description of Process Variables of Hydrogen Production Reactor DFM Model

GCC8	Instruction from group controller to controller C8
GCC8R	Instruction from group controller to controller C8 received
DM1	Change in motor M1-1 speed
M1P	Motor M1-1 speed in previous cycle
M1S	Motor M1-1 status
M1	Motor M1-1 speed
F13	Line 13 flow
F15	Line 15 flow

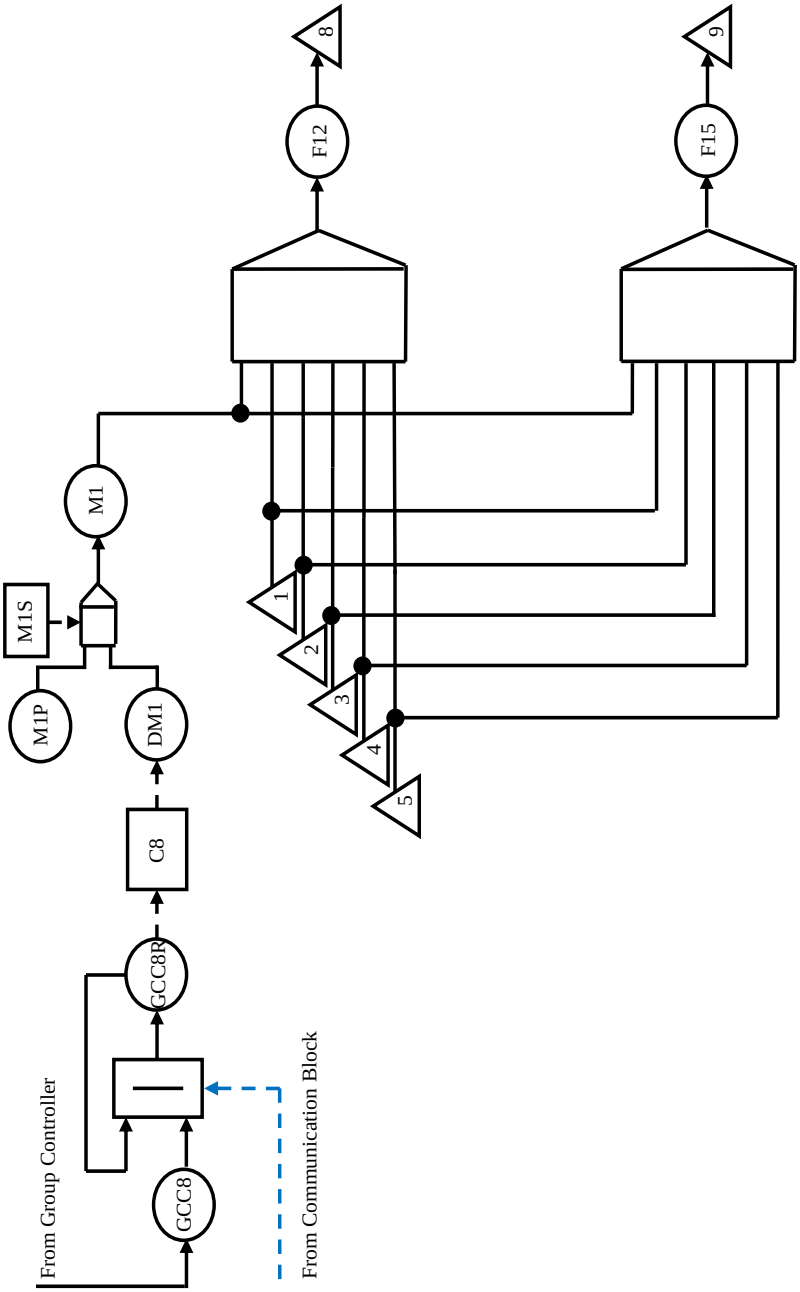

Figure 4.13 DFM Model of Hydrogen Production Reactor

4.5.2 Piping and Instrumentation Diagram: Part 2

The second part of the P&ID shown in Figure 4.14 demonstrates how the produced molten CuCl is fed to the sedimentation and quenching units. In the figure, molten CuCl is transported after sedimentation to the quenching cell through Line 1-17. The pumps and valves along Line 1-17 control the amount of CuCl molten flow into the cell. The DFM model of the flow through the stream is shown in Figure 4.15. The inputs to the model are the CuCl and Cu flow and CuCl requirement sent from group controller to C17. The outputs of the model are the CuCl solid flow and measurement sent from C7 to group controller. The description of the variables in the DFM model is shown in Table 4.8.

Table 4.8 Description of Process Variables of Line 1-17 Flow DFM Model

F17B	Flow through line 17 from sedimentation cell
F17	Flow through line 17 after pumps and valves
F17MP	Measurement of line 17 flow in previous cycle
F17SS	Line 17 flow sensor status
F17M	Measurement of line 17 flow
F17MC	Measurement of line 17 flow used by controller
DF17V	Change in line 17 flow valve position
F17VP	Line 17 flow valve position in previous cycle
F17VS	Line 17 flow valve status
F17V	Line 17 flow valve position
DF17P	Change in line 17 flow pump speed
F17PP	Line 17 flow pump speed in previous cycle
F17PS	Line 17 flow pump status
F17P	Line 17 flow pump speed
DF17	Change in line 17 flow

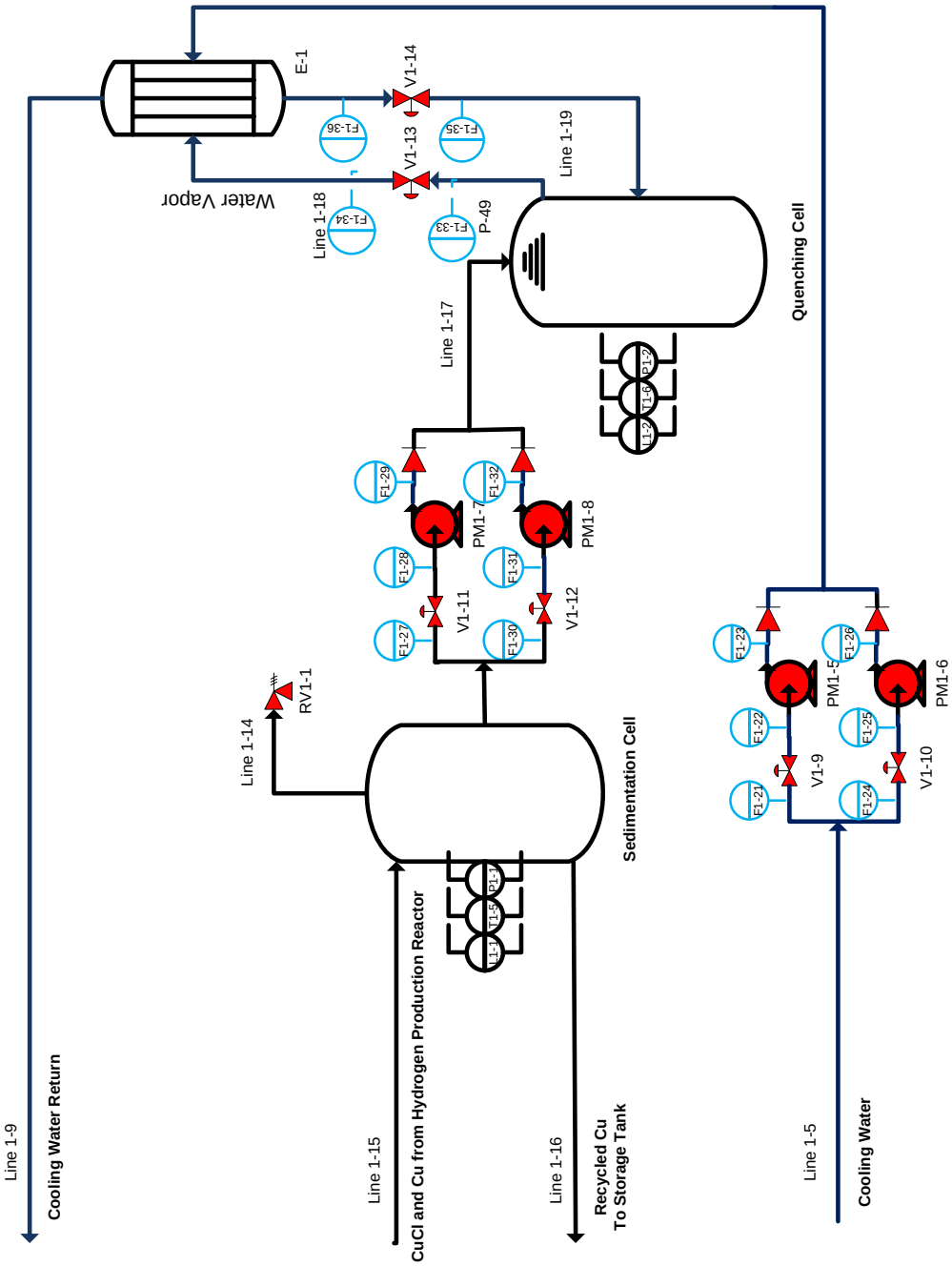

Figure 4.14 P&ID of Quenching and Sedimentation Unit

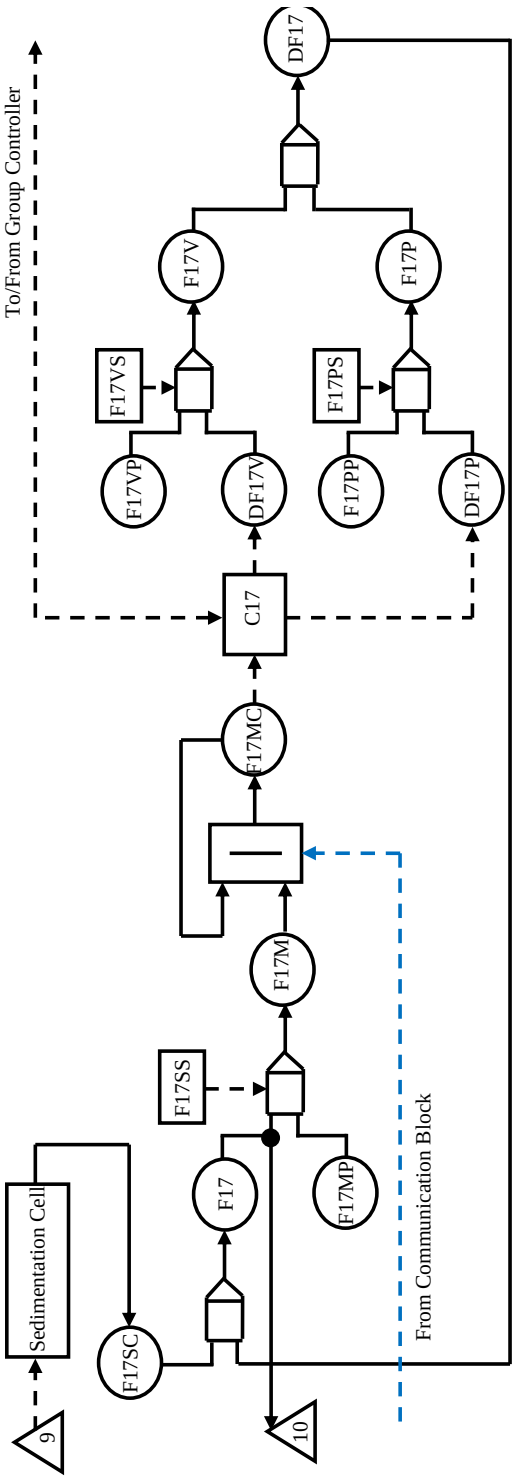

Figure 4.15 DFM Model of Line 1-17 Flow

In Figure 4.14, the device controller of the quenching cell communicates with the controllers of V1-13 in Line 1-18 and V1-14 in Line 1-19 to adjust the rate of liquid water inflow and water vapour outflow where flow sensors are provided for each stream. The DFM model of both streams is shown in Figure 4.16. The inputs to the model are the following: water vapour from quenching cell, valve position instruction sent from group controller to C18, water supply to supply unit E, and valve position instruction sent from group controller to C19. The outputs of the model are the following: water vapour measurement sent from C18 to group controller, water vapour leaving quenching cell, water measurement send from C19 to group controller, and water entering quenching cell. The description of the variables in the DFM model is shown in Table 4.9.

Table 4.9 Description of Process Variables of Line 1-18 and Line 1-19 Flow DFM Model

F18QC	Flow through line 18 coming from quenching cell
F18	Flow though line 18 after the valve
F18MP	Measurement of flow through line 18 in previous cycle
F18SS	Line 18 flow sensor status
F18M	Measurement of flow through line 18
F18MC	Measurement of flow through line 18 used by controller
DF18V	Change in line 18 valve opening
F18VP	Line 18 valve position in previous cycle
F18V	Line 18 valve position
F18VS	Line 18 valve status
F19E	Flow through line 19 coming from E
F19	Flow though line 19 after the valve
F19MP	Measurement of flow through line 19 in previous cycle
F19SS	Line 19 flow sensor status
F19M	Measurement of flow through line 19
F19MC	Measurement of flow through line 19 used by controller
DF19V	Change in line 19 valve opening
F19VP	Line 19 valve position in previous cycle
F19V	Line 19 valve position
F19VS	Line 19 valve status

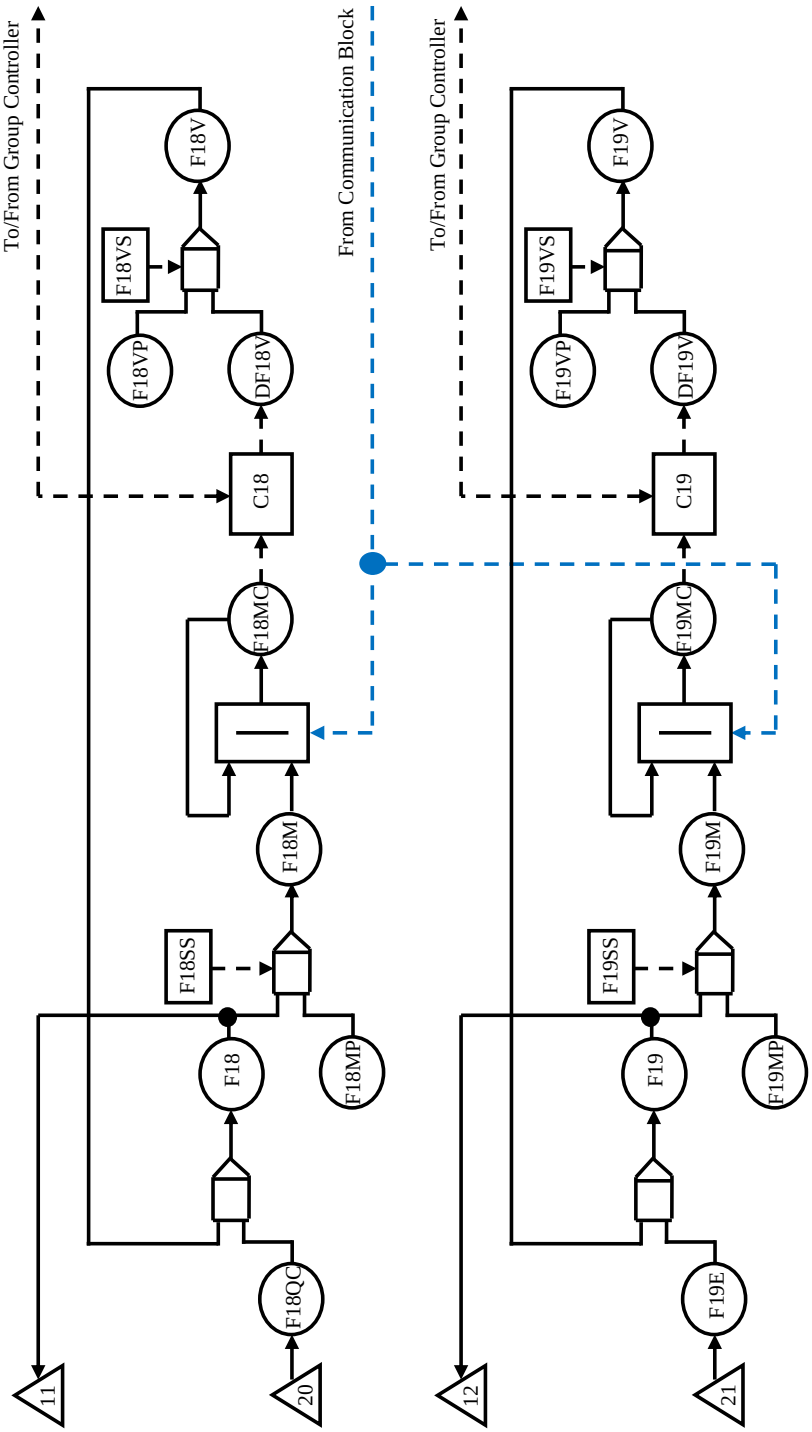

Figure 4.16 DFM Model of Line 1-18 and Line 1-19 Flow

The group controller communicates with the device controller of the quenching cell to exchange data and setpoints with regard to solid CuCl production. The DFM model of the quenching operation is shown in Figure 4.17. The inputs to the model are the water and CuCl molten entering the quenching cell and the water vapour leaving the quenching cell. The outputs of the model are the CuCl solid exiting the quenching cell and the measurement sent to group controller, and the quenching cell pressure measurement sent to group controller. The description of the variables of the DFM model is shown in Table 4.10.

Table 4.10 Description of Process Variables of Quenching Cell DFM Model

CuCl	CuCl production
CuCl_P	Measurement of CuCl in previous cycle
MSS	CuCl production sensor status
CuCl	Measurement of CuCl production
CuClC	Measurement of CuCl production sent to group controller
QCP	Quenching cell pressure
QCPP	Quenching cell pressure measurement in previous cycle
QCSS	Quenching cell pressure sensor status
QCPM	Quenching cell pressure measurement
QCPC	Quenching cell pressure measurement sent to group controller
CuClR2	CuCl flow to reactor 2

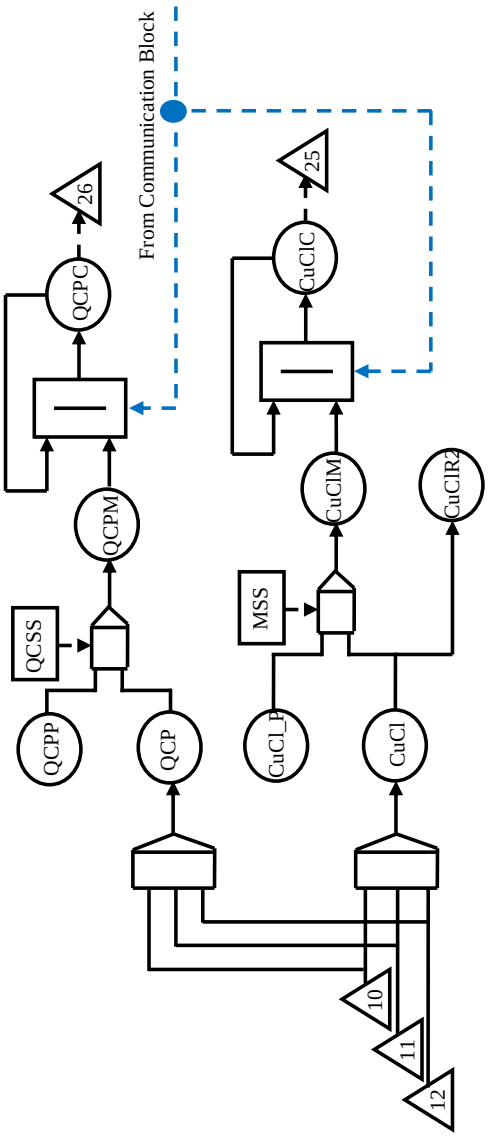

Figure 4.17 DFM Model of Quenching Cell

4.5.3 Piping and Instrumentation Diagram: Part 3

The third part of the P&ID shown in Figure 4.18 demonstrates how the produced HCl and H_2 gases are cooled and separated. In the figure, the device controller of the cooling chamber communicates with the controllers of the valves located in Line 1-12 to control the HCl and H_2 gases that flow into the chamber. Temperature measurements provided by sensors T1-7 and T1-8 are used by the device controller to cool the temperature of the gases down below 60 ˚C prior to entering the HCl absorption tank as specified in (Wang et al., 2008). The device controller also communicates with the controllers of the instruments in Line 1-6 to control the flow of cooling water into the chamber. The device controller of the HCl absorption tank communicates with the controllers of the devices along Line 1-20 to control the inflow of the alkali solution into the absorption tank. It also communicates with the device controllers along Line 1-21 to control the flow of hydrogen gas into the hydrogen storage tank. Flow sensors are used along both streams to provide the device controller with alkali solution and hydrogen gas flow rates.

The DFM model of Line 1-12 temperature and Line 1-6 flow is shown in Figure 4.19. The inputs to the model are the water supply through Line 1-6 and the temperature requirement sent from group control to CCC. The outputs of the model are the temperature measurement sent from CCC to group controller, H_2O requirement from Line 1-6 sent from C6 to group controller and temperature of HCl and H_2 gases. The description of the variables in the DFM model is shown in Table 4.11.

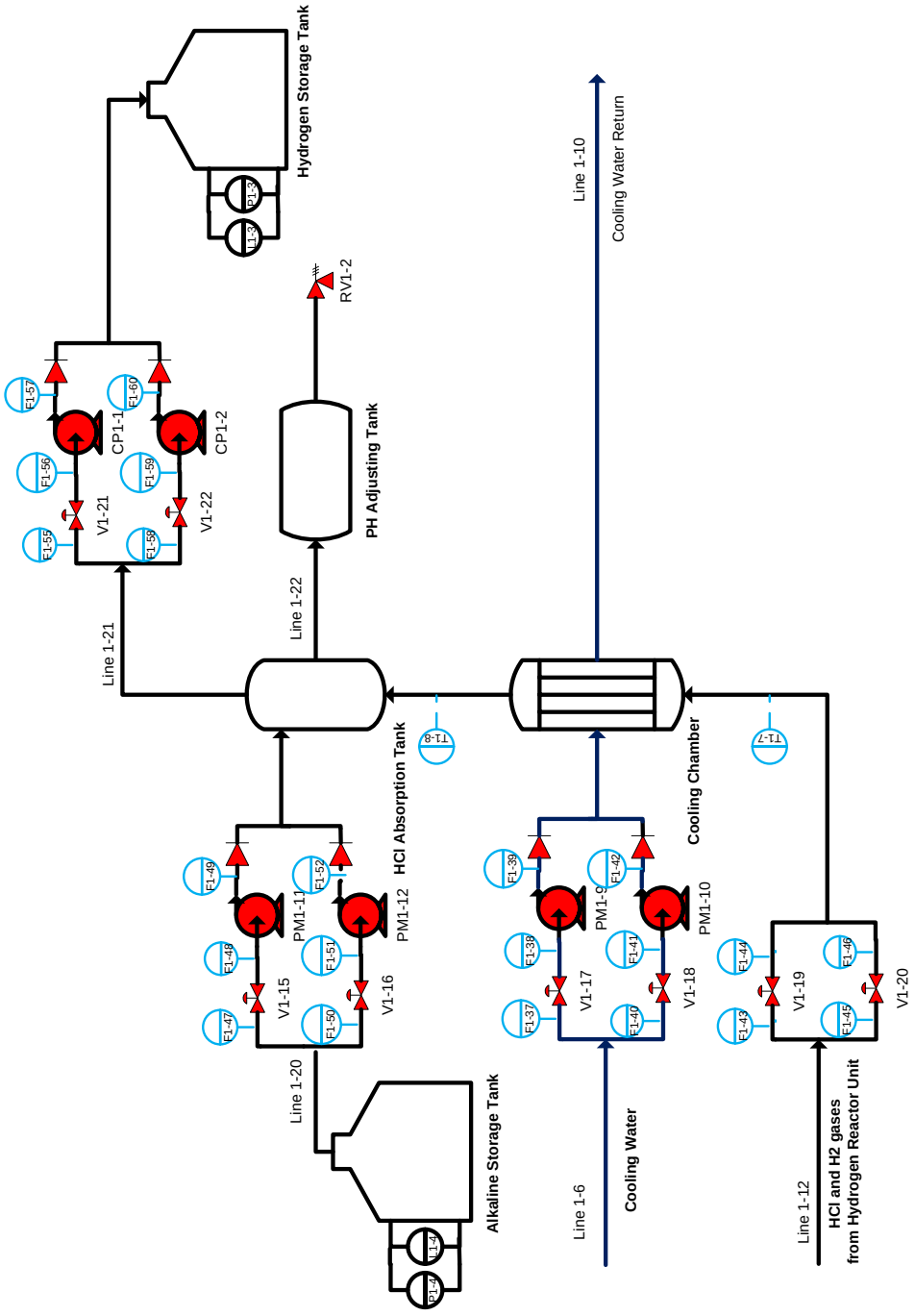

Figure 4.18 P&ID of HCl Absorption Unit

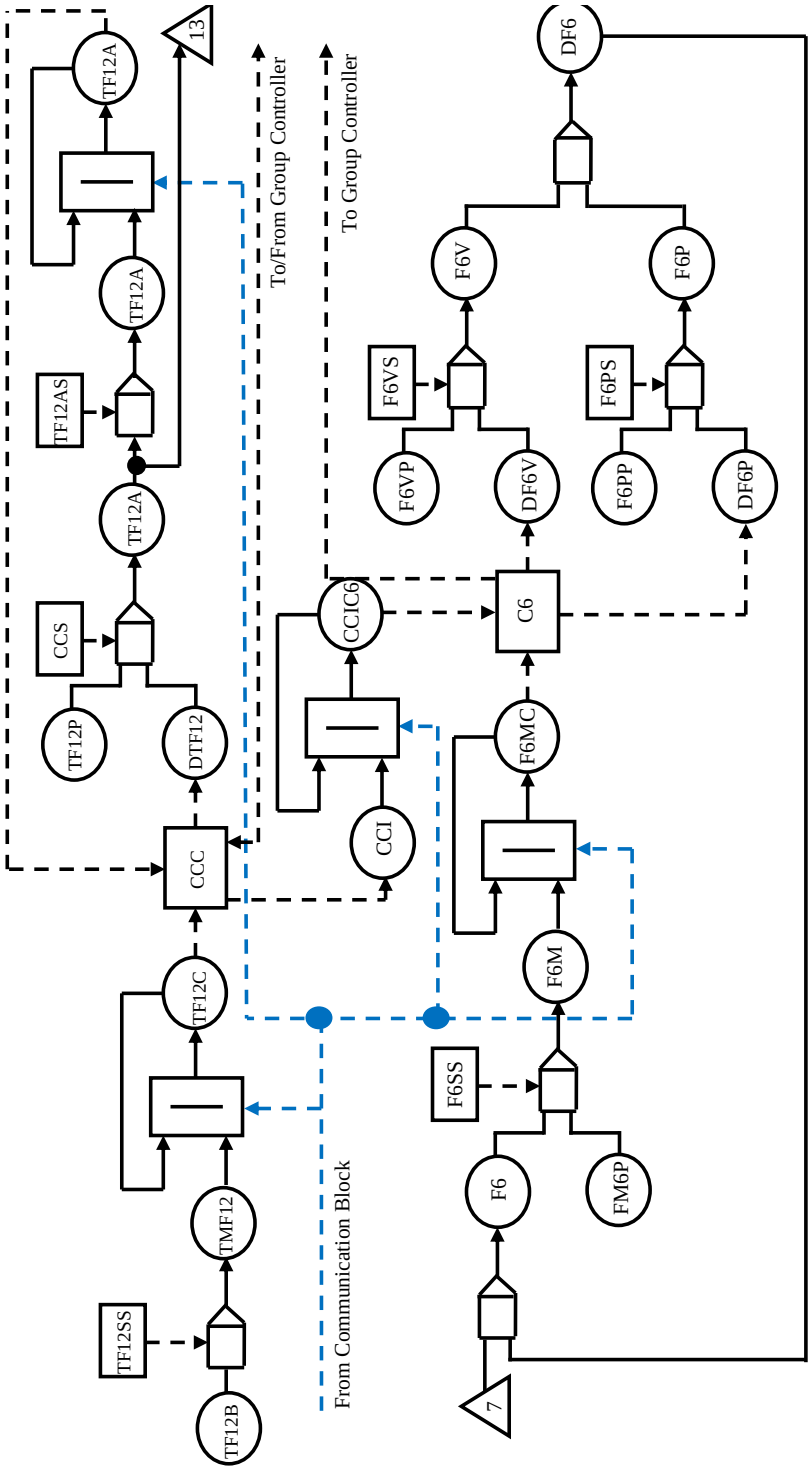

Figure 4.19 DFM Model of Line 1-12 Temperature and Line 1-6 Flow

Table 4.11 Description of Process Variables of Line 1-12 Temperature and Line 1-6 Flow DFM Model

TF12B	Temperature of line 12 flow before cooling
TF12SS	Line 12 flow temperature sensor status
TMF12	Measurement of line 12 flow temperature before cooling
TF1C	Measurement of line 12 flow temperature before cooling used by controller
DTF12	Change in temperature of line 12 flow
TF12P	Temperature of line 12 flow in previous cycle
CCS	Cooling chamber status
TF12A	Temperature of line 12 flow after cooling
TF12A	Measurement of line 12 temperature after cooling
TF12A	Measurement of line 12 flow temperature after cooling used by controller
TF12AS	Line 12 flow temperature sensor status after cooling
F6	Flow though line 6
F6MP	Measurement of line 6 flow in previous cycle
F6SS	Line 6 flow sensor status
F6M	Measurement of line 6 flow
F6MC	Measurement of line 6 flow used by controller
DF6V	Change in line 6 flow valve position
F6VP	Line 6 flow valve position in previous cycle
F6VS	Line 6 flow valve status
F6V	Line 6 flow valve position
DF6P	Change in line 6 flow pump speed
F6PP	Line 6 flow pump speed in previous cycle
F6PS	Line 6 flow pump status
F6P	Line 6 flow pump speed
DF6	Change in line 6 flow
CCI	Cooling chamber instruction
CCIC6	Cooling chamber instruction used by controller 6

The DFM model of the flow through Line 1-12 and Line 1-20 is shown in Figure 4.20. The inputs to the model are the following: HCl and H_2 production from hydrogen production reactor, HCl and H_2 temperature after cooling, HCl and H_2 flow to separation tank sent from group controller to C12 and Alkali flow to separation tank sent from group controller to C20. The outputs of the model are the following: HCl and H_2 production measurement sent from C12 to group controller, HCl and H_2 flow measurement sent from

C12 to group controller, Alkali flow measurement sent from C20 to group controller, Hydrogen flow through line 21 and hydrogen flow through line 21 measurement sent to group controller. The description of the variables in the DFM model is shown in Table 4.12.

Table 4.12 Description of Process Variables of Line 1-12 and Line 1-20 Flow DFM Model

F12	Line 12 flow
F12MP	Line 12 flow measurement in previous cycle
F12SS	Line 12 flow sensor status
F12M	Line 12 flow measurement
F12MC	Line 12 flow measurement used by controller
DF12V	Change in line 12 flow valve position
F12VP	Line 12 flow valve position in previous cycle
F12VS	Line 12 flow valve status
F12V	Line 12 flow valve position
F20AT	Flow through line 20 from alkali storage tank
F20	Flow though line 20
F20MP	Measurement of line 20 flow in previous cycle
F20SS	Line 20 flow sensor status
F20M	Measurement of line 20 flow
F20MC	Measurement of line 20 flow used by controller
DF20V	Change in line 20 flow valve position
F20VP	Line 20 flow valve position in previous cycle
F20VS	Line 20 flow valve status
F20V	Line 20 flow valve position
DF20P	Change in line 20 flow pump speed
F20PP	Line 20 flow pump speed in previous cycle
F20PS	Line 20 flow pump status
F20P	Line 20 flow pump speed
DF20	Change in line 20 flow
F21ST	Line 21 flow from separation tank
F21SS	Line 21 flow sensor status
F21M	Line 21 flow measurement
F21MC	Line 21 flow measurement used by controller

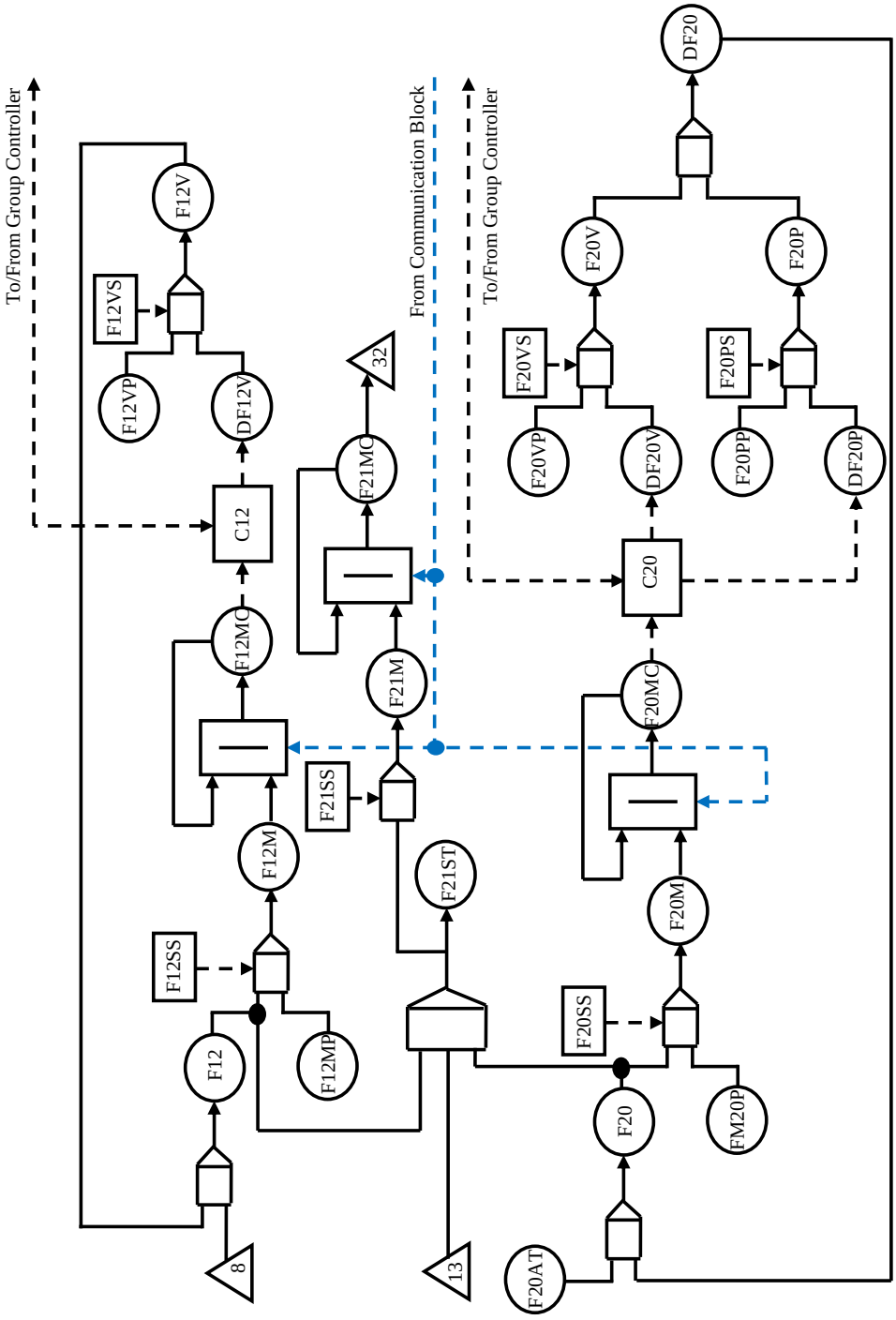

Figure 4.20 DFM Model of Line 1-12 and Line 1-20 Flow

The DFM model for the Cu-Cl cycle is considered complete when knowledge of the components and behaviour of the process is clearly defined. As research continues to design and develop the cycle, complete process design and behaviour, components selection, and control logic and flow should be specified in order to complete the DFM model in future research. The completion of the model will allow deductive and inductive analysis to be performed.

4.6 Chapter Summary

In this chapter, a review of the conceptual design of a nuclear-based thermochemical copper-chlorine cycle was provided. The design of the networked control system for the cycle was addressed. The architecture and the communication structure of the control system were discussed. The dynamic flowgraph methodology was applied to model the Cu-Cl cycle, where the hydrogen reactor unit was used as a case study. The configuration of the instrumentation and control systems for the reactor unit was presented using a piping and instrumentation diagram.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS FOR FUTURE RESEARCH

5.1 Conclusions

This thesis investigates the reliability modelling of networked control systems, where control elements (i.e., controllers, sensors and actuators) are connected by a shared communication network. It is shown that the dynamic flowgraph methodology can be extended to model the behaviour and effect of communication network in networked control systems applications. Timed prime implicants and timed fault trees can be generated to analyze the model and to identify areas of improvement. The former was applied to study the communication network model and the latter was used to study the networked control system model. This thesis also presents the design of a networked and distributed control system for a nuclear-based hydrogen production plant with copper-chlorine thermochemical cycle. The control architecture and communication structure are defined. It is also demonstrated how the dynamic flowgraph methodology can be applied to model the Cu-Cl cycle. The hydrogen reactor unit of the cycle is used as a case study to present the detailed modelling steps.

5.2 Recommendations for Future Research

It is recommended that future research should investigate the computational capability and scalability of the DFM Software Toolkit as well as its performance when implementing DFM models of complex systems and processes. Future research is also recommended to provide a complete and controlled hydrogen production process by

having detailed specifications of instrumentation and control systems. This includes the selection and configuration of I&C systems for the 5 units of the cycle. The availability of a complete process design and specifications allows the finding of reliability data of basic components of the system. This assists in performing detailed reliability analysis. For example, reliability data of basic components can be used in the timed fault trees to measure reliability and occurrence of events of interest. In addition, the control logic and control flow need to be assigned upon completion of process design. This can provide the capability of maintaining an appropriately functioning and controlled system in order to maximize plant's life and minimize risk and plant's failure.

A detailed DFM model to emulate both the behaviour of the plant and the effect of the control system need to be constructed. The model construction will become possible when detailed specifications of the controlled process and I&C systems are available. The detailed model can be used to study the functionality of the system and measure the reliability of the plant. It can be used to predict the occurrence of events and identify the corresponding consequences. A physical prototype of the controlled process and associated control system should be implemented. This can assist in performing experiments to obtain real-time results and observe system's behaviour. It allows the establishment of a reference for comparison with the DFM model implemented for the plant. Also, the knowledge of system behaviour can be used in creating a DFM model with higher accuracy.

REFERENCES

Al-Dabbagh, A., & Lu, L. (2008, October). Reliability and stability analyses of distributed control for nuclear-based hydrogen generation. *Presentations of the ORF Hydrogen Project Workshop at AECL Chalk River Laboratories* (pp. 279 – 285), Chalk River, Ontario, Canada.

Al-Dabbagh, A. W., & Lu, L. (2009). A distributed control system design for nuclear-based hydrogen production with copper-chlorine thermochemical cycle. *Proceedings of the 30th Annual CNS Conference & 33rd Annual CNS-CNA Student Conference*, Calgary, Alberta, Canada.

Aldemir, T., Miller, D. W., Stovsky, M. P., Kirschenbaum, J., Bucci, P., Fentiman, A. W., & Mangan, L. T., (2006). Current state of reliability modeling methodologies for digital systems and their acceptance criteria for nuclear power plant assessments. NUREG/CR-6901, U.S. Nuclear Regulatory Commission.

Aldemir, T., Miller, D. W., Stovsky, M., Kirschenbaum, J., Bucci, P., Mangan, L. A.,...Arndt S. A. (2007). Methodologies for the probabilistic risk assessment of digital reactor protection and control systems. *Nuclear Technology*, 159, 167 – 191.

Brown, R., & Basso, R. (2004). Advanced CANDU reactor distributed control system design. *25th Annual Conference of the Canadian Nuclear Society*.

Bucci, P., Kirschenbaum, J., Mangan, L. A., Aldemir, T., Smith, C., & Wood, T. (2008). Construction of event-tree/fault-tree models from a Markov approach to dynamic system reliability. *Reliability Engineering and Safety System*, 93, 1616 – 1627.

Campelo, J. C., Yuste, P., Rodriguez, F., Gil, P. J., & Serrano, J. J. (1999). Hierarchical reliability and safety models of fault tolerant distributed industrial control systems. *Proceedings of the 18th International Conference on Computer Computer Safety*, Reliability and Security (pp. 202 – 215).

Chiou, S. -N., & Li, V. O. K. (1986). Reliability analysis of communication networked with multimode components. *IEEE Journal on Selected Areas in Communications*, 4, 1156 – 1161.

Choi, J. Y. (2002). Evaluation of Ethernet based control network used in the distributed control system. *Proceedings on the 15th CISL Winter Workshop*.

Cloosterman, M., Van de Wouw, N., Heemels, M., & Nijmeijer, H. (2006). Robust stability of networked control systems with time-varing networked-induced delays. *Proceedings of the 45th IEEE Conference on Decision & Control* (pp. 4980 – 4985). San Diego, California, United States of America.

Cosgrove, J., Guarro, S., Romanski, G., & Yau, M. (1996). Dynamic modeling and verification of safe-set architectures. *WESCON/96* (pp. 528 – 533).

Dugan, J. B., Bavuso, S. J., & Boyd, M. A. (1993). Fault trees and Markov models for reliability analysis of fault-tolerant digital systems. *Reliability Engineering and System Safety*, 39, 291 – 307.

Ebeling, C. (1996), *An introduction to reliability and maintainability engineering*. McGraw-Hill.

Fieguth, W. (2008). *Computer Control - DCC vs DCS* [PowerPoint slides]

Fullwood, R., Gunther, W., Valente, J., & Azarm, M. A. (1991). Advanced reactor instrumentation and control reliability and risk assessment. *IEEE Nuclear Science Symposium*, 2, 1394 – 1399.

Galdun, J., Takac, L., Lingus, J., Thiriet, J. M., & Sarnovsky, J. (2008). Distributed control systems reliability: consideration of multi-agent behaviour. *6th International Symposium on Applied Machine Intelligence and Informatics* (pp. 157 – 162).

Garrett, C. J., & Apostolakis, G. E. (2002). Automated hazard analysis of digital control systems. *Reliability Engineering and Safety Systems*, 77, 1 – 17.

Garrett, C. J., Guarro, S. B., & Apostolakis, G. E. (1995). The dynamic flowgraph methodology for assessing the dependability of embedded software systems. *IEEE Transactions on Systems, Man, and Cybernetics*, 25, 824 – 840.

Garrett, C. J., Guarro, S. B., & Apostolakis, G. E. (1993). Assessing digital control system dependability using the dynamic flowgraph methodology. *Transactions of the American Nuclear Society, American Nuclear Society Winter Meeting*, 69, 290 – 291.

Ghostine, R., Thiriet, J. -M., Aubry, J. -F., & Robert, M. (2008). A framework for the reliability evaluation of networked control systems. *17th IFAC World Congress*.

Guarro, S., & Yau, M. (1994). Dynamic flowgraph methodology as a tool for process control software PRA. *Annual Meeting of the American Nuclear Society*, 70, 222 – 223.

Guarro, S. B., & Yau, M. K. (1996). Analysis of control software in advanced reactors using the dynamic flowgraph methodology (DFM). *Proceedings of the 1996 ANS International Topical Meeting on Nuclear Plant Instrumentation Control and Human Machine Interface Technologies* (pp. 1025 – 1032).

Guarro, S., Yau, M., & Motamed, M. (1996). Development of tools for safety analysis of control software in advanced reactors. NUREG/CR-6465, U.S. Nuclear Regularity Commission.

Hemeida, A. M., El-Sadek, M. Z., & Younies, S. A. (2004). Distributed control system approach for a unified power system. *39th International Universities Power Engineering Conference* (pp. 304 – 307).

Harber, J. E., Kattan, M. K., & MacBeth, M. J. (1996). Distributed control system for CANDU 9 nuclear power plant. *17th Annual Conference of the Canadian Nuclear Society*.

Hespanha, J. P., Naghshtabrizi, P., & Xu, Y. (2007). A survey of recent results in networked control systems. *Proceedings of the IEEE*, 95(1), 138 – 162.

Houtermans, M., Apostolakis, G., Brombacher, A., & Karydas, D. (2000). Programmable electronic system design & verification utilizing DFM. *Proceedings of the 19th International Conference on Computer Safety, Reliability and Security* (pp. 275 – 285).

Huo, Z., & Fang, H. (2007). Research on robust fault-tolerant control for NCS with data packet dropout. *Journal of Systems Engineering and Electronics*, 18, 76 – 82.

Huo, Z., & Zhang, Z. (2008). Robust stability analysis for networked control systems. *International Symposium on Intelligent Information Technology Application Workshops* (pp. 164 – 167).

Jia, H., Zhuang, W., Bai, Y., Fan, P., & Huang, Q. (2007). The distributed control system for light space manipulator. *International Conference on Mechatronics and Automation* (pp. 3525 – 3530).

Jian, S., & Shaoping, W. (2006). Reliability analysis and congestion control on network nodes. *IEEE Conference on Robotics, Automation and Mechatronics* (pp. 1 – 6).

Kadri, A. (2006). Survey of networked control systems and their potential application in nuclear power plants. *27th Annual CNS Conference & 30th CNS/CNA Student Conference*, Toronto, Ontario, Canada.

Kim, H. S., Lee, J. M., Park, T., & Kwon, W. H. (2000). Design of networks for distributed digital control systems in nuclear power plants. *International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies*.

Kim, W. -J., Ji, K., & Ambike, A. (2006). Real-time operating environment for networked control systems. *IEEE Transactions on Automation Science and Engineering*, 3, 287 – 296.

Kirschenbaum, J., Stovsky, M., Mandelli, D., Bucci, P., Aldemir, T., Miller, D. W.,...Arndt, S. A. (2006). A benchmark system for the assessment of reliability modeling methods for digital instrumentation and control sstems in nuclear plants. *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation Control and Human Machine Interface Technologies* (pp. 277 – 283).

Kumar, M., Verma, A. K., & Srividya, A. (2009). Probabilistic modeling of network-induced delays in networked control systems. *International Journal of Applied Mathematics and Computer Science*, 5, 43 – 54.

Le, K. V., & Li, V. O. K. (1989). Modeling and analysis of systems with multimode components and dependent failures. *IEEE Transactions on Reliability*, 38, 68 – 75.

Lian, F, Moyne, J. R., & Tilbury, D. M. (2001). Performance evaluation of control networks: Ethernet, ControlNet, and DeviceNet. *IEEE Control Systems Magazine*, 21, 66 – 83.

Lian, F. -L., Moyne, J., & Tilbury, D. (2002). Network design consideration for distributed control systems. *IEEE Transactions on Control Systems Technology*, 10, 297 – 307.

Lu, L., & Jiang, J. (2004). Probabilistic safety assessment for instrumentation and control systems in nuclear power plants: an overview. *Journal of Nuclear Science and Technology*, 41, 323 – 330.

Milici, A., Wu, J. –S., & Apostolakis, G. (1996). The use of the dynamic flowgraph methodology in modeling human performance and team effects. *Proceedings of 1996 ANS International Topical Meeting on Nuclear Plant Instrumentation Control and Human Machine Interface Technologies* (pp. 653 – 659).

Naterer, G. F., Daggupati, V., Marin, G., Gabriel, K., & Wang, Z. (2008). Thermochemical hydrogen production with a copper-chlorine cycle, II: flashing and drying of aqueous cupric chloride. *International Journal of Hydrogen Energy*, 33, 5451 – 5459.

Nolte, T., Hansson, H., & Norstrom, C. (2003). Probabilistic worst-case response-time analysis for the controller area network. *Proceedings of the 9th IEEE Real-Time and Embedded Technology and Applications Symposium* (pp. 200 – 207).

Park, T. R., Lee, J. M., Choi, J. Y. Shin, S. Y., Kim, H. S., Lee, J. Y., & Kwon, W. H. (2000). Implementation of PICNET+ as the control network of the distributed control system for the nuclear power plant. *International Topical Meeting on Nuclear Plant Instrumentation, Controls and Human-Machine Interface Technologies*.

Rosen, M. A., Naterer, G. F, Sadhankar, R. & Suppiah, S. (2006). Nuclear-based hydrogen production with a thermochemical copper-chlorine cycle and supercritical water reactor. *Canadian Hydrogen Association Workshop*.

Smith, D. J. (2005). *Reliability, maintainability and risk*. Elsevier Butterworth-Heinemann.

Soglo, A. B., & Xianhui, Y. (2006). Networked control system simulation design and its application. *Tsinghua Science and Technology*, 11, 287 – 294.

Tian, Y. -C., & Levy, D. (2008). Compensation for control packet dropout in networked control systems. *Information Sciences*, 178, 1263 – 1278.

Wang, Z, Naterer, G. F. & Gabriel, K. (2008). Multiphase reactor scale-up for Cu-Cl thermochemical hydrogen production. *International Journal of Hydrogen Energy*, 33, 6934 – 6946.

Wu, J., Deng, F. -Q., & Gao, J. -G. (2005). Modelling and stability of long random delay networked control systems. *Proceedings of the Fourth International Conference on Machine Learning and Cybernetics* (pp. 947 – 952).

Yau, M., Guarro, S., & Apostolakis, G. (1995). Demonstration of the dynamic flowgraph methodology using the titan II space launch vehicle digital flight control system. *Reliability Engineering and System Safety*, 49, 335 – 353.

Yildiz, B, & Kazimi, M. S. (2006). Efficiency of hydrogen production systems using alternative nuclear energy technologies. *International Journal of Hydrogen Energy*, 31, 77 – 92.

Zagar, K. (2005). Dependability considerations in distributed control systems. *10th International Conference on Accelerator & Large Expt. Physics Control Systems*.

Zhang, W., Branicky, M. S., & Philips, S. M. (2001). Stability of networked control systems. *IEEE Control Systems Magazine*, 84 – 99.

Zhang, Z., Zheng, Y., & Lu, G. (2006). Stochastic stability of networked control systems with network-induced delay and data dropout. *Proceedings of the 24th IEEE Conference on Decision & Control* (pp. 5006 – 5011), San Diego, California, United States of America.

Zhang, Y., Zhong, Q., & Wei, L. (2008). Stability of networked control systems with communication constraints. *Chinese Control and Decision Conference* (pp. 335 – 339).

APPENDIX

```
%%This MATLAB code is used to calculate the total network delay
%produced in a NCS example.
%%BY: AHMAD W. AL-DABBAGH


%% Variables initialization

% preprocessing time at the source node when processor is unavailable -
% in microseconds
Tau_x = 10000000;
% status of source node hardware and software
SHSS = 0;
% preprocessing time at source node when processor is available - in
% microseconds
Tau_pre = 1;
% postprocessing time at destination node when processor is unavailable
% - in microseconds
Tau_y = 10000000;
% status of destination node hardware and software
DHSS = 0;
% postprocessing time at destination node when processor is available -
% in microseconds
Tau_post = 1;
% message size - in bits
ms = 240;
% bit time - in microseconds
Tau_bit = 0.2;
% network delay when communication network is unavailable - in
% microseconds
Tau_k = 10000000;
% availability of communication network link
NTA = 0;
% waiting time at the source node - in milliseconds
Tau_wait = rand(1)*2000;


%% Device delay calculations

if (SHSS == 0)
   pre = Tau_pre;
else
   pre = Tau_x;
end
```

```
if (DHSS == 0)
   post = Tau_post;
else
   post = Tau_y;
end

% device delay
device_delay = pre + post;

%% Network delay calculations

% transmission delay
Tau_trans = ms*Tau_bit;

if (Tau_wait >1200)
   Tau_wait = 1200;
else
   Tau_wait = Tau_wait;
end

Tau_wait = Tau_wait*1000;
network_del = Tau_wait + Tau_trans;

if (NTA == 0)
   network_delay = network_del;
else
   netwrok_delay = Tau_k;
end



%% Total delay calculation

% total time delay - in seconds
total_delay = (device_delay + network_delay)/1000000
```