SECURE TRILATERAL ACCESS CONTROL FOR NETWORK-INTEGRATED
NUCLEAR OPERATION AND CONDITION-BASED NUCLEAR MAINTENANCE

by

Herman Cheung

B.Eng., Ryerson University, 2012

A thesis

presented to Ryerson University

in partial fulfillment of the

requirement for the degree of

Master of Applied Science

in the Program of

Electrical and Computer Engineering

Toronto, Ontario, Canada, 2015

© Herman Cheung 2015

AUTHOR'S DECLARATION FOR ELECTRONIC SUBMISSION OF A THESIS

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

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

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

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

ABSTRACT

SECURE TRILATERAL ACCESS CONTROL FOR NETWORK-INTEGRATED NUCLEAR OPERATION AND CONDITION-BASED NUCLEAR MAINTENANCE

Master of Applied Science in the Program of Electrical and Computer Engineering, 2015

Herman Cheung

Ryerson University

The intent of this thesis research is to develop a new methodology to improve existing nuclear process in an efficient, precise, and cost-effective way.

This thesis presents three new designs: Secure Trilateral Access Control (***STAC***), Network-Integrated Nuclear Operation (***NINO***), and network-driven Condition-Based Nuclear Maintenance (***CBNM***).

STAC design has three tiers: Tier-1 ensures security controls of external accesses to the new nuclear network. Tier-2 ensures qualification controls for carrying nuclear operations. Tier-3 ensures qualification controls for nuclear maintenances.

NINO design is to increase efficiency of conducting nuclear operations and ensure correctness of executing targeted operations

CBNM design is to increase efficiency and cost savings for conducting nuclear maintenance and schedule maintenance based on equipment conditions to avoid extremely expensive forced outages.

Feasibility and practicality of these new designs are illustrated analytically and numerically in the thesis. The significance of these designs is tremendous, resulting in huge nuclear operation cost savings.

ACKNOWLEDGEMENTS

I would like to express my heartfelt gratitude to Dr. Truman Cungang Yang, my supervisor, for his expert supervision and remarkable encouragement during my graduate study and this thesis research.

I would like to express special thanks to my father Professor Richard Cheung, my mother Mrs. Linda Cheung, and my sister Dr. Helen Cheung for their continuous encouragement and support.

TABLE OF CONTENTS

	page
Author's Declaration	ii
Abstract	iii
Acknowledgements	iv
Table of Contents	v
List of Tables	vii
List of Figures	viii
Chapter 1: INTRODUCTION	1
1.1 Review of Current States of Industrial Controls and Network Access Controls	4
1.2 Introduction of Nuclear Generation Basic	6
1.3 Base for Nuclear Network Access Control	7
1.4 Base for Network-Integrated Nuclear Operation (<i>NINO</i>)	9
1.5 Base for network-driven Condition-Based Nuclear Maintenance (<i>CBNM</i>)	11
1.6 Overall Motivation and Significance	13
Chapter 2: NUCLEAR NETWORK SECURE TRILATERAL ACCESS CONTROL	14
2.1 Secure Trilateral Access Control (<i>STAC</i>) – Basic Architecture	15
2.2 Authentication for Nuclear Network Access Control	21
2.3 Authorization for Network-Integrated Nuclear Operations (<i>NINO</i>)	23
2.4 Authorization for Condition-Based Nuclear Maintenance (<i>CBNM</i>)	25
2.5 Specifications of Certifications for Secure Access to Tier-1, 2, 3 Networks	27
2.6 Design Evaluation for <i>STAC</i>	31
Chapter 3: NETWORK-INTEGRATED NUCLEAR OPERATIONS	34
3.1 Architecture of Network-Integrated Nuclear Operations	36
3.2 Nuclear Reactor Control Division - D_{NRC} (0,0,0,0,0,1)	41
3.3 Reactor Heat Transport Control Division – D_{HTC} (0,0,0,0,0,2)	55
3.4 Live <i>NINO</i> Data Base	63
3.5 Design Evaluation of <i>NINO</i>	64
Chapter 4: NETWORK-DRIVEN CONDITION-BASED NUCLEAR MAINTENANCE	66

4.1	Network-assisted Nuclear Condition-Based Maintenance	68
4.2	Operation Conditions {OC-set}	71
4.3	System Conditions {SC-set}	73
4.4	Equipment Conditions {EC-set}	77
4.5	Maintenance Conditions {MC-set}	79
4.6	Security Conditions {SL-set}	82
4.7	Live <i>CBNM</i> Data Base	85
Chapter 5:	DESIGN, MODELLING, AND EVALUATION OF NETWORK-DRIVEN CONDITION-BASED NUCLEAR MAINTENANCE	86
5.1	<i>CBNM</i> Design, Modelling, and Evaluation Focus	88
5.2	<i>CBNM</i> for <i>Valves</i> equipment group {EC-1}	91
5.3	<i>CBNM</i> for Pumps equipment group {EC-2}	109
5.4	<i>CBNM</i> for Controllers equipment group – condition {EC-3}	125
Chapter 6:	CONCLUSION	133
6.1	Major Research Work Completed	134
6.2	Major Research Contributions	136
6.3	Future Work	139
APPENDIX I		140
REFERENCES		149

LIST OF TABLES

	page
Table 2.1: $CNA(ID_X, PK_X)$	27
Table 2.2: $COQ(ID_X, \{LoQ\}_x)$	29
Table 2.3: $\{L_{(n1...n6)}\}$	29
Table 2.4: $CMQ(ID_X, \{LMQ\}_x)$	30
Table 2.5: $\{L_{(OC)}\}$	30

LIST OF FIGURES

	page
Figure 2.1: Basic Secure Trilateral Access Control (STAC)	16
Figure 2.2: Tier-1 Nuclear Network Access Control	17
Figure 2.3: Tier-2 <i>NINO</i> network access control	18
Figure 2.4: Tier-3 Condition-based Nuclear Maintenance	19
Figure 2.5: <i>Tier-1</i> secure network access authentication flow diagram	21
Figure 2.6: <i>Tier-2</i> secure <i>NINO</i> authorization flow diagram	23
Figure 2.7: <i>Tier-2</i> secure <i>NINO</i> authorization flow diagram	25
Figure 3.1 Tier 2 of STAC	34
Figure 3.2: <i>OSL-1</i> and <i>OSL-2</i> <i>NINO</i> and Codes	36
Figure 3.3: Nuclear Reactor Control (<i>NRC</i>) in <i>OSL-1</i>	39
Figure 3.4: Heat Transport Control (<i>HTC</i>) in <i>OSL-1</i>	40
Figure 3.5: Reactor Reactivity Control Systems	42
Figure 3.6: Reactor Flux/Power Measuring Equipment	43
Figure 3.7: Liquid Zone Resistivity Controlling Equipment	46
Figure 3.8: Reactor Control Systems	49
Figure 3.9: Reactor ShutDown Systems	51
Figure 3.10: Moderator Temperature Control Systems	53
Figure 3.4: Heat Transport Control (<i>HTC</i>) in <i>OSL-1</i>	55
Figure 3.11: Heat transport Feed control Systems	56
Figure 3.12: Heat transport Bleed control Systems	58
Figure 3.13: Heat transport Condenser control Systems	60
Figure 4.1: Tier-3 CBMM	66
Figure 4.2: Condition-Based Nuclear Maintenance (CBNM)	68
Figure 4.3: Architecture for <i>CBNM</i>	69
Figure 4.4: $\{OC-set\}$ for E_{CBNM}	71
Figure 4.5: $\{SC-set\}$ for E_{CBNM}	73
Figure 4.6: $\{EC-set\}$ for E_{CBNM}	77
Figure 4.7: $\{MC-set\}$ for E_{CBNM}	79
Figure 4.8: $\{SL-set\}$ for E_{CBNM}	82
Figure 5.1: <i>CBNM</i> condition sets $\{EC-1, EC-2, EC-3\}$	86
Figure 5.2: Nuclear equipment groups selected for CBNM designs evaluation	88
Figure 5.3: Rate of valve leakage (q_m) versus differential pressure across orifice (ΔP)	94

Figure 5.4: Base curve for acceptable valve stroke versus actuator pressure performance	96
Figure 5.5: Valve seat degradation	98
Figure 5.6: Broken valve stem	99
Figure 5.7: Excessive friction	100
Figure 5.8: Bent valve stem	102
Figure 5.9: Broken actuator multi-springs	103
Figure 5.10: Double Preload	104
Figure 5.11: Valve stem misalignment	105
Figure 5.12: Failed full stroke	107
Figure 5.13: Localized wear stem	108
Figure 5.14: Base pump curve	118
Figure 5.15: Base curve for an unregulated valve used as pump load	120
Figure 5.16: Base curves for a pump and its valve load	120
Figure 5.17: Base pump, two parallel-connected pumps, and two series-connected pumps	122
Figure 5.18: Base valve, two parallel-connected valves, and two series-connected valves	123
Figure 5.19: Composite pump-valve load configurations	124
Figure 5.20: Base current-to-pressure valve control	127
Figure 5.21: Drift on current-to-pressure control	128
Figure 5.22: Dynamic error on current-to-pressure control	129
Figure 5.23: NonLinear (cam) current-to-position control	131
Figure 5.24: Dynamic-error on NonLinear (cam) current-to-position control	132

Chapter 1

INTRODUCTION

The intent of this thesis research is to develop a new methodology to improve the existing nuclear practices, both operations and maintenances, in an efficient, precise, and cost-effective way.

The existing nuclear practice is lagging of the pace of modern process control technology. For example, the current smart process control equipment/system has networking capability with intelligent features for central data processing, equipment operations optimizing and coordinating, condition-based (predictive) maintenance scheduling, etc. Conversely, many nuclear units such as those in Ontario were built about thirty or forty years ago with the best technologies of that time or earlier, but many of their process control equipment and procedures are obsolete and cannot offer the intelligent features just mentioned. Even though there is an increasing number of obsolete nuclear equipment replaced by equipment with new technology, the intelligent features with networking capability available in these new equipment, however, are either not used or substantially limited due to security concerns. Therefore, the potential benefits from the use of the networking intelligent feature, such as efficiency, safety, increased productivity and revenue, cost savings in the nuclear process, virtually cannot be realized.

This thesis research develops an innovative way with three new designs for improving the existing nuclear operations and maintenances, utilizing the modern process control equipment with networking intelligent feature. The three new designs are: the *Secure Trilateral Access Control (STAC)*, the *Network-Integrated Nuclear Operation (NINO)*, and the network-driven *Condition-Based Nuclear Maintenance (CBNM)*.

The *STAC* design has three tiers: Tier-1 is to ensure the security control of external accesses to the new nuclear process network, to stop unauthorized entrance into the nuclear network, and to minimize the safety concerns on the networking for nuclear operations. Tier-2 is to ensure the qualification control for conducting nuclear operations that is to increase the quality control of live safety-critical nuclear operations. Tier-3 is to ensure the qualification control for carrying out nuclear maintenance work that is to increase the quality control of online nuclear maintenance [1-15].

The *NINO* design has three folds: One is to fully utilize the networking intelligent feature in the modern smart process control equipment/systems for central data processing, equipment operations optimizing and coordinating, etc. One is to minimize the nuclear workers' exposure to potential nuclear radiations by conducting the nuclear operations remotely through the network, as much as possible. One is to increase

the efficiency of conducting the nuclear operations with available online information and online authorization by minimizing the well-known paper work burden in the nuclear industry, as well as to improve the correctness and precision of the nuclear operations being carried out [16-29].

The **CBNM** design has a supreme objective that is the cost saving in nuclear process. As being well known, a nuclear unit outage is extremely expensive, probably up to one million dollars one day for one nuclear unit outage, due to mainly loss of revenue as well as maintenance costs. The **CBNM** design is to carry out condition-based maintenance that is to monitor continuously the performance/condition of the nuclear equipment and to schedule a maintenance for the next available nuclear unit outage when the equipment condition reaches a defined maintenance criterion. One purpose of the condition-based maintenance is to schedule a maintenance for an equipment when its performance is deteriorating to a defined criterion, prior to equipment failure such that if the criterion is properly set up, then the chance for the expensive forced outage can be minimized, leading to significant cost savings (one day of forced outage may cost one million dollars per nuclear unit). The other purpose is to extend the operating time before the need to call for the next outage maintenance that also has significant cost savings.

This thesis presents:

- Chapter 1: This chapter presents an introduction of this thesis research.
- Chapter 2: This chapter presents a new design, the *Secure Trilateral Access Control* (STAC) for the security control of external access to a new nuclear process network.
- Chapter 3: This chapter presents a new design, the *Network-Integrated Nuclear Operation* (NINO) and establishes a *NINO*-coded network base to be used for carrying out nuclear operations through the *NINO* network.
- Chapter 4: This chapter presents a new design, the network-driven *Condition-Based Nuclear Maintenance* (CBNM) and establishes a *CBNM*-coded network base to be used for carrying out nuclear maintenances through the *CBNM* network.
- Chapter 5: This chapter presents the design and evaluation of the condition-based maintenance **CBNM** in association with **NINO** under **STAC** access control, all of which are created in this thesis.
- Chapter 6: This chapter presents the conclusion of this thesis research.

This chapter presents:

- Section 1.1: This section presents a review of the current states of industrial process controls and network access controls.
- Section 1.2: This section introduces the basic of Ontario nuclear power electricity generation using the CANDU reactor.
- Section 1.3: This section presents the base for an access control to a nuclear operation network. The base includes considerations of underlining environment, intended features, and the nuclear industry well-known requirements of COMS (Constructable, Operateable, Maintainable, Safety) in the development of the access control.
- Section 1.4: This section presents the base for the *NINO* development. The base includes considerations of underlining environment, intended features, and the nuclear industry requirements of COMS (Constructable, Operateable, Maintainable, Safety) in the development of *NINO*.
- Section 1.5: This section presents the base for the network-driven *CBNM* development. The base includes considerations of underlining environment, intended features, and the nuclear industry requirements of COMS in the development of *CBNM*.
- Section 1.6: This section presents the overall motivation and significance of this thesis research.

1.1 Review of Current States of Industrial Controls and Network Access Controls

This presents a review of the current states of industrial process controls and network access controls.

This thesis research is to be focused on the nuclear process control system that falls into the overall category of industrial control systems, but the nuclear system has extra unique requirements due to nuclear safety considerations. Hence, the current state of the industrial controls is to be reviewed in this section as a background study for this thesis research.

This thesis research is to develop a new network-integrated nuclear operation and a new network-driven condition-based nuclear maintenance system that require a secure access control suitable for the nuclear network. Hence, the current state of the network access control is to be reviewed in this section as a background study for this thesis research.

NIST 800-82 *Guide to industrial control systems security* and other NIST publications [5-12] to be good background studies for the security of industrial control systems. The NIST 800-82 guide lists typical considerations for the security of industrial control systems that cover the nuclear process control system focused in this thesis research as highlighted below:

- *Performance Consideration:* The industrial control system is time-critical with limited tolerable delay. Many industrial control systems require deterministic responses but their high throughput may not be very essential, as compared to information technology (IT) systems.
- *Availability Consideration:* Many industrial control systems are continuous operating system, of which unexpected outages typically are not acceptable. Outages of these systems must be scheduled in advance. Many industrial control systems require high availability, reliability and maintainability. Therefore some IT strategies for example rebooting a component are usually not acceptable to many industrial control systems that include the nuclear process control system.
- *Risk Consideration:* The primary considerations for the industrial control systems include human safety and fault tolerance to prevent loss of life or endangerment of public health or confidence, regulatory compliance, loss of equipment, loss of intellectual property, etc. On the other hand, the primary considerations for the IT systems are data confidentiality and integrity.
- *Time Criticality Consideration:* The industrial control system automated response time or the system response to operator interaction is very critical, but this usually is not critical for IT systems.

However, the nuclear process control has much strict requirements due to nuclear safety concerns.

ANSI INCITS 359: Role Based Access Control (RBAC) and other access control publications [16-29] to be good background studies for the network access controls. A review of the 359 RBAC standard is provided as follows:

- The RBAC consists of a reference model that defines the sets of basic elements (users, roles, permissions, operations and objects) and relations. This model identifies the minimum set of features, aspects of role hierarchies, aspects of static constraint relations, and aspects of dynamic constraint relations. This model can be defined in terms of Core RBAC, Hierarchical RBAC, Static Separate of Duty (SSD), and Dynamic Separate of Duty (DSD). The core RBAC specifies a minimum collection of RBAC elements that include users, roles, permissions, operations, and objects, and a minimum collection of RBAC relations that include user-role and permission-role assignments. The hierarchical RBAC augments relations to support role hierarchies, of which a hierarchy is a partial order defining a seniority relation between roles, whereby senior roles acquire the permissions of their juniors and junior roles acquire users of their seniors. The RBAC SSD relation adds exclusivity relations among roles with respect to user assignments in the presence and absence of role hierarchies. The RBAC DSD relation defines exclusivity relations with respect to roles that are activated as part of a user session.
- The RBAC consists of a system and administrative functional specification that specifies the features of administrative operations, administrative reviews, and system level functionality. The administrative operations define functions and semantics to create, delete and maintain RBAC elements and relations. The administrative reviews define functions and semantics to perform query operations on RBAC elements and relations. The system level functionality defines the creation of user sessions to perform role activation/deactivation, enforcement of constraints on role activation, and access decision.

However, there are limitations in the RBAC when it is used for the control of access to the nuclear process operations. Here provides an illustration: In the RBAC, if a user is assigned with a role, then the user will have all the privileges of that role and can execute all the operations or can access all the objects associated with the permissions assigned to that role. However, the RBAC cannot fully satisfy all the strict requirements for access to the nuclear process operations, because the operation of each of over a thousand of devices in a nuclear plant is often fairly unique and any mis-operations could cause tremendous serious nuclear consequences or even casualties and the nuclear devices operations require the operators' currency of technologies that can only be accredited with constant trainings. Therefore, it is not simply assigning a role that the nuclear user can have the privileges of that role to carry out all the nuclear operations.

1.2 Introduction of Nuclear Generation Basic

This section introduces the basic of Ontario nuclear power electricity generation using the CANDU (CANada Deuterium Uranium) reactor, of which the nuclear operation is the subject matter of this thesis research.

The CANDU reactor is a Canadian invented pressurized heavy water reactor. The fuel used in the reactor is natural uranium that consists of mainly U238 and a small amount of fissile U235. The fission of U235 produces heat that is used to generate electricity.

The CANDU reactor is operated to sustain a steady rate of fission such that an equilibrium condition known as criticality is achieved when the neutrons released by U235 fission cause an equal number of fissions in other U235 atoms. The neutrons released by fission are however fairly energetic and are not readily captured by other sparse fissile U235. The neutrons must have their energy moderated to sustain the chain reaction of fission.

Light water (just ordinarily available water) is a too good moderator of which the hydrogen atoms can absorb a lot of energy in a single collision, but the hydrogen also absorbs neutrons too effectively such that too few neutrons are left to react with the other sparse fissile U235 in the natural uranium. This prevents the criticality for sustained chain reaction of fission for electricity generation.

Heavy water (deuterium-oxide) used as moderator has advantage over light water in terms of non-absorption of neutrons, because the deuterium (also known as heavy hydrogen) in the heavy water already has the extra neutron that reduces the tendency to capture excessive neutrons. The use of heavy water can sustain the criticality of chain reaction of fission. This allows the use of unenriched natural uranium as fuel in the reactor that is the unique feature of the CANDU reactor.

In a CANDU nuclear generating unit, the fission reaction in the reactor core heats the pressurized heavy water in the calandria. The moderator uses heavy water to slow down fast and energetic neutrons released by fission to an energy level suitable for sustaining the chain reaction fission.

The pressurized heavy water is circulated between reactor fuel channels and steam generators, known as primary heat transport. The steam generator (boiler) transfers the heat to the light water (feedwater) in the secondary cooling loop.

The steam from the boiler powers a steam turbine that run an electricity generator. The generator connects to the grid for electricity transmission. The exhausted steam from the turbine is condensed with lake water and returned as feedwater to the boiler.

1.3 Base for Nuclear Network Access Control

This section presents the base for an access control to a nuclear operation network. The base includes considerations of underlining environment, intended features, and the well-known nuclear requirements of COMS (Constructable, Operateable, Maintainable, Safety) in the development of the access control.

The access control to the nuclear operation network must be extremely secure because it is a safety-critical, economic-critical, infrastructure-critical, and availability-critical network, as well as the access control is required to be efficient as it is a live online operating network.

This thesis research creates a trilateral access control for the nuclear application. This control is termed as the *Secure Trilateral Access Control (STAC)* which is composed of:

- *Tier-1* for external entry to nuclear process network access control.
- *Tier-2* for the network-integrated nuclear operation access control.
- *Tier-3* for the network-driven nuclear condition-based maintenance access control.

The rationale for this three-tier access control is for achieving *security*, *correctness* and *efficiency* performance and meeting the nuclear *COMS* requirements. This forms the base for this access control development, as described in the following:

Security:

Tier-1 provides a high secure access control of external access to the nuclear process network by authenticating network-access requester (mostly the nuclear worker)'s certificate of network access authorization. This is the first and most important nuclear process network access control to stop all unauthorized access requests. This access control uses a new design of authentication procedure that employs state-of-the-art public-private key encryption and mutual authentication technology.

A mutual (two-way) authentication is designed between the nuclear worker for requesting access to the nuclear process network and the authentication server for checking the authorization of the requester. In this mutual authentication process, the nuclear worker is to ensure that he/she is not communicating with a malicious network server by authenticating the server. If this property is absent, a malicious network server is capable of mounting a person/device-in-the-middle attack to gather data/information from the nuclear worker. Also the authentication server is to ensure that it is not communicating with a malicious worker by authenticating the worker. If this property is absent, a malicious worker is capable of accessing the live safety-critical nuclear operations.

Details of *Tier-1* authentication procedure are given in section 2.2.

Correctness and Efficiency:

Tier-2 access control uses a new design of *NINO* authorization procedure that employs the secure key for encryption based on the nonces that are generated by the nuclear worker and nuclear authentication server during the Tier-1 mutually authentication. The operation access authorization requires the access requester to have operation qualifications satisfying all the requirements for the requested nuclear operation. The operation qualification is composed of both engineering and field knowledge with more weighting on engineering aspects.

Tier-3 access control uses a new design of *CBNM* authorization procedure that employs the secure key as for the Tier-2 access. The maintenance access authorization requires the access requester to have maintenance qualifications satisfying all the requirements for the requested nuclear maintenance. The maintenance qualification is composed of both field and engineering experiences with more weighting on field aspects.

An unilateral (one-way) authentication is designed either, between the nuclear network user requesting for access to the *NINO* network and the operation server in the *Tier-2* access control or, between the nuclear user requesting for access to the *CBNM* network and the maintenance server in *Tier-3* access control.

The unilateral authentication is more *efficient* of less processing time but of lower security than the mutual authentication. The unilateral authentication is more suitable for Tier-2 operation qualifications authentication as well as for Tier-3 maintenance qualifications authentication. It is because first, all the nuclear workers' authorizations for network uses have been authenticated in Tier-1 that already provides a high level of security and second, the authentication process efficiency is crucial to improve the responsiveness of the new network-driven nuclear process.

Details of *Tier-2* and *Tier-3* authorization procedures are given in sections 2.3 and 2.4, respectively.

COMS (Constructable, Operatable, Maintainable, and Safety):

As the *Tier-1* authentication procedure in section 2.2, the *Tier-2* authorization procedure in section 2.3, and the *Tier-3* authorization procedure in section 2.4 have a clear layout, simple logic, and make use of standard authentication algorithms, these procedures are constructable, operateable, maintainable, and safe to use. Therefore they satisfy the nuclear industry's well-known requirements of COMS.

1.4 Base for Network-Integrated Nuclear Operation (*NINO*)

This section presents the base for the *NINO* development. The base includes considerations of underlining environment, intended features, and the nuclear industry requirements of COMS (Constructable, Operateable, Maintainable, Safety) in the development of *NINO*.

NINO is an efficient, simple, practical design that can transform the access to the tremendous complex safety-critical nuclear operations involving with over a thousand devices into a simple systematic access with proficient secure control. To realize the transformation feature, each requested network-integrated nuclear operation is assigned with a unique 6-number *NINO* access code and a secure operation pass code.

The 6-number *NINO* access code and the secure operation pass code form the base for the *NINO* development, as illustrated in the following:

Operation Pass Code:

1. Obtain a nuclear network pass code.

The nuclear worker submit his/her certificate of network access authorization to the authentication server for authentication and for obtaining a nuclear process *network pass code*.

2. Obtain a nuclear operation pass code.

The nuclear user submit his/her requested nuclear operation with a 6-number code and certificates of operation qualifications using the network pass code to the operation server for authorization and for obtaining an *operation pass code*.

3. Access *NINO* network for operation.

The user using the operation pass code to carry out the requested nuclear operation.

6-number NINO Code:

A *NINO* code is assigned for each nuclear operation, which is defined with a group of 6 numerical items in the form of:

(function #, device #, equipment #, system #, group-system #, division #)

where	division	= all nuclear control systems are divided into 4 divisions.
	group system	= each division is grouped into group systems based on key operations.
	system	= each group system is divided into systems based on specific operations.
	equipment	= key nuclear equipment in a system.

device = components in an equipment.
function = device/equipment monitoring, processing, or controlling function.

Details are given in chapter 3

For streamlining the security aspect, *NINO* defines two operation security levels (*OSL-1*, *OSL-2*):

- *OSL-1* is for the reactor-direct operations
- *OSL-2* is for the reactor-indirect operations.

NINO is divided into four nuclear operation access divisions, defined as:

- *OSL-1* Nuclear Reactor Control (NRC) division
- *OSL-1* reactor Heat Transport Control (HTC) division
- *OSL-2* Boiler Steam Control (BSC) division
- *OSL-2* Turbine Generator Condenser Control (TGC) division

Further, each *NINO* division is divided into group systems, each group system is divided into system, each system is divided into equipment and devices, and finally the functions of the nuclear devices are grouped into monitoring, processing, and controlling.

Eventually, the 6-number coded *NINO* transforms the access to the tremendous complex safety-critical nuclear operations involving with over a thousand devices into a simple systematic number code-guided access.

Details for *NINO* are given in chapter 3.

1.5 Base for network-driven Condition-Based Nuclear Maintenance (*CBNM*)

This section presents the base for the network-driven *CBNM* development. The base includes considerations of underlining environment, intended features, and the nuclear industry requirements of COMS (Constructable, Operateable, Maintainable, Safety) in the development of *CBNM*.

Condition-based (predictive) maintenance is the key for significant reduction of operation and maintenance (O&M) costs for the industry, especially for the nuclear industry of which the cost for *one day outage* for maintenance would be close to *one million dollars* for *one nuclear unit*. This thesis research is therefore focused on the reduction of the frequency and length of nuclear unit outage, leading to huge nuclear station cost savings or revenue increase.

In order to effectively implement the condition-based maintenance, this thesis research creates *CBNM*, the condition-based maintenance of nuclear process. The success of *CBNM* is based on the correct and timely assessments of nuclear devices/equipment on-going operations.

CBNM Security Levels

CBNM consists of three maintenance security levels:

- *MSL-1* for nuclear *On-line Critical CBNM*,
- *MSL-2* for nuclear *On-line Non-Critical CBNM*,
- *MSL-3* for nuclear *Outage CBNM*.

CBNM Code

Each authorized condition-based maintenance network access is assigned with one *CBNM* code which is defined in the form of:

$$\mathbf{CBNM\ code} = (\{\mathbf{SL-set}\}, \{\mathbf{MC-set}\}, \{\mathbf{EC-set}\}, \{\mathbf{SC-set}\}, \{\mathbf{OC-set}\})$$

where ***SL-set*** = Security Levels set: MSL-1, MSL-2, and MSL-3 security divisions

MC-set = Maintenance Conditions set: device adjustment, correction, replacement, etc.

EC-set = Equipment Conditions set: control valve, sensor, transmitters, etc.

SC-set = System Conditions set: high risk, low risk, critical, non-critical, backup, etc.

OC-set = Operation Condition set: a NINO code represents the set of nuclear operation.

Details are given in chapter 4.

CBNM Basic Process

- 1) A nuclear network user can initiate a maintenance work order after successfully passes the required authentication, and then the work order is sent to the *CBNM* network access control central system.
- 2) The maintenance work order is then processed with the components of the *CBNM* code that include *SL-set*, *MC-set*, *EC-set*, *SC-set*, and *OC-set* (the attributes of these *CBNM* components are to be detailed in the following sections). After all the *CBNM* components are determined, a *CBNM* access code is formed and then assigned for the maintenance work order.
- 3) With the access code, the *CBNM* can be linked to the *Tier-2 NINO* control divisions: *NRC*, *HTC*, *BSC*, or *TGC* (discussed in Chapter 3).
- 4) The *SL-set* is used for linking the security divisions: *MSL-1*, *MSL-2*, and *MSL-3*.

CBNM Design Base

The base for the *CBNM* is on the correct and timely assessments of nuclear devices/equipment's on-going operating *conditions*. In order to facilitate the secure, accurate and non-delayed assessments, the network-assisted *CBNM* is coded with **5 conditions sets**:

{*SL-set*}, {*MC-set*}, {*EC-set*}, {*SC-set*}, {*OC-set*}

These 5 conditions sets of the *CBNM* elements are required to be determined, prior to performing the actual physical condition-based maintenance.

Details for *CBNM* are given in chapter 4.

1.6 Overall Motivation and Significance

The creation of the network-driven condition-based nuclear maintenance network base is the major motivation and significance of this thesis research. The reasons are as follows:

- *Dual significance on practical and innovative R&D*

The creation of *CBNM* network base has dual significance on both practical and innovative R&D described below.

- *Success leading to enormous impact in industry and cost savings*

The significance of a practical R&D can be weighted with respect to the extent of its impacts in the industry. The condition-based nuclear maintenance is the most effective, practical way to avoid extremely expensive forced nuclear outages to the largest extent, as well as to reduce the frequency of outage that is to extend the operating period before calling for a scheduled outage. A forced outage, even if it is caused by a single device failure that only requires a quick fix, usually last at least two days. The use of condition-based maintenance to avoid forced outages or to reduce the frequency of outages has a huge cost saving implication as the cost could be a million dollars one day for one nuclear unit outage.

- *Innovative design: – First-of-the-kind practical development on safety-critical nuclear process*

For effectiveness of implementing the condition-based maintenance in the tremendous complex, safety-critical and economic-critical nuclear facility, the use of modern networking technology is the most effective way. The network-driven condition-based nuclear maintenance developed in this thesis research is first-of-the kind practical development on the safety-critical nuclear process.

- *Core design initiative to associated new designs*

The innovative design of the network-driven condition-based nuclear maintenance can be regarded as the core design that initiates other new designs for supporting it. The two major designs to be initiated and presented in this thesis are: ***STAC*** and ***NINO***.

Chapter 2

NUCLEAR NETWORK SECURE TRILATERAL ACCESS CONTROL

This chapter presents a new design, termed the *Secure Trilateral Access Control (STAC)* for the security control of external access to a new nuclear process network for carrying out the *Network-Integrated Nuclear Operation (NINO)* and *Condition-Based Nuclear Maintenance (CBNM)*. The *NINO* is to be presented in chapter 3, and *CBNM* is to be presented in chapter 4. All these designs are created in this thesis research.

The *STAC* is composed of three access controls:

- *Tier-1* for external entry to nuclear process network access control.
- *Tier-2* for the network-integrated nuclear operation access control.
- *Tier-3* for the network-driven nuclear condition-based maintenance access control.

First, this chapter defines the *Tier-1* network access authentication procedure, *Tier-2* nuclear operation authorization procedure, and *Tier-3* nuclear maintenance authorization procedure, with the features of:

- The *Tier-1* access control is the first and most important nuclear process network access control to stop all unauthorized access requests. This access control uses a new design of authentication procedure that employs state-of-the-art public-private key encryption and mutual authentication technology incorporated with the nuclear operation culture/established COMS (Constructable, Operable, Maintainable, and Safety).
- The *Tier-2* access control uses a new design of *NINO* authorization procedure that employs the secure key for encryption based on the nonces that are generated by the nuclear worker and nuclear authentication server during the *Tier-1* mutually authentication. The operation access authorization requires the access requester to have operation qualifications satisfying all the requirements for the requested nuclear operation. The operation qualification is composed of both engineering and field knowledge with more weighting on engineering aspects.
- The *Tier-3* access control uses a new design of *CBNM* authorization procedure that employs the secure key as for the *Tier-2* access. The maintenance access authorization requires the access requester to have maintenance qualifications satisfying all the requirements for the requested nuclear maintenance. The maintenance qualification is composed of both field and engineering experiences with more weighting on field aspects.

Second, this chapter describes the specifications of certifications and qualifications for the trilateral access controls, of which: *Certification of Network Access (CNA)*, *Certification of Operation Qualifications (COQ)*, *Certification of Maintenance Qualifications (CMQ)*, *List of Operation Qualifications (LOQ)* versus *List of operation requirements (L_(n1...n6))* and *List of Maintenance Qualifications (LMQ)* versus *List of maintenance requirements (L_(COA))* are specified in section 2.5.

Third, this chapter provides a design evaluation of the *STAC*. The evaluation covers: 1) the mutual (two-way) authentication designed between the nuclear worker requesting for access to the nuclear process network and the authentication server checking the authorization of the requester, in the *Tier-1* network access control; 2) the unilateral (one-way) authentication designed either, between the nuclear network user requesting for access to the *NINO* network and the operation server in the *Tier-2* access control or, between the user requesting for access to the *CBNM* network and the maintenance server in *Tier-3* access control.

This chapter presents:

- Section 2.1: This section presents a basic architecture of *STAC*, the new control for access to the new nuclear process operation and maintenance network.
- Section 2.2: This section details the authentication procedure for ***Tier-1***, the secure control of external access to the nuclear process network.
- Section 2.3: This section details the authorization procedure for ***Tier-2***, the secure control of access to the Network-Integrated Nuclear Operations (*NINO*).
- Section 2.4: This section details the authorization procedure for ***Tier-3***, the secure control of access to the Condition-Based Nuclear Maintenance (*CBNM*).
- Section 2.5: This section presents the specifications of certifications and qualifications for secure access to *Tier-1*, *Tier-2* and *Tier-3* nuclear networks.
- Section 2.6: This section presents the evaluation of the new design Secure Trilateral Access Control (*STAC*) for the security control of access to a new nuclear process network developed in this thesis research.

2.1 Secure Trilateral Access Control (STAC) – Basic Architecture

This section presents a basic architecture of *STAC*, the new control for access to the new nuclear process operation and maintenance network, developed in this thesis research, as shown in Figure 2.1. The *STAC* has a three-tier access control structure that includes:

- *Tier-1* for external entry to nuclear process network access control.
- *Tier-2* for the network-integrated nuclear operation access control.
- *Tier-3* for the network-driven nuclear condition-based maintenance access control.

There is an automatic inter-tier control between *Tier-2* and *Tier-3* for transfer of nuclear operating data for implementing the condition-based maintenance.

Figure 2.1: Basic Secure Trilateral Access Control (STAC)

2.1.1 *Outline of Tier 1 - Nuclear Network Access Control*

Tier 1 of the *STAC* is designed to control the external access to the nuclear process network. The key steps of this network access control, as illustrated in Figure 2.2, are:

Figure 2.2: Tier-1 Nuclear Network Access Control

- n1:** a nuclear worker- x (Wx) makes a request for access to the nuclear process network.
- n2:** Wx sends his/her *Certificate of Network Access (CNA)* to the *Authentication Server (AS)*.
- n3:** Wx and AS perform a mutual authentication using individual selected *nonces*. After mutual authentication is successful, a network-access pass code is formed using one nonce (NxI) from Wx and one nonce (NsI) from AS .

The network-access pass code is in the form of $\{N\mathbf{x}I, N\mathbf{s}I\}$.

- n4:** AS registers Wx as authorized nuclear network user- x (Ux) for a specified period of time.
- n5:** the Wx can use the pass code $\{NxI, NsI\}$ to log into the nuclear network as Ux , within the authorized time period, without requiring any further authentication.

2.1.2 Outline of Tier 2 - Nuclear Operation Access Control

Tier 2 of the *STAC* is designed to control the secure access to the network-integrated nuclear operation divisions/systems. The key steps of this operation access control, as illustrated in Figure 2.3, are:

Figure 2.3: Tier-2 *NINO* network access control

- o1:** *Ux* makes a request for access to the *Network-Integrated Nuclear Operations (NINO)* network to carry out a certain nuclear operation specified with a 6-digit *NINO* code (*n1...n6*). The *NINO* codes are to be developed in chapter 3.
- o2:** *Ux* sends his/her *Certificates of Operation Qualifications (COQ)* required for the requested nuclear operation specified by the *NINO* code (*n1...n6*) to the *Operation Server (OS)* for operation authorization.
- o3:** If *Ux*'s *COQ* is verified by *OS* to be qualified for *Ux*'s requested nuclear operation *NINO* (*n1...n6*), then *OS* issues a nonce (*NoI*) to *Ux* to form a pass code.
The operation-access pass code is in the form of $\{NxI, NsI, NoI\}$.
- o4:** *OS* registers *Ux* for the authorized nuclear operations, for a specified period of time.
- o5:** *Ux* can use $\{NxI, NsI, NoI\}$ to log in to perform the authorized nuclear operations, within the authorized time period, without requiring any further authorization.

2.1.3 Outline of Tier 3 - Nuclear Maintenance Access Control

Tier 3 of the *STAC* is designed to control the secure access to the network-driven condition-based maintenance systems. The key steps of this maintenance access control, as illustrated in Figure 2.4 are:

Figure 2.4: Tier-3 Condition-based Nuclear Maintenance

- m1:** *U_x* makes a request for access to the *Condition-Based Nuclear Maintenance (CBNM)* network to carry out a certain nuclear maintenance work specified by with one set of the *CBNM* code, termed as $\{OC\}$ which is formed from $\{NINO\text{ code } (n1 \dots n6)\}$. The *CBNM* codes are to be developed in chapter 4.
- m2:** *U_x* sends his/her *Certificates of Maintenance Qualifications (CMQ)* required for the requested nuclear maintenance specified by the *CBNM* $\{OC\}$ to the *Maintenance Server (MS)* for maintenance authorization.
- m3:** If *U_x*'s *CMQ* is verified by *MS* to be qualified for *U_x*'s requested nuclear maintenance work *CBNM* $\{OC\}$, then *MS* issues a nonce (*Nm1*) to *U_x* to form a pass code.
The maintenance-access pass code is in the form of $\{Nx1, Ns1, Nm1\}$.
- m4:** *MS* registers *U_x* for the authorized nuclear maintenance, for a specified period of time.
- m5:** *U_x* can use $\{Nx1, Ns1, Nm1\}$ to log in to perform the authorized nuclear maintenance work, within the authorized time period, without requiring any further authorization.

2.1.4 *Inter-Tier Transfer of Access Control*

There is an inter-tier transfer of access control: *Tier-2* $\Leftrightarrow$ *Tier-3*. This transfer is designed to be carried out automatically by the network access control program and is transparent to the nuclear worker / network users.

There are frequent automatic data transfers / communications between Tier 2 of operation and Tier 3 of maintenance, as they are tied closely together (see chapters 4 and 5).

2.2 Authentication for Nuclear Network Access Control

This section presents the authentication procedure for *Tier-1*, the secure control of external access to the nuclear process network, as shown in Figure 2.2.

This is the first and most important cyber security measure to stop any unauthorized access to the safety critically important nuclear process network.

Tier-1 secure network access authentication is proceeded, as shown in Figure 2.5, in 7 steps below.

Figure 2.5: *Tier-1* secure network access authentication flow diagram

Step-TI.1: A nuclear worker- x (Wx) makes a request for access to the *nuclear process network*; Wx sends his/her *Certificate of Network Access* $CNA(IDx, PKx)$ that contains information of Wx 's identity (IDx) and public key (PKx), to the *Authentication Server* (AS):

$$Wx: CNA(IDx, PKx) \Rightarrow AS \quad (2.1)$$

Step-TI.2: AS verifies $CNA(IDx, PKx)$ that is detailed in section 2.5;
 AS generates two nonces N_{S1} and N_{S2} , if $CNA(IDx, PKx)$ is verified;
 AS encrypts the two nonces using Wx 's public key (PKx) and sends the encrypted values to Wx :

$$AS: E_{(PKx)}\{N_{S1}, N_{S2}\} \Rightarrow Wx \quad (2.2)$$

Step-TI.3: Wx decrypts $[E_{(PKx)}\{N_{S1}, N_{S2}\}]$ using Wx 's private key (PRx) to obtain N_{S1} and N_{S2} :

$$Wx: D_{(PRx)}[E_{(PKx)}\{N_{S1}, N_{S2}\}] \Rightarrow \{N_{S1}, N_{S2}\} \quad (2.3)$$

Wx generates two nonces N_{X1} and N_{X2} ;

Wx encrypts the nonces using AS 's public key (PKs) and sends the encrypted values to AS :

$$Wx: E_{(PKs)}\{N_{X1}, N_{X2}, N_{S2}\} \Rightarrow AS \quad (2.4)$$

Step-TI.4: AS decrypts $[E_{(PKs)}\{N_{X1}, N_{X2}, N_{S2}\}]$ using AS 's private key (PRs) to obtain N_{X1} , N_{X2} and N_{S2} :

$$AS: D_{(PRs)}[E_{(PKs)}\{N_{X1}, N_{X2}, N_{S2}\}] \Rightarrow \{N_{X1}, N_{X2}, N_{S2}\} \quad (2.5)$$

AS sends N_{X2} to Wx for declaring “ Wx is authenticated by AS ”, if N_{S2} is the correct one that was sent by AS in Step-1.2:

$$AS: N_{X2} \Rightarrow Wx \quad (2.6)$$

Step-TI.5: Wx sends N_{S2} to AS for declaring “ AS is authenticated by Wx ”:

$$Wx: N_{S2} \Rightarrow AS \quad (2.7)$$

Step-TI.6: AS transfers $\{N_{X1}, N_{S1}\}$ internally to NINO Operation Server (OS) and to CBNM Maintenance Server (MS) for future communication with Ux , after nuclear worker-x enters the nuclear network and becomes the nuclear network user Ux :

$$AS: \{N_{X1}, N_{S1}\} \Rightarrow OS \quad (2.8)$$

$$AS: \{N_{X1}, N_{S1}\} \Rightarrow MS \quad (2.9)$$

Step-TI.7: Ux , AS , OS , and MS can use (N_{X1}, N_{S1}) to encrypt future communication:

$$Ux: E_{(N_{X1}, N_{S1})}\{\text{message}_{Ux}\} \Rightarrow AS, OS, \text{ or } MS \quad (2.10)$$

$$Ux \Leftarrow AS: E_{(N_{X1}, N_{S1})}\{\text{message}_{AS}\}$$

$$Ux \Leftarrow OS: E_{(N_{X1}, N_{S1})}\{\text{message}_{OS}\}$$

$$Ux \Leftarrow MS: E_{(N_{X1}, N_{S1})}\{\text{message}_{MS}\} \quad (2.11)$$

2.3 Authorization for Network-Integrated Nuclear Operations (NINO)

This section presents the authorization procedure for *Tier-2*, the secure control of access to the Network-Integrated Nuclear Operations (NINO), as shown in Figure 2.4.

This security measure is to stop any unauthorized access to the safety critically important live nuclear operations. The *NINO* likes a two-side blade, of which one side can cut down the burdens of currently heavy paper work and physical manual access to the equipment particularly for those located in the radiation zones; the other side of blade can cut off the normal nuclear operation and may impact on the nuclear safety if the *NINO* is not properly authorized to access.

Tier-2 secure *NINO* authorization is proceeded, as shown in Figure 2.6, in 7 steps below.

Figure 2.6: *Tier-2* secure *NINO* authorization flow diagram

Step-T2.1: A nuclear network user- x (Ux) makes a request for access to *NINO* network to carry out a nuclear operation $NINO\{(n1...n6)_x\}$ that is detailed in chapter 3;

Ux encrypts his/her requested nuclear operation $NINO\{(n1...n6)_x\}$ using the network pass code $\{N_{x1}, N_{s1}\}$ and sends the encrypted valves to the *Operation Server* (OS):

$$Ux: E_{(Nx1,Ns1)}\{(n1...n6)_x\} \Rightarrow OS \quad (2.12)$$

Step-T2.2: Ux encrypts, using the network pass code $\{N_{x1}, N_{s1}\}$, his/her *Certificates of Operation Qualifications* $COQ(IDx, \{L_{OQ}\}_x)$ that contains Ux 's operation identity (IDx) and operation qualification list ($\{L_{OQ}\}_x$), as detailed in section 2.5.

Ux sends the encrypted valves to OS for support of the requested nuclear operation:

$$Ux: E_{(Nx1,Ns1)}\{COQ(IDx, \{L_{OQ}\}_x)\} \Rightarrow OS \quad (2.13)$$

Step-T2.3: *OS* decrypts $[E_{(NxI, NsI)}\{(n1 \dots n6)_x\}]$ and $[E_{(NxI, NsI)}\{COQ(IDx, \{LoQ\}_x)\}]$ using the network pass code $\{N_{XI}, N_{SI}\}$:

$$OS: D_{(NxI, NsI)}[E_{(NxI, NsI)}\{(n1 \dots n6)_x\}] \Rightarrow (n1 \dots n6)_x \quad (2.14)$$

$$OS: D_{(NxI, NsI)}[E_{(NxI, NsI)}\{COQ(IDx, \{LoQ\}_x)\}] \Rightarrow \{LoQ\}_x \quad (2.15)$$

Step-T2.4: *OS* verifies *Ux*'s requested nuclear operation $(n1 \dots n6)_x$ requirement list $\{L_{(n1 \dots n6)_x}\}$ versus *Ux*'s qualifications list $\{LoQ\}_x$, to ensure $\{L_{(n1 \dots n6)_x}\}$ is a subset of $\{LoQ\}_x$:

$$\{L_{(n1 \dots n6)_x}\} \in \{LoQ\}_x \quad (2.16)$$

Step-T2.5: *OS* generates a nonce N_{OI} , if (2.16) is satisfied;

OS encrypts the nonce using the network pass code $\{N_{XI}, N_{SI}\}$ and sends the encrypted valves to *Ux*,

$$OS: E_{(NxI, NsI)}\{N_{OI}\} \Rightarrow Ux \quad (2.17)$$

Step-T2.6: *Ux* decrypts $[E_{(NxI, NsI)}\{N_{OI}\}]$ using the network pass code $\{N_{XI}, N_{SI}\}$

$$Ux: D_{(NxI, NsI)}[E_{(NxI, NsI)}\{N_{OI}\}] \Rightarrow N_{OI} \quad (2.18)$$

Step-T2.7: *Ux* and *OS* can use $\{N_{XI}, N_{OI}\}$ for continuous communications, with respect to nuclear operation *NINO* $(n1 \dots n6)_x$ access.

$$Ux: E_{(NxI, N_{OI})}\{message_U\} \Rightarrow OS \quad (2.19)$$

$$Ux \Leftarrow OS: E_{(NxI, N_{OI})}\{message_O\} \quad (2.20)$$

2.4 Authorization for Condition-Based Nuclear Maintenance (CBNM)

This section presents the authorization procedure for *Tier-3*, the secure control of access to the Condition-Based Nuclear Maintenance (CBNM), as shown in Figure 2.6.

This security measure is to stop any unauthorized access to critically important nuclear maintenance CBNM that also links to the safety-related NINO for data transfer for maintenance use.

Tier-3 secure CBNM authorization is proceeded, as shown in Figure 2.7, in 7 steps below.

Figure 2.7: *Tier-2* secure NINO authorization flow diagram

Step-T3.1: A nuclear network user- x (Ux) makes a request for access to CBNM network to carry out a nuclear maintenance work $CBNM\{(OC)_x\}$ that is detailed in chapter 4;

Ux encrypts his/her requested nuclear maintenance $CBNM\{(OC)_x\}$ using the network pass code $\{N_{xI}, N_{sI}\}$ and sends the encrypted values to the Maintenance Server (MS):

$$Ux: E_{(NxI, NsI)}\{(OC)_x\} \Rightarrow MS \quad (2.21)$$

Step-T3.2: Ux encrypts, using the network pass code $\{N_{xI}, N_{sI}\}$, his/her *Certificates of Maintenance Qualifications* $CMQ(ID_x, \{L_{MQ}\}_x)$ that contains Ux 's maintenance identity (ID_x) and maintenance qualification list ($\{L_{MQ}\}_x$), as detailed in section 2.5.

Ux sends the encrypted values to MS , for support of the requested nuclear maintenance:

$$Ux: E_{(NxI, NsI)}\{CMQ(ID_x, \{L_{MQ}\}_x)\} \Rightarrow MS \quad (2.22)$$

Step-T3.3: MS decrypts $[E_{(NxI, NsI)}\{(OC)_x\}]$ and $[E_{(NxI, NsI)}\{CMQ(ID_x, \{L_{MQ}\}_x)\}]$ using the network pass code $\{N_{xI}, N_{sI}\}$:

$$MS: D_{(NxI, NsI)}[E_{(NxI, NsI)}\{(OC)_x\}] \Rightarrow (OC)_x \quad (2.23)$$

$$MS: D_{(NxI, NsI)}[E_{(NxI, NsI)}\{CMQ(IDx, \{L_{MQ}\}_x)\}] \Rightarrow \{L_{MQ}\}_x \quad (2.24)$$

Step-T3.4: *MS* verifies *Ux*'s requested nuclear maintenance work $(OC)_x$ requirement list $\{L_{(OC)x}\}$ versus *Ux*'s qualifications list $\{L_{MQ}\}_x$, to ensure $\{L_{(OC)x}\}$ is a subset of $\{L_{MQ}\}_x$.

$$\{L_{(oc4)_x}\} \in \{L_{MQ}\}_x \quad (2.25)$$

Step-T3.5: *MS* generates a nonce N_{mI} , if the list $\{L_{MQ}\}_x$ satisfies the maintenance requirements; *MS* encrypts the nonce using the network pass code $\{N_{XI}, N_{SI}\}$ and sends the encrypted values to *Ux*,

$$MS: E_{(NxI, NsI)}\{N_{mI}\} \Rightarrow Ux \quad (2.26)$$

Step-T3.6: *Ux* decrypts $[E_{(NxI, NsI)}\{N_{mI}\}]$ using the network pass code $\{N_{XI}, N_{SI}\}$

$$Ux: D_{(NxI, NsI)}[E_{(NxI, NsI)}\{N_{mI}\}] \Rightarrow N_{mI} \quad (2.27)$$

Step-T3.7: *Ux* and *MS* can use $\{N_{XI}, N_{mI}\}$ for continuous communications with respect to nuclear maintenance *CBNM* $(OC)_x$ access.

$$Ux: E_{(NxI, N_{mI})}\{message_U\} \Rightarrow MS \quad (2.28)$$

$$Ux \Leftarrow MS: E_{(NxI, N_{mI})}\{message_M\}$$

2.5 Specifications of Certifications for Secure Access to Tier-1, 2, 3 Networks

This section presents the specifications of certifications for secure access to Tier-1, Tier-2 and Tier-3 nuclear networks. Abstract Syntax Notation One (ASN.1) [30,31] and FIPS-196 [2] notations are adopted for the specifications.

2.5.1 Specification of *CNA* for secure access to Tier-1 process network

The specification for *CNA*, the *Certificate of Network Access* for nuclear worker-x, is as defined below:

Table 2.1: $CNA(ID_X, PK_X)$

$CNA(ID_X, PK_X) ::= \text{SIGNED SEQUENCE}$		
{		
ID_X {	version	Version
	serialNumber	CertSerialNumber
	signature	Signature
	issuer	Issuer
	validity	Validity
}		
PK_X {	publicKey	PublicKey
}		
}		

Version ::= INTEGER

CertSerialNumber ::= INTEGER

Signature {OfSignature} ::= SEQUENCE		
{		
	algorithmId	AlgorithmId
	ENCRYPTED {	HASHED {OfSignature}
	}	
}		

Issuer ::= ALPHANUMERIC

Validity ::= SEQUENCE

{		
	notBefore	Time
	notAfter	Time
}		

PublicKey ::= SEQUENCE

{		
	algorithmId	AlgorithmID
	subjectPublicKey	SubjectPublicKey
}		

AlgorithmID ::= SEQUENCE

{		
	algorithm	ALGORITHM
	parameter	TEXT, OPTIONAL
}		

SubjectPublicKey ::= BIT STRING

ALGORITHM {ToBeSpecified} ::= TYPE – IDENTIFIER

ENCRYPTED {ToBeEnciphered} ::= BIT STRING

HASHED {ToBeHashed} ::= OCTET STRING

TEXT ::= BIT STRING

2.5.2 Specification of *COQ* and $\{L_{(n1...n6)}\}$ for secure access to Tier-2 operation network

The following defines the specifications of *COQ* and $\{L_{(n1...n6)}\}$ for *NINO* network access:

Table 2.2: *COQ*(ID_X , $\{Log\}_x$)

<i>COQ</i> (<i>ID</i> _x , { <i>Log</i> } _x) ::= SIGNED SEQUENCE		
{ <i>IDx</i>	{ opSerialNumber signature	CertSerialNumber Signature
}	}	
{ <i>Log</i> } ::= SEQUENCE		
{	nq	NumberOfQuali
	{ opQuali-1 Validity	QualiRegNumber Validity
	opQuali-2 opValidity	QualiRegNumber Validity
		
		
	opQuali-nq opValidity	QualiRegNumber Validity }
}	}	
}		

CertSerialNumber ::= INTEGER

Signature {OfSignature} ::= SEQUENCE

{ algorithmId	AlgorithmId
ENCRYPTED {	HASHED {OfSignature}
}	

NumberOfQuali ::= INTEGER

QualiRegNumber ::= ALPHANUMERIC

Validity ::= SEQUENCE {

notBefore	Time
notAfter	Time

}

Table 2.3: $\{L_{(n1...n6)}\}$

$\{L_{(n1...n6)}\}$::= SEQUENCE		
{	nr	NumberOfQuali
	{ opRequire-1	QualiRegNumber
	opRequire-2	QualiRegNumber
		
	opRequire-nr	QualiRegNumber }
}	}	
}		

2.5.3 Specifications of CMQ and $L_{(COA)}$ for secure access to Tier-3 maintenance network

The following defines the specifications of CMQ and $L_{(COA)}$ for $CBNM$ network access:

Table 2.4: $CMQ(ID_X, \{L_{MQ}\}_x)$

$CMQ(ID_X, \{L_{MQ}\}_x) ::=$ SIGNED SEQUENCE		
{ ID_X	{ mSerialNumber signature	CertSerialNumber Signature
}	}	
$\{L_{MQ}\} ::=$ SEQUENCE		
{	nq	NumberOfQuali
	{ mQuali-1	QualiRegNumber
	mValidity	Validity
	mQuali-2	QualiRegNumber
	mValidity	Validity
		
		
	mQuali-nq	QualiRegNumber
	mValidity	Validity }
}	}	
}		
CertSerialNumber ::= INTEGER		
Signature {OfSignature} ::= SEQUENCE		
{	algorithmId	AlgorithmId
	ENCRYPTED {	HASHED{OfSignature} }
}	}	
NumberOfQuali ::= INTEGER		
QualiRegNumber ::= ALPHANUMERIC		
Validity ::= SEQUENCE {		
	notBefore	Time
	notAfter	Time
}		

Table 2.5: $\{L_{(OC)}\}$

$\{L_{(OC)}\} ::=$ SEQUENCE		
{	mr	NumberOfQuali
	{ mRequire-1	QualiRegNumber
	mRequire-2	QualiRegNumber
		
	mRequire-mr	QualiRegNumber }
}	}	
}		

2.6 Design Evaluation for *STAC*

This section presents an evaluation of the new design *Secure Trilateral Access Control (STAC)*, as described above for the security control of access to the new nuclear process network for carrying out the network-integrated nuclear operation (*NINO*) and the network-driven condition-based nuclear maintenance (*CBNM*) created in this thesis research.

A comprehensive evaluation of the *STAC* created in this thesis first, starts from the underling requirements for the design of a *network-driven* nuclear process, being an innovative way of operating a nuclear process with network drive. The circumstance under which an innovative network-driven nuclear process is to be operated can be challenging, due to:

- An error or deficiency in the access control that leaks out an unauthorized access into the safety-critical nuclear process would cause extremely serious consequences to public health and safety and/or huge economical loss and/or key infrastructure damage.
- Any fault action due to unauthorized access would be irreversible as the access would directly go to the live nuclear operations.
- The access control implementation must be maintainable, modifiable, and ungradable in practical terms, because the operating conditions or the means of operations may change with various levels.
- The access control procedures must be precisely defined and must be verifiable online with affecting live nuclear operations.
- The access control during the live nuclear operations must be reliable, quality-controlled, well-guided, and most importantly comprehensible to all nuclear network users of having mandatory basic trainings so that users will not easily fall into wrong accesses that possibly lead to undesired or even disaster operations.

The access control procedures presented in the sections above are strong, economical, practical secure tool for controls of access to the innovative network-driven nuclear operations and maintenances developed in this thesis research. The following evaluates the features of the access control procedures design presented in this chapter.

a) ***Mutual authentication for Tier-1 access control***

- A mutual (two-way) authentication is designed between the nuclear worker-x (***Wx***) requesting for access to the nuclear process network and the authentication server (***AS***) checking the authorization of the requester, in the *Tier-1* network access control.
- ***Wx*** is to ensure that he/she is not communicating with a malicious network server by authenticating the server. If this property is absent, a malicious network server is capable of mounting a person/device-in-the-middle attack to gather data/information from ***Wx***.
- ***AS*** is to ensure that it is not communicating with a malicious worker by authenticating the worker. If this property is absent, a malicious worker is capable of accessing the live safety-critical nuclear operations.

b) ***Unilateral authentication for Tier-2 and Tier-3 access controls***

- An unilateral (one-way) authentication is designed either, between the nuclear network user-x (***Ux***) requesting for access to the *NINO* network and the operation server (***OS***) in the *Tier-2* access control or, between ***Ux*** requesting for access to the *CBNM* network and the maintenance server (***MS***) in *Tier-3* access control.
- The unilateral authentication is more *efficient* of less processing time but of lower security than the mutual authentication. The unilateral authentication is more suitable for Tier-2 operation qualifications authentication as well as for Tier-3 maintenance qualifications authentication. It is because first, all nuclear workers' authorization for network uses have been authenticated in Tier-1 that already provides a level of security and second, the higher authentication process efficiency is crucial to improve the responsiveness of the new network-driven nuclear process.

c) ***Use of state-of-the-art key-based authentication technology in STAC***

- Tier-1 external-to-nuclear network authentication is a public-private, key-based authentication. A private key is a cryptographic key uniquely associated with its owner and mathematically linked with a corresponding public key. The public key may be made public but the private key is not made public. The key is used to verify a digital signature of the certificates.
- Tier-2 and Tier 3 use random number challenges and digital signatures to eliminate the need of a secure mean for transmitting passwords for network access authentication.

- The use of digital signatures in Tier-2 and Tier-3 is to reduce threat of compromise that would allow an attacker to use the same information including passwords to authenticate repeatedly.
- The use of a private key to generate digital signatures for Tier-1 authentication is to make computationally infeasible for an attacker to masquerade as another user.

d) ***General features of STAC***

- Efficiency is a design parameter considered in the development of the *STAC*. Efficiency is crucial to achieve the high availability requirement in the online nuclear operations and the authentication shall not incur excess procedures and redundancy.
- The *STAC* authentication can resist malicious attacks, such as forgery attacks, replay attacks, and denial-of-service attacks.
- The *STAC* is to minimize the use of passwords. Even with the use of random number challenges and digital signatures, the implementation may still rely on passwords for users to access their private keys, and thus the passwords must be kept secure.

Chapter 3

NETWORK-INTEGRATED NUCLEAR OPERATIONS

This chapter presents the new design, *Network-Integrated Nuclear Operations (NINO)* developed in this thesis research. Two Operation Security Levels (*OSL-1*, *OSL-2*) are defined in *NINO*, of which *OSL-1* is for the *reactor-direct* operations and *OSL-2* is for the *reactor-indirect* operations.

First, this chapter presents the overall architecture of *NINO* in *Tier 2* of the Secure Trilateral Access Control (*STAC*), the new nuclear network access control designed in this thesis research. This thesis is focused on the *STAC* design for the major operations and maintenance in the current live nuclear electricity generating stations using CANDU reactors, as an initial prime step in the nuclear practices modernization.

The *NINO* is designed with two operation security levels, as shown in Figure 3.1. They are defined as:

- Operation Security Level 1 (*OSL-1*) for nuclear *Reactor-Direct NINO*
- Operation Security Level 2 (*OSL-2*) for nuclear *Reactor-Indirect NINO*

Figure 3.1 Tier 2 of STAC

The Tier-2 *NINO* is designed with four nuclear operation access divisions, defined as:

- *OSL-1 Nuclear Reactor Control (NRC)* division
- *OSL-1 reactor Heat Transport Control (HTC)* division
- *OSL-2 Boiler Steam Control (BSC)* division
- *OSL-2 Turbine Generator Condenser Control (TGC)* division

Second, this chapter presents *OSL-1*, the highest network access security level that covers the two reactor-direct *NINO* divisions: *NRC* and *HTC*. This chapter defines the protocols for the operation security access control for the *NINO*, and details the key nuclear operations and their operation security network access codes. *OSL-2* that covers the *BSC* and *TGC* divisions is to be presented in Appendix I.

Third, this chapter presents an evaluation of *NINO*, with the use of a typical example of the access control designed in this thesis, for carrying out a specific regulation of nuclear reactor reactivity.

This chapter presents:

- Section 3.1: This section presents the overall architecture of *NINO* in *Tier 2* of *STAC*. This section creates two (2) nuclear-network access security levels and four (4) access control divisions for key network-integrated nuclear operations, and defines the protocol for the operation security access to *NINO*.
- Section 3.2: This section presents the *Nuclear Reactor Control (NRC)* division in the reactor-direct operation security level *OSL-1*. This section creates 4 *NRC* control groups: *Reactor Reactivity (RR)*, *Reactor Control (RC)*, *Reactor ShutDown (SD)*, and *Moderator Temperature (MT)*. This section details each control group in *NRC* and the key control systems and equipment in each group, and defines their secure access *NINO* codes.
- Section 3.3: This section presents the reactor *Heat Transport Control (HTC)* division in *OSL-1*. This section creates 4 *HTC* control groups: *Heat-transport Feed (HF)*, *Heat-transport Bleed (HB)*, *Heat-transport Condenser (HC)*, and *Heat-transport Pressure (HP)*. This section details each control group in *HTC* and the key control systems and equipment in each group, and defines their secure access *NINO* codes.
- Section 3.4: This section presents a data base established for *NINO*. This *NINO* data base is a “live” data base that is continuously updated (added, deleted, changed, re-organized, etc.).
- Section 3.5: This section presents an evaluation of *NINO* using a typical example of access to the control of nuclear reactor reactivity, as by means of controlling the light water flow into a specific liquid zone for reactivity adjustment.

3.1 Architecture of Network-Integrated Nuclear Operations

This section presents the architecture of *Tier-2 NINO* nuclear operations created in this thesis.

The Tier-2 consists of four nuclear operation access divisions: *OSL-1-NRC* the nuclear reactor control division, *OSL-1-HTC* the reactor heat transport control division, *OSL-2-BSC* the boiler steam control division, and *OSL-2-TGC* the turbine generator condenser control division.

A *NINO* code is assigned for each operating element, which is defined with a group of 6 numerical items in the form of:

(function #, device #, equipment #, system #, group-system #, division #)

where division = all nuclear control systems are divided into 4 divisions.
group system = each division is grouped into group systems based on key operations.
system = each group system is divided into systems based on specific operations.
equipment = key nuclear equipment in a system.
device = components in an equipment.
function = device/equipment monitoring, processing, or controlling function.

These items, as illustrated in Figure 3.2, are to be detailed in the following sections.

Figure 3.2: *OSL-1* and *OSL-2* NINO and Codes

Figure 3.2 illustrates that a nuclear network user can access his/her requested nuclear operation via a *NINO* code, such as via (0 0 0 0 0 1) to D_{NRC} the nuclear reactor control division.

3.1.1 *Partition of Nuclear Process for Tier-2 NINO*

Prior to grouping the nuclear process operations for the design of the *Tier-2 NINO*, a comprehensive understanding of the basic nuclear process in the live nuclear power plants can facilitate the design work, such as follows.

In a typical CANDU nuclear generating unit (one power plant may have 8 nuclear units), the fission reaction in the reactor core heats the pressurized heavy water in the calandria that is a cylindrical reactor vessel that contains the heavy water moderator. The moderator is used to slow down fast and energetic neutrons released by fission to an energy level suitable for sustaining the chain reaction fission. This forms the base for *OSL-1-NRC* the nuclear reactor control division.

The heat generated by the nuclear chain reaction in the reactor core is transported to steam boiler by circulating the pressurized heavy water between the reactor fuel channels and the boiler. This forms the base for *OSL-1-HTC* the reactor heat transport control division.

The boiler or steam generator transfers the heat from the heavy water in the primary heat transport loop to the light water in the secondary cooling loop. The steam from the boiler runs a steam turbine. This forms the base for *OSL-2-BSC* the boiler steam control division.

The turbine then runs a generator that produces electricity. The generator connects to the grid for electricity transmission. The exhausted steam from the turbine is condensed with lake water and returned as feedwater to the boiler. This forms the base for *OSL-2-TGC* the turbine generator condenser control division.

The above-mentioned operations form the chain of energy transfer from the reactor to the generator. The prime importance of operating a nuclear unit is first, to cool the reactor whether or not the unit generates electricity and second, to augment the safe and uninterrupted production of electricity. Continuous safe electricity generation, on the other hand, is the basic justification for the existence of a nuclear power plant.

In order to ensure the safe operation of the nuclear unit and the continued generation of electricity, each link in the above-mentioned energy transfer chain must be controlled by carefully designed process controls. The new *NINO* design takes one important step further that is to reduce the costs of the nuclear process operations, particularly for the promotion of new idea of network-integrated and condition-based nuclear maintenance.

NINO divides the core control of the nuclear process into 4 divisions, as shown in Figure 3.2. The 4 divisions are defined as follows:

OSL-1 – Reactor-Direct NINO:

<i>Division</i>	<i>Description</i>	<i>NINO codes</i>
D_{NRC} :	Nuclear Reactor Control division	(0,0,0,0,0,1)
D_{HTC} :	Heat Transport Control division	(0,0,0,0,0,2)
<i>NINO code:</i>	Division: D _{NRC} = 1, D _{HTC} = 2 (6 th #); others = 0	

OSL-2 – Reactor-Indirect NINO:

<i>Division</i>	<i>Description</i>	<i>NINO codes</i>
D_{BSC} :	Boiler Steam Control division	(0,0,0,0,0,3)
D_{TGC} :	Turbine-Generator-Condenser control division	(0,0,0,0,0,4)
<i>NINO code:</i>	Division: D _{BSC} = 3, D _{TGC} = 4 (6 th #); others = 0	

OSL-1 the Reactor-Direct *NINO* design is presented in this chapter; *OSL-2* the Reactor-Indirect *NINO* design is to be presented in Appendix I.

3.1.2 Nuclear Reactor Control Division - **D_{NRC}** (0,0,0,0,0,1)

NINO sub-divides the Nuclear Reactor Control (*NRC*) division into 4 control group-systems as shown in Figure 3.3, and defines them as follows:

<i>Group-System</i>	<i>Description</i>	<i>NINO code</i>
G_{RR}D_{NRC} :	Reactor Reactivity control Group-system	(0,0,0,0,1,1)
G_{RC}D_{NRC} :	Reactor Control, Stepback/Setback control Group-system	(0,0,0,0,2,1)
G_{SD}D_{NRC} :	Shut Down reactor control Group-system	(0,0,0,0,3,1)
G_{MT}D_{NRC} :	Moderator Temperature control Group-system	(0,0,0,0,4,1)
<i>NINO code:</i>	Group system: G _{RR} = 1, G _{RS} = 2, G _{SD} = 3, G _{MT} = 4 (5 th #) Division - Nuclear Reactor Control: D _{NRC} = 1 (6 th #) others = 0

Figure 3.3: Nuclear Reactor Control (NRC) in OSL-1

3.1.3 Heat Transport Control Division – D_{HTC} (0,0,0,0,0,2)

NINO sub-divides the Boiler-Heat-transport (*BH*) control division into 3 control group-systems as shown in Figure 3.4, and defines them as follows:

Group-System	Description	<i>NINO</i> code
$G_{HF}D_{HTC}$:	Heat-transport Feed control Group-system	(0,0,0,0,1,2)
$G_{HB}D_{HTC}$:	Heat-transport Bleed control Group-system	(0,0,0,0,2,2)
$G_{HC}D_{HTC}$:	Heat-transport Condenser control Group-system	(0,0,0,0,3,2)
$G_{HP}D_{HTC}$:	Heat-transport Pressure control Group-system	(0,0,0,0,4,2)
<i>NINO</i> code:	Group system: Division - Heat Transport Control:	$G_{HF} = 1$, $G_{HB} = 2$, $G_{HC} = 3$, $G_{HP} = 4$, (5 th #) $D_{HTC} = 2$ (6 th #) others = 0

Figure 3.4: Heat Transport Control (HTC) in OSL-1

3.2 Nuclear Reactor Control Division - D_{NRC} (0,0,0,0,0,1)

This section presents the Nuclear Reactor Control Division (D_{NRC}) that composes of 4 Group-systems:

$G_{RR}D_{NRC}$:	Reactor Reactivity control Group-system	(0,0,0,0,1,1)
$G_{RC}D_{NRC}$:	Reactor Control, Stepback and Setback Group-system	(0,0,0,0,2,1)
$G_{SD}D_{NRC}$:	Shut Down reactor control Group-system	(0,0,0,0,3,1)
$G_{MT}D_{NRC}$:	Moderator Temperature control Group-system	(0,0,0,0,4,1)

3.2.1 Reactor Reactivity control Group-system, $G_{RR}D_{NRC}$ (0,0,0,0,1,1)

$G_{RR}D_{NRC}$, the reactor reactivity control group-system is to adjust various reactivity control equipment/devices to maintain the power produced in the nuclear reactor, in accordance with selected nuclear operation modes and setpoints. The reactivity devices are to control both spatial and bulk reactor power. The control of the spatial reactor power is to assure that individual fuel bundles and fuel channels are within their power limits and to minimize the possibility of channel dryout and fuel failures. The control of bulk reactor power control is to assure that the nuclear operation is within the reactor operating license limit, and otherwise it may increase the probability of fuel failures and the radiological releases following an accident that may expose the public to high risk.

This group system has devices to measure the nuclear reactor power, to change the reactor power, and to monitor and process signals from other nuclear systems for the need of adjusting the reactor power. This group consists of two control systems as shown in Figure 3.5.

NINO defines the two control systems, as follow:

<i>System</i>	<i>Description</i>	<i>NINO code</i>
$S_{RFM}G_{RR}D_{NRC}$:	Reactor Flux/Power Measuring System	(0,0,0,1,1,1)
$S_{LZC}G_{RR}D_{NRC}$:	Liquid Zone reactivity Control System	(0,0,0,2,1,1)
<i>NINO code:</i>	System - Reactor Flux/power Measuring:	$S_{RFM} = 1$ (4 th #)
	Liquid Zone reactivity Control:	$S_{LZC} = 2$ (4 th #)
	Group system - Reactor Reactivity control:	$G_{RR} = 1$ (5 th #)
	Division - Nuclear Reactor Control:	$D_{NRC} = 1$ (6 th #)

Figure 3.5: Reactor Reactivity Control Systems

3.2.1-1 Reactor Flux/Power Measuring System - $S_{RFM} G_{RR} D_{NRC} (0,0,0,1,1,1)$

$S_{RFM} G_{RR} D_{NRC}$, the reactor flux/power measuring system is to measure the power produced in the nuclear reactor, prior to controlling/regulating the reactor reactivity. The system uses two methods: one measures the reactor flux that varies swiftly and proportionally with the power generated inside the reactor; the other measures the thermal power from the flow of the heavy water through the reactor and this measurement is accurate but the response is slow.

$E_{IC} S_{RFM} G_{RR} D_{NRC}$, the ion-chamber reactor flux detecting equipment is installed outside of the calandria to measure the neutron flux leaking out from the nuclear reactor. An ion-chamber flux detector can generate a signal that is proportional to the reactor power in the reactor core region, outside of which the detector is located, but the signal does not represent the reactor power of the core regions that are remote from the detector location. The ion-chamber detector can accurately generate a signal proportional to the reactor power as low as 100W. The detector can also generate a signal up to full power, but with poor resolution for the control of the reactor power higher than 100MW.

$E_{IZ} S_{RFM} G_{RR} D_{NRC}$, the in-core zone reactor flux detecting equipment is installed in 14 zones as the liquid zone controls, inside the reactor core. An in-core flux detector can generate a signal that is proportional to the neutron flux in the region where the detector is installed. The in-core detector cannot accurately measure low neutron flux of below 10MW. Also the in-core detector generates the signal that decreases with time as the detector neutron sensing material is continually being

depleted by its neutron absorption due to exposure to the neutron flux. This deficiency can be corrected using the reactor thermal power measuring signal.

$E_{ZT}S_{RFM}G_{RR}D_{NRC}$, the reactor thermal power detecting equipment measures the reactor power based on the coolant flows through the reactor and the temperature rises across the fuel channels, of which the average product of the flows and temperature rises provides the reactor thermal power signal. The thermal power measurement is too slow for the control of the reactor power. A reactor zone thermal power signal is calculated using the average of the inlet temperature, outlet temperature, and flow in a zone pair in the reactor. The zone thermal power signal is used to correct the signal from the in-core detector of the same zone.

These reactor flux/power monitoring equipment, as shown in Figure 3.6, are described in the following.

NINO defines the equipment for the reactor flux/power measuring system, as follow:

<i>Equipment</i>	<i>Description</i>	<i>NINO code</i>
$E_{IC}S_{RFM}G_{RR}D_{NRC}$:	Ion Chamber reactor flux detecting equipment	(0,0,1,1,1,1)
$E_{IZ}S_{RFM}G_{RR}D_{NRC}$:	In-core Zone reactor flux detecting equipment	(0,0,2,1,1,1)
$E_{ZT}S_{RFM}G_{RR}D_{NRC}$:	Zone Thermal reactor power detecting equipment	(0,0,3,1,1,1)

NINO code: Equipment - Reactor Flux/power detecting: $E_{IC} = 1, E_{IZ} = 2, E_{ZT} = 3$ (3rd #)
 System - Reactor Flux/power Measuring: $S_{RFM} = 1$ (4th #)
 Group system - Reactor Reactivity control: $G_{RR} = 1$ (5th #)
 Division - Nuclear Reactor Control: $D_{NRC} = 1$ (6th #)

Figure 3.6: Reactor Flux/Power Measuring Equipment

1) Reactor Power Detector Function: Monitoring

NINO defines the monitoring functions of the reactor power detectors as follows:

Monitoring	Description	NINO code
$f_M-d_{IC}E_{IC}S_{RFM}G_{RR}D_{NRC}$	6 Ion Chamber reactor flux monitoring devices	(1,[1..6],1,1,1,1)
$f_M-d_{IZ}E_{IZ}S_{RFM}G_{RR}D_{NRC}$	14 In-core Zone reactor flux monitoring devices	(1,[1..14],2,1,1,1)
$f_M-d_{ZT}E_{ZT}S_{RFM}G_{RR}D_{NRC}$	14 Zone Thermal reactor power monitoring devices	(1,[1..14],3,1,1,1)
NINO code:	function - Monitoring: device - reactor flux/power detectors: Equipment - reactor flux/power detecting: System - Reactor Flux/power Measuring: Group system - Reactor Reactivity control: Division - Nuclear Reactor Control:	$f_M = 1$ (1 st #) $d_{IC}=1..6, d_{IZ}=1..14, d_{ZT}=1..14$ (2 nd #) $E_{IC} = 1, E_{IZ} = 2, E_{ZT} = 3$ (3 rd #) $S_{RFM} = 1$ (4 th #) $G_{RR} = 1$ (5 th #) $D_{NRC} = 1$ (6 th #)

- The monitoring of the reactor flux from start 0 to 75MW is covered by $f_M-d_{IC}E_{IC}S_{RFM}G_{RR}D_{NRC}$.
- The monitoring of the reactor flux from 75MW to full power is covered by $f_M-d_{IZ}E_{IZ}S_{RFM}G_{RR}D_{NRC}$.
- The monitoring of the reactor power from start to full power is covered by $f_M-d_{ZT}E_{ZT}S_{RFM}G_{RR}D_{NRC}$.

2) Reactor Power Detector Function: Data Processing

NINO defines the data processing functions of the reactor power detectors as follows:

Processing	Description	NINO code
$f_P-d_{IC}E_{IC}S_{RFM}G_{RR}D_{NRC}$	6 Ion Chamber reactor flux processing devices	(2,[1..6],1,1,1,1)
$f_P-d_{IZ}E_{IZ}S_{RFM}G_{RR}D_{NRC}$	14 In-core Zone reactor flux processing devices	(2,[1..14],2,1,1,1)
$f_P-d_{ZT}E_{ZT}S_{RFM}G_{RR}D_{NRC}$	14 Zone Thermal power processing devices	(2,[1..14],3,1,1,1)
NINO code:	function - Processing: device - reactor flux/power detectors: Equipment - reactor flux/power detecting: System - Reactor Flux/power Measuring: Group system - Reactor Reactivity control: Division - Nuclear Reactor Control:	$f_P = 2$ (1 st #) $d_{IC}=1..6, d_{IZ}=1..14, d_{ZT}=1..14$ (2 nd #) $E_{IC} = 1, E_{IZ} = 2, E_{ZT} = 3$ (3 rd #) $S_{RFM} = 1$ (4 th #) $G_{RR} = 1$ (5 th #) $D_{NRC} = 1$ (6 th #)

- The processing function $f_P-d_{IC}E_{IC}S_{RFM}G_{RR}D_{NRC}$ converts the ion-chamber reactor flux signal into the reactor power data and expresses it in the “log” scale, in order to enhance the reactor power monitoring in low range from 100W to 75MW.
- The processing function $f_P-d_{IZ}E_{IZ}S_{RFM}G_{RR}D_{NRC}$ converts the in-core zone reactor flux signal into the reactor power data and expresses it in the “linear” scale, for the range from 75MW to full power.

- The processing function $f_{p-dZT}E_{ZT}S_{RFM}G_{RR}D_{NRC}$ corrects the in-core zone reactor flux signal which is decaying signal, using the reactor zone thermal power signal.

3.2.1-2 **Liquid Zone reactivity Control System - $S_{LZC}G_{RR}D_{NRC}$ (0,0,0,2,1,1)**

$S_{LZC}G_{RR}D_{NRC}$, the liquid zone reactivity control system is the main fast control among the reactor reactivity controlling systems in $G_{RR}D_{NRC}$, the reactor reactivity control group-system. The function of $G_{RR}D_{NRC}$ is to maintain the power produced in the nuclear reactor according to the selected operation setpoints. Light water is an effective nuclear absorber to slow down the reactivity in the reactor.

This control system adjusts the reactivity in the nuclear reactor by varying the light water content in the 14 zones inside the reactor. The level of the light water in the zones can be adjust either concurrently for bulk reactor flux/power control or individually for reactor spatial flux/power control. The LZRC is designed to circulate and condition the light water.

These liquid zone reactivity control equipment, as shown in Figure 3.7, are described in the following.

NINO defines the equipment for LZRC, the liquid zone reactivity control system as follow:

<i>Equipment</i>	<i>Description</i>	<i>NINO code</i>
$E_{LP}S_{LZC}G_{RR}D_{NRC}$:	light water circulating Pumps	(0,0,1,2,1,1)
$E_{IV}S_{LZC}G_{RR}D_{NRC}$:	light-water Inflow Control Valves	(0,0,2,2,1,1)
$E_{IL}S_{LZC}G_{RR}D_{NRC}$:	Inflow level differential Pressure Transmitters	(0,0,3,2,1,1)
$E_{OF}S_{LZC}G_{RR}D_{NRC}$:	Outflow differential Pressure Transmitter	(0,0,4,2,1,1)
$E_{HC}S_{LZC}G_{RR}D_{NRC}$:	liquid-zone Helium Compressors	(0,0,5,2,1,1)

<i>NINO code:</i>	Equipment - Light-water circulating Pumps:	$E_{LP} = 1$ (3 rd #);
	Light-water Inflow control Valves:	$E_{IV} = 2$ (3 rd #);
	light-water Inflow Level monitoring:	$E_{IL} = 3$ (3 rd #);
	light-water OutFlow monitoring:	$E_{OF} = 4$ (3 rd #);
	Helium pressure Compressors:	$E_{HC} = 5$ (3 rd #);
	System - Liquid Zone reactor reactivity Control:	$S_{LZC} = 2$ (4 th #);
	Group system - Reactor Reactivity control:	$G_{RR} = 1$ (5 th #);
	Division - Nuclear Reactor Control:	$D_{NRC} = 1$ (6 th #)

Figure 3.7: Liquid Zone Resistivity Controlling Equipment

1) Liquid Zone Light Water Circulating Pumps Control

The light water is pumped from a delay tank by 3 pumps through a heat exchanger into the reactor liquid zones. A portion of the water is circulated through an ion exchanger for purification.

NINO defines the control of the 3 liquid-zone light-water circulating pump controls as follows:

Controlling	Description	<i>NINO</i> code
f_C-d_{PC}E_{LP}S_{LZC}G_{RR}D_{NRC}:	3 light water circulating Pump Controllers	(3,[1..3],1,2,1,1)
<i>NINO</i> code:	function - Controlling: device - Pump Controllers: Equipment - Light-water circulating Pumps: System - Liquid Zone reactor reactivity Control: Group system - Reactor Reactivity control: Division - Nuclear Reactor Control:	f _C = 3 (1 st #); d _{PC} = 1 to 3 (2 nd #); E _{LP} = 1 (3 rd #); S _{LZC} = 2 (4 th #); G _{RR} = 1 (5 th #); D _{NRC} = 1 (6 th #)

2) Liquid Zone Light Water Inflow Controls

The inflow of the light water is varied by using control valves. The levels of the light water in the 14 reactor liquid zones are regulated individually by 14 control valves that are pneumatically actuated.

NINO defines the 14 liquid-zone light-water inflow control valves as follows:

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
fc-d_{ICV}E_{IV}S_{LZC}G_{RR}D_{NRC}	14 light-water Inflow Control Valves	(3,[1..14],2,2,1,1)
<i>NINO code:</i>	function - Controlling: device - Inflow Control Valves: Equipment - light-water Inflow control Valves: System - Liquid Zone reactor reactivity Control: Group system - Reactor Reactivity control: Division - Nuclear Reactor Control:	f _C = 3 (1 st #); d _{ICV} = 1 to 14 (2 nd #); E _{IV} = 2 (3 rd #); S _{LZC} = 2 (4 th #); G _{RR} = 1 (5 th #); D _{NRC} = 1 (6 th #)

3) *Liquid Zone Light Water Level Monitoring*

The water levels in the 14 zones are monitored by using *14 differential pressure transmitters* that are used to record differential pressure between the top and the bottom of each zone, individually.

NINO defines the 14 light-water inflow level monitoring differential pressure transmitters as follows:

<i>Monitoring</i>	<i>Description</i>	<i>NINO code</i>
fc-d_{IPt}E_{IL}S_{LZC}G_{RR}D_{NRC}	14 Inflow level differential Pressure Transmitters	(3,[1..14],3,2,1,1)
<i>NINO code:</i>	function - controlling: device - Inflow differential Pressure Transmitters: Equipment - light-water Inflow Level monitoring: System - Liquid Zone reactor reactivity Control: Group system - Reactor Reactivity control: Division - Nuclear Reactor Control:	f _C = 3 (1 st #); d _{IPt} = 1 to 14 (2 nd #); E _{IL} = 3 (3 rd #); S _{LZC} = 2 (4 th #); G _{RR} = 1 (5 th #); D _{NRC} = 1 (6 th #)

The outflow of the light water from each zone is kept constant by maintaining a constant differential pressure between the helium gas over the water in the zones and the delay tank.

4) *Liquid Zone Light Water Outflow Monitoring*

NINO defines the light-water outflow monitoring differential pressure transmitter as follows:

<i>Monitoring</i>	<i>Description</i>	<i>NINO code</i>
fc-d_{OPT}E_{OF}S_{LZC}G_{RR}D_{NRC}	Outflow differential Pressure Transmitter	(3,1,4,2,1,1)
<i>NINO code:</i>	function - controlling: device - Outflow differential Pressure Transmitters: Equipment - light-water OutFlow monitoring: System - Liquid Zone reactor reactivity Control: Group system - Reactor Reactivity control: Division - Nuclear Reactor Control:	f _C = 3 (1 st #); d _{OPT} = 1 (2 nd #); E _{OF} = 4 (3 rd #); S _{LZC} = 2 (4 th #); G _{RR} = 1 (5 th #); D _{NRC} = 1 (6 th #)

5) Liquid Zone Helium Pressure Compressors Control

The water flows from the liquid zones back to the delay tank. The helium storage tank supplies the helium and maintains the constant differential pressure between the zones and the delay tank. Excess pressure is bled to the delay tank. If the pressure in the helium storage tank falls below a setpoint, one of the 2 compressors starts to pump helium from the delay tank to the storage tank.

NINO defines the control of the 2 liquid-zone helium pressure compressors as follows:

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
f_C-d_{CC}E_{Hc}S_{LZC}G_{RR}D_{NRC}:	2 liquid-zone Helium Compressor Controllers	(3,[1,2],5,2,1,1)
<i>NINO code:</i>	function - Controlling: device - Compressor Controllers: Equipment - Helium pressure Compressors: System - Liquid Zone reactor reactivity Control: Group system - Reactor Reactivity control: Division - Nuclear Reactor Control:	f _C = 3 (1 st #); d _{CC} = 1, 2 (2 nd #); E _{Hc} = 5 (3 rd #); S _{LZC} = 2 (4 th #); G _{RR} = 1 (5 th #); D _{NRC} = 1 (6 th #)

3.2.2 Reactor Control Group-system, *G_{RC}D_{NRC}* (0,0,0,0,2,1)

G_{RC}D_{NRC}, the reactor control and stepback/setback control group-system is to adjust various reactivity control equipment/devices to minimum the deviation (control error) of the reactor power from the desired setpoint. The reactor reactivity controls include the liquid zone control, adjuster rods control, mechanical-control absorbers control, and poison injection control.

This group uses three control systems as shown in Figure 3.8.

NINO defines the two control systems, as follow:

<i>System</i>	<i>Description</i>	<i>NINO code</i>
S_{LZC}G_{RR}D_{NRC}:	Liquid Zone reactivity Control System	(0,0,0,2,1,1)
S_{ARC}G_{RC}D_{NRC}:	Adjuster Rods Control System	(0,0,0,1,2,1)
S_{AMC}G_{RC}D_{NRC}:	Absorber Mechanical Control System	(0,0,0,2,2,1)
<i>NINO code:</i>	System - Liquid Zone reactivity Control: Adjuster Roles Control: Absorber Mechanical Control: Group system - Reactor Reactivity control: Reactor Control: Division - Nuclear Reactor Control:	S _{LZC} = 2 (4 th #); S _{ARC} = 1 (4 th #); S _{AMC} = 2 (4 th #); G _{RR} = 1 (5 th #); G _{RC} = 2 (5 th #); D _{NRC} = 1 (6 th #)

Figure 3.8: Reactor Control Systems

3.2.2-1 Liquid Zone reactivity Control System - $S_{LZC}G_{RR}D_{NRC}$ (0,0,0,2,1,1)

$S_{LZC}G_{RR}D_{NRC}$, the liquid zone reactivity control is one of the three controls used for the reactor power control and has already described in section 3.2.1-2.

3.2.2-2 Adjuster Rods Control System - $S_{ARC}G_{RC}D_{NRC}$ (0,0,0,1,2,1)

$S_{ARC}G_{RC}D_{NRC}$, the adjuster rods control system is to provide reactivity for overriding xenon poisoning following a power reduction or they can be used as reactivity shims. The 21 reactor reactivity adjuster rods are normally inserted completely inside the reactor for flux flattening. However, these adjuster rods can be driven in and out in a designed sequence per on-going reactor reactivity conditions. The withdrawn of these adjuster rods are to provide additional reactivity to the reactor core for certain operating conditions such as lacking of fuel, returning to full power operation after reactor power reduction, etc.

NINO defines the control of the 21 reactor reactivity adjuster rods as follows:

Controlling	Description	<i>NINO</i> code
f_C-d_{AD}E_{AC}S_{ARC}G_{RC}D_{NRC}:	21 reactor reactivity Adjuster Drive Controllers	(3,[1..21],1,1,2,1)

<i>NINO</i> code:	function - Controlling:	f _C = 3 (1 st #);
	device - Adjuster Drivers:	d _{AD} = 1...21 (2 nd #);
	Equipment - Adjuster drive Control:	E _{AC} = 1 (3 rd #);
	System - Adjuster Reactor Control:	S _{ARC} = 1 (4 th #);

Group system - Reactor reactivity Control:	$G_{RC} = 2$ (5 th #);
Division - Nuclear Reactor Control:	$D_{NRC} = 1$ (6 th #)

3.2.2-3 **Absorber Mechanical Control System - $S_{AMC}G_{RC}D_{NRC}$ (0,0,0,2,2,1)**

$S_{AMC}G_{RC}D_{NRC}$, the absorbers mechanical control system is to supplement the liquid zone control and the adjuster rods control. The 4 mechanical control absorbers have sufficient reactivity capacity to compensate for the fresh fuel power reactivity for shutdown from full power. These absorbers can be driven in and out of the reactor or can be dropped by releasing a clutch upon the gravity. They are normally out of the reactor core and are driven into the reactor core to supplement the negative reactivity from the liquid zone control and the adjuster rods control, or they can be dropped into the reactor core to provide a fast reactor power reduction such as for a reactor stepback control.

NINO defines the control of the 4 mechanical-controlled absorbers as follows:

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
fc-dAdE_{AC}S_{AMC}G_{RC}D_{NRC}	4 mechanical control absorbers	(3,[1..4],1,2,2,1)
<i>NINO code:</i>	function - Controlling: device - Absorber Controllers: Equipment - Absorber mechanical Control: System - Absorbers Mechanical control: Group system - Reactor reactivity Control: Division - Nuclear Reactor Control:	$f_C = 3$ (1 st #); $d_{AC} = 1 \dots 4$ (2 nd #); $E_{AC} = 1$ (3 rd #); $S_{AMC} = 2$ (4 th #); $G_{RC} = 2$ (5 th #); $D_{NRC} = 1$ (6 th #)

3.2.3 **ShutDown reactor control Group-system, $G_{SD}D_{NRC}$ (0,0,0,0,3,1)**

$G_{SD}D_{NRC}$, the nuclear reactor shutdown control is to limit radioactive releases to the public in the event of a serious nuclear process failure. There are two shutdown systems in the CANDU design: ShutDown System #1 (SDS1) and ShutDown System #2 (SDS2). The philosophy for the design of the two shutdown systems is to keep them functionally and geometrically independent of each other and functionally independent of the reactor regulating/control systems and other nuclear process systems. The functional independence is achieved by using two different shutdown principles: SDS1 uses shutoff rods; SDS2 uses poison injection. The geometric independence of the two shutdown systems is achieved by SDS1 having the shutoff rods dropped vertically from the top of the reactor core, and SDS2 having the poison injection tubes inserted horizontally in the side of the reactor core. The access control to SDS1 and SDS2 is shown in Figure 3.9.

NINO defines the access to SDS1 and SDS2 systems, as follow:

<i>System</i>	<i>Description</i>	<i>NINO code</i>
$S_{SD1}G_{SD}D_{NRC}$	Reactor ShutDown System #1	(0,0,0,1,3,1)
$S_{SD2}G_{SD}D_{NRC}$	Reactor ShutDown System #2	(0,0,0,2,3,1)

<i>NINO code:</i>	System - ShutDown System 1:	$S_{SD1} = 1$ (4 th #);
	ShutDown System 2:	$S_{SD2} = 2$ (4 th #);
	Group system - Reactor Shutdown:	$G_{SD} = 3$ (5 th #);
	Division - Nuclear Reactor Control:	$D_{NRC} = 1$ (6 th #)

Figure 3.9: Reactor ShutDown Systems

3.2.3-1 Reactor ShutDown System #1 - $S_{SD1}G_{SD}D_{NRC}$ (0,0,0,1,3,1)

$S_{SD1}G_{SD}D_{NRC}$, the reactor shutdown system, dropping 28 mechanical shutoff rods into the reactor, is the preferred system for quickly shutting off the reactor operation when the reactor safety parameters become unacceptable. SDS1 uses an independent triplicated logic system that senses the conditions for reactor trip and then de-energizes the direct current clutches to release the spring-assisted gravity drop shutoff rods into the reactor core.

NINO defines the control of dropping 28 shutoff rods into the reactor core as follows:

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
$f_C-d_{SR}E_{SC}S_{SD1}G_{SD}D_{NRC}$	28 shutoff rods control	(3,[1..28],1,1,3,1)

<i>NINO code:</i>	function - Controlling:	$f_C = 3$ (1 st #);
	device - Shutoff Robs Controller:	$d_{SR} = 1 \dots 28$ (2 nd #);
	Equipment - Shutoff rods Control:	$E_{SC} = 1$ (3 rd #);
	System - ShutDown System 1:	$S_{SD1} = 1$ (4 th #);
	Group system - Reactor Shutdown:	$G_{SD} = 3$ (5 th #);
	Division - Nuclear Reactor Control:	$D_{NRC} = 1$ (6 th #)

3.2.3-2 **Reactor ShutDown System #2 - $S_{SD2}G_{SD}D_{NRC}$ (0,0,0,2,3,1)**

$S_{SD2}G_{SD}D_{NRC}$, the reactor shutdown system, using the gadolinium poison injection into the moderator, is activated on a high positive power error with the reactor power being increasing. Also this control is to overcome a reactivity increase from xenon decay or poison removal by inadvertent purification system operation. A gadolinium poison addition mixing tank connects into moderator-outlet line near the cross-connection line between the two pump suction lines.

NINO defines the control of the gadolinium poison injection into the moderator as follows:

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
f_C-d_{IC}E_{PI}S_{SD2}G_{SD}D_{NRC}:	gadolinium poison addition control	(3,1,1,2,3,1)
<i>NINO code:</i>	function - Controlling: device - Injection Controller: Equipment - Poison Injection Controller: System - ShutDown System 2: Group system - Reactor reactivity Control: Division - Nuclear Reactor Control:	f _C = 3 (1 st #); d _{IC} = 1 (2 nd #); E _{PI} = 1 (3 rd #); S _{SD2} = 3 (4 th #); G _{SD} = 2 (5 th #); D _{NRC} = 1 (6 th #)

3.2.4 **Moderator Temperature control Group-system, $G_{MT}D_{NRC}$ (0,0,0,0,4,1)**

$G_{MT}D_{NRC}$, the moderator temperature control group system is to control the temperature of the moderator at the calandria outflow of the moderator heavy water to a setpoint. During the normal reactor operation, the moderator heavy water is *pumped* from the bottom of the calandria through two parallel-connected heat exchangers to cool the heavy water, and then the cooled heavy water is returned to the calandria at the horizontal centerline. The moderator temperature control is achieved by steering the two service water *control valves* that control the amount of cooling flow to two heat exchangers.

This group uses two control systems as shown in Figure 3.10.

NINO defines the moderator temperature control systems, as follow:

<i>System</i>	<i>Description</i>	<i>NINO code</i>
S_{MHC}G_{MT}D_{NRC}	Moderator Heavy-water Circulating System	(0,0,0,1,4,1)
S_{MSC}G_{MT}D_{NRC}	Moderator Service-water Cooling System	(0,0,0,2,4,1)
<i>NINO code:</i>	System - Moderator Heavy-water Circulating: Moderator Service-water Cooling: Group system - Moderator Temperature Control: Division - Nuclear Reactor Control:	S _{MHC} = 1 (4 th #); S _{MSC} = 2 (4 th #); G _{MT} = 4 (5 th #); D _{NRC} = 1 (6 th #)

Figure 3.10: Moderator Temperature Control Systems

3.2.4-1 Moderator Heavy-water Circulating System - $S_{MHC}G_{MT}D_{NRC}$

$S_{MHC}G_{MT}D_{NRC}$, the moderator heavy-water circulating control system is to pump the moderator heavy water from the bottom of the calandria through two parallel-connected heat exchangers that cool the heavy water, and then to pump the heavy water back to calandria at the horizontal centerline to increase heat convection.

NINO defines the control of 5 pumps for moderator heavy water circulation as follows:

Controlling	Description	<i>NINO</i> code
$f_C-d_{PC}E_{HP}S_{MHC}G_{MT}D_{NRC}$	moderator temperature control	(3,[1..5],1,1,4,1)

<i>NINO</i> code:	function - Controlling:	$f_C = 3$ (1 st #);
	device - Pump Controllers:	$d_{PC} = [1..5]$ (2 nd #);
	Equipment - Heavy water Pump control:	$E_{HP} = 1$ (3 rd #);
	System - Moderator Heavy-water Circulating:	$S_{MHC} = 1$ (4 th #);
	Group system - Moderator Temperature control:	$G_{MT} = 4$ (5 th #);
	Division - Nuclear Reactor Control:	$D_{NRC} = 1$ (6 th #)

3.2.4-2 Moderator Service-water Cooling System - $S_{MSC}G_{MT}D_{NRC}$

$S_{MSC}G_{MT}D_{NRC}$, the moderator service-water cooling control system is to control the flow of cool service water to the two heat exchanger for the temperature control of the moderator.

NINO defines the control of 4 valves for regulating the service-water cooling flow as follows:

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
f _C -d _{VC} E _{VD} S _{MSC} G _{MT} D _{NRC} :	moderator temperature control	(3,[1..4],1,2,4,1)
<i>NINO code:</i>	function - Controlling: device - Valves Controllers: Equipment - control Valve Drive: System - Moderator Service-water Cooling: Group system - Moderator Temperature control: Division - Nuclear Reactor Control:	f _C = 3 (1 st #); d _{VC} = [1..4] (2 nd #); E _{VD} = 1 (3 rd #); S _{MSC} = 2 (4 th #); G _{MT} = 4 (5 th #); D _{NRC} = 1 (6 th #)

3.3 Reactor Heat Transport Control Division – D_{HTC} (0,0,0,0,2)

This section presents reactor Heat Transport Control Division (D_{HTC}). The key control in this division is to maintain a pressure such that the heavy water coolant in the heat transport system remains in a subcooled liquid state to ensure that no bulk boiling occurs. This heat transport pressure control warrants an adequate margin to dryout conditions to avoid fuel and fuel sheath failures and maintain the integrity of the first and second barriers to radiological releases. This pressure control also prevents the heat transport piping from over-pressurized to avoid rupture causing the failure of the third barrier to radiological releases.

The heat transport pressure control relieves an overpressure above the normal feed-bleed controlling range to the bleed condenser through the separate relief control valves. The heavy water coolant pressure must be kept below saturation to maintain the control capability for measuring the channel outlet temperatures to detect flow blockages or channel overpowering. However at the saturation condition, a channel flow reduction or overpower cannot be measured by temperature increase as this condition does not increase the outlet temperature. The pressure at the reactor outlet headers is selected as a reference as it is of lower pressure and highest temperature, and therefore prevention of any boiling at the reactor outlet headers ensures no bulk boiling in the heat transport system.

D_{HTC} composes of 3 Group-systems:

$G_{HF}D_{HTC}$:	Heat-transport Feed control Group-system	(0,0,0,0,1,2)
$G_{HB}D_{HTC}$:	Heat-transport Bleed control Group-system	(0,0,0,0,2,2)
$G_{HC}D_{HTC}$:	Heat-transport Condenser control Group-system	(0,0,0,0,3,2)
$G_{HP}D_{HTC}$:	Heat-transport Pressure control Group-system	(0,0,0,0,4,2)

Figure 3.4: Heat Transport Control (HTC) in OSL-1

3.3.1 Heat Transport Feed control Group-system, $G_{HF}D_{HTC}$ (0,0,0,0,1,2)

$G_{HF}D_{HTC}$, the heat transport feed control group-system is one of the two controls, namely feed and bleed, that are used to maintain the heat transport pressure to the desired setpoint by compensating for the normal changes in heavy water coolant volume caused by the temperature variations in the heat transport system and the inventory losses due to leaks. The temperature variation occurs during startup, shutdown, power steering, etc.

The heat transport feed control group-system operates when the heat transport pressure is *below* the setpoint by using two feed control valves and two feed pressurizing pumps. This group has two control systems as shown in Figure 3.11.

NINO defines the heat transport feed control systems, as follow:

System	Description	NINO code
$S_{HFV}G_{HF}D_{HTC}$	Heat-transport Feed Valves control System	(0,0,0,1,1,2)
$S_{HFP}G_{HF}D_{HTC}$	Heat Transport Feed Pumps control System	(0,0,0,2,1,2)
NINO code:	System - Heat transport Feed Valves control: Heat transport Feed Pumps control: Group system - Heat transport Feed control: Division - Heat Transport Control:	$S_{HFV} = 1$ (4 th #); $S_{HFP} = 2$ (4 th #); $G_{HF} = 1$ (5 th #); $D_{HTC} = 2$ (6 th #)

Figure 3.11: Heat transport Feed control Systems

3.3.1-1 *Heat-transport Feed Valves control System - $S_{HFV}G_{HF}D_{HTC}$ (0,0,0,1,1,2)*

The heat transport feed for pressure increase is controlled by the two feed control valves that feed the heavy water from the pressurizing header into the reactor outlet headers.

NINO defines the control of the 2 heat-transport feed control valves as follows:

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
f_C-d_{VC}E_{FCV}S_{HFV}G_{HF}D_{HTC}:	2 heat-transport feed valves controllers	(3,[1,2],1,1,1,2)

<i>NINO code:</i>	function - Controlling:	f _C = 3 (1 st #);
	device - Valve Controllers:	d _{VC} = 1 to 2 (2 nd #);
	Equipment - heavy water Feed Control Valves:	E _{FCV} = 1 (3 rd #);
	System - Heat transport Feed Valves control:	S _{HFV} = 1 (4 th #);
	Group system - Heat transport Feed control:	G _{HF} = 1 (5 th #);
	Division - Heat Transport Control:	D _{HTC} = 2 (6 th #)

3.3.1-2 *Heat Transport Feed Pumps control System - $S_{HFP}G_{HF}D_{HTC}$ (0,0,0,2,1,2)*

Two pumps for heat-transport pressure increase are used to pressurize the heavy water from the heat transport heavy water storage tank and feed the heavy water to the pressurizing header.

NINO defines the control of the 2 heat-transport pressurizing feed pumps as follows:

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
f_C-d_{PC}E_{FPC}S_{HFP}G_{HF}D_{HTC}:	2 heat-transport pressurizing feed pumps Controllers	(3,[1,2],1,2,1,2)

<i>NINO code:</i>	function - Controlling:	f _C = 3 (1 st #);
	device - Pump Controllers:	d _{PC} = 1 to 2 (2 nd #);
	Equipment - heavy water Feed Pumps Control:	E _{FPC} = 1 (3 rd #);
	System - Heat transport Feed Pumps control:	S _{HFP} = 2 (4 th #);
	Group system - Heat transport Feed control:	G _{HF} = 1 (5 th #);
	Division - Heat Transport Control:	D _{HTC} = 2 (6 th #)

3.3.2 *Heat Transport Bleed control Group-system, $G_{HB}D_{HTC}$ (0,0,0,0,2,2)*

$G_{HB}D_{HTC}$, the heat transport bleed control system is one of the two controls, namely feed and bleed that are used to maintain the heat transport pressure to the desired setpoint by compensating for the normal changes in heavy water coolant volume caused by the temperature variations in the heat transport system and the inventory losses due to leaks.

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
fc-d_{VC}E_{BCV}S_{HBV}G_{HB}D_{HTC} :	2 heat transport bleed controllers	(3,[1,2],1,1,2,2)

<i>NINO code:</i>	function - Controlling:	f _C = 3 (1 st #);
	device - Valve Controllers:	d _{VC} = 1 to 2 (2 nd #);
	Equipment - heavy water Bleed Control Valves:	E _{BCV} = 1 (3 rd #);
	System - Heat transport Bleed Valves control:	S _{HBV} = 1 (4 th #);
	Group system - Heat transport Bleed control:	G _{HB} = 2 (5 th #);
	Division - Heat Transport Control:	D _{HTC} = 2 (6 th #)

3.3.2-2 *Heat Transport Reflux Valve control System - S_{HRV}G_{HB}D_{HTC} (0,0,0,2,2,2)*

The heavy water flows from the bleed control valves into the bleed condenser is cooled and condensed by the cooling flow of heavy water from the pressurizing header. This cooling flow is controlled by the reflux control valve.

NINO defines the control of the heat-transport reflux control valve as follows:

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
fc-d_{VC}E_{RCV}S_{HRV}G_{HB}D_{HTC} :	reflux control valve controller	(3,1,1,2,2,2)

<i>NINO code:</i>	function - Controlling:	f _C = 3 (1 st #);
	device - Valve Controller:	d _{VC} = 1 (2 nd #);
	Equipment - heavy water Reflux Control Valve:	E _{RCV} = 1 (3 rd #);
	System - Heat transport Reflux Valve control:	S _{HRV} = 2 (4 th #);
	Group system - Heat transport Bleed control:	G _{HB} = 2 (5 th #);
	Division - Heat Transport Control:	D _{HTC} = 2 (6 th #)

3.3.2-3 *Heat Transport Spray Valve control System - S_{HSV}G_{HB}D_{HTC} (0,0,0,3,2,2)*

When the reflux heavy water flow is not sufficient to maintain the pressure in the bleed condenser, a direct spray cooling flow from the pressurizing header into the condenser. This cooling flow is controlled by the spray control valve.

NINO defines the control of the heat-transport spray control valve as follows:

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
fc-d_{VC}E_{SCV}S_{HSV}G_{HB}D_{HTC} :	spray control valve controller	(3,1,1,3,2,2)

<i>NINO code:</i>	function - Controlling:	f _C = 3 (1 st #);
	device - Valve Controller:	d _{VC} = 1 (2 nd #);
	Equipment - heavy water Spray Control Valve:	E _{SCV} = 1 (3 rd #);
	System - Heat transport Spray Valve control:	S _{HSV} = 3 (4 th #);
	Group system - Heat transport Bleed control:	G _{HB} = 2 (5 th #);
	Division - Heat Transport Control:	D _{HTC} = 2 (6 th #)

3.3.3 Heat Transport Condenser control Group-system, $G_{HC}D_{HTC} (0,0,0,0,3,2)$

This heat transport condenser control group-system is to control the level and the overpressure in the bleed condenser. The bleed condenser is to receive the normal bleed and overpressure relief flows from the heat transport system. This group has two control systems as shown in Figure 3.13.

NINO defines the heat transport condenser control systems, as follow:

System	Description	NINO code
$S_{CLV}G_{HC}D_{HTC}$	Bleed Condenser Level Valves control System	(0,0,0,1,3,2)
$S_{CRV}G_{HC}D_{HTC}$	Bleed Condenser Relief Valves control System	(0,0,0,2,3,2)
NINO code:		
	System - Bleed Condenser Level control:	$S_{CLV} = 1$ (4 th #);
	Bleed Condenser Relief control:	$S_{CRV} = 2$ (4 th #);
	Group system - Heat transport Condenser control:	$G_{HC} = 3$ (5 th #);
	Division - Heat Transport Control:	$D_{HTC} = 2$ (6 th #)

Figure 3.13: Heat transport Condenser control Systems

3.3.3-1 Bleed Condenser Level Valves control System – $S_{BCL}G_{HC}D_{HTC} (0,0,0,1,3,2)$

The heavy water level in the bleed condenser is controlled by two level control valves. The inflow of the level control valves is from the outlet of the bleed cooler and the cooler inlet is connected to the bleed condenser. The outflow of the level control valves goes to the purification circuit.

NINO defines the control of the 2 bleed-condenser level control valves as follows:

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
f_C-d_{VC}E_{BLV}S_{BCL}G_{HCD}D_{HTC}	2 bleed condenser level control valve controllers	(3,[1,2],1,1,3,2)
<i>NINO code:</i>	function - Controlling:	f _C = 3 (1 st #);
	device - Valve Controller:	d _{VC} = 1,2 (2 nd #);
	Equipment - Bleed condenser Level control Valves:	E _{BLV} = 1 (3 rd #);
	System - Bleed Condenser Level control:	S _{BCL} = 1 (4 th #);
	Group system - Heat transport Condenser control:	G _{HCD} = 3 (5 th #);
	Division - Heat Transport Control:	D _{HTC} = 2 (6 th #)

3.3.3-2 *Bleed Condenser Relief Valves control System - S_{HCR}G_{HCD}D_{HTC} (0,0,0,2,3,2)*

Two bleed condenser relief valves are to relieve any overpressure in the bleed condenser. These valves protect the bleed condenser from overpressure and open the flow from the condenser to a tank in the boiler room for an overpressure condition.

NINO defines the control of the 2 bleed-condenser relief valves as follows:

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
f_C-d_{VC}E_{BRV}S_{HCR}G_{HCD}D_{HTC}	2 bleed condenser relief valve controllers	(3,[1,2],1,2,3,2)
<i>NINO code:</i>	function - Controlling:	f _C = 3 (1 st #);
	device - Valve Controller:	d _{VC} = 1,2 (2 nd #);
	Equipment - Bleed condenser Relief Valves:	E _{BRV} = 1 (3 rd #);
	System - Heat transport Condenser Relief control:	S _{HCR} = 2 (4 th #);
	Group system - Heat transport Condenser control:	G _{HCD} = 3 (5 th #);
	Division - Heat Transport Control:	D _{HTC} = 2 (6 th #)

3.3.4 *Heat-transport Pressure control Group-system, G_{HP}D_{HTC} (0,0,0,0,4,2)*

This heat transport pressure control is to maintain an adequate margin to dryout conditions to avoid fuel and fuel sheath failures and maintain the integrity of the first and second barriers to radiological releases. This pressure control also prevents the heat transport piping from over-pressurized to avoid rupture causing the failure of the third barrier to radiological releases. This is done by the controls described in sections 3.3.1 for heat-transport feed control, section 3.3.2 for bleed control, and section 3.3.3 for condenser control.

G_{HP}D_{HTC} (0,0,0,0,1,2), the heat transport feed control system operates when the heat transport pressure is *below* the setpoint by using two feed control valves and two feed pressurizing pumps (section 3.3.1).

G_{HB}D_{HTC} (0,0,0,0,2,2), the heat transport bleed control system operates when the heat transport pressure is *above* the setpoint by using two bleed control valves, reflux control valve, spray control valve, and bleed condenser level control valves (section 3.3.2).

G_{HC}D_{HTC} (0,0,0,0,3,2), the heat transport condenser to control the level and the overpressure in the bleed condenser. The heat transport pressure control relieves an overpressure above the normal feed-bleed controlling range to the bleed condenser through the separate relief control valves (section 3.3.3).

3.4 Live *NINO* Data Base

This section presents a data base established for *NINO*. This *NINO* data base is a “live” data base that is continuously updated (added, deleted, changed, re-organized, etc.). The data base can be expressed as a set of *NINO* codes in the four nuclear divisions:

$$NINO \text{ data base} = \left\{ \begin{array}{l} (n_1 n_2 n_3 n_4 n_5 1) \dots\dots \\ (n_1 n_2 n_3 n_4 n_5 2) \dots\dots \\ (n_1 n_2 n_3 n_4 n_5 3) \dots\dots \\ (n_1 n_2 n_3 n_4 n_5 4) \dots\dots \end{array} \right\} \begin{array}{l} D_{NRC} = 1 \\ D_{HTC} = 2 \\ D_{BSC} = 3 \\ D_{TGC} = 4 \end{array} \quad (3.1)$$

The *NINO* codes presented in this chapter and in Appendix I are by no means exhaustive, even though they represent the key operations in the existing nuclear process.

This data base is to be added when either an existing equipment becomes ready for network control or a new equipment with networking facility are installed.

3.5 Design Evaluation of *NINO*

This section presents an evaluation of *NINO*, the new design of network-integrated nuclear operation.

NINO is an efficient, simple, practical design that can transform the access to the tremendous complex safety-critical nuclear operations involving with over a thousand devices into a simple systematic access with proficient secure control. The following provides an illustration.

Illustration of Liquid-Zone Inflow Control NINO

a) *Operation Request*

This illustration assumes that a nuclear engineer requests to access the *NINO* network to carry out a control operation on the *control valve #8* in the nuclear reactor liquid-zone light-water inflow control system.

b) *Operation Background Knowledge*

The reactivity in the nuclear reactor can be controlled by varying the light water content in the 14 liquid zones inside the reactor. The level of the light water in the zones can be adjust either concurrently for bulk reactor flux control or individually for reactor spatial flux control.

The inflow of the light water is varied using control valves. The levels of the light water in the 14 reactor liquid zones are regulated individually by *14 control valves* that are pneumatically actuated.

c) *NINO code*

The *NINO* code for the requested control operation is:

(3, 8, 2, 2, 1, 1)

where the 6 numbers in order are: **3** = *function*: control, **8** = *device*: control valve #8, **2** = *equipment*: water control valve, **2** = *system*: liquid-zone reactivity control, **1** = *group system*: reactor reactivity control, **1** = *division*: nuclear reactor control.

d) *Operation Qualifications List*

Each *NINO* operation has a list of minimum operation qualifications. For illustration, the list for the *NINO* (3,8,2,2,1,1) is $\{L_{(3,8,2,2,1,1)}\}$:

$$\{L_{(3,8,2,2,1,1)}\} = \left\{ \begin{array}{l} \left\{ \begin{array}{ll} \text{QualiRegNumber} & \text{QualiDescription} \\ R1.3.2 & \text{authorized nuclear operator} \\ R2.3.3 & \text{reactor room engineer} \\ R3.2.1 & \text{senior technologist} \end{array} \right\} \\ \left\{ \begin{array}{ll} F2.1.1 & \text{online reactor operation} \\ F2.1.3 & \text{online liquid zone operation} \\ F2.1.4 & \text{online reactivity operation} \end{array} \right\} \\ \left\{ \begin{array}{ll} T1.2.1 & \text{radiation risk identification} \\ T1.3.1 & \text{nuclear cyber security} \\ T2.1.1 & \text{CANDU nuclear process} \\ T3.2.4 & \text{reactor regulating system} \\ T4.1.2 & \text{moderator control} \end{array} \right\} \end{array} \right\} \quad (3.2)$$

e) *User Qualification List*

The user- x 's qualification list $\{LoQ\}_x$ must cover $\{L_{(3,8,2,2,1,1)}\}_x$, the list of minimum qualifications required for the NINO (3,8,2,2,1,1) i.e. $\{L_{(3,8,2,2,1,1)}\}_x$ is a subset of $\{LoQ\}_x$:

$$\{L_{(n1...n6)}\}_x \in \{LoQ\}_x \quad (3.3)$$

f) *NINO Access Control*

The access to *NINO* for carrying out an operation is straightforward, as summarized below:

1. *Obtain a nuclear network pass code.*

The nuclear worker submit his/her *Certificate of Network Access* $CNA(IDx, PKx)$ authorization to the authentication server (*AS*) for authentication and for obtaining a pass code: $\{N_{XI}, N_{SI}\}$.

2. *Obtain a nuclear operation pass code.*

The nuclear user submit his/her requested nuclear operation $NINO\{(n1...n6)\}_x$ and *Certificates of Operation Qualifications* $COQ(IDx, \{LoQ\}_x)$ using the network pass code $\{N_{XI}, N_{SI}\}$ to the operation server (*OS*) for authorization and for obtaining an operation pass code: $\{N_{XI}, N_{OI}\}$.

3. *Access NINO network for operation (n1...n6).*

The user using the operation pass code $\{N_{XI}, N_{OI}\}$ to carry out the requested nuclear operation, for example: (3,8,2,2,1,1) the control of liquid-zone light-water control valve #8.

Chapter 4

NETWORK-DRIVEN CONDITION-BASED NUCLEAR MAINTENANCE

This chapter creates the network-driven *Condition-Based Nuclear Maintenance (CBNM)*, the new nuclear maintenance developed in this thesis research.

Condition-based (predictive) maintenance is the key for significant reduction of operation and maintenance (O&M) costs for the industry, especially for the nuclear industry of which the cost for *one day outage* for maintenance would be close to *one million dollars* for *one nuclear unit*. This thesis research is therefore focused on the reduction of the frequency and length of nuclear unit outage, leading to huge nuclear station cost savings or revenue increase. In order to effectively implement the condition-based maintenance, this thesis research creates *CBNM*, the condition-based maintenance of nuclear process. The success of *CBNM* is based on the correct and timely assessments of nuclear devices/equipment on-going operations.

This chapter presents the architecture of the *CBNM* in *Tier 3* of the Secure Trilateral Access Control (*STAC*), the new nuclear network access control developed in this thesis, as shown in Figure 4.1. This thesis is focused on the *STAC* design for the major operations and maintenance in the current live nuclear electricity generating stations using CANDU reactors, as an initial prime step in the nuclear practices modernization.

Figure 4.1: Tier-3 CBMM

This chapter defines the conditions of the network-assisted *CBNM* for facilitating the determination of which device/equipment/system in the nuclear control unit needs maintenance, when the maintenance is needed, how the maintenance is implemented, where the maintenance is proceeded, etc.

This chapter presents:

- Section 4.1: This section presents the new design for nuclear condition-based maintenance. This section provides an overall view the Tier-3 STAC, the architecture of the condition-based nuclear maintenance, and the design base for the conditions sets used for *CBNM*
- Section 4.2: This section presents the *Operation Conditions* set for *CBNM*.
- Section 4.3: This section presents the *System Conditions* set for *CBNM*.
- Section 4.4: This section presents the *Equipment Conditions* set for *CBNM*.
- Section 4.5: This section presents the *Maintenance Conditions* set for *CBNM*.
- Section 4.6: This section presents the *Security Conditions* set for *CBNM*.
- Section 4.7: This section presents a data base established for *CBNM*. This *CBNM* data base is a “live” data base that is continuously updated including add, delete, change, re-organize, etc.

4.1 Network-assisted Nuclear Condition-Based Maintenance

This section presents the new design for network-assisted nuclear condition-based maintenance that is developed in this thesis research, as follows:

First, present an overall view the Tier-3 STAC.

Second, present the architecture of the condition-based nuclear maintenance.

Third, present the design base for conditions sets for CBNM

4.1.1 Overall View of Tier-3 STAC

Figure 4.2 shows an overall view of Tier-3 for the Maintenance Access Control and its relationship with Tier-1 for the Network Access Control and Tier-2 for the Network-Integrated Nuclear Operation.

Figure 4.2: Condition-Based Nuclear Maintenance (CBNM)

As shown in Figure 4.2, the nuclear network user can access Tier-1 (A), Tier-2 (B), and Tier-3 (C), if the user successfully pass the specified authentications (refer to Chapter 2 for details). Tier 3, the network-assisted nuclear condition-based maintenance can communicate with Tier 2, the network-integrated nuclear operation (D), for transferring nuclear operation data for performing *CBNM*.

4.1.2 Architecture of Condition-Based Nuclear Maintenances

This section presents the architecture of the Condition-Based Nuclear Maintenance developed in this thesis research. The architecture is illustrated in Figure 4.3.

Figure 4.3: Architecture for CBNM

As shown in Figure 4.3, the CBNM consists of three maintenance security levels:

- *MSL-1* for nuclear *On-line Critical CBNM*,
- *MSL-2* for nuclear *On-line Non-Critical CBNM*,
- *MSL-3* for nuclear *Outage CBNM*.

Each authorized condition-based maintenance network access is assigned with one CBNM code which is defined in the form of:

$$\text{CBNM code} = (\{SL\text{-set}\}, \{MC\text{-set}\}, \{EC\text{-set}\}, \{SC\text{-set}\}, \{OC\text{-set}\}) \quad (4.1)$$

- where
- SL-set* = Security Levels set: MSL-1, MSL-2, and MSL-3 security divisions
 - MC-set* = Maintenance Conditions set: device adjustment, correction, replacement, etc.
 - EC-set* = Equipment Conditions set: control valve, sensor, transmitters, etc.
 - SC-set* = System Conditions set: high risk, low risk, critical, non-critical, backup, etc.
 - OC-set* = Operation Condition set: a NINO code represents the set of a nuclear operation, as described in chapter 3.

The basic process of *CBNM* is illustrated in Figure 4.3 as follows:

- (1) A nuclear network user can initiate a maintenance work order after successfully passes the required authentication, and then the work order is sent to the *CBNM* network access control central system.
- (2) The maintenance work order is then processed with the components of the *CBNM* code that include *SL-set*, *MC-set*, *EC-set*, *SC-set*, and *OC-set* (the attributes of these *CBNM* components are to be detailed in the following sections). After all the *CBNM* components are determined, a *CBNM* access code is formed and then assigned for the maintenance work order.
- (3) With the access code, the *CBNM* can be linked to the *Tier-2 NINO* control divisions: *NRC*, *HTC*, *BSC*, or *TGC* (discussed in Chapter 3).
- (4) The *SL-set* is used for linking the security divisions: *MSL-1*, *MSL-2*, and *MSL-3*.

4.1.3 Design Base for Conditions Sets for *CBNM*

The base for the *CBNM* is on the correct and timely assessments of nuclear devices/equipment's on-going operating *conditions*. In order to facilitate the secure, accurate and non-delayed assessments, the network-assisted *CBNM* is coded with **5 conditions sets**:

$$\{\mathbf{SL-set}\}, \{\mathbf{MC-set}\}, \{\mathbf{EC-set}\}, \{\mathbf{SC-set}\}, \{\mathbf{OC-set}\} \quad (4.2)$$

These 5 conditions sets of the *CBNM* elements are required to be determined, prior to performing the actual physical condition-based maintenance. These conditions sets are developed in the following sections.

For simplicity the *Equipment to be targeted and coded for performing CBNM* is termed as $\mathbf{E_{CBNM}}$ in the development of the *CBNM* codes.

4.2 Operation Conditions {OC-set}

This section presents the *Operation Conditions* set for $CBNM$.

Identify {**OC-set**}, the set of operation conditions imposed on E_{CBNM} . As shown in Figure 4.4, the {**OC-set**} is linked to the 4 *NINO* divisions: *NRC* (nuclear reactor control), *HTC* (heat transport control), *BSC* (boiler steam control), and *TGC* (turbine generator condenser control).

Figure 4.4: {**OC-set**} for E_{CBNM}

The {**OC-set**}, defined for the condition-based maintenance, is presented below:

$$\{\mathbf{OC-set}\} = \{\{\mathbf{OC-4}\} \{\mathbf{OC-3}\} \{\mathbf{OC-2}\} \{\mathbf{OC-1}\}\} \quad (4.3)$$

- {**OC-1**} is condition set for operating *divisions* (*NINO* code ($x, x, x, x, x, n_{\text{division}}$))

Condition OC-1.1: Identify the operating division that E_{CBNM} is in.

Condition OC-1.2: Determine the criticality of the effects on nuclear safety and uninterruptable operation if E_{CBNM} is taken out for maintenance, which the tightness of the conditions that $CBNM$ is based on.

In general, the tightness of the condition for E_{CBNM} decreases from *NRC*, *HTC*, *BSC*, to *TGC*, as the operating division is physically located away from the nuclear reactor that is the focus of nuclear safety.

- {**OC-2**} is condition set for operating *systems/group-systems* (*NINO* code($x, x, x, n_{\text{system}}, n_{\text{group-system}}, x$))

Condition OC-2.1: Identify the operating system or group system that E_{CBNM} is in.

Condition OC-2.2: Determine the effects if E_{CBNM} is taken out for maintenance on the system or group system where E_{CBNM} is in.

Condition OC-2.3: Identify if other equipment of the same system or group system are affected by taking E_{CBNM} out of service.

Condition OC-2.4: Assess if other equipment need to be changed in order to any adverse effects when E_{CBNM} is taken out for maintenance, and determine the changes.

- {OC-3} is condition set for operating *devices* or *equipment* (NINO code ($x, n_{\text{devices}}, n_{\text{equipment}}, x, x, x$))

Condition OC-3.1: Identify the operating state of E_{CBNM} , online or out of service.

- {OC-4} is condition set for device/equipment *functions* (NINO code ($n_{\text{function}}, x, x, x, x, x$))

Condition OC-4.1: Identify the function of E_{CBNM} , monitoring, processing, or controlling.

In general, the tightness of condition is increasing from monitoring, processing, to controlling, for the same level of security and nuclear safety.

Finally, the superset of {OC-set} in the CBNM code consists of:

$$\{\text{OC-set}\}_{\text{superset}} = \{\{1.1, 1.2\} \{2.1, 2.2, 2.3, 2.4\} \{3.1\} \{4.1\}\}_{\text{superset}} \quad (4.3)$$

4.3 System Conditions {SC-set}

This section presents the *System Conditions* set for $CBNM$.

Identify $\{SC-set\}$, the set of nuclear system conditions imposed on E_{CBNM} . As shown in Figure 4.5, the $\{SC-set\}$ is classified as: $\{SC-1\}$ to $\{SC-5\}$ conditions subsets, and the classification is based on the nuclear safety and electricity production point of view (not from the operation function point of view as shown in Chapter 3).

Figure 4.5: $\{SC-set\}$ for E_{CBNM}

The $\{SC-set\}$, defined for condition-based maintenance, is presented below:

$$\{SC-set\} = \{\{SC-1\} \{SC-2\} \{SC-3\} \{SC-4\} \{SC-5\}\} \quad (4.4)$$

- $\{SC-1\}$ is condition set for **high risk** system.

Condition **SC-1.1**: Assess risks associated with E_{CBNM} , particularly with respect to the nuclear safety, if E_{CBNM} is in the *high-risk* system and to be taken out for maintenance.

Condition **SC-1.2**: If the assessment shows such risks, determine whether the maintenance of E_{CBNM} can be delayed until the next schedule outage, without causing any nuclear safety problem.

Condition **SC-1.3**: If the assessment shows such risk and the maintenance of E_{CBNM} cannot be delayed without causing further potential damages, perform an emergency

outage and shut down the nuclear reactor to carry out an immediate maintenance for E_{CBNM} . Return E_{CBNM} to service and resume the nuclear operation as soon as possible because the huge loss of revenue for shutting down one nuclear unit is close to a million dollar a day.

- {SC-2} is condition set for *critical* system.

Condition SC-2.1: Assess any risks associated with E_{CBNM} , with respect to the well-being of the nuclear operations and the continuing production of electricity, if E_{CBNM} is in the *critical* system and to be taken out for maintenance.

Condition SC-2.2: If the assessment shows such risks, determine whether the maintenance of E_{CBNM} can be delayed until the next schedule outage, without causing any nuclear safety problem.

Condition SC-2.3: If the assessment shows such risk and the maintenance of E_{CBNM} cannot be delayed without causing further possible damages, perform an emergency outage and shutdown the nuclear reactor in order to carry out an immediate maintenance for E_{CBNM} . Return E_{CBNM} to service and resume the nuclear operation as soon as possible

- {SC-3} is condition set for *non-critical* system.

Condition SC-3.1: If E_{CBNM} is in the *non-critical* system and to be taken out for maintenance, assess whether the maintenance can be carried out during the *online* operation (while the nuclear reactor is operating at full power) or has to be conducted during the *outage* (while the nuclear reactor is shut down).

Condition SC-3.2: If the assessment confirms that the equipment taken out of service will not cause any nuclear safety problem or any electricity production interruption, perform the online maintenance to correct any defects on E_{CBNM} .

Since E_{CBNM} is in the non-critical system, the level of risks associated with E_{CBNM} be taken out of service is *less* than the equipment in S-1 and S-2 above.

Condition SC-3.3: If the assessment shows that E_{CBNM} cannot be taken out for maintenance during online operation, determine whether the maintenance of E_{CBNM} can be delayed until the next schedule outage, without causing any nuclear operation

interruption. If it can be delayed, schedule the maintenance of that equipment in the next outage.

Condition SC-3.4: If the assessment shows that E_{CBNM} cannot be taken out during online operation and its maintenance cannot be delayed, perform an emergency outage to carry out an immediate maintenance on E_{CBNM} and quickly return it to services.

- {SC-4} is condition set for *supplementary* system.

Condition SC-4.1: If E_{CBNM} in the *supplementary* system is required for maintenance, determine whether E_{CBNM} can be delayed until the next scheduled outage, or must be taken out for maintenance during the online operation.

Usually, the maintenance of an equipment in the supplementary system can be delayed to the next scheduled outage.

Condition SC-4.2: If the maintenance of E_{CBNM} can be delayed, perform the maintenance in the next scheduled outage.

Condition SC-4.3: If the maintenance of E_{CBNM} cannot be delayed, perform the maintenance on E_{CBNM} during the online operation.

Usually, the maintenance of an equipment in the supplementary system can be performed during the online operation, without shutting down the nuclear unit.

- {SC-5} is condition set for *backup* system.

Condition SC-5.1: If E_{CBNM} in the *backup* system is required for maintenance, determine whether E_{CBNM} can be delayed until the next scheduled outage, or must be taken out for maintenance during the online operation.

Usually, the maintenance of an equipment in the backup system can be delayed to the next scheduled outage.

Condition SC-5.2: If the maintenance of E_{CBNM} can be delayed, perform the maintenance in the next scheduled outage.

Condition SC-5.3: If the maintenance of E_{CBNM} cannot be delayed under usual conditions, perform the maintenance on E_{CBNM} during the online operation.

Usually, the maintenance of an equipment in the backup system can be performed during the online operation, without shutting down the nuclear unit.

Finally, the superset of $\{SC\text{-}set\}$ in the *CBNM* code consists of:

$$\{SC\text{-}set\}_{\text{superset}} = \{\{1.1, 1.2, 1.3\} \{2.1, 2.2, 2.3\} \{3.1, 3.2, 3.3, 3.4\} \{4.1, 4.2, 4.3\} \{5.1, 5.2, 5.3\}\}_{\text{superset}} \quad (4.5)$$

4.4 Equipment Conditions {EC-set}

This section presents the *Equipment Conditions* set for *CBNM*.

Identify {*EC-set*}, the sets of equipment conditions imposed on E_{CBNM} . There is often over a thousand of devices operating in one traditional nuclear unit (one nuclear station may have up to 8 nuclear units). This thesis research is focused on those devices that can readily be modernized using *CBNM* the network-assisted condition-based maintenance developed in this thesis research. The objective of using *CBNM* is to achieve huge cost savings, particularly from minimizing the number of emergency forced outages and from increasing the operation service period before the need for an outage (An outage of *one* nuclear unit would cost close to one *million* dollars, *each* day).

For the nuclear devices that are ready to be implemented with the network-assisted condition-based maintenance, the CBNM is initially designed with 3 sets of E_{CBNM} as shown in Figure 4.6.

Figure 4.6: {*EC-set*} for E_{CBNM}

The $\{EC\text{-}set\}$, defined for condition-based maintenance, is presented below:

$$\{EC\text{-}set\} = \{\{EC\text{-}1.x\} \{EC\text{-}2.x\} \{EC\text{-}3.x\}\} \quad (4.6)$$

- $\{EC\text{-}1.x\}$ is the condition set for **Controls** equipment group (to be detailed in Section 5.2):

$\{EC\text{-}1.1\}$	Condition for valves' <i>static</i> wellbeing <i>CBNM</i>
$\{EC\text{-}1.2\}$	Conditions for valves' dynamic wellbeing <i>CBNM</i> illustrated with 10 typical conditions:
$\{EC\text{-}1.2.1\}$:	Base conditions for acceptable valve stroke
$\{EC\text{-}1.2.2\}$:	Conditions for valve seat degradation <i>CBNM</i>
$\{EC\text{-}1.2.3\}$:	Conditions for broken valve stem <i>CBNM</i>
$\{EC\text{-}1.2.4\}$:	Conditions for excessive friction on stroke <i>CBNM</i>
$\{EC\text{-}1.2.5\}$:	Conditions for bent valve stem <i>CBNM</i>
$\{EC\text{-}1.2.6\}$:	Conditions for actuator spring broken <i>CBNM</i>
$\{EC\text{-}1.2.7\}$:	Conditions for incorrect preloading <i>CBNM</i>
$\{EC\text{-}1.2.8\}$:	Conditions for valve stem misalignment <i>CBNM</i>
$\{EC\text{-}1.2.9\}$:	Conditions for non-achievable full stroke <i>CBNM</i>
$\{EC\text{-}1.2.10\}$:	Conditions for localized wear stem <i>CBNM</i>

- $\{EC\text{-}2.x\}$ is the condition set for **Pumps** equipment group (to be detailed in Section 5.3):

$\{EC\text{-}2.1\}$	Base conditions for acceptable pump characteristics
$\{EC\text{-}2.2\}$	Base conditions of acceptable characteristics for valves used as pump loads
$\{EC\text{-}2.3\}$	Conditions for acceptable characteristics for composite pump configurations
$\{EC\text{-}2.4\}$	Conditions for acceptable characteristics for composite valve configurations

- $\{EC\text{-}3.x\}$ is the condition set for **Controllers** equipment group (to be detailed in Section 5.4):

$\{EC\text{-}3.1\}$	Conditions for acceptable tolerances on current-to-pressure control
$\{EC\text{-}3.2\}$	Conditions for acceptable drifts on current-to-pressure control
$\{EC\text{-}3.3\}$	Conditions for acceptable dynamic disturbances on current-to-pressure control
$\{EC\text{-}3.4\}$	Conditions for acceptable tolerance on non-linear current-to-position control
$\{EC\text{-}3.5\}$	Conditions for acceptable static-dynamic disturbances on current-to-position control

$$\{EC\text{-}set\}_{\text{superset}} = \{\{1.1, \{1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.2.6, 1.2.7, 1.2.8, 1.2.9, 1.2.10\}\} \{2.1, 2.2, 2.3, 2.4\} \{3.1, 3.2, 3.3, 3.4, 3.5\}\}_{\text{superset}} \quad (4.7)$$

4.5 Maintenance Conditions {MC-set}

This section presents the *Maintenance Conditions* set for *CBNM*.

Identify {**MC-set**}, the set of maintenance conditions imposed on E_{CBNM} . As shown in Figure 4.7, the {**MC-set**} is divided into subsets of {**MC-1**} for equipment performance monitoring, {**MC-2**} for equipment settings adjustment, {**MC-3**} for equipment performance correction, {**MC-4**} for equipment replacement, {**MC-5**} for equipment isolation, and {**MC-6**} for equipment locked up.

Figure 4.7: {**MC-set**} for E_{CBNM}

The {**MC-set**}, defined for the condition-based maintenance, is presented below:

$$\{\mathbf{MC-set}\} = \{\{\mathbf{MC-1}\} \{\mathbf{MC-2}\} \{\mathbf{MC-3}\} \{\mathbf{MC-4}\} \{\mathbf{MC-5}\} \{\mathbf{MC-6}\}\} \quad (4.8)$$

- {**MC-1**} is condition set for equipment performance **monitoring**.

Condition MC-1.1: The monitoring of the equipment performance is usually a necessary action for the condition-based maintenance. Define the equipment performance criteria (such as the design operating ranges and various acceptable performance tolerances depending on the defined operating conditions) for the monitoring of E_{CBNM} .

Condition MC-1.2: If any of the performance criteria for E_{CBNM} is violated, issue a request for action or a warning for investigation, and record the equipment performance and its operating conditions.

- {MC-2} is condition set for equipment settings **adjustment**.

Condition MC-2.1: If the performance of E_{CBNM} deteriorates against the equipment performance specification, issue a warning for investigation, and record the equipment performance and its operating conditions.

Condition MC-2.2: If the rate of E_{CBNM} performance deterioration exceeds the design tolerance, issue a request for action, and record the equipment performance and its operating conditions.

- {MC-3} is condition set for equipment performance **correction**.

Condition MC-3.1: If the performance of E_{CBNM} is incorrect with a small scale with respect to the equipment performance specification, issue a request for corrective action, and record the equipment performance and its operating conditions.

Condition MC-3.2: If the performance of E_{CBNM} is incorrect with a considerable scale that may affect the well-being of the nuclear operation or may even affect the nuclear safety, issue a request for immediate correction, and record the equipment performance and its operating conditions.

Condition MC-3.3: If an immediate correction on E_{CBNM} is required, either perform an online maintenance, or shut down the nuclear reactor for E_{CBNM} correction depending on the results of assessments on {OC-set} and {SC-set}.

- {MC-4} is condition set for equipment **replacement**.

Condition MC-4.1: If the assessment confirms that the fault on E_{CBNM} cannot be corrected, issue a request for replacement, and prepare for the replacement of E_{CBNM} .

Condition MC-4.2: If the assessment confirms that the replacement of faulty E_{CBNM} can be delayed, schedule the E_{CBNM} replacement in the next outage.

Condition MC-4.3: If the assessment confirms that the replacement of faulty E_{CBNM} cannot be delayed, either perform an online replacement, or shut down the nuclear

reactor for E_{CBNM} replacement depending on the results of assessments on $\{OC-set\}$ and $\{SC-set\}$.

- $\{MC-5\}$ is condition set for equipment **isolation**.

Condition MC-5.1: If E_{CBNM} is required to be taken out for maintenance or a faulty ECBNM can affect the performance of other equipment, issue a warning and a request for authorization of E_{CBNM} isolation, then isolate E_{CBNM} after authorized.

- $\{MC-6\}$ for equipment **locked up**.

Condition MC-6.1: If E_{CBNM} is no longer needed for the nuclear operation, or if a faulty E_{CBNM} can affect the nuclear operation or even the nuclear safety, then lock up E_{CBNM} as soon as possible.

Finally, the superset of $\{MC-set\}$ in the $CBNM$ code consists of:

$$\{MC-set\}_{superset} = \{\{1.1, 1.2\} \{2.1, 2.2\} \{3.1, 3.2, 3.3\} \{4.1, 4.2, 4.3\} \{5.1\} \{6.1\}\}_{superset} \quad (4.9)$$

4.6 Security Conditions {SL-set}

This section presents the *Security Conditions* set for *CBNM*.

Identify **{SL-set}**, the security conditions imposed on E_{CBNM} . As shown in Figure 4.8, the **{SL-set}** is linked to the security divisions: *MSL-1* (Online Critical CBNM), *MSL-2* (Online Noncritical CBNM), and *MSL-3* (Outage CBNM).

The classification of the *MSL* security divisions for E_{CBNM} is based on the assessments in the above-mentioned **{OC-set}**, **{SC-set}**, and **{MC-set}**.

Figure 4.8: **{SL-set}** for E_{CBNM}

The **{SL-set}**, defined for condition-based maintenance, is presented below:

$$\{\mathbf{SL-set}\} = \{\{\mathbf{SL-0}\} \{\mathbf{SL-1}\} \{\mathbf{SL-2}\} \{\mathbf{SL-3}\}\} \quad (4.10)$$

- **{SL-0}** is condition set for *Maintenance Security Divisions*.

Condition CL-0.1: Determine the maintenance security level (*MSL-1*, *MSL-2*, or *MSL-3*) for E_{CBNM} , utilizing the results of the assessments mentioned in *O-set*, *S-set*, and *M-set* conditions for CBNM.

- **{SL-1}** is condition set for *Online Critical Maintenance, MSL-1 security division*.

Condition CL-1.1: If the maintenance of E_{CBNM} is classified as *Online Critical Maintenance* of security level *MSL-1*, the working team (see CL-1.3 below) for implementing

the maintenance must pass the highest of the 3 levels in the security checks for network-assisted condition-base maintenance.

Condition CL-1.2: If the maintenance is *MSL-1*, obtain the signed authorization for the online critical maintenance from the nuclear control room shift manager and supervisor prior to implementing the *E_{CBNM}* maintenance.

Condition CL-1.3: If the *E_{CBNM} MSL-1* maintenance is authorized, coordinate the maintenance team work with at least one Authorized Nuclear Operator (ANO) and one Control & Maintenance Technicians (CMT), and the System Responsible Engineer (SRE).

Condition CL-1.4: Prior to implementing the *E_{CBNM} MSL-1* maintenance, prepare and obtain approval for a backout plan according to the established nuclear procedures for placing the nuclear in the safe state in case of nuclear conditions deteriorate from the design safety ranges. Should such conditions occur, speedy implement the backout plan in a safe way.

- {SL-2} is condition set for ***Online Non-critical Maintenance, MSL-2 security division.***

Condition CL-2.1: If the maintenance of *E_{CBNM}* is classified as *Online Non-Critical Maintenance* of security level *MSL-2*, the working team (see CL-1.3 above) for implementing the maintenance must pass the security checks for network-assisted online noncritical maintenance.

Condition CL-2.2: If the maintenance is *MSL-2*, obtain the signed authorization for the online maintenance from the nuclear control room shift supervisor prior to implementing the *E_{CBNM}* maintenance.

Condition CL-2.3: If the *E_{CBNM} MSL-2* maintenance is authorized, coordinate the maintenance team work with at least one Authorized Nuclear Operator (ANO) and one Control & Maintenance Technicians (CMT), and the System Responsible Engineer (SRE).

Condition CL-2.4: Prior to implementing the *E_{CBNM} MSL-2* maintenance, prepare and obtain approval for a backout plan according to the established nuclear procedures for placing the nuclear in the safe state in case of nuclear conditions deteriorate

from the design safety ranges. Should such conditions occur, speedy implement the backout plan in a safe way.

- {**SL-3**} is condition set for ***Outage Maintenance, MSL-3 security division.***

Condition CL-3.1: If the maintenance of E_{CBNM} is classified as *Outage Maintenance* of security level *MSL-3*, the working team for implementing the maintenance is required to pass the normal security checks for maintenance work.

Condition CL-3.2: If the E_{CBNM} maintenance is *MSL-3* outage maintenance, obtain the normal authorization for maintenance and assign the number of nuclear workers as required according to the work plan to the work team.

Finally, the superset of the ***SL-set*** in the *CBNM* code consists of:

$$\{\mathbf{SL-set}\}_{\text{superset}} = \{\{\mathbf{x.1}\} \{1.1, 1.2, 1.3, 1.4\} \{2.1, 2.2, 2.3, 2.4\} \{3.1, 3.2\}\}_{\text{superset}} \quad (4.11)$$

4.7 Live *CBNM* Data Base

This section presents a data base established for *CBNM*. This *CBNM* data base is a “live” data base that is continuously updated (added, deleted, changed, re-organized, etc.). The data base can be expressed as a set of *CBNM* codes in the four nuclear divisions:

$$CBNM \text{ data base} = \left\{ \begin{array}{l} (\{sl_1 \dots\}, \{mc_1 \dots\}, \{ec_1 \dots\}, \{sc_1 \dots\}, \{n_1 n_2 n_3 n_4 n_5 1\}) \dots \\ (\{sl_1 \dots\}, \{mc_1 \dots\}, \{ec_1 \dots\}, \{sc_1 \dots\}, \{n_1 n_2 n_3 n_4 n_5 2\}) \dots \\ (\{sl_1 \dots\}, \{mc_1 \dots\}, \{ec_1 \dots\}, \{sc_1 \dots\}, \{n_1 n_2 n_3 n_4 n_5 3\}) \dots \\ (\{sl_1 \dots\}, \{mc_1 \dots\}, \{ec_1 \dots\}, \{sc_1 \dots\}, \{n_1 n_2 n_3 n_4 n_5 4\}) \dots \end{array} \right\} \begin{array}{l} D_{NRC} = 1 \\ D_{HTC} = 2 \\ D_{BSC} = 3 \\ D_{TGC} = 4 \end{array} \quad (4.12)$$

The *CBNM* codes presented in this chapter are by no means exhaustive, even though they represent the key condition-based nuclear maintenance in the existing nuclear process.

This data base is to be added when either an existing equipment becomes ready for network drive to carry out condition-based nuclear maintenance work or a new equipment with networking facility can be converted to conduct condition-based nuclear maintenance.

Chapter 5

DESIGN, MODELLING, AND EVALUATION OF NETWORK-DRIVEN CONDITION-BASED NUCLEAR MAINTENANCE

This chapter presents the design and evaluation of the *CBNM*, the *Condition-Based Nuclear Maintenance*, in association with *NINO*, the *Network-Integrated Nuclear Operation*, under *STAC*, the *Secure Trilateral Access Control*, all of which are created in this thesis.

This chapter is focused on the condition-based maintenance on the vast majority nuclear operating devices of *valves* and *pumps*, such that the use of *CBNM* on these devices can generate tremendous huge cost savings for nuclear generating stations [32-37]. This chapter presents the design evaluation with respect to the condition set $\{EC-1\}$ for valves, $\{EC-2\}$ for pumps, and $\{EC-3\}$ for their controllers, as shown in Figure 5.1, the layout of the network-driven *CBNM*.

Figure 5.1: *CBNM* condition sets $\{EC-1, EC-2, EC-3\}$

This chapter presents:

- Section 5.1: This section defines the focus of the design, modelling, and evaluation of *CBNM* on valves, pumps, and their controllers used in the nuclear process.
- Section 5.2: This section first presents the technique for trending the valve stem leakage as an illustrating criterion for assessment of valve *static wellbeing* conditions for determination of maintenance overhauls. Second, this section presents the valve dynamic wellbeing *CBNM*. The trending of 10 typical valve dynamic characteristics, represented by valve strokings versus actuator actions, is used as criteria for assessing the valve dynamic conditions for determination of maintenance overhauls.
- Section 5.3: This section first presents the modelling of characteristics curves for pumps and pump loads of unregulated valves used in the nuclear process. Typical configurations for pumps and valves such as parallel connections and series connections commonly found in the nuclear plant are to be modelled for used in the *CBNM*. Second, this section presents typical conditions as illustrations for implementation of *CBNM* on the pumps and the pump loads of unregulated valves used in the nuclear plants.
- Section 5.4: This section presents the conditions for typical controllers used in the nuclear process, with the focus on control output drifts, static and dynamic disturbances, and control non-linearity, etc. during the online operations. These are used as illustrations for the controllers condition-based maintenance in the application of *CBNM* developed in this thesis research.

5.1 CBNM Design, Modelling, and Evaluation Focus

This section defines the focus of the design, modelling, and evaluation of *CBNM*.

Of over a thousand of devices operating in one traditional nuclear unit, this chapter is focused on the vast majority nuclear operating devices, *valves and pumps*, and their control devices, such that the use of *CBNM* on these devices can generate tremendous huge cost savings for nuclear generating stations.

Figure 5.2 shows that the Equipment Condition sets $\{EC-1\}$, $\{EC-2\}$, and $\{EC-3\}$ for the condition-based maintenances of the valves, pumps, and their control devices, respectively.

Figure 5.2: Nuclear equipment groups selected for CBNM designs evaluation

5.1.1 Valves *CBNM* – $\{EC-1\}$

The valves condition-based assessment, to be carried out online while the nuclear unit is operating, can be used to reduce the frequency of the nuclear unit forced outage because of valves pre-failure conditions monitored, analyzed, predicted, and used to optimize their operating period. The *CBNM* for valves (the largest equipment group in the nuclear process) is to be presented in Section 5.2, where the presentation is divided into two:

- 1) Present the valve *static* wellbeing CBNM. In this presentation, a technique for trending the valve leakage is used as a criterion for assessing the valve static conditions for determination of maintenance overhauls. An intent is to provide an illustration of how a base for CBNM (the first-of-the-kind “network-driven nuclear condition-based maintenance”) can be established. The base for the static wellbeing CBNM is built upon the basic laws of conservation of energy and conservation of mass, the rate of mass flow, the formation of conditions for CBNM decision, and the network access to CBNM.
- 2) Present the valve *dynamic* wellbeing CBNM. The trending of 10 typical valve dynamic characteristics, represented with the valve stroking versus actuator action, is used as criteria for assessing the valve dynamic conditions for determination of maintenance overhauls.

5.1.2 Pumps CBNM – {EC-2}

The pumps condition-based assessment is carried out online while the nuclear unit is in operation and the results of assessment are to be used in the CBNM to reduce the occurrence of forced outages and to extend the duration between the scheduled outages and to achieve huge cost savings. The CBNM for pumps is to be presented in Section 5.3, where the presentation is divided into two:

- 1) Present the modelling of characteristics curves for pumps and pump loads of unregulated valves used in the nuclear process. Typical configurations for pumps and valves such as parallel connections and series connections commonly found in the nuclear plant are to be modelled for used in the CBNM.
- 2) Present typical conditions as illustrations for implementation of CBNM on the pumps and the pump loads of unregulated valves used in the nuclear plants.

5.1.3 Controllers CBNM – {EC-3}

The conditions for typical controllers used in the nuclear process, with the focus on control output drifts, static and dynamic disturbances, and control non-linearity, etc. during the online operations, are to be presented in Section 5.4. The presentation covers:

- Conditions for acceptable tolerances on current-to-pressure control
- Conditions for acceptable drifts on current-to-pressure control
- Conditions for acceptable dynamic disturbances on current-to-pressure control
- Conditions for acceptable tolerance on non-linear current-to-position control
- Conditions for acceptable static-dynamic disturbances on current-to-position control

5.2 *CBNM* for *Valves* equipment group {EC-1}

This section presents the design evaluation of the *CBNM* for *Valves*, the largest equipment group in the nuclear process (generally the largest fluid mechanical control equipment group in the process industries). The presentation is divided into two subsections:

Section 5.2.1 presents the valve *static* wellbeing *CBNM*. A technique for trending the valve leakage is used as a criterion for assessing the valve static conditions for determination of maintenance overhauls.

Section 5.2.2 presents the valve *dynamic* wellbeing *CBNM*. The trending of 10 typical valve dynamic characteristics, represented by valve strokings versus actuator actions, is used as criteria for assessing the valve dynamic conditions for determination of maintenance overhauls.

The following is a list of *CBNM* conditions to be investigated in subsequent subsections.

- {EC-1.1} Condition for valves' *static* wellbeing *CBNM*
- {EC-1.2} Conditions for valves' dynamic wellbeing *CBNM* illustrated with 10 typical conditions:
 - {EC-1.2.1}: Base conditions for acceptable valve stroke
 - {EC-1.2.2}: Conditions for valve seat degradation *CBNM*
 - {EC-1.2.3}: Conditions for broken valve stem *CBNM*
 - {EC-1.2.4}: Conditions for excessive friction on stroke *CBNM*
 - {EC-1.2.5}: Conditions for bent valve stem *CBNM*
 - {EC-1.2.6}: Conditions for actuator spring broken *CBNM*
 - {EC-1.2.7}: Conditions for incorrect preloading *CBNM*
 - {EC-1.2.8}: Conditions for valve stem misalignment *CBNM*
 - {EC-1.2.9}: Conditions for non-achievable full stroke *CBNM*
 - {EC-1.2.10}: Conditions for localized wear stem *CBNM*

5.2.1 Valves Static Wellbeing *CBNM* – condition {EC-1.1}

This section presents the technique for trending the valve stem leakage as an illustrating criterion for assessment of valve *static wellbeing* conditions for determination of maintenance overhauls.

The hardened bushing is used to guide the movement of the valve stem. A small amount of process flow can leak through the clearance between valve stem and the bushing. The rate of this leakage flow can be monitored to determine the current condition of the valve during online operation, particularly the clearance between the stem and bushing. This clearance is critical to the proper operation of the valve. The clearance is affected by the stem and bushing wear.

5.2.1-1 *Mathematical Model for Valve Leakage Flow Condition*

The valve leakage flow can be calculated using an orifice plate installed in the leak-off line of the valve. For the calculation of the leakage flow, two pressure taps are installed on the upstream and downstream flanges for the orifice plate. From these taps, the pressure drop (ΔP) across the orifice plate and the absolute pressure on one side of the orifice can be measured. With the use of these pressure measurements, the following provides the modelling for the calculation of the valve leakage flow.

a) *Bernoullis Equation*

The equation for the flow through an orifice can be derived, based on the basic *Principle of Conservation of Energy*. The energy from side 1 to side 2 of the orifice is conserved. Therefore,

$$E_1 = P_1 V_1 + \frac{1}{2} m_1 u_1^2 = E_2 = P_2 V_2 + \frac{1}{2} m_2 u_2^2 \quad (5.1)$$

where E = energy, P = pressure, V = volume, m = mass, u = speed

From (5.1), *Bernoullis* equation can be obtained:

$$P_1 + \frac{1}{2} \rho_1 u_1^2 = P_2 + \frac{1}{2} \rho_2 u_2^2 \quad (5.2)$$

where ρ = density

b) *Differential Pressure across Orifice*

For the incompressible flow,

$$\rho = \rho_1 = \rho_2 \quad (5.3)$$

From (5.2) and (5.3),

$$\Delta P = P_1 - P_2 = \frac{\rho}{2} (u_2^2 - u_1^2) \quad (5.4)$$

where ΔP = differential pressure across the orifice.

c) **Mass Flow Rate**

The flow rate of the mass, in kg/s or lb/h, can be expressed as:

$$q_m = \frac{m}{t} = \frac{\rho V}{t} = \frac{\rho A d}{t} = \rho A u = \rho \frac{\pi D^2}{4} u \quad (5.5)$$

where $u = \frac{d}{t}$ = speed, D = diameter of orifice hole

For the basic *Principle of Mass*,

$$q_{m1} \left(= \frac{m_1}{t} \right) = q_{m2} \left(= \frac{m_2}{t} \right) = q_m = \frac{m}{t} \quad (5.6)$$

From (5.5) and (5.6),

$$u_1 = \frac{4q_m}{\rho \pi D_1^2} \quad \text{and} \quad u_2 = \frac{4q_m}{\rho \pi D_2^2}$$

$$\text{Therefore,} \quad u_1^2 = \frac{4^2 q_m^2}{\rho^2 \pi^2 D_1^4} \quad \text{and} \quad u_2^2 = \frac{4^2 q_m^2}{\rho^2 \pi^2 D_2^4} \quad (5.7)$$

From (5.4) and (5.7),

$$\Delta P = \frac{\rho}{2} (u_2^2 - u_1^2) = \frac{\rho}{2} \left(\frac{4^2 q_m^2}{\rho^2 \pi^2 D_2^4} - \frac{4^2 q_m^2}{\rho^2 \pi^2 D_1^4} \right) = \frac{4^2 q_m^2}{2 \rho \pi^2} \left(\frac{1}{D_2^4} - \frac{1}{D_1^4} \right) \quad (5.8)$$

From (5.8),

$$2 \Delta P \rho \pi^2 D_2^4 = 4^2 q_m^2 \left(1 - \frac{D_2^4}{D_1^4} \right) \Rightarrow q_m^2 = \frac{1}{(1 - \frac{D_2^4}{D_1^4})} \frac{\pi^2}{4^2} D_2^4 \cdot 2 \cdot \Delta P \cdot \rho \Rightarrow$$

$$q_m = \frac{1}{\sqrt{(1 - \frac{D_2^4}{D_1^4})}} \frac{\pi}{4} D_2^2 \sqrt{2 \cdot \Delta P \cdot \rho} \quad (5.9)$$

Assume that orifice diameter is d and $\beta = \frac{D_2}{D_1}$. Introduce a discharge coefficient C that is to be defined as $C d^2 = D_2^2$.

From (5.9), the *mass flow equation* can be obtained, as below:

$$q_m = \frac{C}{\sqrt{1-\beta^4}} \frac{\pi}{4} d^2 \sqrt{2 \cdot \Delta P \cdot \rho} \quad (5.10)$$

The values of C can be obtained from the manufacturers, with β adjusted to $\beta = \frac{d}{D_1}$ where D_1 is the diameter of the input pipe connecting to the orifice. Alternative, the values of C can be obtained by calibration.

d) **Rate of Valve Leakage**

For a *calibrated* control valve system, the rate of the valve leakage q_m and the differential pressure ΔP can be simplified from (5.10) as follows:

$$\text{Model:} \quad q_m = K_m \sqrt{\Delta P} \quad (5.11)$$

where $K_m = \frac{C}{\sqrt{1-\beta^4}} \frac{\pi}{4} d^2 \sqrt{2\rho}$ can be obtained by calibration and calculation.

5.2.1-2 **{EC-1.1} – condition for excessive rate of valve leakage**

- 1) Establish a limiting condition curve according to the actual valve system operating conditions in the nuclear site. However, most likely the information on the actual valve conditions is not available. Therefore a model for the limiting condition is designed in this thesis, as follows:

The limiting condition is designed to have a tight range relative to the acceptable curve at higher differential pressure, as the valve stem is typically under higher pressure for fail-safe operation. The limiting condition is modelled with three components: *Component 1* is the condition given in (5.11). *Component 2* is a tolerance Δq_m added on the condition (5.11). *Component 3* is an exponential decaying function with a decaying constant λ and an initial value Δq_{md} .

CBNM condition model for valve leakage:

$$q_m \leq q_{m,limiting} = K_m \sqrt{\Delta P} + \Delta q_m + \Delta q_{md} e^{-\lambda q_m} \quad (5.12)$$

- 2) If the valve leakage exceeds the limiting condition of which the trend of the valve leakage is above the limiting curve, then the maintenance of the valve should be scheduled as soon as possible, preferably the next nuclear unit outage.

- 3) If the valve leakage becomes seriously such that it may jeopardize the nuclear operation or even may affect the nuclear safety, then perform the online maintenance on the valve if it can be done safely, but if not then the extremely expensive forced outage is required for the valve maintenance.

CBNM code for valve leakage: {EC-set} = {1.1}

5.2.1-3 Simulation of valve leakage condition

The criterion for the acceptable condition of the rate of valve leakage is to be determined according to the actual nuclear valve system.

Figure 5.3 provides an illustration of the new concept developed in this thesis for the monitoring of the rate of valve leakage. This graph shows two curves: one simulates the acceptable condition for the rate of valve leakage; the other simulates the limit for the acceptable condition. The acceptable condition is simulated using $K_m = 1.5 \text{ lb. psig}^{1/2}/\text{hr.}$ The limiting condition for the acceptable valve leakage is simulated with $\Delta q_m = 0.05 \text{ lb./hr.}$, $\lambda = 5$ and $\Delta q_{md} = 0.4 \text{ lb./hr.}$

Figure 5.3: Rate of valve leakage (q_m) versus differential pressure across orifice (ΔP)

5.2.2 Valves Dynamic Wellbeing *CBNM* – condition {EC-1.2}

This section presents the trending of 10 typical conditions of valve stroking versus actuator actions, as illustrating criteria for assessing the valve *dynamic wellbeing* conditions for determination of maintenance overhauls.

5.2.2-1 Base curve for acceptable valve stroke – condition {EC-1.2.1}

An actuator is used to stroke (open-close) the valve by applying an appropriate pressure. Figure 5.4 shows a typical curve for the valve stroke versus the actuator pressure (by convention, the graph is drawn with the actuator pressure on the y-axis and the stroke position on the x-axis).

Figure 5.4 displays the base curve for the stroking characteristic for a normally open valve. The actuator must apply sufficient pressure continuously on the valve base against the valve spring in order to keep the valve open. For fail-safe valve operation, if the actuator fails to apply the pressure, for whatever the reason, the valve spring will push the valve to close, ensuring that the nuclear operation is placed on a safe mode.

Figure 5.4 displays a typical hysteresis curve for the valve open-close operating loop in the nuclear operation. This graph shows that the pressure required for the valve opening operation is a bit higher than that for the valve closing operation. It is because in the opening operation the actuator has to provide an appropriate pressure to move the valve spring and against the friction, but in the closing operation the friction acts on the opposite direction and helps to reduce the pressure required from the actuator. The following establishes the base *CBNM* condition.

{EC-1.2.1} – base condition for acceptable valve stroke:

- 1) Measure the hysteresis curve of the actuator pressure versus the stroke position by stroking the valve open and close, at the valve commissioning. This curve is used as the base curve for comparison in the *CBNM* developed in this thesis research. Record this base hysteresis curve for each valve and store it in the *CBNM* server for use in the condition-based maintenance.
- 2) Establish the acceptable hysteresis for the actuator pressure versus the stroke position. The average width in pressure (Wp_{base}) of the base hysteresis curve and the maximum stroke position (S_{base}) obtained at the commissioning of the valve can be used as a model for acceptance:

CBNM condition model for base valve stroke:

$$\begin{aligned} Wp_{acceptable} &\geq Wp_{base} + \Delta Wp_{tolerance} \\ S_{acceptable} &\geq S_{base} + \Delta S_{tolerance} \end{aligned} \quad (5.13)$$

- 3) Check the base valve stroking hysteresis curve against the valve manufacturer data to ensure that the width of the hysteresis curve is within the manufacturer specification that indicates the valve is in a good condition with respect to valve stroking.
- 4) If the base valve stroking hysteresis width exceeds the manufacturer specification, arrange a replacement of the valve.

CBNM code for base valve stroke {EC-set} = {1.2.1}

Simulation: A simulation of the base hysteresis curve of the actuator pressure versus the stroke position is given in Figure 5.4, of which $Wp_{base} = 1 \text{ psig}$ and $S_{base} = 35 \text{ cm}$.

Figure 5.4: Base curve for acceptable valve stroke versus actuator pressure performance

5.2.2-2 Valve seat degradation – condition {EC-1.2.2}

When the valve seat wears out or is eroded, or the seat angle is altered, the friction increases for both the valve entering into the valve seat (closing) and leaving the seat (opening). Figure 5.5 shows a typical hysteresis curve of a valve stroking condition when the valve seat is degraded.

As shown in Figure 5.5, at the start of valve opening, if the actuator applies the same amount of pressure as the base case on the valve, the valve will not move. The actuator pressure is being increased by the feedback control until the actuator can overcome the additional friction due to the valve seat degradation, then the valve suddenly moves fast back to the base case of opening trajectory as this can be seen in Figure 5.5.

As shown in Figure 5.5, near the end of valve closing, the required actuator pressure is less than that for the base case, because the additional friction due to the valve degradation helps to reduce the required actuator pressure.

{EC-1.2.2} – condition for valve seat degradation:

- 1) Monitor if any abnormality of the actuator pressure versus the stroke position, at the start of the valve opening, or near the end of the valve closing.
- 2) If additional actuator pressure is required to start the valve opening that is followed with a fast movement of the valve stroke position, or if less actuator pressure is required near the end of the valve closing, then the valve seat is be examined.
- 3) Define the limit of acceptable abnormality of the actuator pressure (P) with respect to the stroke position (S) due to seat degradation, as follows:

CBNM condition model for valve seat degradation:

$$\begin{aligned} P_{opening\ measured} - P_{opening\ base} &\leq \Delta P_{acceptable\ tolerance} & 0 \leq S \leq 10\%S_{max} \\ P_{closing\ base} - P_{closing\ measured} &\leq \Delta P_{acceptable\ tolerance} & 0 \leq S \leq 10\%S_{max} \end{aligned} \quad (5.14)$$

- 4) If the limit of the acceptable abnormality is exceeded, call for the valve maintenance. This kind of maintenance can be implemented during the nuclear outage, unless a sudden catastrophic seat degradation that may endanger the nuclear operation and warrant for an online maintenance or even the extremely expensive forced outage.

CBNM code for seat degradation {EC-set} = {1.2.2}

Simulation: A simulation of the valve seat degradation is given in Figure 5.5, of which the maximum deviations of the measured actuator pressures from the base actuator pressures for a period of $0 \leq S \leq 10\%S_{max}(= 3.5cm)$ are: $\Delta P_{opening\ max} = 0.655psig$ and $\Delta P_{closing\ max} = 0.812psig$. This is just an illustration but whether a particular

maximum deviation of pressure is acceptable will depend on the actual application of the valve under *CBNM* in the live nuclear process.

Figure 5.5: Valve seat degradation

5.2.2-3 Broken valve stem – condition {EC-1.2.3}

Figure 5.6 shows a condition that the stroke position increases considerably, as compared to the base case. This is an evidence that the valve stem is broken. At the same time, the new hysteresis curve has a narrower width. This is a side support of the assumption of a broken valve stem, because the friction on the valve disk travelling with the broken stem reduces.

{EC-1.2.3} – condition for broken valve stem:

- 1) Monitor if the stroke position increases significantly as compared to the base case, then it is likely the valve stem is broken.
- 2) Define the deviation ($\Delta S_{acceptable}$) for the maximum stroke position ($S_{measured\ max}$) from the maximum base stroke position ($S_{base\ max}$) to be not classified as a broken valve stem condition:

CBNM condition model for broken stem:

$$S_{measured\ max} - S_{base\ max} \leq \Delta S_{acceptable} (\leq 15\% S_{base\ max}) \quad (5.15)$$

- 3) If the valve stem is broken, assess the impact of broken valve stem on the nuclear operation. If there is no significant impact, schedule the valve maintenance to be carried out during the nuclear unit outage.
- 4) If there may be an impact on the nuclear operation or even on the nuclear safety, then arrange an online maintenance for the valve. However if the valve is a key equipment in the nuclear process, a forced outage is likely required, because the maintenance for a broken valve stem require to take the valve out of service.

CBNM code for broken stem {EC-set} = {1.2.3}

Simulation: A simulation of a broken valve stem condition is given in Figure 5.6, of which the maximum deviation of the maximum stroke position from the maximum base stroke position $\Delta S = 50 - 35 = 15\text{cm} \nless 15\%S_{base\ max}$.

Figure 5.6: Broken valve stem

5.2.2-4 Excessive friction – condition {EC-1.2.4}

Figure 5.7 shows a condition of a wide hysteresis in the curve of the actuator pressure versus the stroke position, which may be due to excessive friction in the valve assembly probably between the valve stem and the stem bushing.

{EC-1.2.4} – condition for excessive friction:

- 1) Define the condition for excessive friction in the valve assembly, in terms of the *increased* average width in pressure (ΔWp) of the hysteresis curve for the actuator pressure versus the stroke position:

CBNM condition for excessive friction:

$$\Delta Wp = Wp_{measured} - Wp_{base} \leq \Delta Wp_{tolerance} \quad (5.16)$$

- 2) If the increased width of the measured hysteresis (ΔWp) exceeds the tolerance ($\Delta Wp_{tolerance}$), then arrange maintenance for the valve.
- 3) The maintenance if caused by the excessive friction in the valve assembly can normally be implemented during the nuclear outage, unless a sudden catastrophic increase of friction that may endanger the nuclear operation and warrant for an online maintenance or even the extremely expensive forced outage.

CBNM code for excessive friction {EC-set} = {1.2.4}

Simulation: A simulation of an excessive friction condition is given in Figure 5.7, of which the increased hysteresis width $\Delta Wp = 0.8 \text{ psig}$. This is just an illustration but whether a particular increased hysteresis width is acceptable will depend on the actual application of the valve under CBNM in the live nuclear process.

Figure 5.7: Excessive friction

5.2.2-5 Bent valve stem – condition {EC-1.2.5}

Figure 5.8 shows a condition of a localized increase in the hysteresis width in the curve of the actuator pressure versus the stroke position. This may be due to a bent valve stem in the stroke position where the abnormal hysteresis width increase is measured. The friction increases in the location where the stem is bent, and causes the hysteresis to be wider.

{EC-1.2.5} – condition for bent valve stem:

- 1) Define the condition for the bent valve stem, in terms of the *maximum increase* in the hysteresis width (ΔWp_{max}) in the curve of the actuator pressure versus the stroke position, as follows:

CBNM condition model for bent stem:

$$\Delta Wp_{max} = Wp_{measured\ max} - Wp_{base} \leq \Delta Wp_{tolerance\ max} \quad (5.17)$$

- 2) If the largest increase in the measured hysteresis width (ΔWp_{max}) exceeds the maximum tolerance ($\Delta Wp_{tolerance\ max}$), then arrange maintenance for the valve.
- 3) The maintenance if caused by the bent valve stem in the valve assembly can normally be implemented during the nuclear outage, unless the bent stem becomes a broken stem that may endanger the nuclear operation and warrant for an online maintenance or even the extremely expensive forced outage.

CBNM code for bent valve stem {EC-set} = {1.2.5}

Simulation: A simulation of a bent valve stem condition is given in Figure 5.8, of which the largest increase in the hysteresis width, $\Delta Wp_{max} = 1\ psig$. This is just an illustration but whether a particular increased hysteresis width is acceptable will depend on the actual application of the valve under CBNM in the live nuclear process.

Figure 5.8: Bent valve stem

5.2.2-6 Actuator spring broken – condition {EC-1.2.6}

Figure 5.9 shows a condition of half of the actuator multi-springs broken. This graph illustrates that the slopes of change of the actuator pressure versus the stroke position for both opening and closing are reduced by 50%. Correspondingly the action or movement of opening or closing will be slower.

{EC-1.2.6} – condition for acceptable broken actuator multi-springs:

- 1) Define the condition for acceptable broken actuator multi-springs, in terms of the slope of change ($\frac{\Delta P}{\Delta S}$) of the actuator pressure (P) versus the stroke position (S), as follows:

CBNM condition model for acceptable broken actuator multi-springs:

$$\frac{\Delta P}{\Delta S_{max}} = \frac{P_{@S1} - P_{@S2}}{S_1 - S_2} \geq \frac{\Delta P}{\Delta S_{tolerance}} \quad (5.18)$$

- 2) If the slope of change of the actuator pressure versus the stroke position ($\frac{\Delta P}{\Delta S}$) is less than the tolerable slope ($\frac{\Delta P}{\Delta S_{tolerance}}$) then arrange maintenance for the actuator.

- 3) The maintenance if caused by some of the actuator multi-springs being broken may be able to delay until the next outage. However if the broken actuator springs affects the nuclear operation or nuclear safety, an online maintenance or even the extremely expensive forced outage is required.

CBNM code for actuator spring problem {EC-set} = {1.2.6}

Simulation: A simulation of a broken actuator multi-springs condition is given in Figure 5.9, of which half of the actuator multi-springs are broken. The graph shows the slope of the hysteresis loop is reduced by half. This is just an illustration but whether a particular reduced slope or reduced valve opening and closing is acceptable will depend on the actual application of the valve under *CBNM* in the live nuclear process.

Figure 5.9: Broken actuator multi-springs

5.2.2-7 Incorrect Preloading – condition {EC-1.2.7}

Figure 5.10 shows a condition of incorrect preloading, of which the preload is double. The preloading problem is usually due to the installation of an incorrect spring or the setting of incorrect pre-load value. If the preload is too high, the actuator pressure may not be high enough to stroke. On the other hand, if the preload is too low, the stroke may be too slow to satisfy the application.

{EC-1.2.7} – condition for acceptable preload range:

- 1) Define the condition for an acceptable preload range, as of the following:

CBNM condition model for acceptable preload range:

$$P_{base,max} - \Delta P_{tolerance,low} \leq P_{preload} \leq P_{base,max} + \Delta P_{tolerance,high} \quad (5.19)$$

- 2) If the preload exceeds the acceptable preload range defined in 1) above, then arrange a maintenance for the preload correction.
- 3) The maintenance if caused by incorrect preload may be delayed until the next outage. However if the incorrect preload affects the nuclear operation or nuclear safety, an online maintenance or even the extremely expensive forced outage is required.

CBNM code for preloading {EC-set} = {1.2.7}

Simulation: A simulation of an incorrect preload condition is given in Figure 5.10, of which the preload is doubled. The graph shows the required actuator pressure is twice of the base pressure due to double preload. This is just an illustration but whether a particular increase of preload is acceptable will depend on the actual application of the valve under CBNM in the live nuclear process.

Figure 5.10: Double Preload

5.2.2-8 Valve stem misalignment – condition {EC-1.2.8}

Figure 5.11 shows a condition caused by a misalignment between the valve stem and the stem bushing. The misalignment causes the friction to increase. The graph shows that the amount of the increased friction tends to be more seriously towards the opening position.

{EC-1.2.8} – condition for acceptable stem misalignment:

- 1) Define the condition for an acceptable stem misalignment, as of the following:

CBNM condition model for acceptable stem misalignment: (5.20)

$$P_{base,max@opening} - \Delta P_{tolerance,low} \leq P_{max@opening} \leq P_{base,max@opening} + \Delta P_{tolerance,high}$$

$$P_{base,max@closing} - \Delta P_{tolerance,low} \leq P_{max@closing} \leq P_{base,max@closing} + \Delta P_{tolerance,high}$$

- 2) If the increased actuator pressure exceeds the acceptable range defined in 1) above, then arrange a maintenance for the stem alignment.
- 3) The maintenance if caused by stem misalignment may be able to delay until the next outage. However if the misalignment affects the nuclear operation or nuclear safety, an online maintenance or even the extremely expensive forced outage is required.

CBNM code for misalignment stem {EC-set} = {1.2.8}

Simulation: A simulation of a misalignment condition is given in Figure 5.11, of which the misalignment causes the rate of the actuator pressure change by 8% and initial change of 5% as an illustrating case. It is just an illustration but whether a particular increase is acceptable will depend on the actual application of the valve under *CBNM* in the live nuclear process.

Figure 5.11: Valve stem misalignment

5.2.2-9 Non-achievable full stroke – condition {EC-1.2.9}

Figure 5.12 shows a non-achievable full stroke condition. The full stroke cannot be achieved probably due to an incorrect valve setup or because of some foreign materials inside stopping the full stroke. This graph shows the stroke travel cannot reach the full stroke position.

{EC-1.2.9} – condition for non-achievable full stroke:

- 1) Define the condition for an acceptable non-achievable full stroke, as of the following:

CBNM condition model for acceptable non-full stroke:

$$S_{base\ full\ stroke} - S_{operating\ max} \leq \Delta S_{tolerance} \quad (5.21)$$

- 2) If the maximum stroke travel ($S_{operating\ max}$) fails to reach the base full stroke position ($S_{base\ full\ stroke}$) by exceeding the tolerance ($\Delta S_{tolerance}$) as defined in 1) above, then arrange a maintenance for the full stroke correction.
- 3) The maintenance if caused by full stroke failure may not allow to be delayed to the next outage. The non-achievable full stroke condition often affects the nuclear operation or even the nuclear

safety, such that an online maintenance or even the extremely expensive forced outage is required to correct the full-stroke failure.

CBNM code for non-achievable full stroke {EC-set} = {1.2.9}

Simulation: A simulation of a non-achievable full stroke condition is given in Figure 5.12, of which the stroke travel can only reach 89% of the base full stroke position. It is just an illustration but whether a particular non-achievable full stroke is acceptable will depend on the actual application of the valve under *CBNM* in the live nuclear process.

Figure 5.12: Failed full stroke

5.2.2-10 Localized wear stem – condition {EC-1.2.10}

Figure 5.13 shows a condition of localized wear stem, of which changes shown in the hysteresis curve in the plot of the actuator pressure versus the stroke position. The stem may be wear out locally as a result of valve oscillations occurring repeatedly in a particular area of the valve. The consequence of repeatedly wearing the stem and making it smaller in a local area and thus the friction on that area reduces. Due to the reduction of friction when the stroke travel to the position, the required actuator pressure is reduced because of against less friction on the opening operation. On the other hand, in the closing operation, the required actuator pressure is increased because of less friction available for helping, as friction is working opposite of the movement that can be seen in Figure 5.13.

{EC-1.2.10} – condition for localized wear stem:

- 1) Define the condition for an acceptable localized wear stem, as of the following:

CBNM condition model for acceptable localized wear stem:

$$\begin{aligned} P_{opening} - P_{base\ reference} &\geq (P_{base\ opening} - P_{base\ referenc})/2 \\ P_{closing} - P_{base\ reference} &\geq (P_{base\ closing} - P_{base\ referenc})/2 \end{aligned} \quad (5.22)$$

- 2) If the change of the actuator pressure exceeds the acceptable range as defined in 1) above, then arrange a maintenance for the full stroke correction.
- 3) The maintenance if caused by the localized wear on the stem may be allowed to delay to the next outage. If the stem wear become sever that affects the nuclear operation or even the nuclear safety, an online maintenance or an extremely expensive forced outage is required.

CBNM code for localized wear stem {EC-set} = {1.2.10}

Simulation: A simulation of a localized wear condition is given in Figure 5.13, of which the change in the hysteresis width is as much as 40% of the base hysteresis width. This is just an illustration but whether a particular maximum % of change is acceptable will depend on the actual application of the valve under CBNM in the live nuclear process.

Figure 5.13: Localized wear stem

5.3 *CBNM* for Pumps equipment group {EC-2}

This section presents the development of the conditions to be used in the *CBNM* for the pumps equipment group in the nuclear process. The presentation is divided into two subsections:

Section 5.3.1 presents the modelling of characteristics curves for pumps and pump loads of unregulated valves used in the nuclear process. Typical configurations for pumps and valves such as parallel connections and series connections commonly found in the nuclear plant are to be modelled for used in the *CBNM*.

Section 5.3.2 presents typical conditions as illustrations for implementation of *CBNM* on the pumps and the pump loads of unregulated valves used in the nuclear plants (the regulation/control aspects of the valves *CBNM* will be presented in Section 5.4).

The following is a list of *CBNM* conditions to be investigated for the nuclear-process pumps equipment group in subsequent subsections:

- {EC-2.1} Base conditions for acceptable pump characteristics
- {EC-2.2} Base conditions of acceptable characteristics for valves used as pump loads
- {EC-2.3} Conditions for acceptable characteristics for composite pump configurations
- {EC-2.4} Conditions for acceptable characteristics for composite valve configurations

5.3.1 Modelling of characteristics curves for pumps and loads of unregulated valves

This section develops the modelling of characteristics curves for pumps and pump loads of unregulated valves used in the nuclear process. Typical configurations for pumps and valves such as parallel connections and series connections commonly found in the nuclear plant are to be modelled for used in the *CBNM*.

5.3.1-1 Mathematical models for pumps

Pumps are used to move the fluid and make the flow in the nuclear control process, such as circulating the heavy water from the nuclear reactor to the boiler to remove the heat generated by the nuclear chain reaction, or circulating the light water from the boiler to the turbine to transfer heat energy into mechanical energy.

The following presents the equations for modelling the practical pumps used in the nuclear process.

a) Pump Head

By Newton's law, force equals mass $\times$ acceleration ($F = ma = mg$). Pressure equals force $\div$ area ($P = \frac{F}{A}$). Density equals mass $\div$ volume ($\rho = A \times H$) where H is the height (or Head). Therefore,

$$\Delta H = \frac{\Delta P_{total}}{\rho \cdot g} \quad (5.23)$$

where H = pump head;

ΔP_{total} = differential pressure across the pump;

ρ = density of the fluid flowing through the pump;

g = acceleration due to gravity

b) Flow Rate

The flow through a diameter (D) can be expressed in terms of: linear flow rate ($V = \frac{L}{t}$) and

volume flow rate ($Q = \frac{A \cdot L}{t} = \frac{\pi}{4} D^2 \cdot \frac{L}{t}$). Therefore,

$$Q = \frac{\pi}{4} \cdot D^2 \cdot V \quad (5.24)$$

c) Pump Differential Pressures

The total differential pressure across the pump can be expressed as:

$$\Delta P_{total} = \Delta P_{static} + \Delta P_{dynamic} + \Delta P_{geodetic} \quad (5.25)$$

where ΔP_{total} = total differential pressure across the pump

ΔP_{static} = static differential pressure across the pump

$\Delta P_{dynamic}$ = dynamic differential pressure across the pump

$\Delta P_{geodetic}$ = geodetic differential pressure between two pump pressure sensors

Static differential pressure across the pump can be obtained by measuring the pressure at the pump outlet ($P_{static,out}$) and the pressure at the inlet ($P_{static,in}$), as expressed below:

$$\Delta P_{static} = P_{static,out} - P_{static,in} \quad (5.26)$$

Dynamic differential pressure across the pump can be obtained by measuring the flow rate at the pump outlet (V_{out}) and the flow rate at the inlet (V_{in}), as expressed below:

$$\Delta P_{dynamic} = \frac{\rho}{2} (V_{out}^2 - V_{in}^2) \quad (5.27)$$

From (5.24), $V = \frac{Q}{\pi/4} \left(\frac{1}{D^2} \right)$, then it is combined with (5.27) to obtain:

$$\Delta P_{dynamic} = \frac{\rho}{2} \cdot \left(\frac{Q}{\pi/4} \right)^2 \cdot \left(\frac{1}{D_{out}^4} - \frac{1}{D_{in}^4} \right) \quad (5.28)$$

Geodetic differential pressure between two pump pressure sensors on a height difference (Δh) can be expressed as:

$$\Delta P_{geodetic} = \rho \cdot g \cdot \Delta h \quad (5.29)$$

For many pump applications, both ΔP_{static} and $\Delta P_{geodetic}$ are small compared to $\Delta P_{dynamic}$, then from (5.25) and (5.28) total differential pressure across the pump can be approximated as:

$$\Delta P_{total} \approx \frac{\rho}{2} \cdot \left(\frac{Q}{\pi/4} \right)^2 \cdot \left(\frac{1}{D_{out}^4} - \frac{1}{D_{in}^4} \right) \quad (5.30)$$

d) **Pump Characteristic/Curve Equation**

From (5.23) and (5.30) and assuming that the dynamic pressure is dominate,

$$\Delta H = K_p \cdot Q^2 \quad (5.31)$$

where $K_p = \frac{1}{2g} \cdot \left(\frac{Q}{\pi/4} \right)^2 \cdot \left(\frac{1}{D_{out}^4} - \frac{1}{D_{in}^4} \right)$

When the volume flow is zero ($Q = 0$), the head has the highest value ($H = H_o$). The pump head can be expressed as:

$$H = H_o - \Delta H = H_o - K_p \cdot Q^2 \quad (5.32)$$

Equation (5.32) represents the pump characteristic and is regarded the pump curve equation.

5.3.1-2 Mathematical models for unregulated valves as pump load

Valves are used to regulate the flow created by the pumps, and therefore valves can be regarded as the majority of the pump loads. The following presents the equations for modelling the unregulated valves as a pump load.

a) **Unregulated Valve Differential Pressure**

With a similar derivation as for (5.30), the differential pressure for the unregulated valve can be obtained as below:

$$\Delta P_v = \frac{\rho}{2} \cdot \left(\frac{Q_v}{\pi/4} \right)^2 \cdot \left(\frac{1}{D_{v-out}^4} - \frac{1}{D_{v-in}^4} \right) \quad (5.33)$$

where ΔP_v = unregulated valve differential pressure, Q_v = valve volume flow rate, D_{v-out} = valve outlet diameter, and D_{v-in} = valve inlet diameter.

b) **Characteristic/Curve Equation for unregulated Valves as Pump Load**

Similar to (5.31), the unregulated valve differential pressure can be expressed in terms of differential head (ΔH):

$$\Delta H_v = K_v \cdot Q_v^2 \quad (5.34)$$

In terms of the absolute head, the unregulated valve performs differently from the pump, because when the volume flow is zero ($Q_v = 0$), the unregulated valve differential pressure is also zero ($\Delta P_v = 0$) so as its modelling in head is also zero ($\Delta H_v = 0$). Therefore, the unregulated valve head model can be expressed as:

$$H_v = K_v \cdot Q_v^2 \quad (5.35)$$

Equation (5.35) represents the characteristic of unregulated valves as pump loads and is regarded the unregulated valve load curve equation.

5.3.1-3 *Mathematical Models for Composite Pumps Configurations in Nuclear Processes*

There are composite pumps configurations in the nuclear plant, including multiple pumps working together simultaneously, either in parallel or in series, due to nuclear operation reliability requiring redundant equipment or due to capability requirement demanding two or three pumps operating together. The following develops the mathematical models for such composite pumps configurations.

a) **Parallel-connected Pumps**

Equation (5.32) is modified to develop a model for the two parallel-connected pumps, as follows:

$$H = H_o - K_{p1} \cdot Q_1^2 \quad \text{Pump-1} \quad (5.36)$$

$$H = H_o - K_{p2} \cdot Q_2^2 \quad \text{Pump-2} \quad (5.37)$$

$$H = H_o - K_{p(1,2)} \cdot Q_{(1,2)}^2 \quad \text{Pump-1} \parallel \text{Pump-2} \quad (5.38)$$

Use (5.36), (5.37) and (5.38) to express the flow rates, as follows:

$$Q_1 = \frac{1}{\sqrt{K_{p1}}} \cdot \sqrt{H_o - H} \quad \text{Pump-1} \quad (5.39)$$

$$Q_2 = \frac{1}{\sqrt{K_{p2}}} \cdot \sqrt{H_o - H} \quad \text{Pump-2} \quad (5.40)$$

$$Q_{(1,2)} = \frac{1}{\sqrt{K_{p(1,2)}}} \cdot \sqrt{H_o - H} \quad \text{Pump-1} \parallel \text{Pump-2} \quad (5.41)$$

Combine the individual flow of Pump 1 (5.39) and for Pump 2 (5.40) into the parallel flow (5.41), as follows:

$$Q_{(1,2)} = Q_1 + Q_2 = \left(\frac{1}{\sqrt{K_{p1}}} + \frac{1}{\sqrt{K_{p2}}} \right) \sqrt{H_o - H} \quad \text{Pump 1} \parallel \text{Pump 2} \quad (5.42)$$

By comparing (5.41) and (5.42), the following relationship can be obtained:

$$\frac{1}{\sqrt{K_{p(1,2)}}} = \frac{1}{\sqrt{K_{p1}}} + \frac{1}{\sqrt{K_{p2}}} \quad (5.43)$$

Finally, the model for the combined two-parallel-connected pumps is:

$$H = H_o - K_{p(1,2)} \cdot Q^2 \quad \text{Pump-1} \parallel \text{Pump-2} \quad (5.44)$$

$$\frac{1}{\sqrt{K_{p(1,2)}}} = \frac{1}{\sqrt{K_{p1}}} + \frac{1}{\sqrt{K_{p2}}} \quad (5.43)$$

Similarly, for three pumps connected in parallel, the combined model is:

$$H = H_o - K_{p(1,2,3)} \cdot Q^2 \quad \text{Pump-1} \parallel \text{Pump-2} \parallel \text{Pump-3} \quad (5.45)$$

$$\frac{1}{\sqrt{K_{p(1,2,3)}}} = \frac{1}{\sqrt{K_{p1}}} + \frac{1}{\sqrt{K_{p2}}} + \frac{1}{\sqrt{K_{p3}}} \quad (5.46)$$

b) Series-connected Pumps

The pump model of (5.32) can be expressed for two series-connected pumps, as follows:

$$H_1 = H_{o1} - K_{p1} \cdot Q^2 \quad \text{Pump-1} \quad (5.47)$$

$$H_2 = H_{o2} - K_{p2} \cdot Q^2 \quad \text{Pump-2} \quad (5.48)$$

$$H_1 + H_2 = H_{o1} + H_{o2} - (K_{p1} + K_{p2}) \cdot Q^2 \quad \text{Pump-1} + \text{Pump-2} \quad (5.49)$$

From (5.49), the model for the combined two-series-connected pumps is:

$$H = H_{o(1,2)} - K_{p(1,2)} \cdot Q^2 \quad \text{Pump-1 + Pump-2} \quad (5.50)$$

$$H_{o(1,2)} = H_{o1} + H_{o2} \quad (5.51)$$

$$K_{p(1,2)} = K_{p1} + K_{p2} \quad (5.52)$$

Similarly, for three pumps connected in series, the combined model is:

$$H = H_{o(1,2,3)} - K_{p(1,2,3)} \cdot Q^2 \quad \text{Pump-1 + Pump-2 + Pump-3} \quad (5.53)$$

$$H_{o(1,2,3)} = H_{o1} + H_{o2} + H_{o3} \quad (5.54)$$

$$K_{p(1,2,3)} = K_{p1} + K_{p2} + K_{p3} \quad (5.55)$$

5.3.1-4 *Mathematical Models for Composite Valves Configurations in Nuclear Processes*

There are composite valves configurations in the nuclear plant, including multiple valves working together simultaneously. An example, one pump or one group of pumps branches off to drive two or three valve loads. Another example, one pump or one group of pumps drives two or three valve loads with decreasing pipe sizes for control of different flow rates.

a) **Driving Multiple Valve Loads in parallel**

Equation (5.35) is modified to develop a model for the two valve load from one pump, as follows:

$$H_v = K_{v1} \cdot Q_{v1}^2 \quad \text{Valve-1} \quad (5.56)$$

$$H_v = K_{v2} \cdot Q_{v2}^2 \quad \text{Valve-2} \quad (5.57)$$

$$H_v = K_{v(1,2)} \cdot Q_{v(1,2)}^2 \quad \text{Valve-1} \parallel \text{Valve-2} \quad (5.58)$$

Use (5.56), (5.57), and (5.58) to express the flow rates, as follows;

$$Q_{v1} = \frac{1}{\sqrt{K_{v1}}} \cdot \sqrt{H} \quad \text{Valve-1} \quad (5.59)$$

$$Q_{v2} = \frac{1}{\sqrt{K_{v2}}} \cdot \sqrt{H} \quad \text{Valve-2} \quad (5.60)$$

$$Q_{v(1,2)} = \frac{1}{\sqrt{K_{v(1,2)}}} \cdot \sqrt{H} \quad \text{Valve-1} \parallel \text{Valve-2} \quad (5.61)$$

Combine the flow of Valve-1 and Valve-2, as follows:

$$Q_{v(1,2)} = Q_{v1} + Q_{v2} = \left(\frac{1}{\sqrt{K_{v1}}} + \frac{1}{\sqrt{K_{v2}}} \right) \sqrt{H} \quad \text{Valve-1} \parallel \text{Valve-2} \quad (5.62)$$

By comparing (5.61) and (5.62), the following relationship can be obtained:

$$\frac{1}{\sqrt{K_{v(1,2)}}} = \frac{1}{\sqrt{K_{v1}}} + \frac{1}{\sqrt{K_{v2}}} \quad (5.63)$$

Finally, the model for driving two valves from one pump is:

$$H = K_{v(1,2)} \cdot Q_{v(1,2)}^2 \quad \text{Valve-1} \parallel \text{Valve-2} \quad (5.64)$$

$$\frac{1}{\sqrt{K_{v(1,2)}}} = \frac{1}{\sqrt{K_{v1}}} + \frac{1}{\sqrt{K_{v2}}} \quad (5.63)$$

b) Driving Multiple Valve Loads in series

Equation (5.35) is modified to develop a model for the two valve loads driven by one pump:

$$H_{v1} = K_{v1} \cdot Q_v^2 \quad \text{Valve-1} \quad (5.65)$$

$$H_{v2} = K_{v2} \cdot Q_v^2 \quad \text{Valve-2} \quad (5.66)$$

$$H_{v1} + H_{v2} = (K_{v1} + K_{v2}) \cdot Q_v^2 \quad \text{Valve-1} + \text{Valve-2} \quad (5.67)$$

From (5.67), the model for driving two valve loads is:

$$H_{v(1,2)} = K_{v(1,2)} \cdot Q_v^2 \quad \text{Valve-1} + \text{Valve-2} \quad (5.68)$$

$$K_{v(1,2)} = K_{v1} + K_{v2} \quad (5.69)$$

5.3.2 CBNM for Pumps of various configurations and loads – condition {EC-2.x}

This section presents typical conditions as illustrations for implementation of *CBNM* on the pumps and the pump loads of unregulated valves used in the nuclear plants.

5.3.2-1 Base conditions for **acceptable pump characteristic** – condition {EC-2.1}

The base conditions are to be established for an acceptable characteristic/performance of pumps for applications in the nuclear process. The pump characteristic/curve was modelled in eq. (5.32) that is reformed as below:

$$H_{base} = H_{o,base} - K_{p,base} \cdot Q_{base}^2 \quad (5.70)$$

For implementing the *CBNM* developed in this thesis, eq. (5.70) is first used to match the manufacture pump curve by selecting the appropriate pump characteristic constant of K_p . Figure 5.14 shows an example for a pump characteristic and its base tolerance range.

{EC-2.1} – base condition for acceptable pump characteristic:

- 1) Measure the pump curve in terms of the pump head (H) versus the volume flow rate (Q) by varying the control valve opening, at the pump commissioning. The curve is then used as the base curve for comparison in the *CBNM* developed in this thesis research. Add the tolerance curves according to the pump tolerance specification given by the pump manufacturer, as shown in Figure 5.14, and store it in the *CBNM* server for use in the condition-based maintenance.
- 2) Establish the acceptable tolerance range for the pump head versus the flow rate, according the application but not exceeding the manufacturer specification. Simply, the head measured on an operating pump ($H_{P,online}$) cannot exceed the tolerance ($\pm\Delta H_{P,tolerance}$), which is expressed as:

***CBNM* condition model for base pump characteristic:**

$$H_{P,base} - \Delta H_{P,tolerance} \leq H_{P,online} \leq H_{P,base} + \Delta H_{P,tolerance} \quad (5.71)$$

- 3) Check periodically the operating pump curve to ensure it will not exceed (5.71). If the operating pump head exceeds that specified in (5.71), arrange a maintenance.

- 4) If the tolerance is exceeded and a maintenance is required as identified in (5.71), perform a CBNM assessment to determine if the maintenance can be delayed until the next nuclear outage. If the assessment of the pump condition and the criticality of the pump operation in the nuclear process provides a strong evidence that the maintenance cannot be delayed, then the maintenance has to be carried out online while the nuclear reactor is still operating, if taking the pump out of service will not jeopardize the overall nuclear operation and the nuclear safety. Otherwise, an extremely expensive forced outage for this pump maintenance is unavoidable.

CBNM code for basic pump maintenance {EC-set} = {2.1}

Simulation: A simulation of the base pump characteristic curve is given in Figure 5.14, of which

$$K_{p,base} = 0.01634 \, m \left(\frac{m^3}{hr} \right)^{-2} \text{ and } \pm 2.5\% \text{ tolerance are used to plot the graph.}$$

Figure 5.14: Base pump curve

5.3.2-2 Base acceptable valve characteristic as pump loads – condition {EC-2.2}

The base conditions for acceptable characteristics are to be established for valves used as pump loads in the nuclear process applications. The unregulated valve characteristic/curve was modelled in eq. (5.35) that is reformed as below:

$$H_{v,base} = K_{v,base} \cdot Q_{v,base}^2 \quad (5.72)$$

For implementing the *CBNM*, eq. (5.72) is first used to match the manufacture valve curve by selecting the appropriate valve characteristic constant of $K_{v,base}$. Figure 5.15 shows an example for a valve characteristic and its base tolerance range.

{EC-2.2} – base condition of acceptable characteristic for valves as pump loads:

- 1) Measure the valve curve in terms of the valve head (H) versus the volume flow rate (Q) by varying the valve opening, at the pump commissioning. The curve is then used as the base curve for comparison in the *CBNM* developed in this thesis research. Add the tolerance curves according to the valve tolerance specification given by the valve manufacturer, as shown in Figure 5.15, and store it in the *CBNM* server for use in the condition-based maintenance.
- 2) Establish the acceptable tolerance range for the valve head versus the flow rate, according the application but not exceeding the manufacturer specification. The head measured on an operating valve ($H_{v,online}$) cannot exceed the tolerance ($\pm\Delta H_{v,tolerance}$), which is expressed as:

***CBNM* condition model for base valve characteristic as pump load:**

$$H_{v,base} - \Delta H_{v,tolerance} \leq H_{v,online} \leq H_{v,base} + \Delta H_{v,tolerance} \quad (5.73)$$

- 3) Check periodically the operating valve curve to ensure that it will not exceed (5.73). If the operating valve head exceeds that specified in (5.73), arrange a maintenance.
- 4) If the tolerance is exceeded or a maintenance is required as identified in (5.73), perform a *CBNM* assessment to determine if the maintenance can be delayed until the next nuclear outage. If the assessment of the valve condition and the criticality of the valve operation in the nuclear process provides a strong evidence that the maintenance cannot be delayed, then the maintenance has to be carried out online or by force outage.

***CBNM* code for basic valve maintenance {EC-set} = {2.2}**

Simulation: A simulation of the base characteristic/performance curve for the valve used as pump load is given in Figure 5.15, of which $K_{v,base} = 0.0192 \text{ m} \left(\text{m}^3/\text{hr} \right)^{-2}$ and $\pm 2.5\%$ tolerance are used to plot the graph.

Figure 5.15: Base curve for an unregulated valve used as pump load

Figure 5.16 shows both the base pump curve and its base valve curve.

Figure 5.16: Base curves for a pump and its valve load

5.3.2-3 Conditions for composite pump configurations – condition {EC-2.3}

Figure 5.17 shows the typical pump configurations used in the nuclear process that consist of single pump, two parallel-connected pumps, and two series-connected pumps. The models for these three configurations were developed in (5.32), (5.44) and (5.50), respectively and reformed as below:

$$\text{Single pump:} \quad H_{P,comp,base} = H_o - K_p \cdot Q^2 \quad (5.74)$$

$$\text{Parallel-connected pumps:} \quad H_{P,comp,base} = H_o - K_{p(1,2)} \cdot Q^2 \quad (5.75)$$

$$\frac{1}{\sqrt{K_{p(1,2)}}} = \frac{1}{\sqrt{K_{p1}}} + \frac{1}{\sqrt{K_{p2}}}$$

$$\text{Series-connected pumps:} \quad H_{P,comp,base} = H_{o(1,2)} - K_{p(1,2)} \cdot Q^2 \quad (5.76)$$

$$H_{o(1,2)} = H_{o1} + H_{o2}$$

$$K_{p(1,2)} = K_{p1} + K_{p2}$$

Based on the above equations, the conditions for the acceptance of composite pump configurations can be determined.

{EC-2.3} – conditions for acceptable characteristics for composite pump configurations:

- 1) Measure the composite pump curve ($H_{P,comp,base}$) versus the flow rate (Q) by varying the control valve opening, at the composite pump configuration commissioning. The curve is then used as the base curve for comparison in the *CBNM* developed in this thesis research.
- 2) Establish the acceptable tolerance range for the online composite pump head ($H_{P,online}$), as below:

***CBNM* condition model for base pump characteristic:**

$$H_{P,comp,base} - \Delta H_{P,tolerance} \leq H_{P,online} \leq H_{P,comp,base} + \Delta H_{P,tolerance} \quad (5.77)$$

- 3) Check periodically the operating pump point ($H_{P,online}$) to ensure that it will not exceed (5.77). If the operating pump head exceeds that specified in (5.77), arrange a maintenance.
- 4) Determine whether the maintenance can be delayed until the next nuclear outage. If the maintenance cannot be delayed, then arrange an online or forced outage maintenance.

***CBNM* code for basic pump maintenance {EC-set} = {2.3}**

Simulation: A simulation of the composite pump configurations is given in Figure 5.17, of which

$$K_p = K_{p1} = K_{p2} = 0.01634 \text{ m} \left(\frac{\text{m}^3}{\text{hr}} \right)^{-2} \text{ and } H_o = H_{o1} = H_{o2} = 60 \text{ m}.$$

Figure 5.17: Base pump, two parallel-connected pumps, and two series-connected pumps

5.3.2-4 Conditions for composite valve (pump load) configurations – condition {EC-2.4}

Figure 5.18 shows the typical valve configurations used in the nuclear process that consist of single valve, two parallel-connected valves, and two series-connected valves. The models for these three configurations were developed in (5.35), (5.64) and (5.68), respectively and reformed as below:

$$\text{Single pump: } H_{V,comp,base} = K_v \cdot Q^2 \quad (5.78)$$

$$\text{Parallel-connected pumps: } H_{V,comp,base} = K_{v(1,2)} \cdot Q^2 \quad (5.79)$$

$$\frac{1}{\sqrt{K_{v(1,2)}}} = \frac{1}{\sqrt{K_{v1}}} + \frac{1}{\sqrt{K_{v2}}}$$

$$\begin{aligned} \text{Series-connected pumps: } H_{V,comp,base} &= K_{v(1,2)} \cdot Q^2 \\ K_{v(1,2)} &= K_{v1} + K_{v2} \end{aligned} \quad (5.80)$$

Based on the above equations, the conditions for the acceptance of composite valves (pump loads) configurations can be determined.

{EC-2.4} – conditions for acceptable characteristics for composite valve configurations:

- 1) Measure the composite valve curve (H_{comp}) versus the flow rate (Q) by varying the control valve opening, at the composite valve configuration commissioning. The curve is then used as the base curve for comparison in the *CBNM* developed in this thesis research.
- 2) Establish the acceptable tolerance range for the online composite valve head ($H_{V,online}$), as below:

***CBNM* condition model for base valve characteristic as pump load:**

$$H_{V,comp,base} - \Delta H_{v,tolerance} \leq H_{V,online} \leq H_{V,comp,base} + \Delta H_{v,tolerance} \quad (5.81)$$

- 3) Check periodically the operating valve point ($H_{V,online}$) to ensure that it will not exceed (5.81). If the operating pump head exceeds that specified in (5.81), arrange a maintenance.
- 4) Determine whether the maintenance can be delayed until the next nuclear outage. If the maintenance cannot be delayed, then arrange an online or forced outage maintenance.

***CBNM* code for basic valve (pump-load) maintenance {EC-set} = {2.4}**

Simulation: A simulation of the composite pump configurations is given in Figure 5.18, of which

$$K_v = K_{v1} = K_{v2} = 0.0192 \, m \left(m^3/hr \right)^{-2}.$$

Figure 5.18: Base valve, two parallel-connected valves, and two series-connected valves

Figure 5.19 shows the curves for the typical composite pump – valve load configurations. The operating points are the interceptions of the pump curves and the valve curves.

Figure 5.19: Composite pump and valve load configurations

5.4 CBNM for Controllers equipment group – condition {EC-3}

This section presents the conditions for typical controllers used in the nuclear process, with the focus on control output drifts, static and dynamic disturbances, and control non-linearity, etc. during the online operations. These are used as illustrations for the controllers condition-based maintenance in the application of *CBNM* developed in this thesis research.

This section covers the following conditions for the *CBNM*:

- {EC-3.1} Conditions for acceptable tolerances on current-to-pressure control
- {EC-3.2} Conditions for acceptable drifts on current-to-pressure control
- {EC-3.3} Conditions for acceptable dynamic disturbances on current-to-pressure control
- {EC-3.4} Conditions for acceptable tolerance on non-linear current-to-position control
- {EC-3.5} Conditions for acceptable static-dynamic disturbances on current-to-position control

For practical enhancement, simulation examples given for illustration use the industrial standard parameters and ranges such as controllers' input signal of 4 to 20 mA current and output of 0 to 15 psig.

5.4.1 Base current-to-pressure valve control – condition {EC-3.1}

Figure 5.20 shows a typical input-output transfer from the current control signal to the actuator output pressure for the control of valves in the nuclear process. It is ideal to have a linear non-hysteresis transfer from input to output. In practice, a small hysteresis and a little non-linearity may be acceptable, particularly for closed-loop controls used in the industrial controls to overcome a small hysteresis and ride through some non-linearity and small disturbances. This section presents an illustration for establishing a base current-to-pressure transfer control for use in the *CBNM* developed in this thesis.

{EC-3.1} – conditions for acceptable tolerances on current-to-pressure control:

- 1) Measure the transfer curve for the input current versus the output pressure on the controller, during the controller commissioning. The curve is then used as the base curve for comparison in the *CBNM* developed in this thesis research.
- 2) Establish the acceptable tolerance range for the current-to-pressure transfer, as below:

***CBNM* condition tolerance established for acceptable current-to-pressure transfer:**

$$\Delta P_{base,tolerance} = |P_{base,opening} - P_{base,closing}| \quad (5.82)$$

where the maximum value of $\Delta P_{base,tolerance}$ is to be determined according to the allowable tolerance in the specific application that the controller is installed for.

***CBNM* code for base current-to-pressure transfer {EC-set} = {3.1}**

Simulation: A simulation of the current-to-pressure transfer is given in Figure 5.20, of which the base reference of input current is 4 mA to 20 mA, the rise is 0.75 psig/mA, and the hysteresis width is 2.7% of full actuator pressure of 15 psig.

Figure 5.20: Base current-to-pressure valve control

5.4.2 Drift on current-to-pressure valve control – condition {EC-3.2}

Figure 5.21 shows an often-seen drifts on the input-output transfers from the current control signal to actuator output pressure for the valves controllers. This section illustrates the drift on the input current to the output actuator pressure as a key condition for the *CBNM* developed in this thesis.

{EC-3.2} – conditions for acceptable drift on current-to-pressure control:

- 1) Measure/monitor the transfer values of the input current versus the output pressure from the controller, during the online operation.
- 2) Check the acceptance of the current-to-pressure transfer, using the guide given below:

***CBNM* condition for acceptable current-to-pressure transfer drift:**

$$\forall |P_{opening} - P_{closing}| < 2 * \Delta P_{base,tolerance} \quad (5.83)$$

For all ($\forall$) hysteresis width valves in the current-to-pressure transfer must be less than two times (an industrial standard value) of the base tolerance $\Delta P_{base,tolerance}$ established in (5.82).

If the measured hysteresis width exceeds the guide of (5.83), arrange a maintenance.

- 3) Determine whether the maintenance can be delayed until the next nuclear outage. If the maintenance cannot be delayed, then arrange an online or forced outage maintenance.

CBNM code for basic current-to-pressure maintenance {EC-set} = {3.2}

Simulation: A simulation of a drift on the current-to-pressure transfer is given in Figure 5.21, of which the drift is 10% of the base rise.

Figure 5.21: Drift on current-to-pressure control

5.4.3 Dynamic disturbance on current-to-pressure valve control – condition {EC-3.3}

Figure 5.22 shows an often-seen dynamic disturbances (but of a smaller magnitude) on the input-output transfers from the current control signal to actuator output pressure for the valves controllers.

This section illustrates that the dynamic disturbance on the transfer of the input current to the output actuator pressure is another key condition to be monitored for the *CBNM* developed in this thesis.

{EC-3.3} – conditions for acceptable dynamic disturbance on current-to-pressure control:

- 1) Measure/monitor the transfer values of the input current versus the output pressure from the controller, during the online operation.

- 2) Check if there is any dynamic disturbance on the current-to-pressure transfer. If there are disturbances, then check the acceptance of the temporary dynamic disturbances using the guide, as given below:

CBNM condition for acceptable current-to-pressure transfer temporary disturbances:

$$\forall |P_{opening} - P_{closing}| < 5 * \Delta P_{base,tolerance} \quad (5.84)$$

For all ($\forall$) hysteresis width valves caused by the temporary dynamic disturbances in the current-to-pressure transfer must be less than five times (an industrial standard value) of the base tolerance $\Delta P_{base,tolerance}$ established in (5.82). If the measured hysteresis width exceeds the guide of (5.84), arrange a maintenance.

- 3) Determine whether the maintenance can be delayed until the next nuclear outage. If the maintenance cannot be delayed, then arrange an online or forced outage maintenance.

CBNM code for basic current-to-pressure maintenance {EC-set} = {3.3}

Simulation: A simulation of a dynamic disturbance on the current-to-pressure transfer is given in Figure 5.22, of which the disturbance is simulated with a 1% sinusoidal pressure.

Figure 5.22: Dynamic error on current-to-pressure control

5.4.4 NonLinear (cam) current-to-actuator position – condition {EC-3.4}

The large majority of the industrial controls is linear control that usually results in the simplest control for an industrial process. However there are some rare exceptions that a non-linear control can produce the required power for specific applications, such as using a physical *cam* in the current-to-actuator *position* control.

This section presents an illustrating example of establishing a special base for the current-to-position non-linear transfer control for use in the *CBNM* developed in this thesis.

{EC-3.4} – conditions for acceptable tolerance on non-linear current-to-position control:

- 1) Measure the transfer curve for the input current (I_{base}) on the electronic controller versus the output position (S_{base}) on the actuator, during the controller and actuator commissioning. The curve is then used as the base curve for use in the *CBNM*.
- 2) Establish the acceptable tolerance range for the current-to-position transfer, as below:

***CBNM* condition tolerance for acceptable current (I_{base})-to-position (S_{base}) transfer:**

$$\Delta S_{base,tolerance} = |S_{base,opening} - S_{base,closing}| \quad (5.85)$$

where the maximum value of $\Delta S_{base,tolerance}$ is to be determined according to the allowable tolerance in the specific application that the controller is installed for.

***CBNM* code for base current-to-position transfer {EC-set} = {3.4}**

Simulation: A simulation of the current-to-position transfer is given in Figure 5.23, of which the base reference of input current is 4 mA to 20 mA; the rise for the reference is 18/16 cm/mA; the non-linearity is modelled with a 3/18-cm sinusoidal position deviation; and the hysteresis width is 2% of full actuator position of 18 cm.

Figure 5.23: NonLinear (cam) current-to-position control

5.4.5 Static-Dynamic disturbances on NonLinear (cam) current-to-position control – {EC-3.5}

Figure 5.24 shows the static-dynamic disturbances occurring during the actuator cam movement. This graph, compared to Figure 5.23 above, display two additional components: one is the static disturbance that enlarge the width of the hysteresis of the current-to-position transfer curve; the other is the dynamic disturbance that imposes ripple into the transfer curve.

This section illustrates that the static-dynamic disturbance on the transfer of the input current to the output actuator pressure is another key condition to be monitored for the *CBNM* developed in this thesis.

{EC-3.5} – conditions for acceptable static-dynamic disturbances on current-to-position control:

- 1) Measure/monitor the transfer values of the input current (I) from the electronic controller versus the output position (S) from the actuator, during the online operation.
- 2) Check if there is any static and/or dynamic disturbance on the current-to-position transfer. If there are disturbances, then check the acceptance of the temporary disturbances using the guide below:

***CBNM* condition for acceptable current-to-pressure transfer temporary disturbances:**

$$\forall |S_{opening} - S_{closing}| < 5 * \Delta S_{base, tolerance} \quad (5.86)$$

For all ($\forall$) hysteresis width valves caused by the temporary dynamic disturbances in the current-to-position transfer must be less than five times (an industrial standard value) of the base tolerance $\Delta S_{base,tolerance}$ established in (5.85). If the measured hysteresis width exceeds the guide of (5.86), arrange a maintenance.

- 3) Determine whether the maintenance can be delayed until the next nuclear outage. If the maintenance cannot be delayed, then arrange an online or forced outage maintenance.

CBNM code for current-to-position transfer with disturbances {EC-set} = {3.5}

Simulation: A simulation of the current-to-position transfer is given in Figure 5.24, of which the base reference of input current is 4 mA to 20 mA; the rise for the reference is 18/16 cm/mA; the non-linearity is modelled with a 3/18-cm sinusoidal position deviation; and the static disturbance is modelled with a hysteresis width increased to 5%, and the dynamic disturbance is modelled with a sinusoidal function of a maximum magnitude of 1% of full actuator position of 18 cm.

Figure 5.24: Dynamic-error on NonLinear (cam) current-to-position control

Chapter 6

CONCLUSION

This thesis research has successfully completed its intended research objective for development of a new methodology to improve the existing nuclear practices, both operations and maintenances, in an efficient, precise, and cost-effective way.

This thesis development substantially unknots the gridlock due to security concerns for the lagging application of the modern process control networking technology in the nuclear practices. The development also unlocks significant benefits, with potentially huge cost savings, from implementation of modern networking technology for nuclear data central processing, nuclear equipment operations optimizing and coordinating, and most importantly condition-based (predictive) nuclear maintenance scheduling.

This thesis research has successfully completed three new designs:

- Secure Trilateral Access Control (STAC),
- Network-Integrated Nuclear Operation (NINO),
- Network-driven Condition-Based Nuclear Maintenance (CBNM).

These new designs are to be concluded in following sections.

The feasibility and practicality of these new designs have been illustrated in the thesis, by analytical and numerical methods. The significance of these designs is tremendous, resulting in significant cost savings, additionally with increased nuclear operation security and subsequently increased nuclear safety that is invaluable.

This chapter presents:

- Section 6.1: This section lists the major research work completed in this thesis research.
- Section 6.2: This section lists the major research contributions achieved in this thesis research.
- Section 6.3: This section lists the recommendation of future work.

6.1 Major Research Work Completed

The following presents a summary of major research tasks accomplished in this thesis research.

1. *Development of a Secure Access Control to Nuclear Process Network*

The first research task is to develop a secure-effective access control to nuclear process network. This task is completed with a successful new design termed, **STAC**.

This design has three tiers: Tier-1 is to ensure the security control of external accesses to the new nuclear process network, to stop unauthorized entrance into the nuclear network, and to minimize the safety concerns on the networking for nuclear operations. Tier-2 is to ensure the qualification control for conducting nuclear operations that is to increase the quality control of live safety-critical nuclear operations. Tier-3 is to ensure the qualification control for carrying out nuclear maintenance work that is to increase the quality control of online nuclear maintenance.

2. *Development of a Network-Integrated Nuclear Operation Network*

The second research task is to develop an execution-efficient network-integrated nuclear operation network. This task is completed with a successful new design termed, **NINO**.

This design has three folds: One is to fully utilize the networking intelligent feature in the modern smart process control equipment/systems for central data processing, equipment operations optimizing and coordinating, etc. One is to minimize the nuclear workers' exposure to potential nuclear radiations by conducting the nuclear operations remotely through the network, as much as possible. One is to increase the efficiency of conducting the nuclear operations with available online information and online authorization by minimizing the well-known paper work burden in the nuclear industry, as well as to improve the correctness and precision of the nuclear operations being carried out.

3. *Development of a network-driven Condition-Based Nuclear Maintenance Network*

The third research task is to develop a cost saving-effective network-driven condition-based maintenance network. This task is completed with a successful new design termed, **CBNM**.

This design has a supreme objective that is the cost saving in nuclear process. As being well known, a nuclear unit outage is extremely expensive, probably up to one million dollars one day for one nuclear unit outage, due to mainly loss of revenue as well as maintenance costs. The **CBNM** design

is to carry out condition-based maintenance that is to monitor continuously the performance/condition of the nuclear equipment and to schedule a maintenance for the next available nuclear unit outage when the equipment condition reaches a defined maintenance criterion. One purpose of the condition-based maintenance is to schedule a maintenance for an equipment when its performance is deteriorating to a defined criterion, prior to equipment failure such that if the criterion is properly set up, then the chance for the expensive forced outage can be minimized, leading to significant cost savings (one day of forced outage may cost one million dollars per nuclear unit). The other purpose is to extend the operating time before the need to call for the next outage maintenance that also has significant cost savings.

6.2 Major Research Contributions

The following present the major contributions from this thesis research.

- ***Network-driven Condition-based Nuclear Maintenance Network Base***

The creation of the network-driven condition-based nuclear maintenance (***CBNM***) network base, first-of-the-kind development, is the chief contribution from this thesis research. The reasons are as follows:

- *Dual significance on practical and innovative R&D*

The creation of *CBNM* network base has dual significance on both practical and innovative R&D detailed below.

- *Success leading to enormous impact in industry and cost savings*

The significance of a practical R&D can be weighted with respect to the extent of its impacts in the industry. The condition-based nuclear maintenance is the most effective, practical way to avoid extremely expensive forced nuclear outages to the largest extent, as well as to reduce the frequency of outage that is to extend the operating period before calling for a scheduled outage. A forced outage, even if it is caused by a single device failure that only requires a quick fix, usually last at least two days. The use of condition-based maintenance to avoid forced outages or to reduce the frequency of outages has a huge cost saving implication as the cost could be a million dollars one day for one nuclear unit outage.

- *Innovative design: First-of-the-kind practical development on safety-critical nuclear process*

For effectiveness of implementing the condition-based maintenance in the tremendous complex, safety-critical and economic-critical nuclear facility, the use of modern networking technology is the most effective way. The network-driven condition-based nuclear maintenance developed in this thesis research is first-of-the kind practical development on the safety-critical nuclear process.

- *Core design initiative to associated new designs*

The innovative design of the network-driven condition-based nuclear maintenance can be regarded as the core design that initiates other new designs for supporting it. The two major designs initiated and already presented in this thesis are: ***STAC*** and ***NINO***.

- ***Secure Trilateral Access Control to Nuclear Process Network***

The creation of the secure trilateral access control (***STAC***) to the nuclear process network is a crucial development in support of network-driven *CBNM* and in contribution to nuclear process modernization and it is a major contribution from this thesis research.

- *Mutual authentication Tier-1 access control*

A mutual authentication with the use of public-private key cryptographic algorithm for *Tier-1* access control of ***STAC***, to ensure the security control of external accesses to the new nuclear process network, to stop unauthorized entrance into the nuclear network, and to minimize the safety concerns on the networking for nuclear operations.

- *Unilateral authentication Tier-2 and Tier-3 access controls*

The unilateral authentication is more *efficient* of less processing time but of lower security than the mutual authentication. The unilateral authentication is more suitable for Tier-2 operation qualifications authentication as well as for Tier-3 maintenance qualifications authentication. It is because first, all nuclear workers' authorization for network uses is authenticated in Tier-1 that already provides a level of security and second, the higher authentication process efficiency is crucial to improve the responsiveness of the new network-driven nuclear process.

- ***Network-Integrated Nuclear Operations Network Base***

The creation of the network-integrated nuclear operations (***NINO***) network base is essential in support of *CBNM* and nuclear process modernization, and is a major contribution from this thesis research.

- *Transformation of complex nuclear process into systematic access with authorization control*

NINO is an efficient, simple, practical design that transforms accesses to the tremendous complex safety-critical nuclear operations involving with over a thousand devices into a simple systematic access with proficient secure control. To realize the transformation feature, each requested network-integrated nuclear operation is assigned with a unique 6-number *NINO* access code and a secure operation pass code. These codes together with online nuclear-conditioning information simplify the nuclear process significantly.

- *Innovative development with fruitful effects*

The *NINO* design has three folds: fully utilize the networking intelligent feature in the modern smart process control equipment/systems for central data processing, equipment operations optimizing and coordinating, etc.; minimize the nuclear workers' exposure to potential nuclear radiations by conducting the nuclear operations remotely through the network, as much as possible; increase the efficiency of conducting the nuclear operations with available online information and online authorization by minimizing the well-known paper work burden in the nuclear industry, as well as to improve the correctness and precision of the nuclear operations being carried out.

6.3 Future Work

This thesis research has accomplished significant results in secure nuclear network access controls, network-integrated nuclear operations, and network-driven condition-based nuclear maintenance.

However, as stated in the thesis, the *NINO* codes presented in chapter 3 and Appendix I are by no means exhaustive, even though they represent the key operations in the existing nuclear process.

Future Work: The *NINO* data base is a live data base and is to be added when either an existing equipment becomes ready for network control or a new equipment with networking facility are installed.

Similarly, the *CBNM* codes presented in chapter 4 are by no means exhaustive, even though they represent the key condition-based nuclear maintenance in the existing nuclear process.

Future Work: This data base is a live data base and is to be added when either an existing equipment becomes ready for network drive to carry out condition-based nuclear maintenance work or a new equipment with networking facility can be converted to conduct condition-based nuclear maintenance.

Appendix I

NETWORK-INTEGRATED NUCLEAR OPERATIONS SECURE LEVEL 2 – REACTOR-INDIRECTED OPERATIONS

This appendix presents the second *Operation Security Level (OSL-2)* in the *Network-Integrated Nuclear Operations (NINO)*, the new network-driven nuclear process developed in this thesis research. *OSL-1* for the *reactor-direct* operations has been presented in chapter 3. *OSL-2* for the *reactor-indirect* operations is to be presented in this appendix. Figure A.1 shows the *OSL-2* in the Tier-2 *NINO*.

Figure A.1 Reactor-Indirect *NINO*

The Tier-2 *NINO* is designed with four nuclear operation access divisions as defined below:

- *OSL-1 Nuclear Reactor Control (NRC)* division
- *OSL-1 reactor Heat Transport Control (HTC)* division
- *OSL-2 Boiler Steam Control (BSC)* division
- *OSL-2 Turbine Generator Control (TGC)* division

OSL-1 NRC and *HTC NINO* have been presented in chapter 3. *OSL-2 BSC* and *TGC NINO* are to be described in this appendix.

A.1 Boiler Steam Control Division - $D_{BSC} (0,0,0,0,0,3)$

This section presents Boiler Steam Control (BSC) Division that composes of 2 Group-systems:

$G_{BPC}D_{BSC}$:	Boiler Pressure Control Group-system	(0,0,0,0,1,3)
$G_{BLC}D_{BSC}$:	Boiler Level Control Group-system	(0,0,0,0,2,3)

A.1.1 *Boiler Pressure Control Group-system* - $G_{BPC}D_{BSC} (0,0,0,0,1,3)$

$G_{BPC}D_{BSC}$, the boiler pressure control group-system is to maintain the boiler steam generation in equilibrium with the reactor thermal power by controlling the boiler pressure steady. In the steady state full power operation, the boiler pressure control is to ensure an overall nuclear unit heat balance by matching the reactor thermal power output and steam load. During the transient, the boiler pressure control is to balance the reactor thermal power and heatsink capacity to minimize the pressure fluctuations in the heat transport system. There are typically two overall heat imbalances that require the boiler pressure control. (1) The reactor thermal power exceeds steam load caused by turbine-generator trips, reactor runbacks, and unloadings. The boiler pressure control is to increase the steam load to minimize the heat transport system swell and allow the heat-transport pressure control to remain to avoid overpressure in the heat transport system. (2) The reactor thermal power is less than the steam load caused by reactor trips and reactor setbacks. The boiler pressure control is to reduce the steam load to minimize the heat transport in the subcooled liquid state to avoid the bulk boiling.

○ *Turbine Governor Control System* - $S_{TGC}G_{BPC}D_{BSC} (0,0,0,1,1,3)$

During the normal operation, the boiler pressure control is to control the opening of four turbine governor valves to change the amount of steam flow from the boilers. This turbine governor control $S_{TGC}G_{BPC}D_{BSC}$, is to maintain the boiler steam production in equilibrium with the reactor thermal power generation.

NINO defines the control of the 4 turbine governor valves as follows:

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
fc-dgcEGv $S_{TGC}G_{BPC}D_{BSC}$:	4 turbine governor controllers	(3,[1..4],1,1,1,3)
<i>NINO code:</i>	function - Controlling: device - Governor Controllers: Equipment - Governor Valves: System - Turbine Governor Control: Group system - Boiler Pressure control: Division – Boiler Steam Control:	$f_C = 3$ (1 st #); $d_{GC} = 1$ to 4 (2 nd #); $EGV = 1$ (3 rd #); $S_{TGC} = 1$ (4 th #); $G_{BPC} = 1$ (5 th #); $D_{BSC} = 3$ (6 th #)

○ **Steam Release Control System - $S_{SRC}G_{BPC}D_{BSC}$ (0,0,0,2,1,3)**

When the turbine starts to be unavailable for boiler pressure control due to reactor runbacks and unloadings, the boiler pressure control determines the lift of the 12 steam release valves by two methods: one check the error between the boiler pressure and its setpoint; the other examines the mismatch between the reactor power and the turbine power. For steam release demand of less than or equal to 5%, 2 small steam release valves discharge the steam to the forebay; for demand of greater than 5%, 10 large steam release valves discharge the steam to the atmosphere.

NINO defines the control of the 12 steam release valves as follows:

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
f_C-d_{RC}E_{SRV}S_{SRC}G_{BPC}D_{BSC}	12 steam release controllers	(3,[1..12],1,2,1,3)
<i>NINO code:</i>	function - Controlling: device – steam Release Controllers: Equipment – Steam Release Valves: System - Steam Release Control: Group system - Boiler Pressure control: Division - Boiler Steam Control:	f _C = 3 (1 st #); d _{RC} = 1 to 12 (2 nd #); E _{SRV} = 1 (3 rd #); S _{SRC} = 2 (4 th #); G _{BPC} = 1 (5 th #); D _{BSC} = 3 (6 th #)

A.1.2 **Boiler Level Control Group-system, $G_{BLC}D_{BSC} (0,0,0,0,2,3)$**

$G_{BLC}D_{BSC}$, the boiler level control is to maintain sufficient boiler water inventory in the boiler to be capable of providing a full power heat sink, by the control of 12 boiler-level control valves. At steady state, the water level in the boilers is determined by the difference in the rate of the water conversion to steam and the rate of the feedwater from the main boiler feed system flowing to the boilers. At steady state, the temperature of the reactor outlet headers is kept constant by the reactor regulating system and therefore the rate of the steam conversion is also constant. Then the boiler level is maintained by controlling the feedwater flowrate entering the boilers using the 12 boiler-level control valves.

○ **Boiler Level Control Valves control System – $S_{LCV}G_{BLC}D_{BSC} (0,0,0,1,2,3)$**

For the boiler level control, the 12 boilers are arranged into 4 quadrants (3 boilers per quadrant) and similarly the 12 boiler-level control valves are arranged into 4 groups (3 control valves per group). Each group of control valves regulates the feedwater flow to one quadrant of boilers. In order to effectively control the boiler level, one group of control valves consists of one small valve for regulating the feedwater flow of up to 10% and two large valves, each for regulating 0% to 100% feedwater flow.

NINO defines the control of the 12 boiler-level control valves as follows:

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
f_C-d_{LC}E_{LCV}S_{BLC}G_{BLC}D_{BSC}	12 boiler-level valve controllers	(3,[1..12],1,1,2,3)
<i>NINO code:</i>	function - Controlling: device – Level Controllers: Equipment – Level Control Valves: System - Boiler Level Control: Group system - Boiler Level control: Division - Boiler Steam Control:	f _C = 3 (1 st #); d _{LC} = 1 to 12 (2 nd #); E _{LCV} = 1 (3 rd #); S _{BLC} = 1 (4 th #); G _{BLC} = 2 (5 th #); D _{BSC} = 3 (6 th #)

A.2 Turbine Generator Control Division – $D_{TGC} (0,0,0,0,4)$

This section presents Turbine Generator Control (*TGC*) Division that composes of 2 Group-systems:

$G_{UPC}D_{TGC}$:	Unit Power control Group-system	(0,0,0,0,1,4)
$G_{TGC}D_{TGC}$:	Turbine Generator Control Group-system	(0,0,0,0,2,4)

A.2.1 Unit Power Control Group-system, $G_{UPC}D_{TGC} (0,0,0,0,1,4)$

$G_{UPC}D_{TGC}$, the unit power control is to process the changes of the reactor power to meet the electrical power demand set by the authorized nuclear operator. Then, the reactor control group-system $G_{RC}D_{NR} (0,0,0,0,2,1)$ is used to raise or lower the reactor power, while the boiler pressure control group-system $G_{BPC}D_{BSC} (0,0,0,0,1,3)$ maintains the boiler pressure at a setpoint by adjusting the turbine governor valves.

○ Unit Power Processing Control System - $S_{UP}G_{UPC}D_{TGC} (0,0,0,1,1,4)$

The unit power processing control is to process the signals of power demand set by authorized nuclear operator, reactor power control, and boiler pressure control to generate a command signal for changing the reactor power to meet the unit power demand.

NINO defines the processing of the nuclear unit power control as follows:

Controlling	Description	NINO code
$F_P-d_{PP}E_{UPP}S_{UP}G_{UPC}D_{TGC}$:	unit power control processing	(2,1,1,1,1,4)
<i>NINO</i> code:	function - Processing: device - Power Processors: Equipment - Unit Power control Processor: System - Unit Power control: Group system - Unit Power Control: Division - Turbine Generator Control:	$f_P = 2$ (1 st #); $d_{PP} = 1$ (2 nd #); $E_{UPP} = 1$ (3 rd #); $S_{UP} = 1$ (4 th #); $G_{UPC} = 1$ (5 th #); $D_{TGC} = 4$ (6 th #)

○ Reactor Control Group-system, $G_{RC}D_{NRC} (0,0,0,0,2,1)$

As already described in section 3.2.2, the reactor control group-system to adjust various reactivity control equipment/devices to minimum the deviation (control error) of the reactor power from the desired setpoint. The reactor reactivity controls include the liquid zone control, adjuster rods control, mechanical-control absorbers control, and poison injection control. This control is also used in the unit power processing control system.

NINO defines the two control systems, as follow:

<i>System</i>	<i>Description</i>	<i>NINO code</i>
$S_{LZC}G_{RR}D_{NRC}$:	Liquid Zone reactivity Control System	(0,0,0,2,1,1)
$S_{ARC}G_{RC}D_{NRC}$:	Adjuster Rods Control System	(0,0,0,1,2,1)
$S_{AMC}G_{RC}D_{NRC}$:	Absorber Mechanical Control System	(0,0,0,2,2,1)
<i>NINO code:</i>	System - Liquid Zone reactivity Control: Adjuster Roles Control: Absorber Mechanical Control: Group system - Reactor Reactivity control: Reactor Control: Division - Nuclear Reactor Control:	$S_{LZC} = 2$ (4 th #); $S_{ARC} = 1$ (4 th #); $S_{AMC} = 2$ (4 th #); $G_{RR} = 1$ (5 th #); $G_{RC} = 2$ (5 th #); $D_{NRC} = 1$ (6 th #)

A.2.2 **Turbine Generator Control Group-system, $G_{TGC}D_{TGC}$ (0,0,0,0,2,4)**

$G_{TSC}D_{TGC}$ the turbine steam control group-system consists of two systems:

$S_{TSM}G_{TGC}D_{TGC}$	Turbine steam monitoring system	(0,0,0,1,2,4)
$S_{TEC}G_{TGC}D_{TGC}$	Turbine electrohydraulic monitoring system	(0,0,0,2,2,4)
$S_{GHC}G_{TGC}D_{TGC}$	Generator hydrogen cooling monitoring system	(0,0,0,3,2,4)

Turbine Steam Monitoring System - This system monitors the main steam flows from the boilers to four steam chests, from the chests to the inlets of the double flow high pressure cylinder, from the high pressure cylinder to the four separators, from each separator to a live steam reheater, and from the reheater to the low pressure cylinders.

Turbine Electrohydraulic Monitoring System - This system is to monitor the operation of the turbine electrohydraulic governor. This governor regulates the opening of 4 governor valves that controls the flow of steam into the turbine, running the turbine-generator set to generate electricity. The governor controls the turbine speed is effective from the turning gear speed to the overspeed trip point. The governor also controls load from zero to full power when the generator is synchronized to the grid. The electrohydraulic control provides a more flexible and responsive turbine governing unit compared to older hydromechanical control. The control reliability is improved by the use of triplex redundant sensors, signal channels and electronic modules. On-load valve testing is incorporated in the governor that enables an early detection of any malfunction of the valve operating logic and valve operations.

Generator Hydrogen Cooling Monitoring System – This system is to monitor the operation of the generator hydrogen cooling. Hydrogen gas is used for cooling of the generator because of its low density and high specific heat. The low density of hydrogen gas minimizes windage losses and the high specific heat of hydrogen (14 times greater than that of air) increases transfer of heat from the rotor and stator core to the gas. The use of hydrogen for generator cooling requires a completely enclosed generator casing with oil seals to prevent leakage of hydrogen from the casing along the shaft. Hydrogen purity is maintained at least at 96% hydrogen to air in order to prevent forming an explosive gas mixture.

○ **Turbine Steam Monitoring system - $S_{TSM}G_{TGC}D_{TGC}$ (0,0,0,1,2,4)**

This system is to monitor the transfer of the steam from the boilers to turbine cylinders (one high pressure cylinder and three low pressure cylinders in Ontario CANDU systems) for all operating conditions. The main stream flows from the boilers to four steam chests mounted on floating links

at the front end of the high pressure turbine. Each steam chest consists of a steam strainer, an emergency stop valve, a governor valve and associated relays. Four high pressure loop pipes transfer the steam from the chests to the inlets of the double flow high pressure cylinder. The steam increases in wetness as it is flowing through the fourteen stages of the high pressure blading. The steam from the high pressure cylinder with over 10% wetness is transferred through four pipes to the four separators. A bladed assembly spins the steam and the moisture is centrifuged off. The steam exits with less than 1% wetness. The steam is transferred from each separator to a live steam reheater and becomes superheated, as live steam tapped off the main steam header flows through the reheater giving up its latent heat of vaporization and is then condensed. The steam expands through the 19 stage blading of the low pressure cylinder and increases in wetness. To limit the rate of erosion from water on the leading edges of the last three stages of rotating blades, erosion shields are brazed on to the blades. The steam leaving the low pressure cylinder exhaust and entering the condenser is about 10% wet.

NINO defines the monitoring of turbine steam flow as follows:

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
F_M-d_{FM}E_{SFM}S_{TSM}G_{TGC}D_{TGC}	turbine steam monitoring	(1,1,1,1,2,4)
<i>NINO code:</i>	function - Monitoring: device – Flow Monitor: Equipment – Steam Flow Monitor: System - Turbine Steam Monitoring: Group system - Turbine Generator Control: Division - Turbine Generator Control:	f _M = 1 (1 st #); d _{FM} = 1 (2 nd #); E _{SFM} = 1 (3 rd #); S _{TSM} = 1 (4 th #); G _{TGC} = 2 (5 th #); D _{TGC} = 4 (6 th #)

○ ***Turbine Electrohydraulic Monitoring System - S_{TEC}G_{TGC}D_{TGC} (0,0,0,2,2,4)***

This system is to monitor the controls of the electrohydraulic governor system, which include: prevent a turbine overspeed trip due to a large load change/load rejection, with the use of speed limiter circuits and opening/closing the governor and intercept valves; compensate non-linear steam flow/valve opening characteristics of the governor valves and the reheat intercept valves by means of linearizing networks; control the generated load as a function of frequency using a feedback load control loop to obtain a more accurate match of the generated load and the load setpoint; provide power system emergency actions such as the fast valving and the fast load runback; respond rapidly to the load changes to avoid a reactor trip and to maintain the grid stability by employing acceleration detection circuits arranged to provide appropriate signals to the boiler pressure control system; provide on-load testing of the steam valves; provide facilities for various controlled run-

up and loading in auto computer and manual modes; and provide online testing of overspeed governor and process trip.

NINO defines the monitoring of turbine electrohydraulic control system as follows:

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
F_M-d_{SM}E_{TEM}S_{TEC}G_{TGC}D_{TGC}	turbine electrohydraulic control monitoring	(1,1,1,2,2,4)
<i>NINO code:</i>	function - Monitoring: device – Signal Monitor: Equipment – Turbine Electrohydraulic Monitor: System – Turbine Electrohydraulic Control: Group system - Turbine Generator Control: Division - Turbine Generator Control:	f _M = 1 (1 st #); d _{SM} = 1 (2 nd #); E _{TEM} = 1 (3 rd #); S _{TEC} = 1 (4 th #); G _{TGC} = 2 (5 th #); D _{TGC} = 4 (6 th #)

○ **Generator Hydrogen Cooling Monitoring System- S_{GHC}G_{TGC}D_{TGC} (0,0,0,3,2,4)**

This system is to monitor the controls of the hydrogen gas circulation. The hydrogen gas is circulated through the rotor and the stator core by the fans mounted at each end of the rotor. The hot hydrogen gas is forced into four hydrogen gas coolers that are longitudinally mounted on the generator casing. After passing through the coolers, the hydrogen gas is directed partly into the annulus feeding the rotor ends and partly into a number of axial ducts in the stator core. The hydrogen gas cools the stator core as it passes through the axial ducts and leaves the core at its center through a number of radial ducts and goes directly to the hydrogen coolers.

NINO defines the monitoring of turbine electrohydraulic control system as follows:

<i>Controlling</i>	<i>Description</i>	<i>NINO code</i>
F_M-d_{HM}E_{HFM}S_{GHC}G_{TGC}D_{TGC}	turbine electrohydraulic control monitoring	(1,1,1,3,2,4)
<i>NINO code:</i>	function - Monitoring: device – Hydrogen Monitor: Equipment – Hydrogen Flow Monitor: System – Generator Hydrogen Cooling: Group system - Turbine Generator Control: Division - Turbine Generator Control:	f _M = 1 (1 st #); d _{HM} = 1 (2 nd #); E _{HFM} = 1 (3 rd #); S _{GHC} = 3 (4 th #); G _{TGC} = 2 (5 th #); D _{TGC} = 4 (6 th #)

REFERENCES

- [1] Herman Cheung, Cungang Yang, Helen Cheung, New Smart-Grid Operation-Based Network Access Control, paper EC-1295, IEEE Energy Conversion Congress & Exposition, 2015.
- [2] FIPS PUB 196, Entity Authentication Using Public Key Cryptography, February 1997.
- [3] FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.
- [4] FIPS PUB 200, Minimum Security Requirements for Federal Information and Information System, March 2006.
- [5] NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, 2013
- [6] NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems, February 2006.
- [7] NIST SP 800-28, Guidelines on Active Content and Mobile Code, October 2001.
- [8] NIST SP 800-30, Risk Management Guide for Information Technology Systems, July 2002.
- [9] NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, June 2002.
- [10] NIST SP 800-37, Guide for Security Certification and Accreditation of Federal Information Systems, May 2004.
- [11] NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002.
- [12] NIST SP 800-53 Revision 1, Recommended Security Controls for Federal Information Systems, July 2006.
- [13] NIST SP 800-61, Computer Security Incident Handling Guide, January 2004.
- [14] John Bethencourt, Amit Sahai, Brent Waters, Ciphertext-Policy Attribute-Based Encryption, IEEE Symposium on Security and Privacy (SP'07), 2007.
- [15] Elisa Bertino, Ravi Sandhu, Database Security - Concepts, Approaches, and Challenges, IEEE Transactions on Dependable and Secure Computing, Vol. 2, No. 1, January-March 2005.
- [16] ANSI INCITS 359-2004, Role Based Access Control, 2004.

- [17] Haibin Zhu, MengChu Zhou, Role-Based Collaboration and Its Kernel Mechanisms, IEEE Transactions on Systems, Man, and Cybernetics—Part C: Applications and Reviews, Vol. 36, No. 4, July 2006.
- [18] Tomoya Enokido, Makoto Takizawa, Role-Based Concurrency Control for Distributed Systems, Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA'06), 2006.
- [19] Haibin Zhu, MengChu Zhou, Roles in Information Systems: A Survey, IEEE Transactions on Systems, Man, and Cybernetics—Part C: Applications and Reviews, Vol. 38, No. 3, May 2008.
- [20] Mohammad A. Al-Kahtani, Ravi Sandhu, Rule-Based RBAC with Negative Authorization, Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04), 2004.
- [21] James B.D. Joshi, Elisa Bertino, Arif Ghafoor, An Analysis of Expressiveness and Design Issues for the Generalized Temporal Role-Based Access Control Model, IEEE Transactions On Dependable and Secure Computing, Vol. 2, No. 2, April-June 2005
- [22] Karsten Sohr, et al., Analyzing and Managing Role-Based Access Control Policies, IEEE Transactions on Knowledge and Data Engineering, Vol. 20, No. 7, July 2008.
- [23] James B.D. Joshi, et al., A Generalized Temporal Role-Based Access Control Model, IEEE Transactions on Knowledge and Data Engineering, Vol. 17, No. 1, January 2005.
- [24] Ravi S. Sandhu, et al., Role-Based Access Control: A Multi-Dimensional View, IEEE publication 1063-9527B, 1994.
- [25] Matthew J. Moyer, Mustaque Ahamad, Generalized Role-Based Access Control, IEEE publication, 1063-6927/0, 2001.
- [26] Anas Abou El Kalam, Rania El Baida, Philippe Balbiani, Organization Based Access Control, Proceedings of the 4th International Workshop on Policies for Distributed Systems and Networks (POLICY'03), 2003.
- [27] Basit Shafiq, et al., Secure Interoperation in a Multidomain Environment employing RBAC Policies, IEEE Transactions on Knowledge and Data Engineering, Vol. 17, No. 11, November 2005
- [28] Shen Haibo, Hong Fan, A Context-Aware Role-Based Access Control Model for Web Services, Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE'05), 2005.

- [29] Gustavo H. M. B. Motta, Sergio S. Furuie, A Contextual Role-Based Access Control Authorization Model for Electronic Patient Record, IEEE Transactions on Information Technology in Biomedicine Vol. 7, No. 3, September 2003.
- [30] J. Larmouth, ASN.1 Complete (book), Open Systems Solutions, 1999.
- [31] O. Dubuisson, ASN.1 Communication between heterogeneous systems (book), ISBN: 0-12-6333361-0, June, 2000.
- [32] EPRI 1022954, Nuclear Maintenance Applications Center: Air-Operated Valve Diagnostic Testing Guide, December 2004.
- [33] EPRI 1022954, Nuclear Maintenance Applications Center: Air-Operated Valve Diagnostic Testing Guide, December 2004.
- [34] P. Lau, Calculation of flow rate from differential pressure devices, Ematem Sommerschule, Kloster Seeon, SP Technical Research Institute of Sweden, August, 2008
- [35] ANSI/ISA-5.1-2009, Instrumentation Symbols and Identification, September 2009.
- [36] ANSI/ISA-75.05.01-2000 (R2005), Control Valve Terminology, February 2005.
- [37] ANSI/ISA-84.00.01-2004, Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 3: Guidance for the Determination of the Required Safety Integrity Levels, September 2004.